

|                                                                                   |                                                                                      |                |             |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                      | strana:        | <b>1/39</b> |

## FINA

### Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA

Verzija 1.0

|                                                                                   |                                                                                      |                |             |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                      | strana:        | <b>2/39</b> |

## Informacije o dokumentu

|                     |                                                                               |
|---------------------|-------------------------------------------------------------------------------|
| Ime dokumenta:      | Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA |
| Oznaka distribucije | Javno                                                                         |
| Vlasnik dokumenta   | FINA                                                                          |
| Kontakt             | <a href="mailto:info.pki@fina.hr">info.pki@fina.hr</a>                        |

## Povijest izmjena

| Verzija | Datum       | Razlog izmjene     |
|---------|-------------|--------------------|
| 1.0     | 29.08.2023. | Inicijalna verzija |

|                                                                                   |                                                                                              |                |             |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                              | strana:        | <b>3/39</b> |

## SADRŽAJ

|    |                                                                                       |    |
|----|---------------------------------------------------------------------------------------|----|
| 1. | Uvod .....                                                                            | 5  |
| 2. | Razlozi uvođenja promjena .....                                                       | 5  |
| 3. | Produkcijska okolina izdavanja certifikata u Fina.....                                | 6  |
| 4. | Promjene u certifikatima.....                                                         | 7  |
| 5. | Utjecaj promjene na softverska rješenja koje koriste Fina certifikate .....           | 8  |
| 6. | Profili certifikata .....                                                             | 9  |
|    | Osobni EU kvalificirani certifikat za e-potpis (QCP-n-qscd) .....                     | 10 |
|    | Osobni EU kvalificirani certifikat za e-potpis (QCP-n) .....                          | 11 |
|    | Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd).....             | 12 |
|    | Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n) .....                 | 13 |
|    | Osobni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n) .....  | 14 |
|    | Osobni autentikacijski certifikat (NCP+) .....                                        | 15 |
|    | Osobni udaljeni certifikat (NCP+) .....                                               | 16 |
|    | Osobni soft certifikat (NCP) .....                                                    | 17 |
|    | Osobni udaljeni certifikat (LCP) .....                                                | 18 |
|    | Poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd).....                    | 19 |
|    | Poslovni EU kvalificirani certifikat za e-potpis (QCP-n).....                         | 20 |
|    | Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd) .....          | 21 |
|    | Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n) .....               | 22 |
|    | Poslovni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n)..... | 23 |
|    | Poslovni autentikacijski certifikat (NCP+) .....                                      | 24 |
|    | Poslovni udaljeni certifikat (NCP+) .....                                             | 25 |
|    | Poslovni soft certifikat (NCP) .....                                                  | 26 |
|    | Poslovni soft certifikat (LCP) .....                                                  | 27 |
|    | Poslovni udaljeni certifikat (LCP).....                                               | 28 |
|    | EU kvalificirani certifikat za e-pečat (QCP-l-qscd).....                              | 29 |
|    | EU kvalificirani PSD2 certifikat za e-pečat (QCP-l) .....                             | 30 |
|    | EU kvalificirani certifikat za udaljeni e-pečat (QCP-l-qscd) .....                    | 32 |
|    | EU kvalificirani certifikat za udaljeni e-pečat (QCP-l) .....                         | 33 |
|    | EU kvalificirani soft certifikat za e-pečat (QCP-l).....                              | 34 |
|    | Aplikacijski certifikat razine 1 (NCP).....                                           | 35 |
|    | Aplikacijski certifikat razine 2 (NCP).....                                           | 36 |
|    | Aplikacijski certifikat razine 2 (NCP+).....                                          | 37 |
|    | Aplikacijski certifikat razine 3 (NCP+).....                                          | 38 |
|    | Certifikat za e-pečat Trusted liste (NCP+).....                                       | 39 |

|                                                                                   |                                                                                              |                |             |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                              | strana:        | <b>4/39</b> |

## AUTORSKA PRAVA

Ovaj dokument je u Fininom vlasništvu, administriran je od strane Fina PMA te je podložen zaštiti autorskih prava prema zakonima u Republici Hrvatskoj.

|                                                                                   |                                                                                      |                |             |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                      | strana:        | <b>5/39</b> |

## 1. Uvod

Fina priprema promjenu u izdavanju certifikata koje izdaju subordinirani Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi. Sve certifikate koje trenutno izdaju Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi, **od 20.11.2023.** će izdavati subordinirani Fina RDC 2020 CA. Ova promjena ne obuhvaća certifikate za autentikaciju mrežnih stranica (TLS/SSL certifikate, uključujući QWAC i PSD2 QWAC) jer će njih i dalje izdavati Fina RDC 2015 CA.

Od gore navedenog datuma Fina u potpunosti prestaje s izdavanjem certifikata na subordiniranom Fina RDC 2015 CA, osim certifikata za autentikaciju mrežnih stranica.

Ovom promjenom, s navedenim datumom Fina u potpunosti prestaje s izdavanjem TDU certifikata na subordiniranom Fina RDC-TDU 2015 CA te će se oni od tog datuma za zaposlenike tijela državne uprave također izdavati na subordiniranom Fina RDC 2020 CA.

Ova promjena se ne odnosi na certifikate (soft i udaljeni LCP certifikati) koje od 2020. godine izdaje subordinirani Fina RDC 2020 CA na period važenja od 5 godina, poput certifikata za fiskalizaciju, aplikacijskih certifikata standardne razine sigurnosti i dr.

## 2. Razlozi uvođenja promjena

Kao svi digitalni certifikati, tako i certifikati subordiniranih CA-ova imaju ograničeno vrijeme važenja. Vrijeme važenja CA certifikata Fininih subordiniranih CA-ova je 10 godina te za Fina RDC 2015 i Fina RDC-TDU 2015 CA-ove ovi certifikati važe do 25.11.2025. godine.

Budući da se velika većina korisničkih certifikata na Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovima izdaje na vremenski period važenja od dvije godine, nakon 25.11.2023. godine ovi CA-ovi neće više biti u mogućnosti izdavati certifikate na dvije godine.

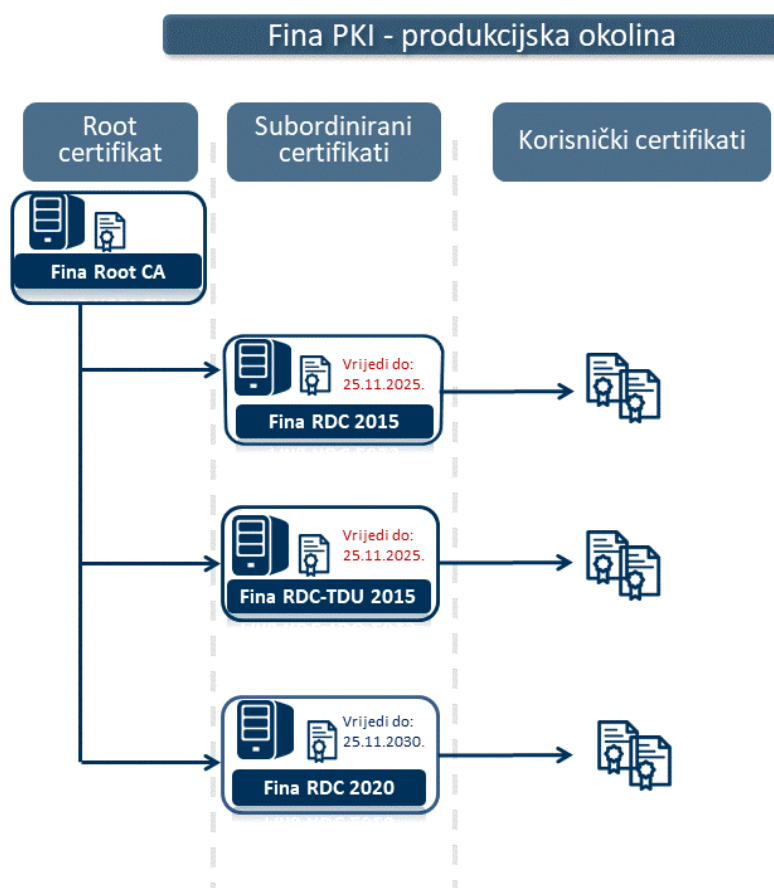
Iz tog razloga sve korisničke certifikate koje su prije promjene izdavali Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi, od 20.11.2023. započet će izdavati noviji Fina RDC 2020 CA, a period važenja korisničkih certifikata izdanih na tom novijem CA-u ostat će nepromijenjen, sukladno važećim pravilima o postupcima certificiranja.

|                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Cilj ove promjene je korisnicima omogućiti izdavanje novih certifikata sukladno važećim pravilima o postupcima certificiranja bez skraćivanja vremenskog perioda važenja certifikata.</p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                   |                                                                                      |                |             |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                      | strana:        | <b>6/39</b> |

### 3. Producerska okolina izdavanja certifikata u Fini

Na Slici 1. je prikazana shema Finine producerske okoline u kojoj se korisnicima izdaju certifikati (Fina PKI okolina).



Slika 1.: Producerska okolina Fina PKI

Producerska okolina Fina PKI zasnovana je na Fina Root CA koji je izdao CA certifikate za tri subordinirana CA:

- Fina RDC 2015,
- Fina RDC-TDU 2015,
- Fina RDC 2020.

CA certifikati za Fina RDC 2015 i Fina RDC-TDU 2015 važe do 25.11.2025. godine.

Ovom promjenom Fina RDC 2020 CA će 20.11.2023. početi izdavati korisničke certifikate koje su prije ove promjene izdavali Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovi. Ova promjena ne obuhvaća certifikate za autentikaciju mrežnih stranica jer će te certifikate i dalje izdavati Fina RDC 2015 CA.

Fina RDC 2020 CA se zajedno s Fina RDC 2015 i Fina RDC-TDU 2015 CA-ovima nalazi u istoj hijerarhiji zasnovanoj na Fina Root CA pa će softversko rješenje koje prilikom provjere certifikata ostvaruje povjerenja u Fina Root CA, uspješno prihvatiti korisničke certifikate izdane na Fina RDC 2020 CA.

|                                                                                   |                                                                                      |                |             |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                      | strana:        | <b>7/39</b> |

## 4. Promjene u certifikatima

Promjene u certifikatima koje izdaju Fina RDC 2015 i Fina RDC-TDU 2015, a čije izdavanje preuzima Fina RDC 2020 CA su sljedeće:

- Vrijednost atributa commonName (CN) u polju Issuer se mijenja na način će umjesto vrijednosti „Fina RDC 2015“ ili „Fina RDC-TDU 2015“ imati vrijednost „Fina RDC 2020“.
- Fina OID u certificatePolicies ekstenziji mijenja se tako da se šesta komponenta OID-a mijenja u „13“, npr. Fina OID „1.3.124.1104.5.12.11.8.2“ mijenja se u Fina OID „1.3.124.1104.5.13.11.8.2“. Popis certifikata s pripadajućim Fina OID-ovima nalazi se u Tablici 1 ovog dokumenta. Također u svakom opisu profila certifikata u poglavlju 6. „Profili certifikata“ naveden je Fina OID za pojedini tip certifikata.
- URL-ovi u ekstenziji CRLDistributionPoints koji opisuju lokaciju CRL liste se mijenjaju i biti će sljedeći:

„[1] URI: <http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl>

URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary“

- URL CA certifikata izdavatelja u ekstenziji Authority Information Access se mijenja u „<http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer>“

Tablica 1. niže u ovom dokumentu prikazuje popis **svih tipova korisničkih certifikata** koje će nakon ove promjene izdavati Fina RDC 2020 CA. Crvenom bojom su označeni tipovi certifikata koje Fina RDC 2020 CA započinje izdavati od 20.11.2023. (certifikati koje do datuma promjene izdaju Fina RDC 2015 CA ili Fina RDC-TDU 2015 CA ). Crnom bojom su označeni tipovi certifikata koje Fina RDC 2020 CA već izdaje od 2020 godine.

| Popis tipova certifikata - Fina RDC 2020 CA |                                                                                |                           |
|---------------------------------------------|--------------------------------------------------------------------------------|---------------------------|
| NAZIV GRUPE                                 | NAZIV TIPA CERTIFIKATA                                                         | FINA OID                  |
| Osobni certifikati                          | Osobni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)                    | 1.3.124.1104.5.13.11.8.2  |
|                                             | Osobni EU kvalificirani certifikat za e-potpis (QCP-n)                         | 1.3.124.1104.5.13.11.2.2  |
|                                             | Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd)           | 1.3.124.1104.5.13.11.7.2  |
|                                             | Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)                | 1.3.124.1104.5.13.11.6.2  |
|                                             | Osobni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n) | 1.3.124.1104.5.13.11.6.12 |
|                                             | Osobni autentikacijski certifikat (NCP+)                                       | 1.3.124.1104.5.13.11.4.2  |
|                                             | Osobni udaljeni certifikat (NCP+)                                              | 1.3.124.1104.5.13.11.10.2 |
|                                             | Osobni soft certifikat (NCP)                                                   | 1.3.124.1104.5.13.11.3.1  |
|                                             | Osobni udaljeni certifikat (LCP)                                               | 1.3.124.1104.5.13.11.9.1  |

|                                                                                   |                                                                                      |                |             |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                      | strana:        | <b>8/39</b> |

| NAZIV GRUPE                                                           | NAZIV TIPRA CERTIFIKATA                                                          | FINA OID                  |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------------|
| <b>Poslovni certifikati</b>                                           | Poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)                    | 1.3.124.1104.5.13.12.8.2  |
|                                                                       | Poslovni EU kvalificirani certifikat za e-potpis (QCP-n)                         | 1.3.124.1104.5.13.12.2.2  |
|                                                                       | Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd)           | 1.3.124.1104.5.13.12.7.2  |
|                                                                       | Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)                | 1.3.124.1104.5.13.12.6.2  |
|                                                                       | Poslovni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n) | 1.3.124.1104.5.13.12.6.12 |
|                                                                       | Poslovni autentikacijski certifikat (NCP+)                                       | 1.3.124.1104.5.13.12.4.2  |
|                                                                       | Poslovni udaljeni certifikat (NCP+)                                              | 1.3.124.1104.5.13.12.10.2 |
|                                                                       | Poslovni soft certifikat (NCP)                                                   | 1.3.124.1104.5.13.12.3.1  |
|                                                                       | Poslovni soft certifikat (LCP)                                                   | 1.3.124.1104.5.13.12.5.1  |
|                                                                       | Poslovni udaljeni certifikat (LCP)                                               | 1.3.124.1104.5.13.12.9.1  |
| <b>Certifikati za elektronički pečat</b>                              | EU kvalificirani certifikat za e-pečat (QCP-I-qscd)                              | 1.3.124.1104.5.13.13.8.2  |
|                                                                       | EU kvalificirani PSD2 certifikat za e-pečat (QCP-I)                              | 1.3.124.1104.5.13.13.1.4  |
|                                                                       | EU kvalificirani certifikat za udaljeni e-pečat (QCP-I-qscd)                     | 1.3.124.1104.5.13.13.7.2  |
|                                                                       | EU kvalificirani certifikat za udaljeni e-pečat (QCP-I)                          | 1.3.124.1104.5.13.13.6.2  |
|                                                                       | EU kvalificirani soft certifikat za e-pečat (QCP-I)                              | 1.3.124.1104.5.13.13.1.1  |
| <b>Poslovni certifikati za IT opremu</b>                              | Aplikacijski certifikat razine 1 (NCP)                                           | 1.3.124.1104.5.13.15.3.1  |
|                                                                       | Aplikacijski certifikat razine 2 (NCP)                                           | 1.3.124.1104.5.13.15.3.2  |
|                                                                       | Aplikacijski certifikat razine 2 (NCP+)                                          | 1.3.124.1104.5.13.15.4.2  |
|                                                                       | Aplikacijski certifikat razine 3 (NCP+)                                          | 1.3.124.1104.5.13.15.4.3  |
| <b>Certifikati za e-pečat Trusted liste koje izdaje Fina RDC 2020</b> | Certifikat za e-pečat Trusted liste (NCP+)                                       | 1.3.124.1104.5.13.17.4.2  |

Tablica 1.: Popis tipova certifikata - Fina RDC 2020 CA

## 5. Utjecaj promjene na softverska rješenja koja koriste Fina certifikate

Ova promjena može utjecati na ispravan rad softverskih rješenja koja koriste Fina certifikate. Obzirom na različitosti u izvedbi rješenja koja koriste certifikate potrebno je za svako rješenje provjeriti ima li ova promjena utjecaj na pojedino rješenje. U nastavku su smjernice za tu provjeru.

Ako ste vlasnik softverskog rješenja koje koristi Finine certifikate molimo vas da obratite pažnju na sljedeće važne informacije i obavite pripadajuće provjere.

- Softversko rješenje koje već koristi certifikate izdane na Fina RDC 2020 CA ujedno ima ostvareno povjerenje u certifikate koje izdaje Fina RDC 2020 CA.
- Za softversko rješenje koje još ne koristi certifikate izdane na Fina RDC 2020 CA potrebno je provjeriti i provesti sljedeće:
  - Ako vaše softversko rješenje provjeru certifikata obavlja putem Pouzdanog popisa kvalificiranih pružatelja usluga povjerenja (en. *Trusted list*) temeljenog na Uredbi (EU) br. 910/2014 (eIDAS uredba) tada će ono uspješno validirati



|                                                                                   |                                                                                      |                |             |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|-------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |             |
|                                                                                   |                                                                                      | strana:        | <b>9/39</b> |

certifikate koje izdaje Fina RDC 2020 CA jer se Fina nalazi na Pouzdanom popisu.

- Ako vaše softversko rješenje ima [Fina Root CA certifikat](#) importiran kao *Trust anchor* (root certifikat kojem se vjeruje) vrlo je vjerojatno da ove promjene u izdavanju novih certifikata na subordiniranom Fina RDC 2020 CA neće imati nikakav utjecaj na ispravan rad rješenja, ali preporučujemo provjeru rada rješenja s novim certifikatima.
- Ako vaše softversko rješenje nema importiran [Fina Root CA certifikat](#) kao Trust anchor (root certifikat kojem se vjeruje), molimo vas da ga dodate u pohranu (engl. store) root certifikata kojima se vjeruje. Ako to nije moguće, potrebno je importirati [Fina RDC 2020 CA certifikat](#) kako biste ostvarili povjerenje u ovaj CA, a time i u nove certifikate koje će taj CA početi izdavati od 20. studenog 2023.
- Postojeće RDC 2015 CA i Fina RDC-TDU 2015 CA certifikate treba zadržati u pohrani (engl. store) CA certifikata vašeg rješenja sve do 25.11.2025. kada će isteći zadnji certifikat izdan na tim CA-ovima.
- Ako vaše softversko rješenje uključuje provjeru Fininih policy OID-ova u Certificate Policies ekstenziji certifikata potrebno je u rješenje uz postojeće dodati prihvaćanje Fina OID-ova novih certifikata. Popis certifikata s pripadajućim Fina OID-ovima nalazi se u Tablici 1. Također u svakom opisu profila certifikata u poglavlju 6. Profili certifikata naveden je Fina OID za pojedini tip certifikata.

Ako ste korisnik nekog poslovnog rješenja koje koristi Finine certifikate za potpis unutar svoje tvrtke provjerite s održavateljem vašeg rješenja jesu li napravljene potrebne promjene.

## 6. Profili certifikata

U nastavku je opis **svakog pojedinog tipa korisničkog certifikata** koje će nakon ove promjene izdavati Fina RDC 2020 CA.

Crvenom bojom su označeni nazivi tipova certifikata koje Fina RDC 2020 CA započinje izdavati od 20.11.2023. (certifikati koje do datuma promjene izdaju Fina RDC 2015 CA ili Fina RDC-TDU 2015 CA). Isto tako, crvenkastom bojom označena je ćelija u kojoj je promijenjena vrijednost sukladno promjenama navedenim u poglavlju 4. „Promjene u certifikatima“.

Crnom bojom su označeni nazivi tipova certifikata koje Fina RDC 2020 CA već izdaje od 2020 godine i kod kojih nema promjena.

|                                                                                   |                                                                                              |                |              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                              | strana:        | <b>10/39</b> |

**Osobni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)**

| Osnovna polja                |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                    | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                    | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                    | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                    | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                    | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                    | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                    | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                    | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                    | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber            |                    | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=32                                                                                                                                                                                                              |
|                              | commonName (CN)         |                    | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName               |                    | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            |                    | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)        |                    | Mjesto prebivališta potpisnika                                                                                                                                                                                                                                                                                                                                                         |
|                              | organizationName (O)    |                    | OSOBNI                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| subjectPublic KeyInfo        | AlgorithmIdentifier     |                    | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                    | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut            | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation     | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier   | FINA OID: 1.3.124.1104.5.13.11.8.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers   | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier   | qcp-natural-qscd (2), OID: 0.4.0.194112.1.2                                                                                                                                                                                                                                                                                                                                            |
| qCStatements                 | NE                      | esi4-qcStatement-1 | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-4 | OID: 0.4.0.1862.1.4                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5 | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDSO-en.pdf">https://rdc.fina.hr/pds/PDSO-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDSO-hr.pdf">https://rdc.fina.hr/pds/PDSO-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6 | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name         | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint  | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020,<br>O=Financijska agencija,<br>C=HR?certificateRevocationList;binary                                                                                                                                                 |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                    | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp         | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-calssuers    | Access Method=Certification Authority Issuer<br>accessLocation:<br><a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                             |

Tablica 2. Osnovna polja i ekstenzije profila Osobnog EU kvalificiranog certifikata za e-potpis (QCP-n-qscd)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>11/39</b> |

**Osobni EU kvalificirani certifikat za e-potpis (QCP-n)**

| Osnovna polja                |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                    | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                    | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                    | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                    | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                    | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                    | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                    | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                    | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                    | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber            |                    | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=23                                                                                                                                                                                                                 |
|                              | commonName (CN)         |                    | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName               |                    | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            |                    | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)        |                    | Mjesto prebivališta potpisnika                                                                                                                                                                                                                                                                                                                                                         |
|                              | organizationName (O)    |                    | OSOBNi                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| subjectPublic KeyInfo        | AlgorithmIdentifier     |                    | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                    | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut            | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation     | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier   | FINA OID: 1.3.124.1104.5.13.11.2.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers   | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier   | qcp-natural (0), OID: 0.4.0.194112.1.0                                                                                                                                                                                                                                                                                                                                                 |
| qCStatements                 | NE                      | esi4-qcStatement-1 | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5 | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDSO-en.pdf">https://rdc.fina.hr/pds/PDSO-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDSO-hr.pdf">https://rdc.fina.hr/pds/PDSO-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6 | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name         | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint  | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                    | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp         | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers    | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

**Tablica 3. Osnovna polja i ekstenzije profila Osobnog EU kvalificiranog certifikata za e-potpis (QCP-n)**

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>12/39</b> |

**Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd)**

| Osnovna polja                |                         |                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=47 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto prebivališta potpisnika                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | OSOBNi                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation                                                                                                                                                         | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                       | FINA OID: 1.3.124.1104.5.13.11.7.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                       | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                       | qcp-natural-qscd (2), OID: 0.4.0.194112.1.2                                                                                                                                                                                                                                                                                                                                            |
| qCStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                     | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-4                                                                                                                                                     | OID: 0.4.0.1862.1.4                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                     | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDSO-en.pdf">https://rdc.fina.hr/pds/PDSO-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDSO-hr.pdf">https://rdc.fina.hr/pds/PDSO-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                     | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                             | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                      | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                        | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                             | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                        | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 4. Osnovna polja i ekstenzije profila Osobnog EU kvalificiranog certifikata za udaljeni e-potpis (QCP-n-qscd)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>13/39</b> |

**Osobni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)**

| Osnovna polja                |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                    | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                    | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                    | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                    | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                    | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                    | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                    | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                    | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                    | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber            |                    | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=33                                                                                                                                                                                                                 |
|                              | commonName (CN)         |                    | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName               |                    | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            |                    | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)        |                    | Mjesto prebivališta potpisnika                                                                                                                                                                                                                                                                                                                                                         |
|                              | organizationName (O)    |                    | OSOBNi                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| subjectPublic KeyInfo        | AlgorithmIdentifier     |                    | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                    | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut            | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation     | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier   | FINA OID: 1.3.124.1104.5.13.11.6.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers   | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier   | qcp-natural (0), OID: 0.4.0.194112.1.0                                                                                                                                                                                                                                                                                                                                                 |
| qCStatements                 | NE                      | esi4-qcStatement-1 | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5 | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDSO-en.pdf">https://rdc.fina.hr/pds/PDSO-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDSO-hr.pdf">https://rdc.fina.hr/pds/PDSO-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6 | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name         | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint  | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                    | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp         | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers    | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 5. Osnovna polja i ekstenzije profila Osobnog EU kvalificiranog certifikata za udaljeni e-potpis (QCP-n)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>14/39</b> |

**Osobni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n)**

| Osnovna polja                |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                    | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                    | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                    | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                    | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                    | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                    | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                    | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                    | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                    | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber            |                    | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=45                                                                                                                                                                                                                 |
|                              | commonName (CN)         |                    | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName               |                    | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            |                    | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)        |                    | Mjesto prebivališta potpisnika                                                                                                                                                                                                                                                                                                                                                         |
|                              | organizationName (O)    |                    | OSOBNi                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| subjectPublic KeyInfo        | AlgorithmIdentifier     |                    | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                    | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut            | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation     | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier   | FINA OID: 1.3.124.1104.5.13.11.6.12                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | policyQualifiers   | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier   | qcp-natural (0), OID: 0.4.0.194112.1.0                                                                                                                                                                                                                                                                                                                                                 |
| qCStatements                 | NE                      | esi4-qcStatement-1 | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5 | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDSO-en.pdf">https://rdc.fina.hr/pds/PDSO-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDSO-hr.pdf">https://rdc.fina.hr/pds/PDSO-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6 | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name         | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint  | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                    | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp         | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers    | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 6. Osnovna polja i ekstenzije profila Osobnog EU kvalificiranog certifikata za automatizirani udaljeni e-potpis (QCP-n)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>15/39</b> |

**Osobni autentikacijski certifikat (NCP+)**

| Osnovna polja                |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                   | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                   | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                   | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                   | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                   | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                   | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                   | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                   | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                   | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber            |                   | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=22                                                                                                                                                                                                                |
|                              | commonName (CN)         |                   | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName               |                   | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            |                   | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)        |                   | Mjesto prebivališta potpisnika                                                                                                                                                                                                                                                                                                                                                         |
|                              | organizationName (O)    |                   | OSOBNi                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| subjectPublic KeyInfo        | AlgorithmIdentifier     |                   | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                   | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut           | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature  | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment   | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection   | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth        | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                      | policyIdentifier  | FINA OID: 1.3.124.1104.5.13.11.4.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers  | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier  | ncplusplus (2), OID: 0.4.0.2042.1.2                                                                                                                                                                                                                                                                                                                                                    |
| subjectAltName               | NE                      | rfc822Name        | Opcionalno. Sadrži e-mail adresu korisnika.                                                                                                                                                                                                                                                                                                                                            |
| CRLDistributionPoints        | NE                      | DistributionPoint | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                   | cA=FALSE<br>Path Length Constraint=None                                                                                                                                                                                                                                                                                                                                                |
| Authority Information Access | NE                      | id-ad-ocsp        | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers   | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 7. Osnovna polja i ekstenzije profila Osobnog autentikacijskog certifikata (NCP+)



|                                                                                   |                                                                                              |                |              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                              | strana:        | <b>16/39</b> |

**Osobni udaljeni certifikat (NCP+)**

| Osnovna polja                |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                   | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                   | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                   | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                   | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                   | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                   | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                   | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                   | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                   | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber            |                   | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=42                                                                                                                                                                                                                |
|                              | commonName (CN)         |                   | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName               |                   | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            |                   | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)        |                   | Mjesto prebivališta potpisnika                                                                                                                                                                                                                                                                                                                                                         |
|                              | organizationName (O)    |                   | OSOBNi                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| subjectPublic KeyInfo        | AlgorithmIdentifier     |                   | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                   | Javni ključ subjekta: 2048 bita                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut           | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Key Usage                    | DA                      | digitalSignature  | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment   | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection   | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth        | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                      | policyIdentifier  | FINA OID: 1.3.124.1104.5.13.11.10.2                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | policyQualifiers  | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier  | ncplusplus (2) OID: 0.4.0.2042.1.2                                                                                                                                                                                                                                                                                                                                                     |
| subjectAltName               | NE                      | rfc822Name        | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                   | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp        | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers   | Access Method=Certification Authority Issuer<br>accessLocation:<br><a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                             |

**Tablica 8. Osnovna polja i ekstenzije profila Osobnog udaljenog certifikata (NCP+)**



|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>17/39</b> |

**Osobni soft certifikat (NCP)**

| Osnovna polja                |                      |                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|----------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        |                      | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      |                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 |                      | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           |                      | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                      |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)      |                         | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O) |                         | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)      |                         | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore            |                         | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter             |                         | Vrijeme izdavanja certifikata + 60 mjeseci                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber         |                         | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=29                                                                                                                                                                                                                |
|                              | commonName (CN)      |                         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName            |                         | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)         |                         | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)     |                         | Mjesto prebivališta potpisnika                                                                                                                                                                                                                                                                                                                                                         |
|                              | organizationName (O) |                         | OSOBNi                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | countryName (C)      |                         | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| subjectPublic KeyInfo        | AlgorithmIdentifier  |                         | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey     |                         | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                      |                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično             | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Key Usage                    | DA                   | digitalSignature        | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                      | keyEncipherment         | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                   | emailProtection         | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                      | clientAuth              | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                   | policyIdentifier        | FINA OID: 1.3.124.1104.5.13.11.3.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                      | policyQualifiers        | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                      | policyIdentifier        | ncp (1), OID: 0.4.0.2042.1.1                                                                                                                                                                                                                                                                                                                                                           |
| subjectAltName               | NE                   | rfc822Name              | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                   | DistributionPoint       | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                   | keyIdentifier           | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                   | keyIdentifier           | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                   |                         | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                   | id-ad-ocsp              | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                      | id-ad-calssuers         | Access Method=Certification Authority Issuer<br>accessLocation:<br><a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                             |

**Tablica 9. Osnovna polja i ekstenzije profila Osobnog soft certifikata (NCP)**

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>18/39</b> |

**Osobni udaljeni certifikat (LCP)**

| Osnovna polja                |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                   | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                   | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                   | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                   | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                   | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                   | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                   | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                   | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                   | Vrijeme izdavanja certifikata + 60 mjeseci                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber            |                   | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=44                                                                                                                                                                                                              |
|                              | commonName (CN)         |                   | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName               |                   | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            |                   | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)        |                   | Mjesto prebivališta potpisnika                                                                                                                                                                                                                                                                                                                                                         |
|                              | organizationName (O)    |                   | OSOBNI                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| subjectPublic KeyInfo        | AlgorithmIdentifier     |                   | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                   | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut           | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature  | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment   | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection   | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth        | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                      | policyIdentifier  | FINA OID: 1.3.124.1104.5.13.11.9.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers  | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier  | lcp (3), OID: 0.4.0.2042.1.3                                                                                                                                                                                                                                                                                                                                                           |
| subjectAltName               | NE                      | rfc822Name        | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                   | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Authority Information Access | NE                      | id-ad-ocsp        | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers   | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

**Tablica 10. Osnovna polja i ekstenzije profila Osobnog udaljenog certifikata (LCP)**

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>19/39</b> |

**Poslovni EU kvalificirani certifikat za e-potpis (QCP-n-qscd)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=34                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta ili TDU                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaesteroznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: „HR“, OIB. Za ostale poslovne subjekte jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | countryName (C)         | HR                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                                      | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation                                                                                                                                                                                                                                                                                               | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                             | FINA OID: 1.3.124.1104.5.13.12.8.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                             | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                             | qcp-natural-qscd (2), OID: 0.4.0.194112.1.2                                                                                                                                                                                                                                                                                                                                            |
| qCStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                                                                                                                                                           | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-4                                                                                                                                                                                                                                                                                           | OID: 0.4.0.1862.1.4                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                                                                                                                                                           | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDSp-en.pdf">https://rdc.fina.hr/pds/PDSp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDSp-hr.pdf">https://rdc.fina.hr/pds/PDSp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                                                                                                                                                           | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                                   | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                            | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                                | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                                | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                              | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                                   | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                              | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 11. Osnovna polja i ekstenzije profila Poslovnog EU kvalificiranog certifikata za e-potpis (QCP-n-qscd)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>20/39</b> |

**Poslovni EU kvalificirani certifikat za e-potpis (QCP-n)**

| Osnovna polja                |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                    | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                    | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                    | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                    | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                    | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                    | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                    | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                    | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                    | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | serialNumber            |                    | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=25                                                                                                                                                                                                                 |
|                              | commonName (CN)         |                    | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                  |
|                              | givenName               |                    | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            |                    | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                    |
|                              | localityName (L)        |                    | Mjesto sjedišta poslovnog subjekta ili TDU                                                                                                                                                                                                                                                                                                                                             |
|                              | organizationalUnit (OU) |                    | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.                                                                                                                                                                                                                                                                                              |
|                              | organizationalUnit (OU) |                    | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.                                                                                                                                                                                                                                                                                              |
|                              | organizationIdentifier  |                    | Dvoslovnici ISO kod države sjedišta poslovnog subjekta te jedanaestoznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: „HR“, OIB. Za ostale poslovne subjekte jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.                                                                                 |
|                              | organizationName (O)    |                    | Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                                                                                                 |
| subjectPublic KeyInfo        | countryName (C)         |                    | HR                                                                                                                                                                                                                                                                                                                                                                                     |
|                              | AlgorithmIdentifier     |                    | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                    | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                         |                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut            | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation     | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier   | FINA OID: 1.3.124.1104.5.13.12.2.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers   | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier   | qcp-natural (0), OID: 0.4.0.194112.1.0                                                                                                                                                                                                                                                                                                                                                 |
| qCStatements                 | NE                      | esi4-qcStatement-1 | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5 | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDSp-en.pdf">https://rdc.fina.hr/pds/PDSp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDSp-hr.pdf">https://rdc.fina.hr/pds/PDSp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6 | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name         | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint  | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:Idap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                    | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp         | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers    | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 12. Osnovna polja i ekstenzije profila Poslovnog EU kvalificiranog certifikata za e-potpis (QCP-n)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>21/39</b> |

**Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n-qscd)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=48                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta ili TDU                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovnici ISO kod države sjedišta poslovnog subjekta te jedanaestoznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: „HR“, OIB. Za ostale poslovne subjekte jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                                | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation                                                                                                                                                                                                                                                                                         | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                       | FINA OID: 1.3.124.1104.5.13.12.7.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                       | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                       | qcp-natural-qscd (2), OID: 0.4.0.194112.1.2                                                                                                                                                                                                                                                                                                                                            |
| qCStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-4                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.4                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDsp-en.pdf">https://rdc.fina.hr/pds/PDsp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDsp-hr.pdf">https://rdc.fina.hr/pds/PDsp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                             | Opcionalno. E-mail adresa potpisnika u rfc822Name.                                                                                                                                                                                                                                                                                                                                     |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                      | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:Idap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                        | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                             | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                        | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 13. Osnovna polja i ekstenzije profila Poslovnog EU kvalificiranog certifikata za udaljeni e-potpis (QCP-n-qscd)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>22/39</b> |

**Poslovni EU kvalificirani certifikat za udaljeni e-potpis (QCP-n)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                                                                                                                                                                                                                                                                                                        | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                                                                                                                                                                                                                                                                                                        | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                                                                                                                                                                                                                                                                                                        | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                                                                                                                                                                                                                                                                                                        | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                                                                                                                                                                                                                                                                                                        | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=35                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta ili TDU                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovnici ISO kod države sjedišta poslovnog subjekta te jedanaestoznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: „HR“, OIB. Za ostale poslovne subjekte jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | countryName (C)         | HR                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                                | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation                                                                                                                                                                                                                                                                                         | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                       | FINA OID: 1.3.124.1104.5.13.12.6.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                       | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                       | qcp-natural (0), OID: 0.4.0.194112.1.0                                                                                                                                                                                                                                                                                                                                                 |
| qCStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDsp-en.pdf">https://rdc.fina.hr/pds/PDsp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDsp-hr.pdf">https://rdc.fina.hr/pds/PDsp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                             | Opcionalno. E-mail adresa potpisnika u rfc822Name.                                                                                                                                                                                                                                                                                                                                     |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                      | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:Idap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                        | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                             | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                        | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 14. Osnovna polja i ekstenzije profila Poslovnog EU kvalificiranog certifikata za udaljeni e-potpis (QCP-n)



|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>23/39</b> |

**Poslovni EU kvalificirani certifikat za automatizirani udaljeni e-potpis (QCP-n)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                                                                                                                                                                                                                                                                                                        | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                                                                                                                                                                                                                                                                                                        | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                                                                                                                                                                                                                                                                                                        | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                                                                                                                                                                                                                                                                                                        | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                                                                                                                                                                                                                                                                                                        | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=46                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta ili TDU                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovnici ISO kod države sjedišta poslovnog subjekta te jedanaestoznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: „HR“, OIB. Za ostale poslovne subjekte jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | countryName (C)         | HR                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                                | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | nonRepudiation                                                                                                                                                                                                                                                                                         | Uključen nonRepudiation bit                                                                                                                                                                                                                                                                                                                                                            |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                       | FINA OID: 1.3.124.1104.5.13.12.6.12                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                       | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                       | qcp-natural (0), OID: 0.4.0.194112.1.0                                                                                                                                                                                                                                                                                                                                                 |
| qCStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDsp-en.pdf">https://rdc.fina.hr/pds/PDsp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDsp-hr.pdf">https://rdc.fina.hr/pds/PDsp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                                                                                                                                                     | OID: 0.4.0.1862.1.6.1                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                             | Opcionalno. E-mail adresa potpisnika u rfc822Name.                                                                                                                                                                                                                                                                                                                                     |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                      | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                        | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                             | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                        | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 15. Osnovna polja i ekstenzije profila Poslovnog EU kvalificiranog certifikata za automatizirani udaljeni e-potpis (QCP-n)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>24/39</b> |

**Poslovni autentikacijski certifikat (NCP+)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                                                                                                                                                                                                                                                                                                          | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=21                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta ili TDU                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 2. razine.                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationalUnit (OU) | Ovaj atribut opcionalno može sadržavati samo naziv organizacijske jedinice TDU 1. razine.                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovnici ISO kod države sjedišta poslovnog Subjekta te jedanaestoznamenkasti broj. Za poslovne subjekte i za TDU kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB. Za ostale poslovne subjekte jedanaestoznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili TDU, ili naziv poslovnog subjekta ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | countryName (C)         | HR                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                                  | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                         | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment                                                                                                                                                                                                                                                                                          | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection                                                                                                                                                                                                                                                                                          | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth                                                                                                                                                                                                                                                                                               | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                         | FINA OID: 1.3.124.1104.5.13.12.4.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                         | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                         | ncpplus (2), OID: 0.4.0.2042.1.2                                                                                                                                                                                                                                                                                                                                                       |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                               | Opcionalno. Sadrži e-mail adresu korisnika.                                                                                                                                                                                                                                                                                                                                            |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                        | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                            | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                            | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                          | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                               | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                          | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 16. Osnovna polja i ekstenzije profila Poslovnog autentikacijskog certifikata (NCP+)



|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>25/39</b> |

**Poslovni udaljeni certifikat (NCP+)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=41                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaestoznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB. Za ostale poslovne subjekte jedanaestoznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta: 2048 bita                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                         | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment                                                                                                                                                                                                                                                                                 | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection                                                                                                                                                                                                                                                                                 | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth                                                                                                                                                                                                                                                                                      | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                | FINA OID: 1.3.124.1104.5.13.12.10.2                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                | ncplusplus (2) OID: 0.4.0.2042.1.2                                                                                                                                                                                                                                                                                                                                                     |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                      | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                               | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                   | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                   | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                 | cA=FALSE                                                                                                                                                                                                                                                                                                                                                                               |
|                              |                         |                                                                                                                                                                                                                                                                                                 | pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                                 |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                      | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                 | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 17. Osnovna polja i ekstenzije profila Poslovnog udaljenog certifikata (NCP+)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>26/39</b> |

**Poslovni soft certifikat (NCP)**

| Osnovna polja                |                        |                         |                                                                                                                                                                                                                                                                                                                                                                                           |            |
|------------------------------|------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| Polje                        |                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                                                                                                                |            |
| Version                      |                        | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                        |            |
| serialNumber                 |                        | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                       |            |
| signatureAlgorithm           |                        | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                   |            |
| signatureValue               |                        |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                            |            |
| Issuer                       | commonName (CN)        |                         | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                             |            |
|                              | organizationName (O)   |                         | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                      |            |
|                              | countryName (C)        |                         | HR                                                                                                                                                                                                                                                                                                                                                                                        |            |
| Validity                     | notBefore              |                         | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                             |            |
|                              | notAfter               |                         | Vrijeme izdavanja certifikata + 60 mjeseci                                                                                                                                                                                                                                                                                                                                                |            |
| Subject                      | serialNumber           |                         | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaesteroznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=30                                                                                                                                                                                                                 |            |
|                              | commonName (CN)        |                         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                     |            |
|                              | givenName              |                         | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                           |            |
|                              | surname (SN)           |                         | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                                                                                                       |            |
|                              | localityName (L)       |                         | Mjesto sjedišta poslovnog subjekta                                                                                                                                                                                                                                                                                                                                                        |            |
|                              | organizationIdentifier |                         | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaesteroznamenkasti broj, npr. HR12345678901<br><br>Za poslovne subjekte kojima je dodijeljen OIB jedanaesteroznamenkasti broj je OIB poslovnog subjekta.<br><br>Za poslovne subjekte kojima nije dodijeljen OIB i nisu registrirani u Hrvatskoj jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA. |            |
|                              | organizationName (O)   |                         | Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.                                                                                                                                                                                                                                                                     |            |
|                              | countryName (C)        |                         | HR                                                                                                                                                                                                                                                                                                                                                                                        |            |
| subjectPublic KeyInfo        | AlgorithmIdentifier    |                         | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                             |            |
|                              | subjectPublicKey       |                         | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                    |            |
| Ekstenzije                   |                        |                         |                                                                                                                                                                                                                                                                                                                                                                                           |            |
| Polje                        |                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                                                                                                                   | Vrijednost |
| KeyUsage                     | DA                     | digitalSignature        | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                             |            |
|                              |                        | keyEncipherment         | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                              |            |
| extKeyUsage                  | NE                     | emailProtection         | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                    |            |
|                              |                        | clientAuth              | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                    |            |
| certificatePolicies          | NE                     | policyIdentifier        | FINA OID: 1.3.124.1104.5.13.12.3.1                                                                                                                                                                                                                                                                                                                                                        |            |
|                              |                        | policyQualifiers        | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a>    |            |
|                              |                        | policyIdentifier        | ncp (1), OID: 0.4.0.2042.1.1                                                                                                                                                                                                                                                                                                                                                              |            |
| subjectAltName               | NE                     | rfc822Name              | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                              |            |
| CRLDistributionPoints        | NE                     | DistributionPoint       | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:Idap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                          |            |
| AuthorityKeyIdentifier       | NE                     | keyIdentifier           | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                            |            |
| SubjectKeyIdentifier         | NE                     | keyIdentifier           | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                            |            |
| BasicConstraints             | NE                     |                         | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                        |            |
| Authority Information Access | NE                     | id-ad-ocsp              | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                                |            |
|                              |                        | id-ad-caIssuers         | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                   |            |

**Tablica 18. Osnovna polja i ekstenzije profila Poslovnog soft certifikata (NCP)**

|                                                                                   |                                                                                              |                |              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                              | strana:        | <b>27/39</b> |

**Poslovni soft certifikat (LCP)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                                                                                                                                                                                                                                                                                                 | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                                                                                                                                                                                                                                                                                                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                                                                                                                                                                                                                                                                                                 | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                                                                                                                                                                                                                                                                                                 | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                                                                                                                                                                                                                                                                                                 | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 60 mjeseci                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenkasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=28                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaestoznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB. Za ostale poslovne subjekte jedanaestoznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | countryName (C)         | HR                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                         | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment                                                                                                                                                                                                                                                                                 | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection                                                                                                                                                                                                                                                                                 | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth                                                                                                                                                                                                                                                                                      | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                | FINA OID: 1.3.124.1104.5.13.12.5.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                | Icp (3), OID: 0.4.0.2042.1.3                                                                                                                                                                                                                                                                                                                                                           |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                      | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                               | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                   | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                   | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                 | cA=FALSE                                                                                                                                                                                                                                                                                                                                                                               |
|                              |                         |                                                                                                                                                                                                                                                                                                 | pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                                 |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                      | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                 | Access Method=Certification Authority Issuer<br>accessLocation:<br><a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                             |

**Tablica 19. Osnovna polja i ekstenzije profila Poslovnog soft certifikata (LCP)**

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>28/39</b> |

**Poslovni udaljeni certifikat (LCP)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                                                                                                                                                                                                                                                                                               | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 60 mjeseci                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | HR OIB, ili ISO kod države prebivališta potpisnika i jedanaestoznamenasti jedinstveni identifikator, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=43                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Ime i prezime potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | givenName               | Ime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | surname (SN)            | Prezime(na) potpisnika kako je navedeno u identifikacijskoj ispravi                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaestoznamenasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB. Za ostale poslovne subjekte jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | countryName (C)         | HR                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                       | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                              | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment                                                                                                                                                                                                                                                                               | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection                                                                                                                                                                                                                                                                               | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth                                                                                                                                                                                                                                                                                    | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                              | FINA OID: 1.3.124.1104.5.13.12.9.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                              | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                              | Icp (3), OID: 0.4.0.2042.1.3                                                                                                                                                                                                                                                                                                                                                           |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                    | Opcionalno. Sadrži e-mail adresu potpisnika.                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                             | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                 | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                 | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                               | cA=FALSE                                                                                                                                                                                                                                                                                                                                                                               |
|                              |                         |                                                                                                                                                                                                                                                                                               | pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                                 |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                    | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                               | Access Method=Certification Authority Issuer<br>accessLocation:<br><a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                             |

**Tablica 20. Osnovna polja i ekstenzije profila Poslovnog udaljenog certifikata (LCP)**

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>29/39</b> |

**EU kvalificirani certifikat za e-pečat (QCP-I-qscd)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | Jedinstveni jedanaestoznamenasti broj (za pravne osobe kojima je dodijeljen OIB u Republici Hrvatskoj i za TDU: OIB, za ostale pravne osobe jedanaestoznamenasti broj je jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB), te dva broja W i Z koji predstavljaju Finine interne oznake, Z=36 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Naziv kojeg subjekt obično koristi za svoje predstavljanje.                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta pravne osobe ili TDU                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | „VAT“, dvoslovčani ISO kod države, "-", VAT broj (OIB za pravne osobe registrirane u Republici Hrvatskoj i za TDU)                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv pravne osobe ili TDU, ili naziv pravne osobe ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                                     | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                            | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                            | FINA OID: 1.3.124.1104.5.13.13.8.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                            | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                            | qcp-legal-qscd (3), OID: 0.4.0.194112.1.3                                                                                                                                                                                                                                                                                                                                              |
| qCStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                                                                                                                                                          | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-4                                                                                                                                                                                                                                                                                          | OID: 0.4.0.1862.1.4                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                                                                                                                                                          | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDsp-en.pdf">https://rdc.fina.hr/pds/PDsp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDsp-hr.pdf">https://rdc.fina.hr/pds/PDsp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                                                                                                                                                          | OID: 0.4.0.1862.1.6.2                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                                  | Opcionalno. Sadrži e-mail adresu autora pečata.                                                                                                                                                                                                                                                                                                                                        |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                           | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                               | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                               | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                             | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                                  | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                             | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

**Tablica 21. Osnovna polja i ekstenzije profila EU kvalificiranog certifikata za e-pečat (QCP-I-qscd)**

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>30/39</b> |

**EU kvalificirani PSD2 certifikat za e-pečat (QCP-I)**

| Osnovna polja          |                         |                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------|-------------------------|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                  | Atribut                 |                        | Vrijednost                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Version                | Version                 |                        | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| serialNumber           | CertificateSerialNumber |                        | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| signatureAlgorithm     | AlgorithmIdentifier     |                        | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| signatureValue         |                         |                        | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                 | commonName (CN)         |                        | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        | organizationName (O)    |                        | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                        | countryName (C)         |                        | HR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Validity               | notBefore               |                        | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        | notAfter                |                        | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Subject                | serialNumber            |                        | OIB koji je u Republici Hrvatskoj dodijeljen pružatelju platnih usluga te dva broja W i Z odijeljena točkama koji predstavljaju Finine interne oznake, Z=39                                                                                                                                                                                                                                                                                                                                                           |
|                        | commonName (CN)         |                        | Naziv kojeg pružatelj platnih usluga obično koristi za svoje predstavljanje.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                        | localityName (L)        |                        | Mjesto sjedišta pružatelja platnih usluga.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                        | organizationIdentifier  |                        | Identifikator pružatelja platnih usluga kojeg određuje ili dodjeljuje nadležno tijelo matične države članice EU.                                                                                                                                                                                                                                                                                                                                                                                                      |
|                        | organizationName (O)    |                        | Puni registrirani skraćeni naziv pružatelja platnih usluga ili puni naziv pružatelja platnih usluga ako skraćeni naziv nije registriran.                                                                                                                                                                                                                                                                                                                                                                              |
|                        | countryName (C)         |                        | HR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| subjectPublic KeyInfo  | AlgorithmIdentifier     |                        | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        | subjectPublicKey        |                        | Javni ključ subjekta: 2048 bita                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Ekstenzije             |                         |                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Polje                  | Kritično                | Atribut                | Vrijednost                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| KeyUsage               | DA                      | digitalSignature       | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| certificatePolicies    | NE                      | policyIdentifier       | FINA OID: 1.3.124.1104.5.132.13.1.4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                        |                         | policyQualifiers       | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a>                                                                                                                                |
|                        |                         | policyIdentifier       | qcp-legal(1), OID: 0.4.0.194112.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| qCStatements           | NE                      | id-qcs-pkixQCSyntax-v2 | id-etsi-qcs-SemanticsId-Legal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                        |                         | esi4-qcStatement-1     | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                        |                         | esi4-qcStatement-5     | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDsp-en.pdf">https://rdc.fina.hr/pds/PDsp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDsp-hr.pdf">https://rdc.fina.hr/pds/PDsp-hr.pdf</a> , hr                                                                                                                                                                                                                                                                                                       |
|                        |                         | esi4-qcStatement-6     | OID: 0.4.0.1862.1.6.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                        |                         | etsi-psd2-qcStatement  | Uloge dodijeljene pružatelju platnih usluga:<br>0.4.0.19495.1.1 (id-psd2-role-psp-as), PSP_AS) i/ili<br>0.4.0.19495.1.2 (id-psd2-role-psp-pi), PSP_PI) i/ili<br>0.4.0.19495.1.3 (id-psd2-role-psp-ai), PSP_AI) i/ili<br>0.4.0.19495.1.4 (id-psd2-role-psp-ic), PSP_IC)}<br><br>Naziv nadležnog tijela matične države članice:<br>NCAName (UTF8String (SIZE (1..256)))<br><br>Identifikator nadležnog tijela matične države članice<br>NCAId: dvoslovčani ISO kod države, "- ", NCA identifikator (2-8 znakova (A-Z)). |
| subjectAltName         | NE                      | rfc822Name             | Opcionalno. Sadrži e-mail adresu autora pečata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CRLDistributionPoints  | NE                      | DistributionPoint      | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                                                                                                                                                      |
| AuthorityKeyIdentifier | NE                      | keyIdentifier          | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                                                                                   |                                                                                              |                |              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                              | strana:        | <b>31/39</b> |

|                              |    |                 |                                                                                                                                                                            |
|------------------------------|----|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SubjectKeyIdentifier         | NE | keyIdentifier   | SHA-1 sažetak duljine 160 bita                                                                                                                                             |
| BasicConstraints             | NE |                 | cA=FALSE<br>pathLenConstraint=None                                                                                                                                         |
| Authority Information Access | NE | id-ad-ocsp      | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                 |
|                              |    | id-ad-caIssuers | Access Method=Certification Authority Issuer<br>accessLocation:<br><a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a> |

**Tablica 22. Osnovna polja i ekstenzije profila EU kvalificiranog PSD2 certifikata za e-pečat (QCP-I)**



|                                                                                   |                                                                                              |                |              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                              | strana:        | <b>32/39</b> |

**EU kvalificirani certifikat za udaljeni e-pečat (QCP-I-qscd)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | Jedinstveni jedanaestoznamenasti broj (za pravne osobe kojima je dodijeljen OIB u Republici Hrvatskoj: OIB, za ostale pravne osobe jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB), te dva broja W i Z koji predstavljaju Finine interne oznake, Z=51 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Naziv kojeg subjekt obično koristi za svoje predstavljanje.                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta pravne osobe ili TDU.                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | „VAT“, dvoslovčani ISO kod države, "- ", VAT broj (OIB za pravne osobe registrirane u Republici Hrvatskoj ili TDU)                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv pravne osobe ili TDU, ili naziv pravne osobe ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                            | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                   | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                   | FINA OID: 1.3.124.1104.5.13.13.7.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                   | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                   | qcp-legal-qscd (3), OID: 0.4.0.194112.1.3                                                                                                                                                                                                                                                                                                                                              |
| qCStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                                                                                                                                                 | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-4                                                                                                                                                                                                                                                                                 | OID: 0.4.0.1862.1.4                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                                                                                                                                                 | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDsp-en.pdf">https://rdc.fina.hr/pds/PDsp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDsp-hr.pdf">https://rdc.fina.hr/pds/PDsp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                                                                                                                                                 | OID: 0.4.0.1862.1.6.2                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                         | Opcionalno. Sadrži e-mail adresu autora pečata.                                                                                                                                                                                                                                                                                                                                        |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                  | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                    | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                         | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                    | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

**Tablica 23. Osnovna polja i ekstenzije profila EU kvalificiranog certifikata za udaljeni e-pečat (QCP-I-qscd)**

|                                                                                   |                                                                                              |                |              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                              | strana:        | <b>33/39</b> |

**EU kvalificirani certifikat za udaljeni e-pečat (QCP-I)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | Jedinstveni jedanaestoznamenasti broj (za pravne osobe kojima je dodijeljen OIB u Republici Hrvatskoj: OIB, za ostale pravne osobe jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB), te dva broja W i Z koji predstavljaju Finine interne oznake, Z=38 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Naziv kojeg subjekt obično koristi za svoje predstavljanje.                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta pravne osobe ili TDU.                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | „VAT“, dvoslovnici ISO kod države, "- ", VAT broj (OIB za pravne osobe registrirane u Republici Hrvatskoj)                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv pravne osobe ili TDU, ili naziv pravne osobe ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                            | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                   | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                   | FINA OID: 1.3.124.1104.5.13.13.6.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                   | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                   | qcp-legal (1), OID: 0.4.0.194112.1.1                                                                                                                                                                                                                                                                                                                                                   |
| qcStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                                                                                                                                                 | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                                                                                                                                                 | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDsp-en.pdf">https://rdc.fina.hr/pds/PDsp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDsp-hr.pdf">https://rdc.fina.hr/pds/PDsp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                                                                                                                                                 | OID: 0.4.0.1862.1.6.2                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                         | Opcionalno. Sadrži e-mail adresu autora pečata.                                                                                                                                                                                                                                                                                                                                        |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                  | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                      | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                    | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                         | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                    | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 24. Osnovna polja i ekstenzije profila EU kvalificiranog certifikata za udaljeni e-pečat (QCP-I)

|                                                                                   |                                                                                              |                |              |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje<br/>korisničkih certifikata na<br/>Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                              | strana:        | <b>34/39</b> |

**EU kvalificirani soft certifikat za e-pečat (QCP-I)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 60 mjeseci                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | Jedinstveni jedanaestoznamenasti broj (za pravne osobe kojima je dodijeljen OIB u Republici Hrvatskoj i TDU: OIB, za ostale pravne osobe jedanaestoznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB), te dva broja W i Z koji predstavljaju Finine interne oznake, Z=37 |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Naziv kojeg subjekt obično koristi za svoje predstavljanje.                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta pravne osobe ili TDU                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | „VAT“, dvoslovčani ISO kod države, "-", VAT broj (OIB za pravne osobe registrirane u Republici Hrvatskoj)                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv pravne osobe ili TDU, ili naziv pravne osobe ili TDU ako skraćeni naziv nije registriran.                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                                  | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                         | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                         | FINA OID: 1.3.124.1104.5.13.13.1.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                         | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                         | qcp-legal (1), OID: 0.4.0.194112.1.1                                                                                                                                                                                                                                                                                                                                                   |
| qCStatements                 | NE                      | esi4-qcStatement-1                                                                                                                                                                                                                                                                                       | OID: 0.4.0.1862.1.1                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | esi4-qcStatement-5                                                                                                                                                                                                                                                                                       | OID: 0.4.0.1862.1.5<br><a href="https://rdc.fina.hr/pds/PDSp-en.pdf">https://rdc.fina.hr/pds/PDSp-en.pdf</a> , en<br><a href="https://rdc.fina.hr/pds/PDSp-hr.pdf">https://rdc.fina.hr/pds/PDSp-hr.pdf</a> , hr                                                                                                                                                                        |
|                              |                         | esi4-qcStatement-6                                                                                                                                                                                                                                                                                       | OID: 0.4.0.1862.1.6.2                                                                                                                                                                                                                                                                                                                                                                  |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                               | Opcionalno. Sadrži e-mail adresu autora pečata.                                                                                                                                                                                                                                                                                                                                        |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                        | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                            | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                            | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                          | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                               | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                          | Access Method=Certification Authority Issuer<br>accessLocation:<br><a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                             |

**Tablica 25. Osnovna polja i ekstenzije profila EU kvalificiranog soft certifikata za e-pečat (QCP-I)**

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>35/39</b> |

#### Aplikacijski certifikat razine 1 (NCP)

| Osnovna polja                |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|-------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                   | Vrijednost                                                                                                                                                                                                                                                                                                                                                                                       |
| Version                      | Version                 |                   | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                               |
| serialNumber                 | CertificateSerialNumber |                   | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                              |
| signatureAlgorithm           | AlgorithmIdentifier     |                   | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                          |
| signatureValue               |                         |                   | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                                   |
| Issuer                       | commonName (CN)         |                   | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                                    |
|                              | organizationName (O)    |                   | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                             |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                               |
| Validity                     | notBefore               |                   | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                                    |
|                              | notAfter                |                   | Vrijeme izdavanja certifikata + 60 mjeseci                                                                                                                                                                                                                                                                                                                                                       |
| Subject                      | commonName (CN)         |                   | Naziv aplikacije                                                                                                                                                                                                                                                                                                                                                                                 |
|                              | localityName (L)        |                   | Mjesto sjedišta poslovnog subjekta                                                                                                                                                                                                                                                                                                                                                               |
|                              | organizationIdentifier  |                   | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaestoznamenkasti broj.<br>Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB.<br>Za ostale poslovne subjekte jedanaestoznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.<br>Ovaj atribut se ne primjenjuje u certifikatima koji se izdaju za potrebe fiskalizacije. |
|                              | organizationName (O)    |                   | Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.<br>Nakon ovog naziva za certifikate koji se izdaju za potrebe fiskalizacije dodaje se razmak i „HR“ i OIB poslovnog subjekta.                                                                                                                                              |
| subjectPublic KeyInfo        | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                               |
|                              | AlgorithmIdentifier     |                   | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                                    |
|                              | subjectPublicKey        |                   | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                           |
| Ekstenzije                   |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                                  |
| Polje                        | Kritično                | Atribut           | Vrijednost                                                                                                                                                                                                                                                                                                                                                                                       |
| KeyUsage                     | DA                      | digitalSignature  | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | keyEncipherment   | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                                     |
| extKeyUsage                  | NE                      | emailProtection   | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                           |
|                              |                         | clientAuth        | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                           |
| subjectAltName               | NE                      | rfc822Name        | Opcionalno. Sadrži e-mail adresu subjekta.                                                                                                                                                                                                                                                                                                                                                       |
| certificatePolicies          | NE                      | policyIdentifier  | FINA OID: 1.3.124.1104.5.13.15.3.1                                                                                                                                                                                                                                                                                                                                                               |
|                              |                         | policyQualifiers  | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a>           |
|                              |                         | policyIdentifier  | ncp (1), OID: 0.4.0.2042.1.1                                                                                                                                                                                                                                                                                                                                                                     |
| CRLDistributionPoints        | NE                      | DistributionPoint | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                                 |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                                   |
| SubjectKeyIdentifier         | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                                   |
| BasicConstraints             | NE                      |                   | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                               |
| Authority Information Access | NE                      | id-ad-ocsp        | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                                       |
|                              |                         | id-ad-caIssuers   | Access Method=Certification Authority Issuer<br>accessLocation:<br><a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                       |

Tablica 26. Osnovna polja i ekstenzije profila Aplikacijskog certifikata razine 1 (NCP)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>36/39</b> |

**Aplikacijski certifikat razine 2 (NCP)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                                                                                                                                                                                                                                                                                                     | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                                                                                                                                                                                                                                                                                                     | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                                                                                                                                                                                                                                                                                                     | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                                                                                                                                                                                                                                                                                                     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                                                                                                                                                                                                                                                                                                     | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | commonName (CN)         | Naziv aplikacije                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaesteroznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB. Za ostale poslovne subjekte jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                             | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                    | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment                                                                                                                                                                                                                                                                                     | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection                                                                                                                                                                                                                                                                                     | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth                                                                                                                                                                                                                                                                                          | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                          | Opcionalno. Sadrži e-mail adresu subjekta.                                                                                                                                                                                                                                                                                                                                             |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                    | FINA OID: 1.3.124.1104.5.13.15.3.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                    | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                    | ncp (1), OID: 0.4.0.2042.1.1                                                                                                                                                                                                                                                                                                                                                           |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                   | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                       | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                       | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                     | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                          | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                     | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

**Tablica 27. Osnovna polja i ekstenzije profila Aplikacijskog certifikata razine 2 (NCP)**

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>37/39</b> |

**Aplikacijski certifikat razine 2 (NCP+)**

| Osnovna polja                |                         |                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| Version                      | Version                 | V3, vrijednost="2"                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                        |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata + 24 mjeseca                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | commonName (CN)         | Naziv aplikacije                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Mjesto sjedišta poslovnog subjekta                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaesteroznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB. Za ostale poslovne subjekte jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                                                                                                                                                                                                                                             | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                                                                                                                                                                                                                                    | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment                                                                                                                                                                                                                                                                                     | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection                                                                                                                                                                                                                                                                                     | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth                                                                                                                                                                                                                                                                                          | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| subjectAltName               | NE                      | rfc822Name                                                                                                                                                                                                                                                                                          | Opcionalno. Sadrži e-mail adresu subjekta.                                                                                                                                                                                                                                                                                                                                             |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                    | FINA OID: 1.3.124.1104.5.13.15.4.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                                                                                                                                                                                                                                    | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                                                                                                                                                                                                                                    | ncplusplus (2), OID: 0.4.0.2042.1.2                                                                                                                                                                                                                                                                                                                                                    |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                                                                                                                                                                                                                                   | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                       | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                                                                                                                                                                                                                                       | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                                                                                                                                                                                                                                     | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                                                                                                                                                                                                                                          | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                                                                                                                                                                                                                                     | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 28. Osnovna polja i ekstenzije profila Aplikacijskog certifikata razine 2 (NCP+)

|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>38/39</b> |

**Aplikacijski certifikat razine 3 (NCP+)**

| Osnovna polja                |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                   | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                   | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                   | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                   | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                   | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         |                   | Fina RDC 2020                                                                                                                                                                                                                                                                                                                                                                          |
|                              | organizationName (O)    |                   | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                   |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                     |
| Validity                     | notBefore               |                   | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                          |
|                              | notAfter                |                   | Vrijeme izdavanja certifikata + 12 mjeseci                                                                                                                                                                                                                                                                                                                                             |
| Subject                      | commonName (CN)         |                   | Naziv aplikacije                                                                                                                                                                                                                                                                                                                                                                       |
|                              | localityName (L)        |                   | Mjesto sjedišta poslovnog subjekta                                                                                                                                                                                                                                                                                                                                                     |
|                              | organizationIdentifier  |                   | Dvoslovčani ISO kod države sjedišta poslovnog subjekta te jedanaesteroznamenkasti broj. Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB. Za ostale poslovne subjekte jedanaesteroznamenkasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB.                                                                                    |
|                              | organizationName (O)    |                   | Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.                                                                                                                                                                                                                                                                  |
|                              | countryName (C)         |                   | HR                                                                                                                                                                                                                                                                                                                                                                                     |
|                              | commonName (CN)         |                   | Naziv aplikacije                                                                                                                                                                                                                                                                                                                                                                       |
| subjectPublic KeyInfo        | AlgorithmIdentifier     |                   | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                          |
|                              | subjectPublicKey        |                   | Javni ključ subjekta duljine 2048 bita                                                                                                                                                                                                                                                                                                                                                 |
| Ekstenzije                   |                         |                   |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut           | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature  | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
|                              |                         | keyEncipherment   | Uključen keyEncipherment bit                                                                                                                                                                                                                                                                                                                                                           |
| extKeyUsage                  | NE                      | emailProtection   | OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                 |
|                              |                         | clientAuth        | OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                 |
| subjectAltName               | NE                      | rfc822Name        | Opcionalno. Sadrži e-mail adresu subjekta.                                                                                                                                                                                                                                                                                                                                             |
| certificatePolicies          | NE                      | policyIdentifier  | FINA OID: 1.3.124.1104.5.13.15.4.3                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers  | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier  | ncppus (2), OID: 0.4.0.2042.1.2                                                                                                                                                                                                                                                                                                                                                        |
| CRLDistributionPoints        | NE                      | DistributionPoint | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier     | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                   | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp        | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers   | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

Tablica 29. Osnovna polja i ekstenzije profila Aplikacijskog certifikata razine 3 (NCP+)



|                                                                                   |                                                                                      |                |              |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------|--------------|
|  | <b>Opis promjene vezane uz izdavanje korisničkih certifikata na Fina RDC 2020 CA</b> | klasifikacija: |              |
|                                                                                   |                                                                                      | strana:        | <b>39/39</b> |

**Certifikat za e-pečat Trusted liste (NCP+)**

| Osnovna polja                |                         |                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Polje                        | Atribut                 |                                                                                       | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| Version                      | Version                 |                                                                                       | V3, vrijednost="2"                                                                                                                                                                                                                                                                                                                                                                     |
| serialNumber                 | CertificateSerialNumber |                                                                                       | 16 ili 17 okteta, 64 bita entropije                                                                                                                                                                                                                                                                                                                                                    |
| signatureAlgorithm           | AlgorithmIdentifier     |                                                                                       | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                |
| signatureValue               |                         |                                                                                       | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                         |
| Issuer                       | commonName (CN)         | Fina RDC 2020                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Financijska agencija                                                                  |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | notAfter                | Vrijeme izdavanja certifikata +24 mjeseca                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
| Subject                      | serialNumber            | „P“, te dva broja W i Z koji predstavljaju Finine interne oznake, Z=31                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | commonName (CN)         | Naziv kojeg određuje središnje tijelo državne uprave nadležno za poslove gospodarstva |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | localityName (L)        | Zagreb                                                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationIdentifier  | „VATHR-“ OIB središnjeg tijela državne uprave nadležnog za poslove gospodarstva       |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName (O)    | Naziv središnjeg tijela državne uprave nadležnog za poslove gospodarstva              |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | countryName (C)         | HR                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                        |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | subjectPublicKey        | Javni ključ subjekta duljine 2048 bita                                                |                                                                                                                                                                                                                                                                                                                                                                                        |
| Ekstenzije                   |                         |                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                        |
| Polje                        | Kritično                | Atribut                                                                               | Vrijednost                                                                                                                                                                                                                                                                                                                                                                             |
| KeyUsage                     | DA                      | digitalSignature                                                                      | Uključen digitalSignature bit                                                                                                                                                                                                                                                                                                                                                          |
| extKeyUsage                  | NE                      | id-tsl-kp-tslSigning                                                                  | OID: 0.4.0.2231.3.0                                                                                                                                                                                                                                                                                                                                                                    |
| certificatePolicies          | NE                      | policyIdentifier                                                                      | FINA OID: 1.3.124.1104.5.13.17.4.2                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | policyQualifiers                                                                      | policyQualifierId: id-qt-cps { id-qt 1 }<br>cPSuri:<br><a href="https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti">https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti</a><br>cPSuri:<br><a href="https://www.fina.hr/en/legislation-documents-and-conformance-certificates">https://www.fina.hr/en/legislation-documents-and-conformance-certificates</a> |
|                              |                         | policyIdentifier                                                                      | ncppplus (2), OID: 0.4.0.2042.1.2                                                                                                                                                                                                                                                                                                                                                      |
| CRLDistributionPoints        | NE                      | DistributionPoint                                                                     | [1] URI: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2020, O=Financijska agencija, C=HR?certificateRevocationList;binary                                                                                                                                                       |
| AuthorityKeyIdentifier       | NE                      | keyIdentifier                                                                         | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| SubjectKeyIdentifier         | NE                      | keyIdentifier                                                                         | SHA-1 sažetak duljine 160 bita                                                                                                                                                                                                                                                                                                                                                         |
| BasicConstraints             | NE                      |                                                                                       | cA=FALSE<br>pathLenConstraint=None                                                                                                                                                                                                                                                                                                                                                     |
| Authority Information Access | NE                      | id-ad-ocsp                                                                            | Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                             |
|                              |                         | id-ad-caIssuers                                                                       | Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer">http://rdc.fina.hr/RDC2020/FinaRDCCA2020.cer</a>                                                                                                                                                                                                                |

**Tablica 30. Osnovna polja i ekstenzije profila Certifikata za e-pečat Trusted liste (NCP+)**