

## Profili certifikata koje će izdavati Fina RDC 2025 CA

## 1. Uvod

Fina uvodi novi subordinirani Fina RDC 2025 CA na kojem će se izdavati produkcijski nekvalificirani certifikati koji se izdaju na vrijeme važenja od 5 godina.

Planirano je da Fina RDC 2025 CA započne s izdavanjem certifikata 24. studenog 2025. kada ujedno prestaje izdavanje tih certifikata na postojećem Fina RDC 2020 CA.

## 2. Korisnički certifikati na koje se odnosi promjena

Novi Fina RDC 2025 CA će izdavati sljedeće korisničke certifikate:

- Aplikacijski certifikat razine 1 (NCP) što podrazumijeva i Aplikacijski certifikat za Fiskalizaciju i aplikacijski certifikat za servis e-Račun.
- Osobni soft certifikat (NCP),
- Osobni udaljeni certifikat (LCP),
- Poslovni soft certifikat (NCP),
- Poslovni soft certifikat (LCP),
- Poslovni udaljeni certifikat (LCP).

## 3. Promjene u korisničkim certifikatima

Promjene u navedenim korisničkim certifikatima su minimalne, a neophodne su zbog promjene CA koji će izdavati navedene certifikate (Fina RDC 2025).

Promjene u profilima certifikata su sljedeće:

- Vrijednost atributa **commonName (CN)** u polju **Issuer** se mijenja na način da će umjesto vrijednosti „Fina RDC 2020“ imati vrijednost „Fina RDC 2025“.
- **Fina OID u certificatePolicies ekstenziji** mijenja se tako da se šesta komponenta OID-a mijenja u „14“. npr. Fina OID za aplikacijski certifikat razine 1 (NCP) „1.3.124.1104.5.13.15.3.1“ mijenja se u Fina OID „1.3.124.1104.5.14.15.3.1“.
- **URL u ekstenziji CRLDistributionPoints** koji opisuje lokaciju CRL liste se mijenja i biti će:  
<http://rdc.fina.hr/RDC2025/FinaRDCCA2025.crl>.
- **URL CA certifikata izdavatelja u ekstenziji Authority Information Access** se mijenja i biti će  
<http://rdc.fina.hr/RDC2025/FinaRDCCA2025.cer>.

#### 4. Profil Fina RDC 2025 CA certifikata

| Polje                        | Atribut                 | Vrijednost                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Osnovna polja</b>         |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Version                      | Version                 | X.509 V3 (vrijednost="2")                                                                                                                                                                                                                                                                                                                                                                                                           |
| serialNumber                 | CertificateSerialNumber | 16 ili 17 okteta, 32 do 34 HEX znamenki, 64 bita entropija                                                                                                                                                                                                                                                                                                                                                                          |
| signatureAlgorithm           | AlgorithmIdentifier     | sha256WithRSAEncryption                                                                                                                                                                                                                                                                                                                                                                                                             |
| signatureValue               |                         | Potpis izdavatelja certifikata                                                                                                                                                                                                                                                                                                                                                                                                      |
| Issuer                       | commonName              | Fina Root CA                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | organizationName        | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                                                                |
|                              | countryName             | HR                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Validity                     | notBefore               | Vrijeme izdavanja certifikata                                                                                                                                                                                                                                                                                                                                                                                                       |
|                              | notAfter                | Vrijeme izdavanja certifikata + 10 godina.                                                                                                                                                                                                                                                                                                                                                                                          |
| Subject                      | commonName              | <b>Fina RDC 2025</b>                                                                                                                                                                                                                                                                                                                                                                                                                |
|                              | organizationName        | Financijska agencija                                                                                                                                                                                                                                                                                                                                                                                                                |
|                              | countryName             | HR                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| subjectPublic KeyInfo        | AlgorithmIdentifier     | rsaEncryption                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                              | subjectPublicKey        | Javni ključ CA: 4096 bit                                                                                                                                                                                                                                                                                                                                                                                                            |
| Polje                        | Kritično                | Vrijednost                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Ekstenzije</b>            |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| KeyUsage                     | DA                      | KeyCertSign, cRLSign                                                                                                                                                                                                                                                                                                                                                                                                                |
| BasicConstraints             | DA                      | cA=true<br>pathLen=0                                                                                                                                                                                                                                                                                                                                                                                                                |
| AuthorityKeyIdentifier       | NE                      | 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))                                                                                                                                                                                                                                                                                                              |
| SubjectKeyIdentifier         | NE                      | 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (određeno prema RFC 5280, točka 4.2.1.2 metoda (1))                                                                                                                                                                                                                                                                                                              |
| extKeyUsage                  | NE                      | emailProtection<br>OID: 1.3.6.1.5.5.7.3.4                                                                                                                                                                                                                                                                                                                                                                                           |
|                              |                         | clientAuth<br>OID: 1.3.6.1.5.5.7.3.2                                                                                                                                                                                                                                                                                                                                                                                                |
| certificatePolicies          | NE                      | policyIdentifier<br>anyPolicy (OID: 2.5.29.32.0)                                                                                                                                                                                                                                                                                                                                                                                    |
|                              |                         | policyQualifiers<br>policyQualifierId: id-qt-cps { id-qt 1 } (OID: 1.3.6.1.5.5.7.2.1)<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> |
| Authority Information Access | NE                      | id-ad-ocsp<br>Access Method=On-line Certificate Status Protocol<br>accessLocation: <a href="http://ocsp.fina.hr">http://ocsp.fina.hr</a>                                                                                                                                                                                                                                                                                            |
|                              |                         | id-ad-caIssuers<br>Access Method=Certification Authority Issuer<br>accessLocation: <a href="http://rdc.fina.hr/Root/FinaRootCA.cer">http://rdc.fina.hr/Root/FinaRootCA.cer</a>                                                                                                                                                                                                                                                      |
| CRLDistributionPoints        | NE                      | DistributionPoint<br>[1] URI: <a href="http://rdc.fina.hr/Root/FinaRootCA.crl">http://rdc.fina.hr/Root/FinaRootCA.crl</a>                                                                                                                                                                                                                                                                                                           |

**Tablica 1. Osnovna polja i ekstenzije profila Fina RDC 2025 subordiniranog CA certifikata**

## 5. Profili korisničkih certifikata koje će izdavati Fina RDC 2025 CA

### 5.1. 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 2025                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | 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 jedanaesteroznamenasti broj.<br>Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB.<br>Za ostale poslovne subjekte jedanaesteroznamenasti je broj jedinstveni broj kojeg dodjeljuje Fina CA i ne predstavlja OIB. 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.                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | 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: 1.3.124.1104.5.14.15.3.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | 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/RDC2025/FinaRDCCA2025.crl">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.crl</a><br>URI:Idap://rdc-Idap2.fina.hr/CN=Fina RDC 2025, 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/RDC2025/FinaRDCCA2025.cer">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.cer</a>                                                                                                                                                                                                             |

Tablica 2. Osnovna polja i ekstenzije profila Aplikacijskog certifikata razine 1 (NCP)

**5.2. 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 2025                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | 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: 1.3.124.1104.5.14.11.3.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | 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/RDC2025/FinaRDCCA2025.crl">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.crl</a><br>URI:Idap://rdc-ldap2.fina.hr/CN=Fina RDC 2025, 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/RDC2025/FinaRDCCA2025.cer">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.cer</a>                                                                                                                                                                                                             |

**Tablica 3. Osnovna polja i ekstenzije profila Osobnog soft certifikata (NCP)**

### 5.3. 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 2025                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | 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=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: 1.3.124.1104.5.14.11.9.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | 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/RDC2025/FinaRDCCA2025.crl">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2025, 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/RDC2025/FinaRDCCA2025.cer">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.cer</a>                                                                                                                                                                                                                |

Tablica 4. Osnovna polja i ekstenzije profila Osobnog udaljenog certifikata (LCP)

#### 5.4. 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 2025                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | 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 jedanaesteroznamenasti 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 jedanaesteroznamenasti broj, npr. HR12345678901<br><br>Za poslovne subjekte kojima je dodijeljen OIB jedanaesteroznamenasti broj je OIB poslovnog subjekta.<br><br>Za poslovne subjekte kojima nije dodijeljen OIB i nisu registrirani u Hrvatskoj jedanaesteroznamenasti 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: 1.3.124.1104.5.14.12.3.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                        | 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/RDC2025/FinaRDCCA2025.crl">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2025, 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/RDC2025/FinaRDCCA2025.cer">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.cer</a>                                                                                                                                                                                                                |

Tablica 5. Osnovna polja i ekstenzije profila Poslovnog soft certifikata (NCP)

**5.5. 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 2025                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                        |
|                              | 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 jedanaesteroznamenasti 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 jedanaesteroznamenasti broj.<br>Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB.<br>Za ostale poslovne subjekte jedanaesteroznamenasti 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                                                                                                                                                                                                                                                                                                                                                                 |
| certificatePolicies          | NE                      | policyIdentifier                                                                                                                                                                                                                                                                                        | FINA OID: 1.3.124.1104.5.14.12.5.1                                                                                                                                                                                                                                                                                                                                                     |
|                              |                         | 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                                                                                                                                                                                                                                                                                        | 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/RDC2025/FinaRDCCA2025.crl">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.crl</a><br>URI:Idap2://rdc-Idap2.fina.hr/CN=Fina RDC 2025, 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/RDC2025/FinaRDCCA2025.cer">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.cer</a>                                                                                                                                                                                                             |

**Tablica 6. Osnovna polja i ekstenzije profila Poslovnog soft certifikata (LCP)**

**5.6. 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 2025                                                                                                                                                                                                                                                                                                                                                                          |            |
|                              | 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 jedanaesteroznamenasti 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 jedanaesteroznamenasti broj.<br>Za poslovne subjekte kojima je dodijeljen OIB u Republici Hrvatskoj: „HR“, OIB.<br>Za ostale poslovne subjekte jedanaesteroznamenasti 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: 1.3.124.1104.5.14.12.9.1                                                                                                                                                                                                                                                                                                                                                     |            |
|                              |                        | 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        | 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/RDC2025/FinaRDCCA2025.crl">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.crl</a><br>URI:ldap://rdc-ldap2.fina.hr/CN=Fina RDC 2025, 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/RDC2025/FinaRDCCA2025.cer">http://rdc.fina.hr/RDC2025/FinaRDCCA2025.cer</a>                                                                                                                                                                                                             |            |

**Tablica 7. Osnovna polja i ekstenzije profila Poslovnog udaljenog certifikata (LCP)**

## 6. Certifikat za potpis odgovora OCSP servisa za Fina RDC 2025

| 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 2025                              |                                    |
|                        | organizationName (O)    | Financijska agencija                       |                                    |
|                        | countryName (C)         | HR                                         |                                    |
| Validity               | notBefore               | Vrijeme izdavanja certifikata              |                                    |
|                        | notAfter                | Vrijeme izdavanja certifikata + 12 mjeseci |                                    |
| Subject                | commonName (CN)         | Fina RDC 2025 OCSP                         |                                    |
|                        | organizationName (O)    | Financijska agencija                       |                                    |
|                        | 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                      | OCSPSigning                                | OID: 1.3.6.1.5.5.7.3.9             |
| ocsp-nocheck           | NE                      |                                            | OID: 1.3.6.1.5.5.7.48.1.5          |
| AuthorityKeyIdentifier | NE                      | keyIdentifier                              | SHA-1 sažetak duljine 160 bita     |
| SubjectKeyIdentifier   | NE                      | keyIdentifier                              | SHA-1 sažetak duljine 160 bita     |
| BasicConstraints       | DA                      |                                            | cA=FALSE<br>pathLenConstraint=None |

Tablica 8. Osnovna polja i ekstenzije profila Certifikata za potpis odgovora OCSP servisa za Fina RDC 2025