

## PROMJENE U CA CERTIFIKATU NOVOG SUBORDINIRANOG CA

Novi subordinirani Fina RDC 2020 CA biti će izdan (potpisan) od strane postojećeg Fina Root CA (<http://rdc.fina.hr/Root/FinaRootCA.cer>) koji je izdao i postojeći RDC 2015 CA, tj. novi certifikati za Fiskalizaciju će kao i postojeći certifikati za Fiskalizaciju biti „ispod“ istog zajedničkog Fina Root CA.

Novi Fina RDC 2020 CA će imati minimalne promjene u odnosu na postojeći Fina RDC 2015 CA. U nastavku je opis promjena:

- Serijski broj (CertificateSerialNumber) biti će dugačak 16 ili 17 okteta (32 do 34 HEX znamenki), tj. Imat će 64 bitna entropiju. Postojeći certifikat Fina RDC 2015 CA ima 32 bita entropije, što je 12 ili 13 okteta serijskog broja, (24-26 hex znamenki).
- Podaci u polju Subject: CN=Fina RDC 2020, OID.2.5.4.97=VATHR-85821130368, O=Financijska agencija, C=HR, tj. dodan je atribut čiji je OID 2.5.4.97 (organizationIdentifier). Postojeći certifikat Fina RDC 2015 CA ima sljedeće podatke u polju Subject: CN=Fina RDC 2015, O=Financijska agencija, C=HR
- U ekstenziji Certificate Policies mijenjaju se URL-ovi koji će biti „<https://www.fina.hr/regulativa-dokumenti-i-potvrde-o-sukladnosti>“ i „<https://www.fina.hr/en/legislation-documents-and-conformance-certificates>“ Postojeći certifikat Fina RDC 2015 CA ima URL-ove <http://rdc.fina.hr/Root/FinaRootCA-CP1-0-hr.pdf> i „<http://rdc.fina.hr/Root/FinaRootCA-CP1-0-en.pdf>“.
- U ekstenziji više neće postojati adresa segmentirane CRL liste već će ostati upisan samo URL za dohvat CRL liste koju izdaje Fina Root CA i koji ostaje neizmijenjen (<http://rdc.fina.hr/Root/FinaRootCA.crl>)
- Certifikat novog Fina RDC 2020 CA imat će drugačiju vrijednost javnog ključa, ali iste duljine i namijenjen za isti kriptografski algoritam kao i javni ključ Fina RDC 2015 CA (tj. RSA javni ključ duljine 4096 bita)
- Vrijeme važenja Fina RDC 2020 CA certifikata upisano u certifikat biti će 10 godina od trenutka izdavanja (važi do: studeni 2030).