**Bugzilla ID:**

**Bugzilla Summary:** Add “Fina Root CA” root certificate

CAs wishing to have their certificates included in Mozilla products must

1. Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2. Supply all of the information listed in [http://wiki.mozilla.org/CA:Information\_checklist](http://wiki.mozilla.org/CA%3AInformation_checklist).
	1. Review the Recommended Practices at [https://wiki.mozilla.org/CA:Recommended\_Practices](https://wiki.mozilla.org/CA%3ARecommended_Practices)
	2. Review the Potentially Problematic Practices at [https://wiki.mozilla.org/CA:Problematic\_Practices](https://wiki.mozilla.org/CA%3AProblematic_Practices)

**General information about the CA’s associated organization**

|  |  |
| --- | --- |
| CA Company Name | Financijska agencija (Fina) |
| Website URL | <http://www.fina.hr/finadigicert> |
| Organizational type | Government owned company with Public and Commercial services |
| Primary Market / Customer Base | Fina is the biggest Certification Authority in Croatia. Fina is Qualified Trust Service Provider and operates in accordance eIDAS Regulation (Regulation (EU) 910/2014).More than 95% of our certificate users are from business entities and state administration bodies and we also have citizens as users of our certificates, so we have significant demand for SSL and S/MIME certificates.Primary market / customer base:a) Business entities registered in Croatia and outside of Croatiab) State administration bodies of Croatiac) Citizens d) Servers of business entities and state administration bodies |
| Impact to Mozilla Users | Since a large number of our subscribers are using Mozilla Firefox as default internet browser, we need to add our company as a Trusted Root Certificate Authority in Mozilla Firefox browser (Mozilla NSS). |
| Inclusion in other major browsers | We have applied for inclusion in Microsoft Root Certificate Program and we are preparing to apply for Apple Root Certificate Program and for Android Root Certificate store. |
| CA Primary Point of Contact (POC) | POC direct email: pma@fina.hrPOC Phone Number: +385 1 612 8097 |

**Technical information about each root certificate**

|  |  |
| --- | --- |
| Certificate Name | Fina Root CA |
| Certificate Issuer Field | CN = Fina Root CAO = Financijska agencijaC = HR |
| Certificate Summary | There are two subordinate CAs signed by “Fina Root CA”: “Fina RDC 2015” issues certificates for business entities (authentication and signature certificates, electronic seal certificates, SSL certificates, certificates for systems and devices) and for citizens (authentication and signature certificates) and “Fina RDC-TDU 2015” issues certificates for state administration bodies (authentication and signature certificates, electronic seal certificates). |
| Mozilla Applied Constraints | No constraints. |
| Root Cert URL | <http://rdc.fina.hr/Root/FinaRootCA.pem> |
| SHA1 Fingerprint | 62 02 bf 16 9a f2 7f a6 7e d0 ce c6 6b 78 2b 83 22 61 26 e9 |
| Valid From  | 2015-11-24 |
| Valid To  | 2035-11-24 |
| Certificate Version | X509v3 |
| Certificate Signature Algorithm | SHA256RSA |
| Signing key parameters | 4096 |
| Example Certificate (non-SSL) | <http://rdc.fina.hr/RDC2015/FinaRDCCA2015.pem>, <http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.pem>  |
| CRL URL | Fina Root CA certificates CRL: http://rdc.fina.hr/Root/FinaRootCA.crlFina RDC 2015 certificates CRL: http://rdc.fina.hr/RDC2015/FinaRDCCA2015.crlFina RDC-TDU 2015 certificates CRL: http://rdc.fina.hr/RDC-TDU2015/FinaRDC-TDUCA2015.crl |
| OCSP URL (Required now) | <http://ocsp.fina.hr> |
| Requested Trust Bits | Websites trust bit (SSL/TLS) and S/MIME trust bit |
| SSL Validation Type | Organization Validation (OVCP) |
| EV Policy OID(s) | Not Applicable. |
| Non-sequential serial numbers and entropy in cert | Yes, serial number has 16 or 17 octets, with 64 bits entropy. |

**CA Hierarchy information for each root certificate**

|  |  |
| --- | --- |
| CA Hierarchy | See CP/CPS Section 1.1.3  |
| Externally Operated SubCAs | We don’t have any externally operated SubCA. |
| Cross-Signing | Not Allowed. |
| Technical Constraints onThird-party Issuers | We don’t have any Third-party Issuers. |

**Verification Policies and Practices**

|  |  |
| --- | --- |
| Policy Documentation | Fina Root CACP/CPS: <http://rdc.fina.hr/Root/FinaRootCA-CPCPS2-1-en.pdf>SSL CP <http://rdc.fina.hr/RDC2015/FinaRDC2015-CPWSA1-1-en.pdf>QC CP <http://rdc.fina.hr/RDC2015/FinaRDC2015-CPQC1-0-en.pdf>NQC CP <http://rdc.fina.hr/RDC2015/FinaRDC2015-CPNQC1-0-en.pdf>SSL CPS <http://rdc.fina.hr/RDC2015/FinaRDC2015-CPSWSA1-1-en.pdf>QC CPS <http://rdc.fina.hr/RDC2015/FinaRDC2015-CPSQC1-0-en.pdf>NQC CPS <http://rdc.fina.hr/RDC2015/FinaRDC2015-CPSNQC1-0-en.pdf> |
| Audits | Audit Type: ETSI for CAAuditor: TÜVIT, Essen, GermanyAudit Report: <http://rdc.fina.hr/CAR/67100UE_s.pdf>, <http://rdc.fina.hr/CAR/9779UE_s.pdf>, <http://rdc.fina.hr/CAR/9780UE_s.pdf>, <http://rdc.fina.hr/CAR/67101UE_s.pdf>, <http://rdc.fina.hr/CAR/6799UE_s.pdf>, <http://rdc.fina.hr/CAR/6798UE_s.pdf>  |
| Baseline Requirements (SSL) | See audit report <http://rdc.fina.hr/CAR/67100UE_s.pdf>  |
| SSL Verification Procedures | SSL CP: Sections 3.2.2, 3.2.3, 3.2.5SSL CPS: Sections 3.2.2, 3.2.3, 3.2.5 |
| Organization Verification Procedures | All above mentioned CPs: Sections 3.2.2, 3.2.3, 3.2.5All above mentioned CPSes: Sections 3.2.2, 3.2.3, 3.2.5 |
| Email Address Verification Procedures | All above mentioned CPs/CPSes: Section 3.2.4 |
| Code Signing Subscriber Verification Procedures | We don’t issue Code Signing certificates. |
| Multi-factor Authentication | All above mentioned CPs/CPSes: Section 6.5.1 |
| Network Security | All above mentioned CPs, CPSes Section 6.7 |

**Response to Mozilla's CA Recommended Practices** ([https://wiki.mozilla.org/CA:Recommended\_Practices](https://wiki.mozilla.org/CA%3ARecommended_Practices))

|  |  |
| --- | --- |
| [Publicly Available CP and CPS](https://wiki.mozilla.org/CA%3ARecommended_Practices#Publicly_Available_CP_and_CPS) | Yes, see Policy Documentation above. |
| [CA Hierarchy](https://wiki.mozilla.org/CA%3ARecommended_Practices#CA_Hierarchy) | Graphical description: <http://www.fina.hr/Default.aspx?sec=1866>. Textual description in CP/CPS: Section 1.1 |
| [Audit Criteria](https://wiki.mozilla.org/CA%3ARecommended_Practices#Audit_Criteria) | “Trust Service Providers practice” in ETSI EN 319 411-1 v1.1.1 for "TLS" on level OV and for "eMail" on level NCP |
| [Document Handling of IDNs in CP/CPS](https://wiki.mozilla.org/CA%3ARecommended_Practices#Document_Handling_of_IDNs_in_CP.2FCPS) | Not allowed. |
| [Revocation of Compromised Certificates](https://wiki.mozilla.org/CA%3ARecommended_Practices#Revocation_of_Compromised_Certificates) | All above mentioned CPs, CPSes: Section 4.9 for subscriber keys, Section 5.7.3 for CA keys. |
| [Verifying Domain Name Ownership](https://wiki.mozilla.org/CA%3ARecommended_Practices#Verifying_Domain_Name_Ownership) | CP 3.2.2 & CPS 3.2.2.2 Verification of Right to Use the FQDN or Server IP Address |
| [Verifying Email Address Control](https://wiki.mozilla.org/CA%3ARecommended_Practices#Verifying_Email_Address_Control) | All above mentioned CPs/CPSes 3.2.3 Authentication of individual identity |
| [Verifying Identity of Code Signing Certificate Subscriber](https://wiki.mozilla.org/CA%3ARecommended_Practices#Verifying_Identity_of_Code_Signing_Certificate_Subscriber) | We don’t issue Code Signing certificates. |
| [DNS names go in SAN](https://wiki.mozilla.org/CA%3ARecommended_Practices#DNS_names_go_in_SAN) | Yes |
| [Domain owned by a Natural Person](https://wiki.mozilla.org/CA%3ARecommended_Practices#Domain_owned_by_a_Natural_Person) | We don’t issue SSL certificates to natural persons. |
| [OCSP](https://wiki.mozilla.org/CA%3ARecommended_Practices#OCSP) | All above mentioned CPs, CPSes: Section 7.3 |

**Response to Mozilla's list of Potentially Problematic Practices** ([https://wiki.mozilla.org/CA:Problematic\_Practices](https://wiki.mozilla.org/CA%3AProblematic_Practices))

|  |  |
| --- | --- |
| [Long-lived DV certificates](https://wiki.mozilla.org/CA%3AProblematic_Practices#Long-lived_DV_certificates) | The validity period of subscriber SSL certificate is one and two years. The domain name ownership will be re-verified when the certificate is renewed.Fina does not issue DV SSL certificates, Fina only issues Organization–Validated SSL certificates. |
| [Wildcard DV SSL certificates](https://wiki.mozilla.org/CA%3AProblematic_Practices#Wildcard_DV_SSL_certificates) | Not applicable, Fina does not issue Wildcard DV SSL certificates. |
| [Email Address Prefixes for DV Certs](https://wiki.mozilla.org/CA%3AProblematic_Practices#Email_Address_Prefixes_for_DV_Certs) | Not applicable. |
| [Delegation of Domain / Email validation to third parties](https://wiki.mozilla.org/CA%3AProblematic_Practices#Delegation_of_Domain_.2F_Email_validation_to_third_parties) | Not allowed.. |
| [Issuing end entity certificates directly from roots](https://wiki.mozilla.org/CA%3AProblematic_Practices#Issuing_end_entity_certificates_directly_from_roots) | Not allowed. |
| [Allowing external entities to operate subordinate CAs](https://wiki.mozilla.org/CA%3AProblematic_Practices#Allowing_external_entities_to_operate_subordinate_CAs) | Not allowed. |
| [Distributing generated private keys in PKCS#12 files](https://wiki.mozilla.org/CA%3AProblematic_Practices#Distributing_generated_private_keys_in_PKCS.2312_files) | SSL CPS 3.2.1.1: Fina may generate the key pair for SSL Certificate Level 2 (OVCP) at its location. In this case the registered and authenticated Custodian, through the use of Fina CMS service and the secure TLS channel, retrieves the issued key pair and certificate in a PKCS#12 file protected by activation data. |
| [Certificates referencing hostnames or private IP addresses](https://wiki.mozilla.org/CA%3AProblematic_Practices#Certificates_referencing_hostnames_or_private_IP_addresses) | Not applicable. Fina does not issue certificates of this type. |
| [Issuing SSL Certificates for Internal Domains](https://wiki.mozilla.org/CA%3AProblematic_Practices%22%20%5Cl%20%22Issuing_SSL_Certificates_for_Internal_Domains) | Not allowed. |
| [OCSP Responses signed by a certificate under a different root](https://wiki.mozilla.org/CA%3AProblematic_Practices%22%20%5Cl%20%22OCSP_Responses_signed_by_a_certificate_under_a_different_root) | No. |
| [CRL with critical CIDP Extension](https://wiki.mozilla.org/CA%3AProblematic_Practices#CRL_with_critical_CIDP_Extension) | Not applicable. |
| [Generic names for CAs](https://wiki.mozilla.org/CA%3AProblematic_Practices#Generic_names_for_CAs) | Not applicable. |
| [Lack of Communication With End Users](https://wiki.mozilla.org/CA%3AProblematic_Practices%22%20%5Cl%20%22Lack_of_Communication_With_End_Users) | No, Fina provides customer server hotline, email and official website to general publics including subscriber, relying parties. |
| [Backdating the notBefore date](https://wiki.mozilla.org/CA%3AProblematic_Practices#Backdating_the_notBefore_date) | Not allowed – certificates are valid from the issuing day. |