Mozilla - CA Program

Case Information

Case Number	00000310	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Financijska agencija (Fina)	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include Financijska agencija (Fina) root certs	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1449941

General information about CA's associated organization

CA Email Alias 1	pma@fina.hr		
CA Email Alias 2			
Company Website	http://www.fina.hr/finadigicert	**Verified?**	Verified
Organizational Type	Government Agency	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Croatia	**Verified?**	Verified
Primary Market / Customer Base	Fina CAs are intended for use in electronic business inside and outside the Republic of Croatia. Fina is Qualified Trust Service Provider and operates in accordance eIDAS Regulation (Regulation (EU) 910/2014).	**Verified?**	Verified
Impact to Mozilla Users	Croatia user base.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's lists of Required and Recommended Practices, and

			confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	1. Publicly Available CP and CPS: CP/CPS section 2.2 1.1 Revision Table, updated annually: CP/CPS page 2 1.2 CAA Domains listed in CP/CPS: SSL CP/CPS section 4.2.2 1.3 BR Commitment to Comply statement: SSL CPS section 1.1.2 2. Audit Criteria: CP/CPS section 8 3. Revocation of Compromised Certificates: CP/CPS section 4.9 4. Verifying Domain Name Ownership: SSL CP section 3.2.2.3 5. Verifying Email Address Control: NEED: If requesting the Email (S/MIME) trust bit, the CP/CPS must explain how the CA confirms that the certificate subscriber owns/controls the email address to be included in the certificate. Which of the CP/CPS documents apply to S/MIME cert issuance? In the Qualified and Non-Qualified CP/CPS documents, section 3.2.4 says that e-mail address is not verified. Reference: https://wiki.mozilla.org /CA/Required_or_Recommended_Practices#Verifying_Email_Address_Control 6. DNS names go in SAN: SSL CP/CPS section 3.1 7. OCSP: CP/CPS section 4.9.9, 4.10 - OCSP SHALL NOT respond "Good" for unissued certs: 8. Network Security Controls: CP/CPS section 6.7	**Verified?**	Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA/Forbidden_or_Problematic_Practices	**Problematic Practices Statement**	I have reviewed Mozilla's lists of Forbidden and Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	1. Long-lived Certificates: SSL CP/CPS section 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: SSL CP section 3.2.2.3 3. Issuing End Entity Certificates Directly From Roots: CP/CPS section 1.1, 1.3.1 4. Distributing Generated Private Keys in PKCS#12 Files: SSL CP section 3.2.1 5. Certificates Referencing Local Names or Private IP Addresses: SSL CP section 3.2.2.4 6. Issuing SSL Certificates for .int Domains: SSL CP section 3.2.2.3 7. OCSP Responses Signed by a Certificate Under a Different Root: 8. Issuance of SHA-1 Certificates: CP/CPS section 6.1.5 9. Delegation of Domain / Email Validation to Third Parties: CP/CPS section 1.3.2	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Fina Root CA	**Root Case No**	R00000614
Request Status	Information Verification In Process	**Case Number**	00000310

Certificate Data

Certificate Issuer Common Name	Fina Root CA
O From Issuer Field	Financijska agencija
OU From Issuer Field	
Valid From	2015 Nov 24
Valid To	2035 Nov 24
Certificate Serial Number	009833C9A8000000005654BC6E
Subject	CN=Fina Root CA; OU=; O=Financijska agencija; C=HR
Signature Hash Algorithm	SHA256WithRSA
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	6202BF169AF27FA67ED0CEC66B782B83226126E9
SHA-256 Fingerprint	5AB4FCDB180B5B6AF0D262A2375A2C77D25602015D96648756611E2E78C53AD3
Subject + SPKI SHA256	0414F71EAA8C54FE14D9123181A3E56981A24C55FE04B4A81E0956C8443F3D7F
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	Fina Root CA has two internally-operated intermediate certificates, one for state administration bodies, and the other for business entities and citizens.	**Verified?**	Verified
Root Certificate Download URL	http://rdc.fina.hr /Root/FinaRootCA.pem	**Verified?**	Verified
CRL URL(s)	http://rdc.fina.hr/Root/FinaRootCA.crl http://rdc.fina.hr/RDC2015 /FinaRDCCA2015.crl http://rdc.fina.hr/RDC-TDU2015 /FinaRDC-TDUCA2015.crl SSL CP section 4.9.7: nextUpdate is 24 hours	**Verified?**	Verified
OCSP URL(s)	http://ocsp.fina.hr	**Verified?**	Verified

Mozilla Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In		**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid		**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			
Example Cert			
Test Notes	NEED: 3 test websites as per section 2.2 of the CA/Browser Forum's Baseline Requirements: At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.		

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the CA/Browser Forum Baseline Requirements (BRs). BR Lint Test: https://github.com/awslabs/certlint	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: The CA MUST check that they are not issuing certificates that violate any of the X.509 rules. X.509 Lint Test: https://github.com/kroeckx/x509lint	**Verified?**	Need Response From CA
EV Tested	N/A	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CP/CPS section 1.1 http://www.fina.hr/Default.aspx?sec=1866. There are two subordinate CAs signed by “Fina Root CA”: “Fina RDC	**Verified?**	Verified

	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).		
Externally Operated SubCAs	None	**Verified?**	Verified
Cross Signing	Not Allowed	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	External Registration Authorities are allowed: SSL CPS sections 1.3.2 and 9.6.2 RA Network: The complete registration authority network consisting of the Fina RA Network and of external RAs with which Fina concluded an agreement on the registration services. Section 9.6.1: ensures that internal and external verification of compliance of Fina as the provider of trust services are conducted in accordance with Section 8.1 hereof.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Root http://rdc.fina.hr/Root/FinaRootCA-CPCPS2-2-en.pdf SSL http://rdc.fina.hr/RDC2015/FinaRDC2015-CPWSA1-2-en.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CPSWSA1-2-en.pdf QC http://rdc.fina.hr/RDC2015/FinaRDC2015-CPQC1-2-en.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CPSQC1-2-en.pdf NQC http://rdc.fina.hr/RDC2015/FinaRDC2015-CPNQC1-1-en.pdf http://rdc.fina.hr/RDC2015/FinaRDC2015-CPSNQC1-1-en.pdf	**Verified?**	Verified
CA Document Repository	https://www.fina.hr/finadigicert	**Verified?**	Verified
CP Doc Language	English		
CP	http://rdc.fina.hr/RDC2015/FinaRDC2015-CPWSA1-2-en.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	http://rdc.fina.hr/Root/FinaRootCA-CPCPS2-2-en.pdf	**Verified?**	Verified

Other Relevant Documents	Audit Reports: 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	**Verified?**	Verified
Auditor	TÜViT - TÜV Informationstechnik GmbH	**Verified?**	Verified
Auditor Location	Germany	**Verified?**	Verified
Standard Audit	http://rdc.fina.hr/CAR/67100UE_s.pdf	**Verified?**	Not Verified
Standard Audit Type	ETSI EN 319 411	**Verified?**	Not Verified
Standard Audit Statement Date	6/26/2018	**Verified?**	Not Verified
BR Audit	http://rdc.fina.hr/CAR/67100UE_s.pdf	**Verified?**	Not Verified
BR Audit Type	ETSI EN 319 411	**Verified?**	Not Verified
BR Audit Statement Date	6/26/2018	**Verified?**	Not Verified
EV SSL Audit		**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	SSL CPS section 1.1.2	**Verified?**	Verified
BR Self Assessment	NEED: If requesting Websites trust bit, attach BR Self Assessment (https://wiki.mozilla.org/CA/BR_Self-Assessment) to the Bugzilla Bug.	**Verified?**	Need Response From CA
SSL Verification Procedures	SSL CP section 3.2.2.3	**Verified?**	Verified
EV SSL Verification Procedures	N/A	**Verified?**	Not Applicable
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	NEED: If requesting the Email (S/MIME) trust bit, the CP/CPS must explain how the CA confirms that the certificate subscriber owns/controls the email address to be included in the certificate. Which of the CP/CPS documents apply to S/MIME cert issuance? In the Qualified and Non-Qualified CP/CPS documents, section 3.2.4 says that e-mail address is not verified. Reference: https://wiki.mozilla.org /CA/Required_or_Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable

Multi-Factor Authentication	CP/CPS section 6.5.1	**Verified?**	Verified
Network Security	CP/CPS section 6.7	**Verified?**	Verified