Print this page

Mozilla - CA Program

Case Information

Case Number	00000256	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Notarius	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include Notarius Root	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=1431811

General information about CA's associated organization

CA Email Alias 1	officers@notarius.com		
CA Email Alias 2			
Company Website	https://notarius.com	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	USA, Global	**Verified?**	Verified
Primary Market / Customer Base	Issues certificates to the public for S/MIME, document signing, and user authentication. https://notarius.com/en/industry	**Verified?**	Verified
Impact to Mozilla Users	Already included in Microsoft Trusted Root Program and Adobe Trusted Root Program.	**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 section 2.2 1.1 Revision Table, updated annually: CP Version tracking table 1.2 CAA Domains listed in CP/CPS: N/A 2. Audit Criteria: CP section 8 3. Revocation of Compromised Certificates: CP section 4.5 4. Verifying Domain Name Ownership: N/A 5. Verifying Email Address Control: ??? (NEED -- I did not find description in the CP of how the CA/LRA verifies that the email address to be included in the certificate is owned/controlled by the certificate subscriber.) 6. DNS names go in SAN: N/A 7. OCSP: CP section 7 8. Network Security Controls: CP 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: CP sections 3.2.4, 4.2.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: N/A 3. Issuing End Entity Certificates Directly From Roots: No 4. Distributing Generated Private Keys in PKCS#12 Files: CP section 6.1.2 5. Certificates Referencing Local Names or Private IP Addresses: N/A 6. Issuing SSL Certificates for .int Domains: N /A 7. OCSP Responses Signed by a Certificate Under a Different Root: No 8. Issuance of SHA-1 Certificates: CP section 7 9. Delegation of Domain / Email Validation to Third Parties: CP section 1.6.3	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Notarius Root Certificate Authority	**Root Case No**	R00000509
Request Status	Information Verification In Process	**Case Number**	00000256

Certificate Data

Certificate Issuer Common Name	Notarius Root Certificate Authority
O From Issuer Field	Notarius Inc
OU From Issuer Field	
Valid From	2014 Dec 17
Valid To	2034 Dec 17
Certificate Serial Number	5491a8b0
Subject	CN=Notarius Root Certificate Authority, OU=null, O=Notarius Inc, C=CA
Signature Hash Algorithm	sha256WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	1F:3F:14:86:B5:31:88:28:02:E8:7B:62:4D:42:02:95:A0:FC:72:1A
SHA-256 Fingerprint	C7:B8:94:8F:EC:CA:AC:E5:B5:09:A3:43:F3:8D:03:01:D0:79:01:88:56:04:B3:F2:67:27:0E:1E:BB:EF:0F:E7
Certificate ID	8C:3F:6A:B9:CD:A2:A3:E0:8B:94:62:50:4D:8F:E0:02:50:B1:9F:F6:E3:DD:05:B7:29:8B:A5:57:62:36:41:BD
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	This request is to include the 'Notarius Root Certificate Authority' certificate and only enable the email trust bit.	**Verified?**	Verified
Root Certificate Download URL	https://download.notarius.com/certifio/public-root/notarius-root-certificate-authority.cer	**Verified?**	Verified

CRL URL(s)	http://crl.notarius.com/notarius_root_ca/crl/crl_roota1.crl http://crl1.notarius.com/crl1-ca1/crl/notarius_certificate_authority_crlfull.crl http://crl1.notarius.com/crl1-ca2/crl/notarius_certificate_authority_2_crlfull.crl nextUpdate = 48 hours	**Verified?**	Verified
OCSP URL(s)	http://ocsp1.notarius.com/ocsp1-ca1 http://ocsp1.notarius.com/ocsp1-ca2	**Verified?**	Verified
Mozilla Trust Bits	Email	**Verified?**	Verified
SSL Validation Type		**Verified?**	Not Applicable
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Apple; Microsoft	**Verified?**	Verified
Mozilla Applied Constraints		**Verified?**	Not Applicable

Test Websites or Example Cert

Test Website - Valid		**Verified?**	Verified
Test Website - Expired			
Test Website - Revoked			
Example Cert	https://bugzilla.mozilla.org/attachment.cgi?id=8947988		
Test Notes			

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

Revocation Tested		**Verified?**	Not Applicable
CA/Browser Forum Lint Test		**Verified?**	Not Applicable
Test Website Lint Test		**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CP section 1.1 Root CA and all Subordinate CA are operated by Solutions Notarius.	**Verified?**	Verified

	Notarius Certificate Authority : Subordinate CA of Notarius Root Certificate Authority. This subordinate is currently included in the Adobe Approved Trust List, and every user certificate issue by this subordinate CA are AATL approved in Adobe Software. Every certificate issue by this subordinate CA must be generated on Crypto Token. Notarius Certificate Authority 2 : Subordinate CA of Notarius Root Certificate Authority. User certificate issue by this subordinate CA is recognized by Microsoft Trust Store, since our Root CA is also trusted by Microsoft Trusted Root Program. User certificate issue by this subordinate is generated on software crypto-vault.		
Externally Operated SubCAs	None CP section 1.6	**Verified?**	Verified
Cross Signing	None	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	NEED: It's not clear to me if/when LRA's are audited. Or how it is regularly checked that the LRA is only issuing certs that it should be issuing, and following the CP. CP section 1.6.3: All LRAs have signed contractual agreements with the C/RSP, or with a delegated representative of the C/RSP authorized to do so. LRA roles and responsibilities: - Make available at all times at least two people (or one person in the case of legal entities) to act as an Affiliation Verification Agent (AVA), and take all actions necessary to fulfill this requirement; - Manage AVA appointments; - Ensure that at least one (1) AVA is available to fulfill this function on any given business day; - Ensure AVAs comply with all obligations set out in the CP.	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy	Documents are in English.	**Verified?**	Verified
CA Document Repository	https://notarius.com /en/certification-policy/	**Verified?**	Verified
CP Doc Language	English		
CP	http://notarius.com/wp-content /uploads/2018/01/Notarius-PKI-Certificate-Policy.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS		**Verified?**	Not Applicable
Other Relevant Documents		**Verified?**	Not Applicable
Auditor	KPMG	**Verified?**	Verified
Auditor Location	Canada	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org /SealFile?seal=2240&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	4/10/2017	**Verified?**	Verified
BR Audit		**Verified?**	Not Applicable
BR Audit Type		**Verified?**	Not Applicable
BR Audit Statement Date		**Verified?**	Not Applicable
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	N/A	**Verified?**	Not Applicable
BR Self Assessment	N/A	**Verified?**	Not Applicable
SSL Verification Procedures	N/A	**Verified?**	Not Applicable
EV SSL Verification Procedures	N/A	**Verified?**	Not Applicable
Organization Verification Procedures	CP sections 3.2, 4.1	**Verified?**	Verified
Email Address Verification Procedures	NEED: I could not find the description of how the CA verifies that the certificate subscriber owns/controls the email address to be included in the S/MIME	**Verified?**	Need Response From CA