Print this page

Mozilla - CA Program

Case Information

Case Number	00000098	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	TeliaSonera	**Request Status**	Initial Request Received

Additional Case Information

Subject	Enable EV for TeliaSonera Root CA v1 root	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1322668

General information about CA's associated organization

CA Email Alias 1			
CA Email Alias 2			
Company Website	http://www.teliacompany.com/	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)	N/A	**Verified?**	Verified
Geographic Focus	Europe and Russia	**Verified?**	Verified
Primary Market / Customer Base	It is a commercial CA creating SSL and Client certificates for Nordic customers. They are offering certificates for server authentication, client authentication, email (both signing and encrypting), but not for code signing. Now they want to expand to EV SSL certificates.	**Verified?**	Verified
Impact to Mozilla Users		**Verified?**	Need Response From CA

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of 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: https://repository.trust.teliasonera.com/TeliaCompany_Server_Certificate_CPS_v1.6.pdf 2) CA Hierarchy 3) Audit Criteria 4) Document Handling of IDNs in CP/CPS 5) Revocation of Compromised Certificates 6) Verifying Domain Name Ownership	**Verified?**	Need Response From CA

7) Verifying Email Address Control
8) Verifying Identity of Code Signing Certificate Subscriber
9) DNS names go in SAN
10) Domain owned by a Natural Person
11) OCSP
12) Network Security Controls

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of 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 DV certificates: 2) Wildcard DV SSL certificates: 3) Email Address Prefixes for DV Certs: 4) Delegation of Domain / Email validation to third parties: 5) Issuing end entity certificates directly from roots: 6) Allowing external entities to operate subordinate CAs: 7) Distributing generated private keys in PKCS#12 files: 8) Certificates referencing hostnames or private IP addresses: 9) Issuing SSL Certificates for Internal Domains: 10) OCSP Responses signed by a certificate under a different root: 11) SHA-1 Certificates: Stopped issue SHA-1 certificates from September 28th, 2016. 12) Generic names for CAs: 13) Lack of Communication With End Users: 14) Backdating the notBefore date:	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	Enable EV for TeliaSonera Root CA v1 root	**Root Case No**	R00000139
Request Status	Initial Request Received	**Case Number**	00000098

Certificate Data

Certificate Issuer Common Name	
O From Issuer Field	
OU From Issuer Field	
Valid From	
Valid To	
Certificate Serial Number	
Subject	
Signature Hash Algorithm	
Public Key Algorithm	
SHA-1 Fingerprint	
SHA-256 Fingerprint	
Certificate	

Fingerprint	
Certificate Version	

Technical Information about Root Certificate

Certificate Summary	"TeliaSonera Root CA v1" is the main root CA for Telia Company. It is a commercial CA creating SSL and Client certificates for Nordic customers.CA want to expand to EV SSL certificates.	**Verified?**	Verified
Root Certificate Download URL	http://repository.trust.teliasonera.com/teliasonerarootcav1.cer	**Verified?**	Need Clarification From CA
CRL URL(s)	NEED CRL URLs and CRL issuing frequency for subscriber certs, with reference to where this is documented in the CP/CPS	**Verified?**	Need Response From CA
OCSP URL(s)	http://ocsp.trust.teliasonera.com	**Verified?**	Verified
Trust Bits	Email; Websites	**Verified?**	Verified
SSL Validation Type	OV; EV	**Verified?**	Verified
EV Policy OID(s)	2.23.140.1.1	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website URL (SSL) or Example Cert	NEED: - If requesting Websites trust bit: URL to a website whose SSL cert chains up to this root. Note that this can be a test site. - If requesting Email trust bit: attach an example cert to the bug.	**Verified?**	Need Response From CA
Test Website - Expired			
Test Website - Revoked			

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

Revocation Tested	No Errors	**Verified?**	Verified
CA/Browser Forum Lint Test	ERROR: CA certificates must include countryName in subject ERROR: CA certificates must set keyUsage extension as critical NEED: Browse to https://crt.sh/ and enter the SHA-1	**Verified?**	Need Clarification From CA
Test Website Lint Test	Test not currently available.	**Verified?**	Not Applicable
EV Tested	ev-checker exited successfully: Success!	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the	**Verified?**	Need Response From CA

	root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements		
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	https://repository.trust.teliasonera.com/TeliaCompany_Server_Certificate_CPS_v1.6.pdf	**Verified?**	Verified
CA Document Repository	https://repository.trust.teliasonera.com/	**Verified?**	Verified
CP Doc Language			
CP		**Verified?**	Need Response From CA
CP Doc Language			
CPS	https://repository.trust.teliasonera.com/TeliaCompany_Server_Certificate_CPS_v1.6.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Verified
Auditor Name	Ernst&Young	**Verified?**	Verified
Auditor Website	www.ey.com	**Verified?**	Verified
Auditor Qualifications	https://support.partnergate.sonera.com/download/CA/audit2016.pdf https://support.partnergate.sonera.com/repository/TeliaCompanyBRAuditReport.pdf	**Verified?**	Verified
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type		**Verified?**	Need Response From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response

			From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	Ernst&Young	**Verified?**	Need Clarification From CA
EV Audit Type	WebTrust	**Verified?**	Need Clarification From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	NEED: If EV verification is performed, then provide URLs and section/page number information pointing directly to the sections of the CP/CPS documents that pertain to EV and describe the procedures for verifying the ownership/control of the domain name, and the verification of identity, existence, and authority of the organization to request the EV certificate. The EV verification documentation must meet the requirements of the CA/Browser Forum's EV Guidelines, and must also provide information specific to the CA's operations.	**Verified?**	Need Response From CA
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA: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	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to publicly disclosed subordinate CA certificates that chain up to certificates in Mozilla's CA program, as	**Verified?**	Need Response From CA

per Items #8, 9, and 10 of Mozilla's CA Certificate Inclusion Policy.