Bugzilla ID: 539924
Bugzilla Summary: Add TeliaSonera Root CA v1 root certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	TeliaSonera
Website URL	http://www.teliasonera.com/home
Organizational type	Public Corporation
Primary market / customer base	TeliaSonera provides telecommunication services in the Nordic and Baltic countries, the emerging markets of Eurasia, including Russia and Turkey, and in Spain. CA operations currently only in Nordic countries.
CA Contact Information	CA Email Alias: cainfo@sonera.com CA Phone Number: 46 (0)20 32 32 62 Title / Department: TeliaSonera CA Policy Authority

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	TeliaSonera Root CA v1
Cert summary / comments	
Root CA certificate URL	Please provide the url for downloading this root cert.
SHA-1 fingerprint	43 13 bb 96 f1 d5 86 9b c1 4e 6a 92 f6 cf f6 34 69 87 82 37
Valid from	2007-10-18
Valid to	2032-10-18
Cert Version	3
Modulus length / key length	4096
Test Website	For testing purposes, please provide a URL to a website whose SSL cert chains up to this root.
CRL URL	http://crl-2.trust.teliasonera.com/teliasonerarootcav1.crl (Next Update: 7 days) http://crl-2.trust.teliasonera.com/TeliaSoneraClass2CAv1.crl (Next Update: 2 days) http://crl-2.trust.teliasonera.com/TeliaSoneraEmailCAv3.crl (Next Update: 2 days) CPS Section 2.7.2: CRLs are published at least once in a day. The CRL validity period is 168 hours.
OCSP Responder URL	None
CA Hierarchy	TeliaSonera Root CA v1 has the 5 internally-operated subordinate CA's listed below.

	Subordinate CA's will issue end entity certificates for types stated in sub CA names. - TeliaSonera Class1 CA v1 (smart card / usb token based client certificates) - TeliaSonera Class2 CA v2 (software client certificates for VPN services, SSL, Signatures, Authentication, and E-mail encryption) - TeliaSonera Server CA v1 - TeliaSonera Email CA v3 - TeliaSonera VPN CA v1
Sub-CAs operated by 3rd parties	None
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type DV, OV, and/or EV	DV and OV
EV policy OID(s)	Not EV
CP/CPS	Document and CA repository: http://repository.trust.teliasonera.com/index2_en.php TeliaSonera Root CA v1 Practice Statement (English): http://repository.trust.teliasonera.com/download/CA/TeliaSonera_Root_CA_v1_CPS%20Rev_A.pdf TeliaSonera Class2 CA v1/TeliaSonera E-mail v3 Practice Statement (English): http://repository.trust.teliasonera.com/download/CA/TeliaSonera_Class2_CA_v1_Rev_A.pdf Where are the Practice Statements for the other (Class1, Server, and VPN) sub-CAs that are listed above?
AUDIT	Audit Type: WebTrust CA Auditor: Ernst & Young Auditor Website: http://www.ey.com/GL/EN/Home Audit: https://cert.webtrust.org/ViewSeal?id=970 (2009.03.31) The audit includes “TeliaSonera Root CA v1” and its subordinate CAs including “TeliaSonera Class 2 CA v1 and TeliaSonera E-mail CA v3”. What about the other sub-CAs, e.g. Class1, Server, and VPN? What’s the difference between “TeliaSonera Class 2 CA v1” and “TeliaSonera Class2 CA v2” that is listed as one of the 5 sub-CAs for this root above?
Organization Identity Verification	Class 2 CP section 3.2.4: Authentication of organization identity The identity of a new Customer Organization is verified on the basis of information in the order or agreement by verifying

	the existence of the company and the Business Identity Code or other similar identifier from a database maintained by a third party. The Subscriber's administrative contact person who grants the necessary authorizations in the Customer Organization has been identified in the order or agreement. The authenticity of the contact person is checked by calling him via the Customer Organization's PBX number or when there is no switchboard, by making a call to some other number in the organization, which is looked up from a directory maintained by a third party. Section 3.2.4.1: Authentication of identity of Registration Officer acting in Customer Organization Section 3.2.4.2: Authentication of Device for certificate application Class 2 CP section 3.2.5: Verifying of Subject identity and name Verification of the names and identities of Subjects is carried out by Registration Officers acting in Customer Organizations. It is also a Registration Officer's responsibility to ensure that the Subject has the right granted by the Customer Organization to apply for a certificate. The Registration Officers are obliged to follow registration directions given by the CA and included in the document "Sonera CA Customer's Responsibilities" Information on employees or partners who are in an agreement relationship recorded earlier by the Customer Organization is used in the verification of the name and identity of the Subject, or the Registration Officer verifies the information by checking the Subject's identity card.
Domain Name Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Class 2 CP section 3.2.4.2: "As regards server certificates, it is checked from a database maintained by a third party that the IP address or domain name mentioned in the order belongs to the organization which has made the order or to a service provider authorized by the organization." Class 2 CP section 4.1.2: "A Registration Officer in a Customer Organization can be granted the right to apply for certificates to Devices (SSL server certificates) directly from the CA system by using a tool delivered by the CA. The Subscriber defines the IP address space or domains under the right, and the CA verifies that they have been registered for the Subscriber." It is not clear to me how TeliaSonera verifies that the certificate subscriber owns/controls the domain name to be included in the certificate. E.g. how is the information obtained from the third party used to do the verification? I may misunderstand, but it appears that once Registration Officer of a Customer Organization is approved, then that Registration Officer can approve and issue SSL certificates. Correct? How is it controlled which domains the

	Registration Officer issues SSL certs for?
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; Please point me to the documentation of the practices for verifying that the certificate subscriber owns/controls the email address to be included in the certificate.
Identity of Code Signing Subscriber	Not Applicable – Not requesting the Code Signing trust bit.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information and pointers to the relevant sections of the CP/CPS documents. • Long-lived DV certificates o • Wildcard DV SSL certificates o • Delegation of Domain / Email validation to third parties o • Issuing end entity certificates directly from roots o • Allowing external entities to operate unconstrained subordinate CAs o • Distributing generated private keys in PKCS#12 files o • Certificates referencing hostnames or private IP addresses o • Issuing SSL Certificates for Internal Domains o • OCSP Responses signed by a certificate under a different root o OCSP not provided • CRL with critical CIDP Extension

	○ CRLs downloaded into Firefox without error. • Generic names for CAs ○ Root cert name is not generic.