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/
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

Issuer Field	CN = TeliaSonera Root CA v1
	O = TeliaSonera

Cert summary / comments	TeliaSonera Root CA v1 has 6 internally-operated subordinate CAs for server, client, and TeliaSonera internal certificates.
Root CA certificate URL	http://repository.trust.teliasonera.com/teliasonerarootcav1.cer
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	https://juolukka.cover.sonera.net:10443/
CRL URL	http://crl-2.trust.teliasonera.com/teliasonerarootcav1.crl http://crl-3.trust.teliasonera.com/teliasonerarootcav1.crl (NextUpdate: 7 days) Root CPS Section 4.9.7: CRLs are published at least once in a day. The CRL validity period is 168 hours. (7 days)
OCSP Responder URL	http://ocsp.trust.teliasonera.com/ The test cert and intermediate don't have the OCSP URI in the AIA, because OCSP service is coming on line in November, 2012. Will need updated certs when OCSP service is available.

CA Hierarchy	6 internally-operated subordinate CAs: - TeliaSonera Class1 CA v1 (public client certificates issued in Finland) - TeliaSonera Class2 CA v1 (public client certificates issued in Sweden) - TeliaSonera Server CA v1 (public SSL certificates) - TeliaSonera Gateway CA v1 (internal SSL server certificates for TeliaSonera services) - TeliaSonera Email CA v3 (internal client certificates for TeliaSonera internal email system) - TeliaSonera Mobile ID CA v1 (internal mobile certificates for TeliaSonera mobile phone services)
Sub-CAs operated by 3rd parties	None
Cross-Signing	Root CPS section 1.3.1: TeliaSonera Root CA v1 is currently a subordinate CA of Sonera Class 2 CA. It is planned that after the transition period, the TeliaSonera Root CA v1 will be made the ultimate root CA by replacing the current TeliaSonera Root CA v1 certificate signed by Sonera Class 2 CA with a new self-signed CA certificate.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME)
SSL Validation Type	OV
EV policy OID(s)	Not EV
CP/CPS	Repository: https://repository.trust.teliasonera.com Customer Support Site: http://support.partnergate.sonera.com/cavarmennepalvelu_en.html Production CPS: https://repository.trust.teliasonera.com/TeliaSonera_Production_CPS_v2.01.pdf Root CPS: http://repository.trust.teliasonera.com/TeliaSonera_Root_CPS_v2.01.pdf Server Cert CPS: https://repository.trust.teliasonera.com/TeliaSonera_Server_Certificate_CPS_v1.01.pdf Organizational User Cert CPS: https://repository.trust.teliasonera.com/TeliaSonera_Organizational_User_Certificate_CPS_v1.00.pdf Internal Mobile ID cert CPS (Finnish): http://repository.trust.teliasonera.com/mobile-id
AUDIT	Audit Type (WebTrust, ETSI etc.): WebTrust Auditor: Ernst & Young Auditor Website: http://www.ey.com/GL/EN/Home Audit Document URL(s): https://cert.webtrust.org/ViewSeal?id=1369 (2012.03.31)
Baseline Requirements (SSL)	Server Cert CPS section 1.1: This CPS and all certificates containing the OID value reserved for this CPS conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirement, those Requirements take precedence over this document.
Organization Identity Verification	Server Cert CPS section 3.2.2, Authentication of organization identity Server Cert CPS section 3.2.3, Authentication of individual identity TeliaSonera has two different server certificate services: 1) SSL order by public electronic form: TeliSonera authenticates the administrative contact person defined in the certificate application by calling the contact person via the Customer'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. 2) SSL order using TeliaSonera's self service software: The Customer can make an agreement with TeliaSonera to act as a Registration Officer within the Customer Organization (Full SSL Service) and to register TeliaSonera Server certificates

	using TeliaSonera’s RA system for Customers. The Customer Registration Officer is restricted to register certificates only within their own Organization (O) and the domain names authorized by the CA. Before enabling the service or adding new authorized Organization or domain names, the CA verifies the organization identity and the domain names as described in the section 3.2.2. When registering Subjects, the identity of the Registration Officer is verified by means of the Registration Officer’s certificate issued by a TeliaSonera CA.
Domain Name Ownership / Control	Server Cert CPS section 3.2.2: TeliaSonera verifies domain names and IP addresses from a database maintained by a reliable third party registrar e.g.e “domain.fi” (for domain “.fi”), iis.se (for domain “.se”), ripe.net (for IP addresses) and www.networksolutions.com/whosis-search (for non-country domains), that as of the date the Certificate was issued, the Aplication either had the right to use, or had control of, the Fully-Qualified Domain Names(s) and IP address(es) listed int e Certificate, or was authorized by a person having such right or contgrol (e.g. under a Principal-Agent or Licensor-Licensee relationship) to obtain a Certificate Containing the Fully-Qualfiied Domain mames(s) and IP address(es). Comment #2: In enterprise RA cases when Customer Registration Officer is allowed to enroll server certificates for his/her organization each organization and domain value is first inspected by TeliaSonera Registration Officer using the documented checking rules. Then the values are added to the configuration of that customer so that later the customer can use same values without a new verification.
Email Address Ownership / Control	Organizational User Cert CPS section 3.2.3, Authentication of individual identity The procedures to authenticate the identity of the Subject vary between the different TeliaSonera certificate services: TeliaSonera Class 1 CA v1 – TeliaSonera or Customer Registration Officer is responsible for authenticating the Subject data according to Organization’s internal policies. Subject authentication is typically based on a previously recorded ownership of Customer’s email address, device, or mobile phone number. If Common Name or dnsName field of Subject Alternative Name includes public domain names, TeliaSonera verifies that Customer Organization has right to use them by checking the ownership from the official records (e.g. domain.fi (.fk), iis.se (.se) or www.networksolutions.com/whoi-search). A written permission from the registered legal owner is an alternative. TeliaSonera verifies the ownership of an email address by sending a one-time-password to the applied email-address. Then the Subject entity must use the password within limited time frame to prove the access to the email-address. In Enterprise RA cases email-address can be taken from reliable internal source of the Subscriber without additional verification by one-time-password. TeliaSonera Class 2 CA v1 – Customer or TeliaSonera Registration Officer is responsible for authenticating the Subject. The Registration Officers are obliged to follow the policies and instructions given by the CA. The Registration officer should use Organization’s previously recorded directories, databases or other similar information on Organization’s employees, partners or devices to verify the Subject information including the email address, Or the Registration Officer should verify the information by checking the Subject’s identity card.

	TeliaSonera Email CA v3 – Certificates are issued to employees within the TeliaSonera Group and individuals contracted by TeliaSonera. The Subscriber is authenticated using a username and password and information stored in TeliaSonera's directories or databases.
Identity of Code Signing Subscriber	Not Applicable – Not requesting the Code Signing trust bit.
Multi-factor Authentication	Production CPS section 5: Facility, Management, and operational Controls Production CPS section 5.2.3: Identification of the RA roles takes place within the CA and RA system applications and it is based on strong authentication either using personal operator cards, software based keys and certificates or other two factor authentication mechanisms depending on the policy requirements of the applicable CA.
Network Security	Production CPS section 6: Technical Security Controls Production CPS section 6.5: Computer Security Controls Production CPS section 6.7: Network Security Controls
Potentially Problematic Practices	• Long-lived DV certificates o Comment #2: We have always organization validation also (check CPS 3.2.2). We have maximum validity time of three years. After that normal customers have to provide SSL order again and everything is re-checked. In Enterprise RA case we have improvement idea to redo domain checks periodically. We have already added a timestamp on each approved value in our database. Because of that it is easy to find expiring values. • Wildcard DV SSL certificates o SSL certs are OV • Delegation of Domain / Email validation to third parties o Comment #2: Not applicable. We do all domain/email validation ourselves. • Issuing end entity certificates directly from roots o Comment #2: We are stopping this problematic practice during this year when our new TeliaSonera CAs are replacing the old Sonera CAs. • Allowing external entities to operate unconstrained subordinate CAs o Comment #2: Not applicable. All Sub CAs are operated by TeliaSonera. • Distributing generated private keys in PKCS#12 files o Comment #2: Only applicable with some client certificates. When applicable the PKCS#12 file is always PIN protected and transferred using TLS/SSL protected channel. Check 6.1.2 in TeliaSonera Organizational User Certificate Policy and CPS. • Certificates referencing hostnames or private IP addresses o Comment #2: We will stop enrolling these in the schedule that Cab BR 9.2.1 has specified. • Issuing SSL Certificates for Internal Domains o Comment #2: Not applicable. .int is not used and it is considered as valid public suffix. Null character domain values are automatically discarded. We have our own list of valid TLD values. We are not using internal domain names in our internal CAs in the same CA hierarchy. • OCSP Responses signed by a certificate under a different root

	○ Comment #2: Not applicable. Our upcoming OCSP service (live in November 2012) is using the same CA/root as the SSL certificate. • CRL with critical CIDP Extension ○ CRLs downloaded into Firefox without error. • Generic names for CAs ○ Root cert name is not generic.