Bugzilla ID: 463989
Bugzilla Summary: Request to add Finnish Population Register Centre's Root CA Certificates

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.

General Information	**Data**
CA Name	Finland Population Register Centre (Tynnyrintekijänkatu 1C)
Website URL (English version)	http://www.fineid.fi (technical data, Certificate Policies, Certification Practice Statements, PKI Disclosure Statements, FINEID specifications) http://www.vrk.fi (about Population Register centre in general)
Organizational type. (E.g., whether the CA is operated by a private or public corporation, government agency, academic institution or consortium, NGO, etc.)	Government
Primary market / customer base. (Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does it focus its activities on a particular country or other geographic region?)	The Population Register Centre operates under the Finland Ministry of Finance. The Population Register Centre develops and maintains the national Population Information System, the guardianship register and the Public Sector Directory Service. The Population Register Centre serves as the Certification Authority for the State of Finland, and thus develops and maintains the national certificate services to Finnish Citizens, state workers and organizations. All certificates issued to natural persons by the Population Register Centre are qualified certificates, i.e. European-wide certificates based on an EU Directive and Finnish legislation.

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

Info Needed	**Data**	**Status / Notes**
Certificate Name	VRK Gov. Root CA	COMPLETE
Cert summary / comments	This root issues internally-operated intermediate CAs that issue two basic types of certificates: User certificates and service certificates. All user certificates are stored in tokens, except mobile citizen certificates which are stored only in the directory. Smart cards contain Root, CA and two end entity certificates: One for authentication and encryption, and another for non-repudiation digital	In Progress

	signatures. All non-repudiation certificates issued by VRK are Qualified Certificates. VRK issues two types of service certificates. Server certificates are issued using private keys and PKCS#10 Certificate Requests generated by service providers. Service certificate for email usage is a PKCS#12 format file that contains the certificate and corresponding private and public key. It is service providers duty to keep private keys secured using Hardware Security Module, encryption, passwords or by other means.	
The root CA certificate URL Download into FireFox and verify	http://www.fineid.fi/certs/vrkrootc.crt	COMPLETE
SHA-1 fingerprint.	fa:a7:d9:fb:31:b7:46:f2:00:a8:5e:65:79:76:13:d8:16:e0:63:b5	COMPLETE
Valid from	12/18/2002	COMPLETE
Valid to	12/18/2023	COMPLETE
Cert Version	3	COMPLETE
Modulus length / key length or type of signing key (if ECC)	2048	COMPLETE
CRL • URL • update frequency for end-entity certificates	Please provide URL to the CRL **CPS 4.4.9. The frequency of publishing the revocation list** Information on the placing of a certificate on the revocation list shall be available to the public at the latest within one hour from the time when the revocation request has been declared valid and it has been approved. The revocation list shall be valid for two hours.	Can you provide URLs to the CRLs for the intermediate CAs?
OCSP (if applicable) • OCSP Responder URL	OCSP not provided	COMPLETE
List or description of subordinate CAs operated by the CA organization associated with the root CA. (For example, this might include subordinate CAs created to issue different classes or types of end entity certificates: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV	From section 3 of FINEID specification S2: VRK Gov. Root CA issues the following intermediate CAs: -- VRK Gov. CA for Citizen Qualified Certificates End-entity certs are issued to Finnish citizens and aliens living permanently in Finland. -- VRK Gov. CA for Multiplatform Citizen Qualified Certificates End-entity certs are issued to Finnish citizens and aliens living permanently in Finland and stored to a PKI-SIM.	COMPLETE

certificates, SSL certificates vs. email certificates, and so on.) For internally-operated subordinate CAs the key is to confirm that their operation is addressed by the relevant CPS, and that any audit covers them as well as the root.	--VRK CA for Qualified Certificates End-entity certs are issued to employees of company or organization or an associated group. -- VRK CA for Service Providers End-entity certs are issued for public and private sector services. -- VRK CA for Temporary Certificates End-entity certs are issued to employees of company or organization or an associated group. These intermediate CAs can be downloaded from: http://www.fineid.fi/vrk/fineid/home.nsf/pages/FA842EE9BB3C7AA5C2257054002D3FA9 From FINEID specification S2: "All certificates are issued and administrated by Population Register Centre's Certification Authority services unit, VRK."	
For subordinate CAs operated by third parties, if any: General description of the types of third-party subordinates that exist, and what the general legal/technical arrangements are by which those subordinates are authorized, controlled, and audited.		Please confirm that there are no subordinate CAs of this root that are operated by third parties. Eg. all of this root's intermediate CAs are operated internally.
List any other root CAs that have issued cross-signing certificates for this root CA	None	COMPLETE
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code (Code Signing)	• Websites (SSL/TLS) ? • Email (S/MIME) • Code (Code Signing)	Please provide the location of text in the CPS that demonstrates that reasonable measures are taken to verify the following information for end-entity certificates chaining up to this root, as per section 7

		of http://www.mozilla.org/projects/security/certs/policy/. a)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; b)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; c) for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf;
. If SSL certificates are issued within the hierarchy rooted at this root CA certificate: • Whether or not the domain name referenced in the certificate is verified to be owned/controlled by the certificate subscriber. (This is commonly referred to as		If there are SSL certs chaining up to this root, please identify if all SSL certs chaining up to this root are OV, meaning that both the domain name referenced in the certificate is verified to be owned/controlled by the subscriber, **and** the value of the Organization attribute is verified to be that associated with the certificate subscriber.

a DV certificate.) • Whether or not the value of the Organization attribute is verified to be that associated with the certificate subscriber. (This is commonly referred to as an OV certificate.)		
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable. • For SSL certificates this should also include URLs of one or more web servers using the certificate(s). • There should be at least one example certificate for each of the major types of certificates issued, e.g., email vs. SSL vs. code signing, or EV vs. OS vs. DV. • Note: mainly interested in SSL, so OK if no email example.		Need example cert or URL for testing the root inclusion.
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	FINEID specification S2 – VRK (PRC) CA-model and certificate contents, v2.1 http://www.fineid.fi/vrk/fineid/files.nsf/files/24EA4C4CD4A1EAA0C2257054002A55BD/$file/S2v21.pdf Policies are posted at http://www.fineid.fi/vrk/fineid/home.nsf/pages/8159D738E49D3251C2257054002D7EF4 The Population Register Centre prepares a certificate policy for each certificate	Please review the potentially problematic practices,as per http://wiki.mozilla.org/CA:Problematic_Practices and comment as to whether any of these are relevant. If relevant, please provide further info.

	type it issues. VRK Gov. CA for Citizen Qualified Certificates Policy: http://www.fineid.fi/cps1 Issued to Finnish citizens and aliens living permanently in Finland. VRK Gov. CA for Multiplatform Citizen Qualified Certificates Policy: http://www.fineid.fi/cps4 Issued to Finnish citizens and aliens living permanently in Finland and stored to a PKI-SIM. VRK CA for Qualified Certificates Policy: http://www.fineid.fi/cps2 Issued to employees of company or organization or an associated group. VRK CA for Service Providers Policy: http://www.fineid.fi/cps3 Issued for public and private sector services. VRK CA for Temporary Certificates Policy: http://www.fineid.fi/cps5 Issued to employees of company or organization or an associated group.	
. AUDIT: The published document(s) relating to independent audit(s) of the root CA and any CAs within the hierarchy rooted at the root. (For example, for WebTrust for CAs audits this would be the "audit report and management assertions" document available from the webtrust.org site or elsewhere.)	Auditor: Inspecta Finland Auditor Website: www.inspecta.com Audit Statement/Report: ? Auditor: Finnish Communications Regulatory Authority Auditor Website: www.ficora.fi Audit Statement/Report: http://www.ficora.fi/index/palvelut/palvelutaiheittain/sahkoinenallekirjoitus/varmentajarekisteri.html SFS-EN ISO 9001:2000, ISO/IEC 27001:2005 by Inspecta Finland (www.inspecta.com) and Finnish Communications Regulatory Authority (www.ficora.fi) http://www.ficora.fi/index/palvelut/palvelutaiheittain/sahkoinenallekirjoitus/varmentajarekisteri.html (last audit was done **1 July 2008)** FICORA supervises that qualified certificates are provided in Finland in	Do you have a publishable statement or letter from the auditor(s) that states that they have reviewed the practices as outlined in the CP/CPS for these roots, and that the CA does indeed follow these practices and meets the requirements of ETSI TS 101 456?

	compliance with the Act on Electronic Signatures and orders issued under it and that the qualified certificates and systems of qualified certificates comply with the provisions mentioned above. The supervision involves, among other things, annual inspections of qualified certificate operations. As mentioned if the certification-service-provider or the product or service related to electronic signatures meets the requirements of these standards or technical specifications (e.g. **ETSI TS 101 456**), usually they also fulfil the requirements laid down in the Directive and the Act.	

Review CPS sections dealing with subscriber verification
(section 7 of http://www.mozilla.org/projects/security/certs/policy/.)

- For SSL certs, confirm that the CPS describes reasonable measures that are taken to verify that the subscriber owns/controls the domain name.
- For email certs, confirm that the CPS describes reasonable measures that are taken to verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
- For code signing certs, confirm that the CPS describes reasonable measures that are taken to verify that identity info in code signing certs is that of subscriber
- Make sure it's clear which checks are done for which context (cert usage)

Flag Problematic Practices
(http://wiki.mozilla.org/CA:Problematic_Practices)

- 1.1 Long-lived DV certificates
    - Not sure
- 1.2 Wildcard DV SSL certificates
    - Not sure
- 1.3 Issuing end entity certificates directly from roots
    - No. End entity certs are issued from the intermediate CAs.
- 1.4 Allowing external entities to operate unconstrained subordinate CAs
    - No. Subordinate CAs are internally operated.
- 1.5 Distributing generated private keys in PKCS#12 files
    - From FINEID specification S2: VRK issues two types of service certificates. Server certificates are issued using private keys and PKCS#10 Certificate Requests generated by service providers. Service certificate for email usage is a PKCS#12 format file that contains the certificate and corresponding private and public key. It is service providers duty to keep private keys secured using Hardware Security Module, encryption, passwords or by other means.
- 1.6 Certificates referencing hostnames or private IP addresses
    - Not found.

- 1.7 OCSP Responses signed by a certificate under a different root
  - No. OCSP not provided.
- 1.8 CRL with critical CIDP Extension
  - Not sure – need URLs to the CRLs

Verify Audits
(Sections 8, 9, and 10 of http://www.mozilla.org/projects/security/certs/policy/)

- Validate contact info in report, call to verify that they did indeed issue this report.
- Review Audit to flag any issues noted in the report