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.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.)	National 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 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	COMPLETE

	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	URLs to the CRLs for the intermediate CAs: a. VRK Gov. CA for Citizen Qualified Certificates http://proxy.fineid.fi/crl/vrkcqcc.crl b. VRK Gov. CA for Multiplatform Citizen Qualified Certificates Two different CRLs because of two different Teleoperators: http://proxy.fineid.fi/crl/vrkcqt1c.crl http://proxy.fineid.fi/crl/vrkcqe1c.crl c. VRK CA for Qualified Certificates http://proxy.fineid.fi/crl/vrkqcc.crl d. VRK CA for Service Providers http://proxy.fineid.fi/crl/vrkspc.crl e. VRK CA for Temporary Certificates http://proxy.fineid.fi/crl/vrktcc.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.	COMPLETE
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 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.	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. --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	COMPLETE
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.	From FINEID specification S2: “All certificates are issued and administrated by Population Register Centre’s Certification Authority services unit, VRK.” Comment # 2: Population Register Centre is responsible by Finnish law of the CA operations. Third parties are not subordinate CA operators. Maintenance of software and hardware for CA systems is outsourced to the third party. The maintenance is based on a contract where the third party is required to adhere to the same requirements as the Certification Authority is. Population Register Centre audits its subcontractors responsible for CA systems maintenance before a contract is made. The Finnish Communications Regulation	COMPLETE

	Authority audits Population Register Centre and its subcontractors on a regular basis.	
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)	COMPLETE
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 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.)	IV/OV	COMPLETE
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	https://www.intermin.fi	COMPLETE

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.		
CP/CPS • Certificate Policy URL • Certificate Practice Statement(s) (CPS) URL (English or available in English translation)	http://www.fineid.fi (technical data, Certificate Policies, Certification Practice Statements, PKI Disclosure Statements, FINEID specifications) FINEID specification S2 – VRK (PRC) CA-model and certificate contents, v2.1 http://www.fineid.fi/vrk/fineid/files.nsf/files/24EA4C4CD4A1EAA0C2257054002A55BD/$file/S2v21.pdf The Population Register Centre prepares a certificate policy for each certificate type it issues. Service Provider for Server CPS in Finnish http://www.fineid.fi/vrk/fineid/files.nsf/files/B2BC1F39CB3F28AAC225742E004BA2DF/$file/srvcps20080501.pdf Smartcard Citizen Certificates CPS in English http://www.fineid.fi/vrk/fineid/files.nsf/files/7AC8EFBD063A723BC225742C001EA6BC/$file/ccps20080501en.pdf Smartcard Qualified Certificates CPS in English http://www.fineid.fi/vrk/fineid/files.nsf/files/F7A72F2FAD5E83B3C225742C00372EFD/$file/ocps20080501en.pdf Smartcard Temporary Certificates CPS in Finnish http://www.fineid.fi/vrk/fineid/files.nsf/files/9BB25E8FA98D6D6FC22574F300410999/$file/tccps20081101.pdf Software Cert Service Provider for E-mail Use CPS in Finnish	COMPLETE

	http://www.fineid.fi/vrk/fineid/files.nsf/files/AAF4DE2FF17E1015C225742E004B8B3D/$file/spcps20080501.pdf	
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 type: ETSI TS 101.456 equivalent ISO 27001 Audit Certificate http://www.inspecta.fi/sfs/sertifikaattihaku/haku_tulokset.php?type=haljar&nayta=1&id=1400 ISO 27001 Audit Certificate in English https://bugzilla.mozilla.org/attachment.cgi?id=358834 ISO 9001 Audit Certificate http://www.inspecta.fi/sfs/sertifikaattihaku/haku_tulokset.php?type=haljar&nayta=1&id=1401 ISO 9001 Audit Certificate in English https://bugzilla.mozilla.org/attachment.cgi?id=358833 Audits dated: 2/28/2008 Inspecta Finland does not audit the CA against ETSI requirements, but against ISO 9001 and ISO 27001 requirements. The audit letter is not publishable, but the certificates are public. The certificates can be found using certificate search (sertifikaattihaku) from the auditor's webpage http://www.inspecta.fi/sfs Auditor: Finnish Communications Regulatory Authority Auditor Website: www.ficora.fi Audit Statement/Report: 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 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	COMPLETE

	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.
    - Service Provider for Server CPS: http://www.fineid.fi/vrk/fineid/files.nsf/files/B2BC1F39CB3F28AAC225742E004BA2DF/$file/srvcps20080501.pdf
    - Chapters 4.1-4.3 (In Finnish. The translation below was verified via Google Translate)
        - Before issuing the certificate CA to verify the applicant's information
        - Main measures for verifying applicant identity are:
            - The existence of company is checked on the Finnish Company Register
            - Letter of authority is required for the person who is acting on behalf of the company
            - The ownership of domain name must be proved with a certificate of domain name ownership from Finnish Communications Regulation Authority
            - If the applicant is a person then he must prove his identity with valid ID
- For email certs, confirm that the CPS describes reasonable measures that are taken to verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - Comment #7: As Population Register Centre, as a Certification Authority, is a governmental organization, all certificates issued will be put in a governmental certificate register. In Finland, governmental registers are protected by the law. Therefore it is a criminal act for any person to try to misinform governmental register keepers and try to get false information to be put into governmental registers.
    - Certificates on Smartcards:
        - Citizen Certificates CPS Chapters 4.1-4.3, http://www.fineid.fi/vrk/fineid/files.nsf/files/7AC8EFBD063A723BC225742C001EA6BC/$file/ccps20080501en.pdf
            - Comment #7: **In regard to Citizen certificates** the subscriber applies to the certificate at the Police office. The subscriber can ask his email address to be included in the certificate to be issued. **The format of the email address is checked, but the control of the email address is not.** For private persons the domain name part checking of the email address is not possible as the persons are not usually in control of a domain name but get their email from a service provider such as mail.com.

        - Qualified Certificates Chapters 4.1-4.3, http://www.fineid.fi/vrk/fineid/files.nsf/files/F7A72F2FAD5E83B3C225742C00372EFD/$file/ocps20080501en.pdf
            - ID of subscriber is verified.
            - Comment #7: The control of **the domain name part in the email address is verified when the subscriber is an employee of an organization**, the subscriber is not allowed to enter an email address with domain name not in the control of the organization.The ability to order certificates to company employees is based on a contract between the company and Population Register Center. The local part of the email address is not checked (it could be anything, like 123abc).
        - Temporary Certificates CPS Chapters 4.1-4.3, http://www.fineid.fi/vrk/fineid/files.nsf/files/9BB25E8FA98D6D6FC22574F300410999/$file/tccps20081101.pdf
    - Software Certificates:
        - Service Provider for Server Use CPS Chapters 4.1-4.3, http://www.fineid.fi/vrk/fineid/files.nsf/files/B2BC1F39CB3F28AAC225742E004BA2DF/$file/srvcps20080501.pdf
        - Service Provider for E-mail Use CPS Chapters 4.1-4.3, http://www.fineid.fi/vrk/fineid/files.nsf/files/AAF4DE2FF17E1015C225742E004B8B3D/$file/spcps20080501.pdf
- 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
    - Service Provider for Server CPS: http://www.fineid.fi/vrk/fineid/files.nsf/files/B2BC1F39CB3F28AAC225742E004BA2DF/$file/srvcps20080501.pdf
- Make sure it's clear which checks are done for which context (cert usage)
    - Different CPS's based on usage.

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

- 1.1 Long-lived DV certificates
    - Server certs are IV/OV
    - Per Server CPS: Server certs are issued for 1 to 2 years
- 1.2 Wildcard DV SSL certificates
    - Server certs are IV/OV
    - Wildcards certs not issued.
- 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
  - No.
- 1.7 OCSP Responses signed by a certificate under a different root
  - No. OCSP not provided.
- 1.8 CRL with critical CIDP Extension
  - only full CRLs are issued.

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.
  - Audit Certificates are provided on the Inspecta Finland website
- Review Audit to flag any issues noted in the report
  - Full report not available. No known issues.