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	National Government
Primary market / customer base	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**
Certificate Name	VRK Gov. Root CA
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 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.
Root Cert URL	http://vrk.fineid.fi/certs/vrkrootc.crt
SHA-1 fingerprint.	FA:A7:D9:FB:31:B7:46:F2:00:A8:5E:65:79:76:13:D8:16:E0:63:B5
Valid from	12/18/2002
Valid to	12/18/2023
Cert Version	3
Modulus length	2048
Test Website(s)	https://www.intermin.fi
CRL	ARL: http://proxy.fineid.fi/arl/vrkroota.crl When I try to import this CRL I get: "Error Importing CRL to local Database. Error Code:ffffe095" Please see https://wiki.mozilla.org/CA:Problematic_Practices#CRL_with_critical_CIDP_Extension VRK CA for Service Providers CRL: http://proxy.fineid.fi/crl/vrkspc.crl (NextUpdate: 48 hours) Note: This CRL imported into my Firefox browser without error.

OCSP Responder URL	OCSP not provided
List or description of subordinate CAs operated by the CA organization associated with the root CA.	From section 3 of FINEID specification S2, VRK Gov. Root CA has the following intermediate Certificates. These intermediate Certificates can be downloaded from: http://www.fineid.fi/default.aspx?id=596 -- 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.
Externally Operated Subordinate CAs	From FINEID specification S2 section 2: “All certificates are issued and administrated by Population Register Centre’s Certification Authority services unit, later VRK.” Comment: 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 Authority audits Population Register Centre and its subcontractors on a regular basis.
Cross-Signing	None
Requested Trust Bits	Websites (SSL/TLS)
SSL Verification Type	IV/OV
CP/CPS	Policy Documentation (Finnish): http://www.fineid.fi/ FINeID Policies for Server Certificates (English): http://www.fineid.fi/default.aspx?id=520 CP for Server Certs (English): http://www.fineid.fi/default.aspx?docid=4164 CPS for Server Certs (English): http://www.fineid.fi/default.aspx?docid=4162 PKI Disclosure Statement: http://www.fineid.fi/default.aspx?docid=4163 FINEID specification S2 – VRK (PRC) CA-model and certificate contents, v2.1 http://www.fineid.fi/default.aspx?docid=3633&action=publish

AUDIT	Audit Type: ETSI TS 101 456 – Qualified Certificates Auditor: Finnish Communications Regulatory Authority (FICORA) Auditor Website: http://www.ficora.fi Audit Statement: https://bugzilla.mozilla.org/attachment.cgi?id=530535 (2010.04.22) The statement that FICORA has audited the QC certs is posted on the FICORA website. http://www.ficora.fi/index/palvelut/palvelutaiheittain/sahkoinenallekirjoitus/varmentajarekisteri.html Audit Type: ETSI TS 102 042 – Server Certificates Auditor: Inspecta Finland Auditor Website: http://www.inspecta.com/ Audit Statement: https://bugzilla.mozilla.org/attachment.cgi?id=530536 (2010.10.27)
Organization Verification	From CP and CPS for Server Certs section 7.3.1: The Certification Authority (CA) shall ensure that evidence of subjects' identification and accuracy of their names and associated data are properly examined and that certificate requests are complete, accurate and duly authorised. The applicant's official name and other details submitted by the applicant and examined by the Registration Authority shall be used in the naming of the service certificate applicant. A set of attributes that creates the subject name record for the certificate shall be unique and identify the certificate holder in question. Each service certificate holder organization must operate under its own name. A certificate holder's private keys shall be generated on the certificate holder's or its technical supplier's server when the certificate in question is a server or system signing certificate. If the certificate is an email service certificate, the CA shall generate the key pair and certificate and deliver them to the certificate holder. *Verification of the organisation represented by the certificate applicant* The certificate applicant's rights and obligations are specified in the application document and general terms and conditions of use which form the agreement entered into with the certificate applicant. The application document and terms and conditions of use shall clearly indicate that, on signing the document, the service certificate applicant accepts the accuracy of the information and the generation of the service certificate and its publication in a public directory. Furthermore, in doing so the applicant shall accept the rules, terms and conditions governing the use of the service certificate and the duty to notify of any misuse or illegal disclosure of the private key. An agreement shall have been entered into between the CA and the registration authority and other providers supplying elements of certification services that specifies each party's rights, liabilities and obligations indisputably. The service certificate applicant shall be responsible for the accuracy of all information relevant to the certificate submitted by the certificate applicant to the CA or registration authority. The service certificate holder shall only use the service certificate for its intended use.

On issuing a service certificate the CA shall also approve the certificate application.

The certificate holder must immediately report the service certificate for inclusion in the Certificate Revocation List (CRL) if the holder suspects that usage in breach of contract has been enabled.

Service certificate applications shall be submitted using a form that can be downloaded and printed out at http://www.fineid.fi.

Before issuing a certificate, the CA shall verify the applicant's details using sources such as the Trade Register. If the applicant is an enterprise or organisation, a Trade Register extract issued no more than three months earlier must be enclosed to a service certificate application submitted for the first time. Also to be submitted is a proxy if the certificate applicant (such as an IT contact person) acts on behalf of the enterprise/organisation. The Trade Register extract need not be resubmitted in conjunction with certificate renewal. Instead, the Population Register Centre shall check the enterprise's details from the Finnish Business Information System (BIS). Central and local government and church authorities need not submit a Trade Register extract. Internet domain names ending in .fi held by the applicant and details of their management must be made available to the PRC during the processing of the application.

If the applicant is a private individual, the applicant must deliver the service certificate application personally to the CA, in which context the applicant's identity shall be verified by means of an identification document issued by the Police (an ID card, passport or a driving licence issued after 1 October 1990).

Other identification documents accepted are a valid passport or ID card issued by a Member State of the European Economic Area, Switzerland or San Marino, a valid driving licence issued by a Member State of the European Economic Area after 1 October 1990 or a valid passport issued by another country's authority.

A server certificate is issued for a maximum of five years if:
1) The certificate applicant is part of public administration in Finland and the certificate’s public key is a 2048-bit RSA
2) The applicant (a public or private party operating in Finland) applies for the certificates through the certificate order and administration system Vartti and the certificate’s public key is a 2048-bit RSA.

In other cases a server certificate is valid for a maximum of two years. A server certificate may be issued for a maximum of two years, for instance, if the server certificate applicant is a company or other private party and the certificate is not applied for via the order and administration system Vartti.

Certificate renewal shall take place following the same application procedure as for the original application, with the exception that the Trade Register extract shall not be required. The fees charged for certificates shall be based on the annual fee specified in the Population Register Centre's service tariff.

Domain Name Ownership/Control Verification	From CP and CPS section 7.3.1 >> Before issuing a certificate, the CA shall verify the applicant's details using sources such as the Trade Register. How is the information from the Trade Register used? E.g. is a phone call made or an email sent to a particular contact provided by the Trade Register? Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership >> If the applicant is an enterprise or organisation, a Trade Register extract issued no more than three months earlier must be enclosed to a service certificate application submitted for the first time. How is it confirmed that the extract is authentic? >> Also to be submitted is a proxy if the certificate applicant (such as an IT contact person) acts on behalf of the enterprise/organisation. How is it confirmed that this contact person has the authority to act on behalf of the organization? >> Central and local government and church authorities need not submit a Trade Register extract. How is it checked that these organizations own/control the domain name to be included in the certificate?
Email Address Ownership/Control Verification	Not applicable. Not requesting email trust bit.
Code Signing Subscriber Identity Verification	Not applicable. Not requesting 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 translations into English of the CP/CPS where relevant. • 1.1 Long-lived DV certificates o Server certs are IV/OV o Per CP and CPS: Server Certs are valid for up to 5 years. Current Mozilla CA Cert Policy requires re-verification every 39 months or less. See section 6 of http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html • 1.2 Wildcard DV SSL certificates o Wildcards certs not issued. • 1.3 Email Address Prefixes for DV Certs o Server certs are IV/OV • 1.4 Delegation of Domain / Email validation to third parties o Can the RA function ever be performed by someone who is not an employee of the Finland Population

	Register Centre? If yes, Can such RAs do the verification of the subscriber’s ownership/control of the domain name to be included in the certificate? • 1.5 Issuing end entity certificates directly from roots ○ No. End entity certs are issued from the intermediate certificates. • 1.6 Allowing external entities to operate subordinate CAs ○ No. All intermediate certificates are internally operated. • 1.7 Distributing generated private keys in PKCS#12 files ○ Not for SSL certs. • 1.8 Certificates referencing hostnames or private IP addresses ○ ? • 1.9 Issuing SSL Certificates for Internal Domains ○ ? • 1.10 OCSP Responses signed by a certificate under a different root ○ OCSP is not provided. • 1.11 CRL with critical CIDP Extension ○ ? • 1.12 Generic names for CAs ○ CA name and Issuer info is not generic.