Bugzilla ID: 624356
Bugzilla Summary: Add renewed Sertifitseerimiskeskus AS root certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Sertifitseerimiskeskus AS
Website URL	http://www.sk.ee
Organizational type	Commercial CA, covering Baltic region (Estonia, Lithuania, Latvia)
Primark Market / Customer Base	SK (Certification Centre, legal name AS Sertifitseerimiskeskus) is a commercial CA, covering the Baltic region (Estonia, Lithuania, Latvia). SK is Estonia's primary certification authority, providing certificates for authentication and digital signing to Estonian ID Cards. Established in 2001, SK has the backing of Estonian and Nordic financial and telecom sector. SK's customers include the Estonian court system and notaries, Central Bank and commercial banks, and enforcement organisations (e.g. Police).
CA Contact Information	CA Email Alias: pki@sk.ee CA Phone Number: 372 610 1880 Title / Department: Certification Services

Technical information about each root certificate

Certificate Name	EE Certification Centre Root CA
Certificate Issuer Field	E = pki@sk.ee CN = EE Certification Centre Root CA O = AS Sertifitseerimiskeskus C = EE
Certificate Summary	This is the renewed root cert that will eventually replace the "Juur-SK" root cert that was included in bug #414520.
Root Cert URL	http://www.sk.ee/files/EECCRCA.PEM.cer
SHA1 Fingerprint	C9:A8:B9:E7:55:80:5E:58:E3:53:77:A7:25:EB:AF:C3:7B:27:CC:D7
Valid From	2010-10-30
Valid To	2030-12-17
Certificate Version	3
Certificate Signature Algorithm	SHA-1
Signing key parameters	2048
Test Website URL	https://www.openxades.org/
CRL URL	All CRLs: http://www.sk.ee/crls CP section 2.4.2: The revocation list is updated every 12 hours. CRL of this root: http://www.sk.ee/crls/eeccrca/eeccrca.crl CRL for end-entity certs signed by the KLASS3 2010 subCA: http://www.sk.ee/crls/klass3/klass3-2010.crl

OCSP URL	http://ocsp.sk.ee (Access is subject to contract.)
Requested Trust Bits	Websites (SSL/TLS) Code Signing
SSL Validation Type	OV
EV Policy OID(s)	Not EV

CA Hierarchy information for each root certificate

CA Hierarchy	This new root will have the same CA hierarchy as the old "Juur-SK" root that was approved in bug #414520. The Juur-SK root has three types of internally operated subordinate CAs. The first type of subordinate CA is used to issue electronic ID cards which contain certificates for digital signature and for digital identification. The second type of subordinate CA is used to issue internal ID cards of the Republic of Estonia. The third type of subordinate CA is used to issue device, SSL, and code signing certificates. There is a separate CP for each subordinate CA. This new root will have 3 internally-operated sub-CAs: KLASS3 2010 for issuing certificates for organizations (www server, code signing, digital stamping) and two CA-s for issuing certificates for physical persons: ESTEID for Estonian ID-card related services and EID for other personal qualified certificates.
Externally Operated SubCAs	None
Cross-Signing	None

Verification Policies and Practices

Policy Documentation	Document Repository: http://www.sk.ee/en/repository CPS (English): http://www.sk.ee/upload/files/SK_CPS_en_v2_5.pdf CP of Organisation Certificates (English): http://www.sk.ee/upload/files/Asutuse_CPv2_2_EN.pdf
Audits	Audit Type (WebTrust, ETSI etc.): ETSI TS 101 456 Auditor: KPMG Baltics Auditor Website: http://www.kpmg.ee/ Audit Report: http://www.sk.ee/en/repository/audit/ (2011.02.28) Personal Identification Act for Estonia: http://www.legaltext.ee/text/en/X30081K4.htm -------- Original Message -------- Subject: RE: Confirmation of Audit Report for AS Sertifitseerimiskeskus Date: Wed, 13 Apr 2011 09:59:07 +0200 From: Kase, Janno <jkase@kpmg.com> To: Kathleen Wilson <kwilson@mozilla.com> Dear Kathleen, I confirm that the audit report http://www.sk.ee/upload/files/SK%20STO%20ETSI%20audit%202011%20ENG.pdf is issued by KPMG Baltics OÜ and is the same as the original report. Kind Regards, Janno Kase

Organization Verification Procedures	CP of Organisation Certificates (English): http://www.sk.ee/upload/files/Asutuse_CPv2_2_EN.pdf 3.1 Identification of Client During the procedure of application for an organisation certificate the following is verified: • The registered status of the client in accordance with legal acts of its home country; • The identity of the Client's representative; • The authority of the Client's representative to apply for a certificate on behalf of the Client. 4.2.1 Decision Making The acceptance or rejection of the applications for certificates is the decision of the SK. Prior to making a decision, the SK checks the following: • The identity of the Client (including the registered status of the legal person in accordance with the legislation of its home country) • The identity of the Client's representative • The authority of the Client's representative to apply for a certificate and/or for the revocation of a certificate on behalf of the Client • Correctness and completeness of data submitted by the Client • Whether the Client has the right to receive a certificate according to the legislation of the Republic of Estonia and/or this CP In the case of applications for digital seals, the uniqueness of the distinguished name of a certificate is also verified. In the case of applications for web server certificates, the link between the Client and the domain name and/or IP address of the Client's appliance is verified if the appliance is accessible through a public computer network. The decision of the SK is subject to the results of the aforementioned checks and the SK has the right to refuse to issue a certificate. Comment #9: SK issues organizational certificates according to policy specified in http://www.sk.ee/upload/files/Asutuse_CPv2_2_EN.pdf. SK does not currently issue organizational certificates to entities outside Estonia. This is the reason sources of information to verify Estonian legal entity was given in this thread but not in CP as we slightly look forward to expand our activity in other countries. CP states basic principles we would adhere according to specifics of relevant country.
SSL Verification Procedures	From bug #414520: For SSL certs, Sertifitseerimiskeskus verifies the ownership of the domain name by using the whois service for international domains, and by using EENet (www.eenet.ee) for .ee domains. Sertifitseerimiskeskus contacts the domain's administrative contact before issuing a certificate. CP of Organisation Certificates (English): http://www.sk.ee/upload/files/Asutuse_CPv2_2_EN.pdf 3.3 Distinguished Name

	See Clause 3.3 of the CPS. The distinguished name of a certificate is composed in accordance with the document "Profiles of Organisation Certificates" [2]. The uniqueness of a distinguished name is not guaranteed in the case of web server certificates. A web server certificate is assigned a distinguished name on the basis of a link between the Client and the domain name and/or IP address of the Client's appliance if the appliance is accessible through a public computer network. A digital seal certificate is assigned a distinguished name on the basis of the name entered in the register of the Client's home country. 4.2.1 Decision Making: In the case of applications for web server certificates, the link between the Client and the domain name and/or IP address of the Client's appliance is verified if the appliance is accessible through a public computer network. Comment #7: Public registries are consulted in decision-making process, namely Central Commercial Register https://ariregister.rik.ee/index.py?lang=eng and Domain Registry http://www.eestiinternet.ee/eng for domain ownership.
Email Address Verification Procedures	Not applicable – not requesting email trust bit.
Code Signing Subscriber Verification Procedures	Comment #9: SK issues organizational certificates according to policy specified in http://www.sk.ee/upload/files/Asutuse_CPv2_2_EN.pdf. From our position we do not differenciate certificate-issuance principles and policies with regard to code-signing certificates as we have common policy for issuing various (KU/EKU) certificates to organizational entities.

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	CP/CPS are posted on the CA's public website.
CA Hierarchy	The root does not sign end-entity certs directly, it has internally-operated sub-CAs.
Audit Criteria	ETSI 101 456, KPMG
Document Handling of IDNs in CP/CPS	
Revocation of Compromised Certificates	
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	Not applicable – not requesting email trust bit.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	
Domain owned by a Natural Person	
OCSP	

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	SSL certs are OV.
Wildcard DV SSL certificates	SSL certs are OV.
Email Address Prefixes for DV Certs	SSL certs are OV.
Delegation of Domain / Email validation to third parties	Domain/email validation is not delegated to third-party RAs.
Issuing end entity certificates directly from roots	Root is offline. Certs are issued through internally operated sub-CAs.
Allowing external entities to operate subordinate CAs	All sub-CAs are internally operated.
Distributing generated private keys in PKCS#12 files	Not found.
Certificates referencing hostnames or private IP addresses	Not found.
Issuing SSL Certificates for Internal Domains	Not found.
OCSP Responses signed by a certificate under a different root	No.
CRL with critical CIDP Extension	CRLs import into Firefox without error.
Generic names for CAs	In Firefox shows up under AS Sertifitseerimiskeskus
Lack of Communication With End Users	No.