Bugzilla ID: 414520
Bugzilla Summary: Add Sertifitseerimiskeskus AS root CA certificate

General Information	Data
CA Name	Sertifitseerimiskeskus AS
Website URL (English version)	http://www.sk.ee
Organizational type	Commercial CA, covering Baltic region (Estonia, Lithuania, Latvia)
Primary 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).

Info Needed	Data
Certificate Name	Juur-SK
Cert summary / comments	This root issues 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 and SSL certificates.
The root CA certificate URL	http://www.sk.ee/files/JUUR-SK.der
SHA-1 fingerprint	40:9D:4B:D9:17:B5:5C:27:B6:9B:64:CB:98:22:44:0D:CD:09:B8:89
Valid from	2001-08-30
Valid to	2016-08-26
Cert Version	3
Modulus length	2048
Test website	https://digidoccheck.sk.ee
CRL URL	All of the CRLs for the root and sub-CAs can be found at: http://www.sk.ee/pages.php/0202040202,36 Root: http://www.sk.ee/crls/juur/crl.crl Website certs: http://www.sk.ee/crls/klass3/klass3.crl NextUpdate: 12 hours Section 2.4.2 of KLASS3-SK CP: The guaranteed frequency of publication is 12 hours.
OCSP Responder URL	http://ocsp.sk.ee
Subordinate CAs	Hierarchy Diagram: http://www.sk.ee/files/tree.pdf The root and sub-CAs can be downloaded from: http://www.sk.ee/pages.php/0202040501

	Juur-SK has the following subordinate CAs: • EID-SK (2004-2014) • EID-SK 2007 (2007-2016) o Electronic ID cards which contain certificates for digital signature and certificates for digital identification. • ESTEID-SK (2002-2012) • ESTEID-SK 2007 (2007-2016) o Internal ID cards of the Republic of Estonia which contain certificates for digital signature and certificates for digital identification. • KLASS3-SK (2002-2012) o Device and Webserver certificates that can be used for securing data communication between devices (computers). Device certificates cannot be used for digital signature as defined in the Digital Signatures Act. • TEST-SK (2002-2012) Certificates issued under the EID-SK and ESTEID-SK sub-CAs can be used for digital signature as defined in the Digital Signatures Act, electronic identification, and secure e-mail. The Ministry of Internal Affairs of Republic of Estonia is the RA for ESTEID-SK certificates, but the ESTEID-SK CA is operated internally by Sertifitseerimiskeskus AS.
subordinate CAs operated by third parties	All of the subordinate CAs are internally operated by Sertifitseerimiskeskus AS. The Ministry of Internal Affairs of Republic of Estonia is the registration authority for ESTEID-SK certificates, but the ESTEID-SK CA is operated internally by Sertifitseerimiskeskus AS.
List any other root CAs that have issued cross-signing certificates for this root CA	Not Applicable
Requested Trust Bits One or more of: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites (KLASS3-SK) Email (EID-SK and ESTEID-SK) Code Signing (used internally only)
. If SSL certificates are issued within the hierarchy rooted at this root CA certificate: DV, OV, and/or EV	OV
EV Policy OID	Not EV

CP/CPS	AS Sertifitseerimiskeskus Certification Practice Statement CPS (English): http://www.sk.ee/file.php?id=432 EID-SK Certificate Policy (English): http://www.sk.ee/files/eid-sk-1.0.pdf ESTEID-SK Certificate Policy (English): http://www.sk.ee/file.php?id=252 KLASS3-SK, Device Certificates Policy (English): http://www.sk.ee/file.php?id=434 http://www.sk.ee/files/Seadmesert_CP_en-1.00.pdf
AUDIT	Audit Type (WebTrust, ETSI etc.): ETSI TS 101 456 Auditor: KPMG Baltics Auditor Website: http://www.kpmg.ee/ Audit Report: http://www.sk.ee/file.php?id=457 (2008.10.31) Personal Identification Act for Estonia: http://www.legaltext.ee/text/en/X30081K4.htm

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

- Verify domain check for SSL
    - KLASS3-SK CP Section 3.1:
        - The Client and data presented by him are verified in accordance with the rules set in the document “Terms of Use for Device Certificates” [6].
        - The following checks are performed during certificate application processing:
            - Data about the Client as a legal person
            - Personal identity of device administrator and his/her mandates for applying for the legal person for certificate issuance/revocation.
            - Ownership of the domain name and/or IP address in case the device is accessible over public network
    - Comment #9: SK verifies ownership of the domain from appropriate domain registry. In case of .ee domains it is EENet (www.eenet.ee) and for international domains whois.net is used. We always contact domain's administrative contact before issuing certificate.
- 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 #9: SK issues personal certificates for Estonian ID-card. E-mail address in the certificate is not that person claims but generated by the issuer in a form Surname.Lastname[.X]@eesti.ee. The eesti.ee mail server runs just a forwarding service – it is not a full-fledged mail service. The user's duty is to authenticate to the service with his ID-card and register his actual e-mail address with the service.
- Verify identity info in code signing certs is that of subscriber
    - Comment #9: Comment #9: SK currently is not issuing code-signing certificates. Nevertheless, SK itself uses few self-issued code-signing certificates for its own purposes.

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

- Long-lived DV certificates
  - SSL Certs are OV
- Wildcard DV SSL certificates
  - SSL Certs are OV
- Delegation of Domain / Email validation to third parties
  - No
- Issuing end entity certificates directly from roots
  - Root is offline. Certs are issued through internally operated sub-CA's.
- Allowing external entities to operate unconstrained subordinate CAs
  - All sub-CAs are internally operated.
- Distributing generated private keys in PKCS#12 files
  - No
- Certificates referencing hostnames or private IP addresses
  - No
- OCSP Responses signed by a certificate under a different root
  - No
- CRL with critical CIDP Extension
  - The CRL for the root and for website certs (KLASS3) imports into Firefox without error.
  - The CRLs for the ID-Cards and Mobile-ID do have the critical CIDP Extension.
- Generic names for CAs
  - In Firefox shows up under AS Sertifitseerimiskeskus Juur-SK

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.
  - Authenticity of audit report was confirmed via email exchange with the KPMG auditor.
- For EV CA's, verify current WebTrust EV Audit done.
  - Not applicable
- Review Audit to flag any issues noted in the report
  - No issues found in report

> From: Kase, Janno <jkase@kpmg.com>
> Subject: RE: Confirming authenticity of Audit Report for Sertifitseerimiskeskus AS
> Date: Monday, June 8, 2009, 11:39 PM
> Dear Kathleen,
> I confirm that the audit report http://www.sk.ee/file.php?id=457 is issued
> by KPMG Baltics AS and is the same as the original report.
> Kind Regards,
> Janno Kase
> KPMG Baltics AS