TÜV Informationstechnik GmbH • P.O. Box 10 32 61 • 45032 Essen, Germany

Member of
TÜV NORD GROUP

TÜV®

AS Sertifitseerimiskeskus
Mr Kalev Pihl
Pärnu avenue 141
11314 Tallinn, Estonia

Our / Your ref	Contact	Phone / Fax	Date
500-023-15 / -	Mr Clemens Wanko C.Wanko@tuvit.de	Phone: +49 201 8999 - 586 Fax: +49 201 8999 - 555	30-October-2015

Audit Attestation 2015 for the CA- and TSA- Management System of SK

To whom it may concern

This is to confirm, that TÜV Informationstechnik GmbH[1] (hereinafter TÜViT) has successfully audited the Certificate, Time-Stamping and Information Security Management System[2] of AS Sertifitseerimiskeskus (SK), Pärnu Ave. 141, 11314 Tallinn, Estonia in 2015.

Two branches of the public key infrastructure of SK have been covered by the audit,

A.) The operational branch with three issuing CAs as well as one Time-Stamping Authority and OCSP service (see Annex I for the CA identification):

1. ESTEID-SK 2011,
2. EID-SK 2011,
3. KLASS3-SK 2010,
4. SK TIMESTAMPING AUTHORITY,
5. SK OCSP RESPONDER 2011.

These three issuing CA certificates as well as the TSA certificate and the OCSP certificate where issued under the following Root CA, which has been covered during the audit:

- EE Certification Centre Root CA.

B.) The non-operational branch which does not issue any certificates and which will expire by 26th August 2016 with three issuing CAs with corresponding OCSP service certificates (see Annex II for the CA identification):

[1] see Appendix IV. for accreditation information of TUViT
[2] in short: CAMS

1. ESTEID-SK 2007,
2. EID-SK 2007,
3. KLASS3-SK 2010,
4. ESTEID-SK 2007 OCSP RESPONDER 2010;
5. EID-SK 2007 OCSP RESPONDER 2010;
6. KLASS3-SK 2010 OCSP RESPONDER.

These three issuing CA certificates and the three OCSP certificates where issued under the following Root CA, which has been covered during the audit:

- Juur-SK.

The audit has been performed in two stages: stage 1, document assessment and stage 2, on-site inspection. For the CAMS of SK the following standards have been considered during the audit. They were applied to the CAMS against requirements in the following legal acts and standards according to their corresponding policy:

- Digital Signatures Act, Passed 08.03.2000, RT I 2000, 26, 150, Entry into force 15.12.2000,
- Regulation no 68 of the Minister of Economic Affairs and Infrastructure (26th August 2014), titled "Certification and time-stamping service providers information system auditing procedure",
- Personal Data Protection Act, Passed 15.02.2007, RT I 2007, 24, 127, Entry into force 01.01.2008,
- ISO/IEC 27001: 2013,
- ETSI EN 319 401, v 1.1.1,
- ETSI EN 319 411-2, v 1.1.1,
- ETSI EN 319 411-3, v 1.1.1,
- ETSI TS 102 023, v 1.2.2 and
- ETSI TS 102 042, v 2.4.1.

The CAMS of SK was found to comply to these legal requirements and standards according their corresponding policy. No major non-conformities were detected.

The detailed audit results can be found in the audit reports dedicated to the different standards listed above.

Remark: According to existing Estonian law and regulations, SK as the certification service provider does not have the right to revoke certificates issued on identification documents (ID card), the residence permit card (RP card) and the digital personal identification document (Digi-ID, including in the form of Mobile-ID) issued by the Estonian Republic, but only to suspend them. The certification service provider should have the right to revoke certificates at least in the case certificates issued

are not compliant to their certification policy or certification practice statement or the private key of the certification service provider is compromised.

The audit has been performed from August 28th, 2015 (stage 1) until October 31st, 2015 (stage 2 and report finalization) and covered the past time period from October 2014 until October 2015. The next surveillance assessment has to be successfully finalized before October 31st, 2016.

The assessment performed covered the CAMS of SK including the corresponding roots as described above. The full PKI hierarchy has been covered during the audit – see Appendix I and II. to this audit attestation.

AS Sertifitseerimiskeskus may publish this audit attestation in a publicly-accessible location, as required.

In case of any question, please contact Mr Clemens Wanko (phone: 586, fax. –555, email: C.Wanko@tuvit.de).

With kind regards
TÜV Informationstechnik GmbH
IT Infrastructure/Certification Body

i. V.[3] *i. A.*[3]

Dr. Christoph Sutter *Clemens Wanko*

Enclosures: Appendix I: CA Identification and PKI Overview – operational branch
Appendix II: CA Identification and PKI Overview – non-operational branch
Appendix III: Confirmation of SK regarding the completion of the audit during a specified period of time
Appendix IV: Accreditation of the certification body of TÜViT according to EN ISO/IEC 17065: 2013

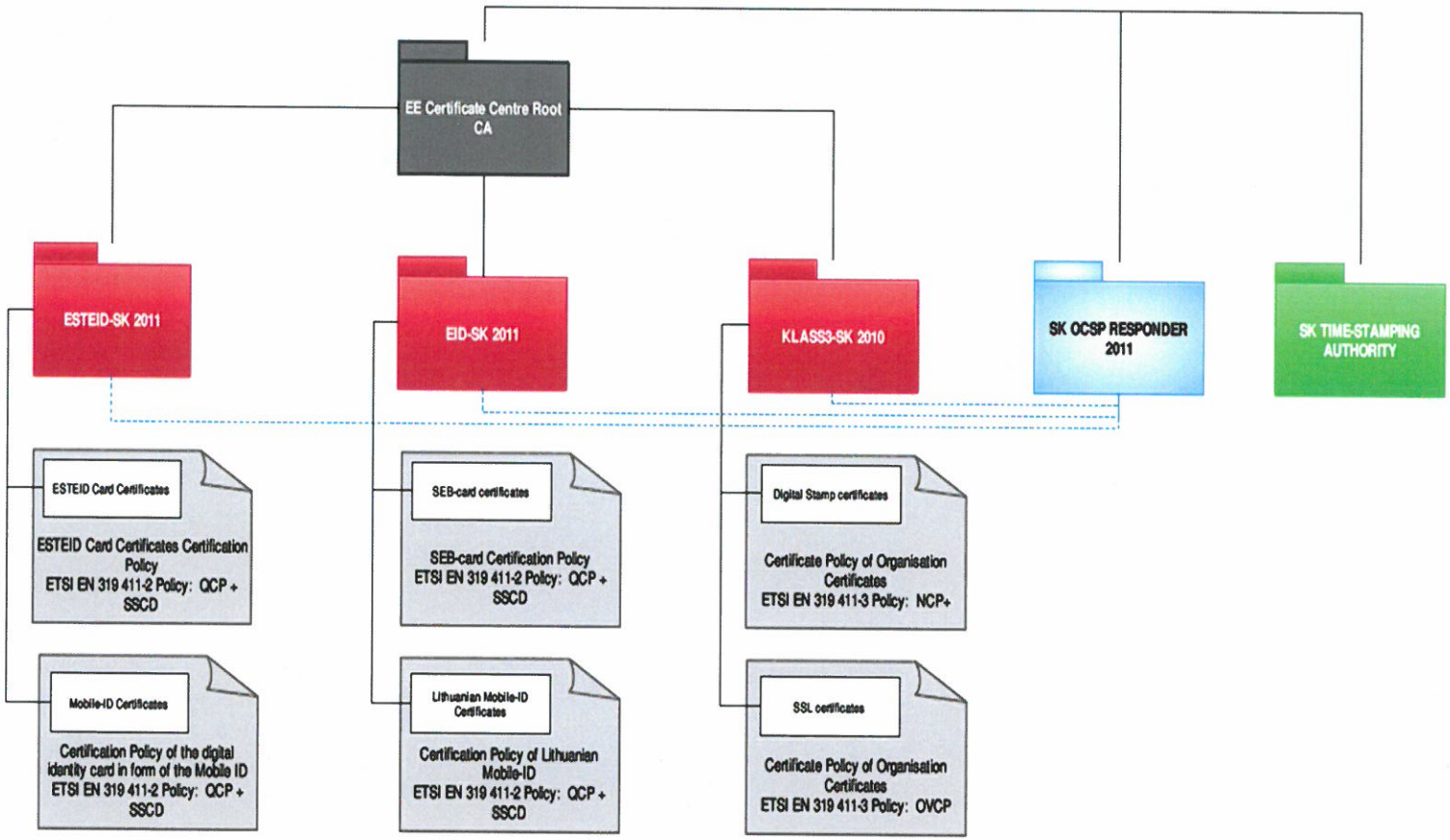
[3] Remark: indicates permission to sign on behalf of the company acc. to German regulation

Appendix I: CA Identification and PKI overview – operational branch

1. ESTEID-SK 2011:
    - cert serial#: 29 52 93 aa fd 8c c6 d4 4d 83 30 a3 c2 64 51 0d,
    - fingerprint: 46 26 74 16 f7 53 b3 12 80 62 23 0f 9c 1f b0 ab 7d 3e ec 1a.
2. EID-SK 2011:
    - cert serial#: 43 2b d4 4e 62 43 6b 46 4d 83 2f bf 7d 2d 2f 5a,
    - fingerprint: e6 be 09 33 b0 e8 96 e2 13 3d 0c bc fb d7 43 4b 5b 13 f5 d2.
3. KLASS3-SK 2010:
    - cert serial#: 0a 19 b7 e3 1f 1a 87 70 55 70 57 9d 96 cd 9c da,
    - fingerprint: 74 9a 7c ee 9d 3e 91 6a 4e 53 5f d3 7d 4b e2 d8 98 62 21 c3.
4. SK TIMESTAMPING AUTHORITY:
    - cert serial#: 24 af ec eb 12 68 d0 02 54 17 f7 86 ed 6f 01 59,
    - fingerprint: b2 d0 21 82 f0 b9 6e 2a 1c 68 7e ce 32 34 08 23 98 19 30 b6.
5. SK OCSP RESPONDER 2011
    - cert serial#: 72 9c 95 99 da ee 45 5c 4d 83 32 37 37 f3 59 41,
    - fingerprint: 75 39 61 3c 0f e7 9f 90 67 8e 30 59 b3 3d 8e 6f f4 30 0e 9c.

These four certificates where issued under the following Root CA:

- EE Certification Centre Root CA
    - cert serial#: 54 80 f9 a0 73 ed 3f 00 4c ca 89 d8 e3 71 e6 4a,
    - fingerprint: c9 a8 b9 e7 55 80 5e 58 e3 53 77 a7 25 eb af c3 7b 27 cc d7.

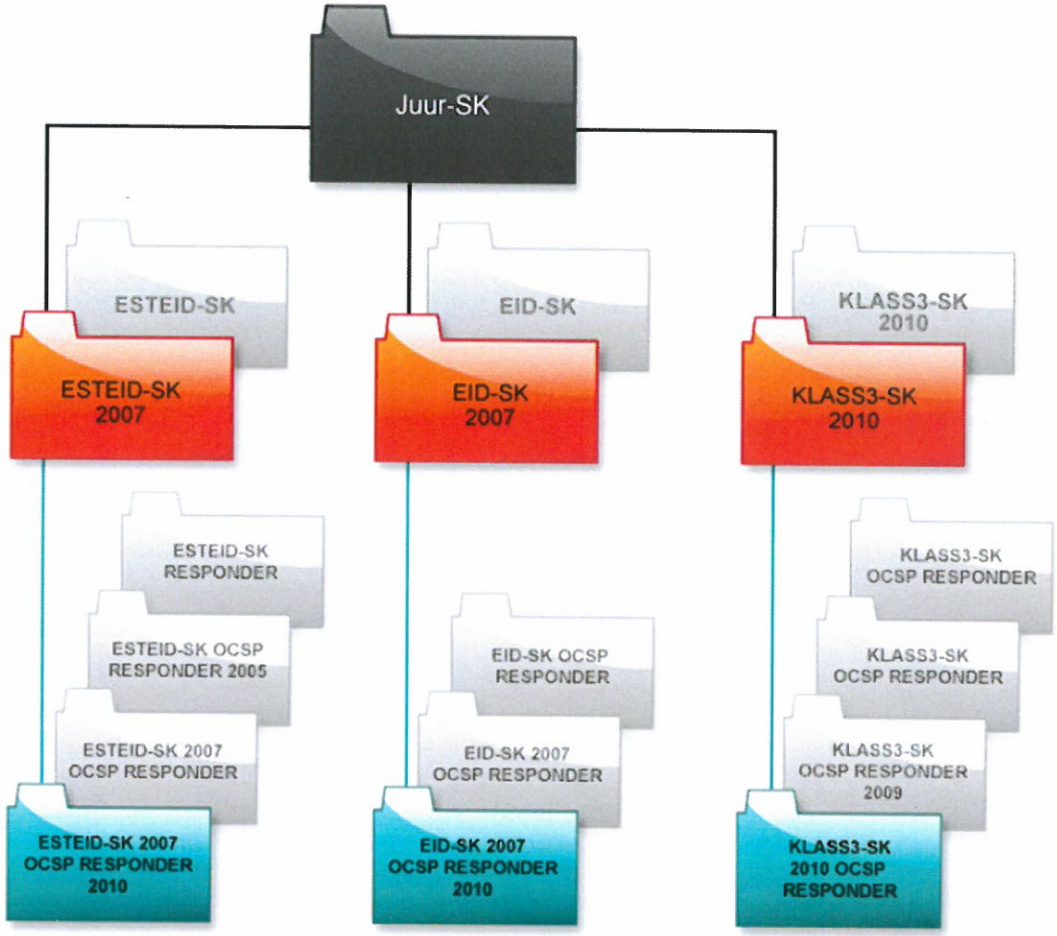

EE Certificate Centre Root CA
ESTEID-SK 2011
EID-SK 2011
KLASS3-SK 2010
SK OCSP RESPONDER 2011
SK TIME-STAMPING AUTHORITY
ESTEID Card Certificates
ESTEID Card Certificates Certification Policy
ETSI EN 319 411-2 Policy: QCP + SSCD
Mobile-ID Certificates
Certification Policy of the digital identity card in form of the Mobile ID
ETSI EN 319 411-2 Policy: QCP + SSCD
SEB-card certificates
SEB-card Certification Policy
ETSI EN 319 411-2 Policy: QCP + SSCD
Lithuanian Mobile-ID Certificates
Certification Policy of Lithuanian Mobile-ID
ETSI EN 319 411-2 Policy: QCP + SSCD
Digital Stamp certificates
Certificate Policy of Organisation Certificates
ETSI EN 319 411-3 Policy: NCP+
SSL certificates
Certificate Policy of Organisation Certificates
ETSI EN 319 411-3 Policy: OVCP

Appendix II: CA Identification and PKI overview – non-operational branch

1. ESTEID-SK 2007
    - cert serial#: 45 9e 27 aa,
    - fingerprint: b0 bd 36 eb ca 18 fe 23 0d 1c 01 be 3b aa 7e d0 17 f8 b6 a0.
2. EID-SK 2007:
    - cert serial#: 45 9b a0 0d,
    - fingerprint: 30 5d 9b 27 3e 69 85 27 62 5b 64 cc cb af bf db 32 a6 42 64.
3. KLASS3-SK 2010:
    - cert serial#: 4b b3 13 28,
    - fingerprint: 18 9d d3 c9 16 d1 42 69 7d 4e ac 07 9a 21 43 bb 8c 05 e1 40.
4. ESTEID-SK 2007 OCSP RESPONDER 2010
    - cert serial#: 4b 15 0f 99,
    - fingerprint: c5 d9 e7 bb a1 6e a6 52 ca 01 34 cb 7e 61 c5 79 cd 63 8f 46.
5. EID-SK 2007 OCSP RESPONDER 2010
    - cert serial#: 4b 15 00 f1,
    - fingerprint: bd 94 b2 30 a3 d8 ec 4b e1 77 b2 9f eb b3 07 58 cd 87 aa 32.
6. KLASS3-SK 2010 OCSP RESPONDER
    - cert serial#: cb,
    - fingerprint: 55 4e 3a 0c f8 5e 35 91 ef b1 f0 3c cd 9b 2e 24 b4 a4 f8 80.

These three certificates where issued under the following Root CA:

- Juur-SK
    - cert serial#: 3b 8e 4b fc,
    - fingerprint: 40 9d 4b d9 17 b5 5c 27 b6 9b 64 cb 98 22 44 0d cd 09 b8 89.


Juur-SK
ESTEID-SK
ESTEID-SK 2007
EID-SK
EID-SK 2007
KLASS3-SK 2010
KLASS3-SK 2010
ESTEID-SK RESPONDER
ESTEID-SK OCSP RESPONDER 2005
ESTEID-SK 2007 OCSP RESPONDER
ESTEID-SK 2007 OCSP RESPONDER 2010
EID-SK OCSP RESPONDER
EID-SK 2007 OCSP RESPONDER
EID-SK 2007 OCSP RESPONDER 2010
KLASS3-SK OCSP RESPONDER
KLASS3-SK OCSP RESPONDER
KLASS3-SK OCSP RESPONDER 2009
KLASS3-SK 2010 OCSP RESPONDER

Appendix III: Confirmation of SK regarding the completion of the audit during a specified period of time

AS Sertifitseerimiskeskus (hereinafter: SK) confirms that in accordance with the contract between SK and TÜV Informationstechnik GmbH (hereinafter TÜViT), we have completed certification and time-stamping authority conformity assessment audit.

The objective of audit was to assess whether management and information system of SK for providing certification and time-stamping services are adequate and in compliance with the following legal requirements and standards:

- **Digital Signatures Act;**
- **Regulation no 68 of the Minister of Economic Affairs and Infrastructure (26th August 2014**), titled "Certification and time-stamping service providers information system auditing procedure"
- **Personal Data Protection Act;**
- **ISO/IEC 27001: 2013** "Information technology – Security techniques – Information security management systems – Requirements" standard
- **ETSI EN 319 401** "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures" v 1.1.1 standard criteria;
- **ETSI EN 319 411-2** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates" v 1.1.1 standard criteria;
- **ETSI EN 319 411-3** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates" v 1.1.1 standard criteria
- **ETSI TS 102 023** "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities", v 1.2.2 standard criteria.
- **ETSI TS 102 042**, "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates", v 2.4.1 standard criteria.

The audit was carried out by certification body of TÜViT and its appointed auditors Mr. Clemens Wanko and Mrs. Boryana Uri from 28th August – 31st October 2015.

Tallinn, 30 October 2015

(*signed digitally*)

Kalev Pihl
CEO
AS Sertifitseerimiskeskus

Appendix IV: Accreditation of the certification body of TÜViT according to EN ISO/IEC 17065: 2013

TÜV Informationstechnik GmbH • P.O. Box 10 32 61 • 45032 Essen, Germany

AS Sertifitseerimiskeskus
c/o Ms Katrin Laas-Mikko
Pärnu avenue 141
11314 Tallinn, Estland

Member of
TÜV NORD GROUP

TÜV®

Our / Your ref	Contact	Phone / Fax	Date
500-156-15 / -	Mr Clemens Wanko C.Wanko@tuvit.de	Phone: +49 201 8999 - 586 Fax: +49 201 8999 - 555	27-October-2015

Accreditation of the certification body of TUViT according to EN ISO/IEC 17065:2013 (D-ZE-12022-01)

To whom it may concern

This is to state that the certification body of TUViT is accredited by the German accreditation body DAkkS to certify products, processes and services according to EN ISO/IEC 17065:2013. The accreditation is valid until July, 17th 2018. It is registered under the No. D-ZE-12022-01 and can be retrieved via the DAkkS website: http://www.dakks.de/en/content/accredited-bodies-dakks.

The accreditation scheme underlying EN ISO/IEC 17065:2013 is organization based (compared to an accreditation for the individual auditing person) where the quality management system of the accredited certification body guarantees the use of adequate resources, like proper skilled auditor and certification personnel.

In order to support the 2015 audit of AS Sertifitseerimiskeskus in Tallinn, Estonia, the certification body of TUViT deployed personnel in the following roles:

- Dr. Christoph Sutter
  Head of certification body, responsible for signing official statements of the certification body, like certificates and audit attestations.
- Mr. Clemens Wanko
  Senior Auditor, responsible for the audit and signing audit reports
- Mrs. Boryana Uri.
  Trainee Auditor, responsible for the audit and signing audit reports.

In case of any question, please contact Mr Clemens Wanko (phone: 586, fax. –555, email: C.Wanko@tuvit.de).

With kind regards
TÜV Informationstechnik GmbH
IT Infrastructure / Certification Body

i. V. *i. A.*

Dr. Christoph Sutter *Clemens Wanko*

Enclosure
DAkkS accreditation certificate of the certification body of TUViT D-ZE-12022-01 as of July, 6th 2015