Audit Attestation for

SK ID Solutions AS

Reference: AA2019051701

Essen, 17.05.2019

To whom it may concern,

This is to confirm that “TÜV Informationstechnik GmbH” has successfully audited the CAs of the “SK ID Solutions AS” without critical or non-critical non-conformities.

This present Audit Attestation Letter is registered under the unique identifier number “AA2019051701” and consist of 11 pages.

Kindly find here-below the details accordingly.

In case of any question, please contact:

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Langemarckstr. 20
45141 Essen, Germany
E-Mail: certtuvit@tuvit.de
Phone: +49 (0) 201 / 8999-9

With best regards,

_________________________ _________________________
Dr. Anja Wiedemann  Boryana Uri
Reviewer  Lead Auditor
### Identification of the conformity assessment body (CAB):

| TÜV Informationstechnik GmbH¹, Langemarckstraße 20, 45141 Essen, Germany registered under HRB 11687, Amtsgericht Essen, Germany Accredited by DAkkS under registration D-ZE-12022-01² for the certification of trust services according to "DIN EN ISO/IEC 17065:2013" and "ETSI EN 319 403 V2.2.2 (2015-08)". |

### Identification of the trust service provider (TSP):

| SK ID Solutions AS, Pärnu avenue 141, 11314 Tallinn, Estonia registered in Commercial register of Estonia with registry code 10747013 |

### Identification of the audited Root-CA:

<table>
<thead>
<tr>
<th>EE Certification Centre Root CA</th>
</tr>
</thead>
</table>
| **Distinguished Name** | E = pki@sk.ee  
CN = EE Certification Centre Root CA  
O = AS Sertifitseerimiskeskus  
C = EE |
| **SHA-256 fingerprint** | 3e 84 ba 43 42 90 85 16 e7 75 73 c0 99  
2f 09 79 ca 08 4e 46 85 68 1f f1 95 cc ba  
8a 22 9b 8a 76 |
| **Certificate Serial number** | 54 80 f9 a0 73 ed 3f 00 4c ca 89 d8 e3 71  
e6 4a |
| **Applied policy** | OVCP and NCP of ETSI EN 319 411-1  
QCP-n, QCP-I, QCP-n-qscd and QCP-I-qscd of ETSI EN 319 411-2  
Time stamp of ETSI EN 319 421 |

---

¹ In the following termed shortly „TÜViT“

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.
The audit was performed as full period of time audit at the TSP’s location in Tallinn, Estonia. It took place from 2019-02-25 until 2019-03-01 and covered the period from September 25th, 2018 until March 1st, 2019. The audit was performed according to the European Standards “ETSI EN 319 411-2, V2.1.1 (2016-02)”, “ETSI EN 319 411-2, V2.2.2 (2018-04)”, “ETSI EN 319 411-1, V1.1.1 (2016-02)”, “ETSI EN 319 411-1, V1.2.2 (2018-04)”, “ETSI EN 319 401, V2.1.1 (2016-02)” and “ETSI EN 319 401, V2.2.1 (2018-04)” as well as CA Browser Forum Requirements “Baseline Requirements, version 1.6.3” considering the requirements of the “ETSI EN 319 403, V2.2.2 (2015-08)” for the Trust Service Provider Conformity Assessment.

The audit was based on the following policy and practice statement documents of the TSP:

3. “SK ID Solutions AS – Trust Services Practice Statement”, version 6.0 as of 2018-10-17, SK ID Solutions AS;
10. CPS SK ID Solutions AS – NQ-SK Certification Practice Statement, version 4.0 as of 2019-05-01, SK ID Solutions AS;
11. “SK ID Solutions AS - EID-SK Certification Practice Statement”, 7.0 as of 2018-11-08, SK ID Solutions AS;
15. “Time-Stamping Authority Practice Statement”, version 3.0, valid from 2019-02-01, SK ID Solutions AS.

The Sub-CAs that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. The TSP assured that all non-revoked Sub-
CA's that are technically capable of issuing server certificates and that have been issued by this Root-CA are in the scope of regular audits.

The TSP has stopped the issuance of TLS certificates on September 1st, 2017, hence prior to the actual audit period. During the audit, it was verified that the CA's “KLASS3-SK 2010” and “KLASS3-SK 2016” are issuing revocation status information but not any new end entity TLS certificates.

The KLASS3-SK 2010 (sha1RSA) CA also has stopped the issuance of certificates since 2015.

Pending major non-conformities have been closed, if any.

In the following areas minor non-conformities have been identified during the audit:

Findings with regard to ETSI EN 319 401:

7.2 Human resources
Documentation and implementation of the maintenance process for training evidences shall be improved. [ETSI EN 319 401, 7.2 b]]

7.5 Cryptographic controls
Documentation and implementation of the HSM life cycle process and its information shall be improved. [ETSI EN 319 401, 7.5]

7.6 Physical and environmental security
Documentation and implementation of physical access rights to the TSP facilities shall be improved. [ETSI EN 319 401, 7.6 a]]

7.7 Operation security
Documentation and implementation of adequate measures instead of dual control for administration of technical components and critical network components shall be improved. [ETSI EN 319 401, 7.7 c]]

7.8 Network security
Documentation and implementation of vulnerability scans shall be improved. [ETSI EN 319 401, 7.8 g]]

Documentation and implementation of penetrations tests shall be improved. [ETSI EN 319 401, 7.8 h]]

7.9 Incident management
Documentation and implementation of monitoring activities shall be improved. [ETSI EN 319 401, 7.9 g]]
Documentation and implementation of system logs and critical IT components shall be improved. [ETSI EN 319 401, 7.9 g]]

Findings with regard to ETSI EN 319 411-1:

6.5 Technical security controls
Documentation and implementation of HSMs in historic state shall be improved. [ETSI EN 319 411-1, 6.5.2 a]]

All minor non-conformites have been scheduled to be remediated within three months after the onsite audit and will be covered by a corresponding audit.
<table>
<thead>
<tr>
<th>Identification of the Sub-CA</th>
<th>Distinguished Name</th>
<th>SHA-256 fingerprint</th>
<th>Certificate Serial number</th>
<th>Applied policy</th>
<th>Service</th>
<th>EKU</th>
<th>Validy</th>
</tr>
</thead>
<tbody>
<tr>
<td>KLASS3-SK 2010</td>
<td>CN = KLASS3-SK 2010 OU = Sertifitseerimisteenused O = AS Sertifitseerimiskeskus C = EE</td>
<td>00 db 86 a7 08 7a 75 0c e0 7b 32 55 d0 d3 12 9e 88 8c a9 e0 ee ca cf 9e 72 bd b2 76 b1 71 47 ef</td>
<td>0a 19 b7 e3 1f 1a 87 70 55 70 57 9d 96 cd 9c da</td>
<td>OVCP of ETSI EN 319 411-1 QCP-I and QCP-I-qscd of ETSI EN 319 411-2</td>
<td>server authentication, qualified electronic seal</td>
<td>Not defined.</td>
<td>2015-06-04 until 2024-03-17, does not issue any certificates from 2016</td>
</tr>
<tr>
<td>KLASS3-SK 2010 (sha1RSA)</td>
<td>CN = KLASS3-SK 2010 OU = Sertifitseerimisteenused O = AS Sertifitseerimiskeskus C = EE</td>
<td>17 f3 02 21 9f cf ce 8f d1 8c ac 17 2f 8b 0d 44 96 ba 5d a8 e4 9f 87 1a bc 1f 9d 0c aa a3 60 e5</td>
<td>03 39 d5 a7 52 da c9 ab 4d 83 2e 9b 37 c7 fd 42</td>
<td>OVCP of ETSI-EN 319-411-1 QCP-I and QCP-I-qscd of ETSI EN 319 411-2</td>
<td>server authentication, qualified electronic seal</td>
<td>Not defined.</td>
<td>2011-18-03 until 2024-18-03</td>
</tr>
<tr>
<td>KLASS3-SK 2016</td>
<td>CN = KLASS3-SK 2016 2.5.4.97 = NTREE-10747013 OU = Sertifitseerimisteenused O = AS Sertifitseerimiskeskus C = EE</td>
<td>a5 a8 59 ce 03 10 a8 5f 42 a5 41 1d a6 3f 83 b4 14 4e b9 4b c8 a6 5a 99 75 ac 86 82 f6 67 db 77</td>
<td>5e 53 3b 13 25 60 34 2b 58 49 57 30 8b 30 78 dc</td>
<td>OVCP of ETSI EN 319 411-1 QCP-I and QCP-I-qscd of ETSI EN 319 411-2</td>
<td>server authentication (certificates issuing only until 01.10.2017), qualified electronic seal</td>
<td>Not defined.</td>
<td>2016-12-08 until 2030-12-17</td>
</tr>
<tr>
<td>Identification of the Sub-CA</td>
<td>Distinguished Name</td>
<td>SHA-256 fingerprint</td>
<td>Certificate Serial number</td>
<td>Applied policy</td>
<td>Service</td>
<td>EKU</td>
<td>Validy</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>---------</td>
<td>-----</td>
<td>--------</td>
</tr>
<tr>
<td>EID-SK 2011</td>
<td>E = <a href="mailto:pki@sk.ee">pki@sk.ee</a></td>
<td>7b 16 66 a7 99 1c fc 28 b6 4d a3 71 f1 71 41 db d6 f5 32 1f 21 b8 3a 1a 65 8d 6a 41 0d 37 4e 05</td>
<td>43 2b d4 4e 62 43 6b 46 4d 83 2f bf 7d 2d 2f 5a</td>
<td>QCP-n and QCP-n-qscd of ETSI EN 319 411-2</td>
<td>qualified electronic signature</td>
<td>Not defined.</td>
<td>2011-03-18 until 2024-03-18, does not issue any certificates from 2016</td>
</tr>
<tr>
<td>EID-SK 2016</td>
<td>CN = EID-SK 2016</td>
<td>e7 3f 1f 19 a4 45 9a 60 67 a4 5e 84 db 58 5d 6c 1d f8 f1 2a 73 9d 73 3f 5b 28 99 65 46 f1 87 5a</td>
<td>3b 80 3a 6b 69 c1 2a 8c 57 c5 50 05 31 1b c4 da</td>
<td>QCP-n and QCP-n-qscd of ETSI EN 319 411-2</td>
<td>qualified electronic signature</td>
<td>OCSP signing (1.3.6.1.5.5.7.3.9), client auth (1.3.6.1.5.5.7.3.2) secure email (1.3.6.1.5.5.7.3.4)</td>
<td>2016-08-30 until 2030-12-17</td>
</tr>
<tr>
<td>SK TIME_STAMPING AUTHORITY</td>
<td>CN = SK TIMESTAMPING AUTHORITY</td>
<td>1e 49 f4 97 d8 9d 43 0a ad 53 4b 62 2d 82 bd 9b 9d 0d 4a fd b7 b7 d3 69 86 c5 df 09 81 d9 06 7d</td>
<td>24 af ec eb 12 68 d0 02 54 17 f7 86 ed 6f 01 59</td>
<td>Time stamp of ETSI EN 319 431</td>
<td>time stamping</td>
<td>time stamping (1.3.6.1.5.5.7.3.8)</td>
<td>2014-09-16 until 2019-09-16</td>
</tr>
<tr>
<td>Identification of the Sub-CA</td>
<td>Distinguished Name</td>
<td>SHA-256 fingerprint</td>
<td>Certificate Serial number</td>
<td>Applied policy</td>
<td>Service</td>
<td>EKU</td>
<td>Validy</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>--------</td>
<td>-----</td>
<td>--------</td>
</tr>
<tr>
<td>SK TIMESTAMPING AUTHORITY 2019</td>
<td>C = EE O = SK ID Solutions AS OU = TSA 2.5.4.97 = NTREE-10747013 CN = SK TIMESTAMPING AUTHORITY 2019</td>
<td>25 d4 5a 83 4c 1e a0 e6 69 a8 a5 88 2d 74 1c 96 18 9f ef c0 8f 8c ae 9a cc ab f7 77 58 33 07 54</td>
<td>7e d7 46 4e e8 d3 0f 4d 5c 1b 5d 04 8e b0 12 6c</td>
<td>Time stamp of ETSI EN 319 421</td>
<td>time stamping</td>
<td>time stamping (1.3.6.1.5.5.7.3.8)</td>
<td>2019-01-01 until 2024-01-01</td>
</tr>
</tbody>
</table>

Table 1: Sub-CA’s issued by the Root-CA

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.
The following issuing CA certificates have been generated under the audited Root-CA. It has been ensured by SK that the Sub-CAs (Issuing CAs) were audited and certified by the conformity assessment body of TÜV AUSTRIA CERT. Corresponding evidences (audit reports) have been reviewed by the auditors:

<table>
<thead>
<tr>
<th>Identification of the Sub-CA</th>
<th>Distinguished Name</th>
<th>SHA-256 fingerprint</th>
<th>Certificate Serial number</th>
<th>Applied policy</th>
<th>Service</th>
<th>EKU</th>
<th>Validy</th>
</tr>
</thead>
<tbody>
<tr>
<td>NQ-SK 2016</td>
<td>CN = NQ-SK 2016 2.5.4.97 = NTREE-10747013 O = AS Sertifitseerimiskeskus C = EE</td>
<td>b5 cf e6 b0 b2 aa 86 1a 0b 36 7c 0c 05 39 5a 53 8a d4 93 a9 df 01 15 44 a8 ef c4 68 7f db 2c c8</td>
<td>57 a9 f3 ec a2 2f 0e 28 57 c5 4e f5 61 36 e0 5a</td>
<td>NCP of ETSI EN 319 411-1</td>
<td>non-qualified electronic signature</td>
<td>OCSP signing (1.3.6.1.5.5.7.3.9), client auth (1.3.6.1.5.5.7.3.2), secure email (1.3.6.1.5.5.7.3.4)</td>
<td>2016-08-30 until 2030-12-18</td>
</tr>
<tr>
<td>ESTEID-SK 2011</td>
<td>E = <a href="mailto:pki@sk.ee">pki@sk.ee</a> CN = ESTEID-SK 2011 O = AS Sertifitseerimiskeskus C = EE</td>
<td>41 ec 80 8e 33 cc a8 65 9e ae a8 16 70 d6 c7 dc 01 44 66 36 e1 f2 27 56 1b 63 07 b8 0b a6 38 62</td>
<td>29 52 93 aa fd 8c c6 d4 4d 83 30 a3 c2 64 51 0d</td>
<td>QCP-n-qscd of ETSI EN 319 411-2</td>
<td>qualified electronic signature</td>
<td>Not defined.</td>
<td>2011-03-18 until 2024-03-18, does not issue any certificates from 2015</td>
</tr>
<tr>
<td>ESTEID-SK 2015</td>
<td>CN = ESTEID-SK 2015 2.5.4.97 = NTREE-10747013 O = AS Sertifitseerimiskeskus</td>
<td>74 d9 92 d3 91 0b cf 7e 34 b8 b5 cd 28 f9 1e ae b4 f4 1f 3d a6 39 4d 78 b8 c4 36 72 d4 3f 4f 0f</td>
<td>45 48 09 0b 87 9c ef 21 56 72 ac d3 de 6c 1b 5b</td>
<td>QCP-n-qscd of ETSI EN 319 411-2</td>
<td>qualified electronic signature</td>
<td>OCSP signing (1.3.6.1.5.5.7.3.9), client auth (1.3.6.1.5.5.7.3.2),</td>
<td>2015-12-17 until 2030-12-17</td>
</tr>
<tr>
<td>Identification of the Sub-CA</td>
<td>Distinguished Name</td>
<td>SHA-256 fingerprint</td>
<td>Certificate Serial number</td>
<td>Applied policy</td>
<td>Service</td>
<td>EKU</td>
<td>Validy</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>--------</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>C = EE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>secure email (1.3.6.1.5.5.7.3.4)</td>
</tr>
</tbody>
</table>

This template (version 2 as of 2018-03-05) was approved for use by ACAB-c. It may only be used to without modification.
Modifications record

<table>
<thead>
<tr>
<th>Version</th>
<th>Issuing Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>2019-05-17</td>
<td>Initial attestation</td>
</tr>
</tbody>
</table>

End of the audit attestation letter.