QSCD-Certificate

of products according article 30 para 1 and article 39 para 2 eIDAS

valid from 2018-12-14 until 2023-12-14

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Certification Body
Am TÜV 1
45307 Essen, Germany

**hereby determines in accordance with Article 30 para. 1 eIDAS[1]
the conformity of the
qualified electronic signature creation device**

Smart-ID SecureZone, Version 10.3.5 & 10.3.7

of

SK ID Solutions AS

**with the requirements of eIDAS mentioned in chapter 2.
The QSCD certificate is re-issued because a new HSM model as a non-TOE component was added.**

The documentation of this certification has been registered under

TUVIT.9801.QSCD.12.2018.

Essen, 2022-03-25

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH is a notified designated certification body under article 30 para 2 of eIDAS[1].

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

The certificate TUVIT.9801.QSCD.12.2018 comprises 9 pages.

0 Description of Changes

This QSCD-certificate was reissued, because a new certified HSM model has been added to the environment. The IT product itself did not change but the version number was increased as an updated guidance documentation was created.

Relating to that:

- the Security Target (ST) was updated with the new HSM model,
- the guidance documentation (AGD) was updated, including additional configuration instructions for the new non-TOE components,
- the initial tests (ATE) including developer and independent evaluation body testing activities have been repeated, and
- the vulnerability assessment (AVA), including a Common Vulnerabilities and Exposures (CVE) analysis and a re-assessment of all potential vulnerabilities including penetration testing were performed.

The changes are described in detail in the developer's impact analysis report:

- Smart-ID QSCD Maintenance Evaluation for SecureZone HSM – Impact Analysis, dated 2022-03-08, SK ID Solutions AS (confidential document).

This QSCD-certificate replaces the QSCD-Certificate as of 2018-12-14 with corrigendum as of 2019-06-17 and 2019-09-10.

1 Certification Scheme

The certification body of TÜV Informationstechnik GmbH is accredited by "DAkkS Deutsche Akkreditierungsstelle GmbH" under ID DE-ZE-12022-01-01 according to EN ISO/IEC 17065 for the scopes IT security and security technology product certification. The certification body performs its certification on the basis of the following accredited certification system:

- Certification System (accredited scope) of the certification body of TÜV Informationstechnik GmbH", version 2.1 as of 2020-03-01, TÜV Informationstechnik GmbH

The certification for the QSCD has been performed based on the following certification scheme:

- Certification Process for eIDAS conformant QSCDs of the certification body of TÜV Informationstechnik GmbH, Version 1.2 as of 2020-10-27; the current version can be downloaded at: www.tuvit.de/en/services/eid-trust-services/qscd/

The Certification Process for eIDAS conformant QSCDs makes use of the alternative method according to article 30.3 (b) of eIDAS.

2 Information about the Product

2.1 Type and Name of the Product

Qualified Electronic Signature Creation Device (QSCD)
Smart-ID SecureZone, Version 10.3.5 & 10.3.7

2.2 Manufacturer of the Product

SK ID Solutions AS
Pärnu avenue 141
11314 Tallinn, Estonia

2.3 Description of the Product

The QSCD consists of software component (short TOE), a mobile client (user interface to the signer) and a Hardware Security Module (HSM) for managing cryptographic keys. It is a remote QSCD where the qualified trust service provider manages the electronic signature creation data on behalf of a signatory.

The TOE is the software product "Smart-ID SecureZone". It is a Java application server package, which implements the server-side functions of the Threshold Signature Scheme Protocol for the signer and the management functions for the administrators.

The Threshold Signature Scheme Protocol consists of a cryptographic protocol and algorithms, which are followed by the signer and the TOE to generate the distributed key pair of the Signer and later using the key pair to produce the signature of the Signer.

The Signer, who follows the client-side functions of the TSSP, can use the TOE services to enrol new key pairs, create digital signatures and to destroy the key pairs. The TOE alone does not create the whole digital signature on behalf of the Signer, but they both participate in the cryptographic protocol.

The TOE is deployed in a dedicated tamper protected environment that is connected to the HSM via a trusted channel. It uses the Signature Activation Data (SAD) that the signer enters on the mobile client to complete the signature computation with the HSM.

2.4 Delivery of the Product

The TOE including the TOE documentation is composed in a software zip-archive, which is delivered via a delivery system. The integrity of the delivered TOE has to be checked comparing the SHA-384 hash values of the TOE.

2.4.1 Version 10.3.5

No.	Type	Item / SHA-384 Hash Value	Form of Delivery
1.	SW	SecureZone binary package (file name: smart-id-sz.war) 0646936b40da8292bcc77c3c f96a2271c631fbf67b5fa748 b2de0fa46d5505e8cca66797 7397a5eba30948d66739b77a	Secure file transfer system
2.	SW	SecureZone Admin CLI binary package (file name: secure-zone-cli-all.jar) 4aefb0d91221eb88c3a264e3 6a38b93acb6c5004910f5860 ba68d99de15b20f425391764 1b629d201d0d29b3ff273ac6	Secure file transfer system

No.	Type	Item / SHA-384 Hash Value	Form of Delivery
3.	SW	Liquibase changesets and scripts for initializing and updating the database schema (file name: liquibase.tar) 45067d91781bd300cd8d2a f780c74b955c888dda0d73 d419aabac0386f15f7ede11 9048417c5c95f063add75c 6cbbe97	Secure file transfer system
4.	DOC / Guidance	Installation Guide for SecureZone, Version 1.7_v112 as of 2018-09-17, file name install_guide.pdf, 7eb3995a7f7f4d74af68f0b1 76f88825ef6414cd607bb70c 45c891e4db905ab81a8b19cc 5f91e6859db5a2838e5b5886	Secure file transfer system
5.	DOC / Guidance	Administration Guide for SecureZone, Version 1.7_v106 as of 2018-09-17, file name: admin_guide.pdf, adfea424f66b84b4ff5967df d33f0c5fffef6768aaeed624 938deb098bb779fbbfee4c99 4e2925794f64b1cb26e40c0d	Secure file transfer system
6.	DOC / Guidance	Signer User Guidance information for SecureZone and TSE library operators, Version 2.2_v26 as of 2018-08-30, file name: signers_guide.pdf 71cf10e9844ad7707c5ea062 8f5edc80ffc2f43a02dc1aa4 b330d79e2d6d6acd333f6526 f2ff9ae03c732f012f2156bc	Secure file transfer system
7.	DOC / Guidance	Smart-ID SecureZone Monitoring Guide, Version 1.1_v18 as of 2018-07-23, file name: monitoring_guide.pdf 8f5ea882e546f1b0a4fe0ec0 109bed8e841c3e60a847b68a a325ddf69a10b2c02226eb42 46b9fe0af5bf4f5a2daf1ffa	Secure file transfer system
8.	DOC / Guidance	Smart-ID SecureZone Technical Architecture, Version 10.12, as of 2018-09-12, file name: Smart-ID_SZ_Architecture_v10.12.pdf d5eb6e143ddaaba3fdda3b10 d80751d77843f44cee3efefe 584a8f63e49476eba562bb28 a6c96739e6c83928c2763ecc	Secure file transfer system

The information for the integrity check process is delivered within a digitally signed delivery report in .asice format.

No.	Type	Item	Form of Delivery
9.	DOC / Configuration	Release Notes document (file name: Smart-ID Release notes-Secure Zone 10.3.5)	Secure file transfer system, Delivered in digitally signed container containing overview of changes and checksums of all delivered components.
10.	txt	Checksums txt (file name: smartid-sz-checksums- 10.3.5)	Secure file transfer system, Delivered in digitally signed container containing overview of checksums of all delivered components.

The delivery of the HSM and mobile client must be performed according to their certification requirements.

2.4.2 Version 10.3.7

No.	Type	Item / SHA-384 Hash Value	Form of Delivery
1.	SW	SecureZone binary package (file name: smart-id-sz.war) e0d1182989b487058c62b79d 65bf1909767ed168ea85811a 47f76ed6b9c775445b4f26b5 5a908673bd6e03bee65c9b8a	Secure file transfer system
2.	SW	SecureZone Admin CLI binary package (file name: secure-zone-cli-all.jar) d552d433516eade4f940fa51 0b59b57bf523de1599652333 c42f92e92dc090bcf18cb0fc 4f51713631f5332b9925e353	Secure file transfer system
3.	SW	Liquibase changesets and scripts for initializing and updating the database schema (file name: liquibase.tar) 9e4332d71053736f366c3999 3b14020d39a3eccb3560ce67 5dd5c41c5a6a90271c1c1976 4ac3004ee8011bd4ee35730b	Secure file transfer system
4.	SW	exportpub.py (file name: exportpub.py) ef2c03507fbda49a191929d0 7b35ca20645f6a6ad2fd1cf5 eb67ba33b2d720c16eaf3771 82bd445b7bb7bccde29f0e7d	Secure file transfer system
5.	SW	generatekey (file name: generatekey) 11d5103892408294a11814d7 51755cdb8b6e10814a5ea1be 85549f0dd6d76bfd1741c992 fefcbd5fdf0fddd2694b42f2	Secure file transfer system

No.	Type	Item / SHA-384 Hash Value	Form of Delivery
6.	SW	nfkmverify (file name: nfkmverify) 74796ad3bc2689398acaca5f433965db349406468a80d1075d5ad525f395a61cbf542bec6cb5344b89e19dd76080f349	Secure file transfer system
7.	DOC / Guidance	Installation Guide for SecureZone, Version 1.8_v117 as of 2021-05-26, file name: install_guide.pdf 01ce97b243bc4d30701d6f32332d2db04d33d3b7e57ec2d76f04552b8b967e5df920942f9fd135dc97123dd20b608975	Secure file transfer system
8.	DOC / Guidance	Administration Guide for SecureZone, Version 1.8_v114 as of 2021-05-26, file name: admin_guide.pdf 23f3bb72a87e9fc371f6df0b86a12bf23daaa41617af2187b976fbafcbd5f2cd4cf323d14da960436392a1bc552a2481	Secure file transfer system
9.	DOC / Guidance	Signer User Guidance information for SecureZone and TSE library operators, Version 2.2_v26 as of 2018-08-30, file name: signers_guide.pdf 71cf10e9844ad7707c5ea0628f5edc80ffc2f43a02dc1aa4b330d79e2d6d6acd333f6526f2ff9ae03c732f012f2156bc	Secure file transfer system
10.	DOC / Guidance	Smart-ID SecureZone Monitoring Guide, Version 1.1_v18 as of 2018-07-23, file name: monitoring_guide.pdf 8f5ea882e546f1b0a4fe0ec0109bed8e841c3e60a847b68aa325ddf69a10b2c02226eb4246b9fe0af5bf4f5a2daf1ffa	Secure file transfer system
11.	DOC / Guidance	Smart-ID SecureZone Technical Architecture, Version 10.12, as of 2018-09-12, file name: Smart-ID_SZ_Architecture_v10.12.pdf d5eb6e143ddaaba3fdda3b10d80751d77843f44cee3efefe584a8f63e49476eba562bb28a6c96739e6c83928c2763ecc	Secure file transfer system

The information for the integrity check process is delivered within a digitally signed delivery report in .asice format.

No.	Type	Item	Form of Delivery
12.	DOC / Configuration	Release Notes document (file name: Smart-ID Release notes-Secure Zone 10.3.7)	Secure file transfer system, Delivered in digitally signed container containing overview of changes and checksums of all delivered components.
13.	txt	Checksums txt (file name: smartid-sz-checksums- 10.3.7)	Secure file transfer system, Delivered in digitally signed container containing overview of checksums of all delivered components.

The delivery of the HSM and mobile client must be performed according to their certification requirements.

3 Compliance with the requirements of eIDAS

Smart-ID SecureZone has provided evidence of conformity with regard to the following requirements for qualified electronic signature devices laid down in eIDAS.

Requirement	Fulfilment by the TOE
Article 30	**Requirements for qualified electronic signature creation devices**
Para. 1	Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.
Annex II eIDAS	**Requirements for qualified electronic signature creation devices**
Para. 1 a-d)	Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least: (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured; (b) the electronic signature creation data used for electronic signature creation can practically occur only once; (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology; (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
Para. 2	Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

Para. 3 Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.

Para. 4 a-b) Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:

(a) the security of the duplicated datasets must be at the same level as for the original datasets;

(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

4 Operating Conditions

The following operational conditions must be fulfilled:

- The TOE must be implemented within the environment of a qualified Trust Service Provider, which fulfils the requirements as specified in the eIDAS.
- The TOE’s environment must be physically secured.
- For the cryptographic key generation and cryptographic operations one of the following HSM model must be installed, configured and used as randomness source for the Secure Zone:
  - CC certified HSM Thales nShield HSM Family v11.72.02 (Certificate No 1/16, as of 2016-03-10 from OCSI – Organismo di Certificazione della Sicurezza Informatica, via Viale America, 201, 00144 Roma, Italy)
  - CC certified HSM nCipher nShield Solo XC v12.60.15 (Report No NSCIB-CC-163968-CR2, as of 2021-03-17 from TÜV Rheinland Nederland B.V, Wstervoortsedijk 73, 6827 CE Arnhem, The Netherlands)
- As user interface, the mobile application with a certified TSE library that is CC evaluated with the Assurance at least level EAL2 must be used by the Signer.
- The administrators must only accept secure digest algorithms (SHA-256 or better) for generation of the data to be signed representation (DTBS/R).
- The Secure Zone server must be synchronized to a trusted time source.
- Only trustworthy, well-trained personal must be assigned to perform administrator duties.
- Administration tasks must be performed with dual control.
- The network-based and channel-based security must be configured in order to protect the transmitted DTBS/R from the disclosure.

5 Algorithms and Corresponding Parameters

For the creation of qualified electronic signatures, the TOE uses the cryptographic algorithm:

- RSASSA-PKCS1-V1_5 according to PKCS#1: RSA Cryptography Specifications, Version 2.2 as of November 2016 (RFC8017) with the cryptographic key sizes 4094, 4095, 4096, 6142, 6143, 6144, 8190, 8191, 8192.

6 Evaluation Assurance Level and Strength of Mechanism

The TOE in version 10.3.5 has been evaluated and certified according to Common Criteria. A certificate has been issued under number TUVIT-TSZ-CC-9263-2018 on 2018-12-14 by the certification body of TÜViT. The security target took into account requirements from the certified Protection Profiles:

- EN 419 221-5:2018, Protection profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services
- prCEN/EN 419 241, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, v0.16, 2018-05-11.

The maintenance report for the TOE version 10.3.5 and 10.3.7, which includes the certification report for TOE version 10.3.5 including the initial and the new Security Target, can be downloaded from TÜViT’s website:

- https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/en/9263BE_s.pdf

The TOE security assurance requirements are based entirely on the assurance components and classes defined in part 3 of Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 4+ (Evaluation Assurance Level 4+) augmented by AVA_VAN.5 (Advanced methodical vulnerability analysis).

7 Validity Period of the QSCD-Certificate

This certificate is only valid in conjunction with the certificate TUVIT-TSZ-CC-9263-2018 as of 2019-10-09 and the corresponding certification report and the maintenance report TUVIT-TSZ-CC-9263-2018-MA01 as of 2022-03-25.

The validity period of the QSCD certificate depends on the strength of security mechanisms and algorithms that are implemented in the product and is limited 14th December 2023 at maximum.

At a given time, the validity period can be extended or shortened if there are new findings regarding the suitability of security mechanisms or algorithms.