TÜVIT

Certificate

TÜVIT
TÜV NORD GROUP
eIDAS
QSCD
2023
tuvit.de
ID: 9803.23

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

SK ID Solutions AS
Pärnu avenue 141
11314 Tallinn, Estonia

Certificate validity:
2023-09-26 – 2028-09-26

to confirm that its qualified electronic signature creation device

Smart-ID SecureZone, version 11.5.23

fulfils the requirements laid down in

Annex II of Reg. (EU) No. 910/2014 (eIDAS).

The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate with the ID 9803.23 and consists of 6 pages.

Essen, 2023-09-26

Dr. Christoph Sutter, Head of Certification Body

To Certificate

TÜV Informationstechnik GmbH
Am TÜV 1 ▪ 45307 Essen, Germany
tuvit.de

TÜVNORDGROUP

Certification scheme

The certification body of TÜV Informationstechnik GmbH is notified as certification body according to article 30.2 of “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” by “Bundesnetzagentur” (Germany).

The certification body performs its certification for qualified signature / seal creation devices (QSCD) 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.

Evaluation / Certification report

- “Certification Report TUVIT-TSZ-CC-9265-2023 Smart-ID SecureZone, version 11.5.23” as of 2023-09-26, TÜV Informationstechnik GmbH

Evaluation requirements

The evaluation requirements are defined in:

- Annex II of 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 evaluation requirements are summarised at the end.

Evaluation target

Evaluation target is the Qualified Electronic Signature Creation Device (QSCD) “Smart-ID SecureZone“, version 11.5.23.

Description of the evaluation target

The QSCD consists of a software component (short TOE) a mobile client (user interface to the signer) and a cryptographic module (HSM) certified against EN 419 221-5[1]. 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.

Delivery of the evaluation target

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.

No.	Type	Item / SHA-384 Hash Value	Form of Delivery
1.	SW	SecureZone binary package (file name: sz-11.5.23_RELEASE-all.jar) 5cfcafdd4ed4dfbd9c414b615985abbb7310bc74b47211c3b541389cbe7b1086eb146a41b39a541b92ed1efd500c94a7	Secure file transfer system
2.	SW	sz-boot-11.5.23_RELEASE-executable.jar (file name: sz-boot-11.5.23_RELEASE-executable.jar) a7fdb96566bad7be962f9095b5bc9d95c76d03e3781213139caa3bf01f4840026ef874de84b20f759801657d8471a924	Secure file transfer system
3.	SW	SecureZone Admin CLI binary package (file name: secure-zone-cli.jar) 2b46995d8fc7b05af99214dbf9a26be935ff6768ac5b5276124bb19b21fcf043f5ac0be1b4833886de73b4a9b84347aa	Secure file transfer system
4.	SW	Liquibase changesets and scripts for initializing and updating the database schema (file name: liquibase.tar) 619252e50b20900cc7e8295b13127903a21407cf98c37ab1b43bd9b4	Secure file transfer system

[1] Protection Profiles for TSP cryptographic modules – Part 5: cryptographic module for Trust Services. English version EN 419221-5:2018

No.	Type	Item / SHA-384 Hash Value	Form of Delivery
		ce687b9fefd14e5c8bf1739672398e05afc96170	
5.	DOC	Installation Guide for SecureZone v2.32_v133 f817289ac42b9241b8d648924746d0b67f92a9deb96b5cab164fde02346518d6092a59acbdebeb8b649944006297988a	Secure file transfer system
6.	DOC	Administration Guide for SecureZone v2.15_v78 7e65d4d7a7b366a0b8f4a12958987161ab51e4e2bd6a0c073ab04e1c51e3277138ce70d1677a1fec6c9a2fd55fccfa7a	Secure file transfer system
7.	DOC	Smart-ID SecureZone monitoring guide v1.6_v19 2dac8a1f63952a00759febb0b868556218861857a1b28eda1172debfebcb4a0661da35e33a4d26e1121e71107f39e844	Secure file transfer system
8.	DOC	Signer User Guidance information for SecureZone and TSE library operators v2.8_v11 1850e329825b29918e538fd0181add2137021a085c7bd6764ee06fabc3d0e0d1ff7c7e58545097082043d8b01a31e66d	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 / SHA-384 Hash Value	Form of Delivery
9.	DOC	Release Notes document (file name: smartid-sz-release-notes-11.5.23.txt)	Secure file transfer system, delivered in digitally signed container containing overview of changes and checksums of all delivered components
10.	DOC	Checksums txt (file name: smartid-sz-checksums-11.5.23.txt)	Secure file transfer system, delivered in digitally signed container containing overview of changes and checksums of all delivered components

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

Evaluation result

- The evaluation target fulfills all applicable evaluation requirements
- The certification requirements defined in the certification scheme are fulfilled.
- The operating conditions listed in the certification report shall be respected.

Summary of the evaluation requirements

Annex II of eIDAS contains the following requirements for QSCDs:

1. 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.

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.

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

4. 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.

Operational 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, Westervoortsedijk 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.

Algorithms and associated parameters

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

- RSA PKCS1-v1_5, RSASSA-PSS with 3071, 3072, 4095, 4096, 6143, 6144, 8191, 8192 Bit Key Length according to PKCS#1: RSA Cryptography Specifications, Version 2.2 as of November 2016 (RFC8017)

Evaluation assurance level

The TOE in version 11.5.23 has been evaluated and certified according to Common Criteria. A certificate has been issued under number TUVIT-TSZ-CC-9265-2023 on 2023-09-26 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

- EN 419 241-2019, Feb. 2019, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing

The certification report for the TOE version 11.5.23, which includes the Security Target, can be downloaded from TÜVIT's website:

- https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/en/9265BE.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).

Validity period of the certificate

This certificate is only valid in conjunction with the certificate TUVIT-TSZ-CC-9265-2023 and the corresponding certification report as of 2023-09-26.

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 26th September 2028 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.

.