Certification report

version 1
May 20, 2026

EXECUTIVE SUMMARY - CERTIFICATION

CERTIFICATION SCHEME:	☐ EUCC ☒ eIDAS QSCD
PRODUCT IDENTIFICATION AND TOE:	Smart-ID SecureZone 11.5.23
PRODUCT TYPE:	R-QSCD
SPONSOR:	SK ID Solutions AS
DEVELOPER(S):	SK ID Solutions AS
CERTIFICATION BODY:	TÜV NORD CERT GmbH Business Entity IT – Data Center Am TÜV 1, 45307 Essen, Germany
ITSEF (INCL. SUBCONTRACTORS):	TÜV Informationstechnik GmbH
STANDARD VERSION:	Common Criteria (CC), Version 3.1 Revision 5 & CEM, Version 3.1 Revision 5
ASSURANCE REQUIREMENTS:	EAL4 augmented with AVA_VAN.5
PP CONFORMANCE:	None
ETR IDENTIFICATION AND DATE (COMPLETION OF EVALUATION):	TUVIT-TSZ-CC-9265-2026, Version 2, 20.05.2026, TÜVIT
CERTIFICATION REPORT REFERENCE	TNCERT-eIDAS-9805-2026, Version 1, 20.05.2026, TN CERT GmbH
CERTIFICATE	9805.26
DATE OF CERTIFICATION	20.05.2026
VALIDITY	5 years (valid until 19.05.2031)

EXECUTIVE SUMMARY - CERTIFICATION

THREATS	Create one or more forged signatures of fresh data to be signed under the name of the legitimate signer Decrease the trust in the signatures created with the service Smart-ID Trust Service Provider (TSP) and in the security of the TOE.
ORGANISATIONAL SECURITY POLICIES	The confidentiality of Signature Creation Data must be reasonably assured. Any given instance of a Signature Creation Data shall occur only once. An electronic signature shall be reliably protected against forgery using currently available technology. It shall not be possible, with reasonable assurance, to derive an electronic signature from data other than the Signature Creation Data. Signature Creation Data of a legitimate Signer shall be reliably protected against use by others. The TOE and its environment shall not alter the data to be signed nor its actually signed representation (digest). The TOE and its environment shall not prevent such data from being presented to the Signer prior to signing.
SECURITY FUNCTIONS	Access Control separating *anonymous users* from *key pair owners (Signers)* and *privileged users* Key generation using the underlying hardware HSM Destruction of cryptographic keys after they are no longer used. Trusted path implementing JSON Web Encryption (JWE) messages for the communication between the TOE and the Smart-ID App TSE. Secure channel ensuring that vendor-specific proprietary communication channel is used, when connecting with HSM or database. Support functions: cryptographic support, management functions, security audit
PATCH PROCEDURE	Not applicable
ASSUMPTIONS	The security target defines assumptions on the HSM, TSP, CGA, TSE, Admin and operational environment as a whole. See section 2.1 for more details
SPECIAL CONFIGURATION OF THE TOE	Java Version: Java 17 64bit JRE JVM Application server: Apache Tomcat application server Database server: PostgreSQL HSM : nShield Connect XC or nShield5s
ADDITIONAL DISCLAIMERS	N/A

Guillaume Tetu
Digitally signed by Guillaume Tetu
Date: 2026.05.26 09:44:01 +02'00'

Guillaume Tetu
Certifier

Guillaume Tetu
Digitally signed by Guillaume Tetu
Date: 2026.05.26 09:44:17 +02'00'

Guillaume Tetu
TIC Manager

Table of contents

1 Identification of the ICT product

1.1 History of certification

Certification	Modification of scope?	Process number	Product ID and version	Valid until
Initial certification	-	TUVIT.9801.QSCD.12.2018	Smart-ID SecureZone, Version 10.3.5	2023-12-14
Recertification	No	9803.23	Smart-ID SecureZone, version 11.5.23	2028-09-26
Recertification	No	9256.26	Smart-ID SecureZone, version 11.5.23	2031-05-14

Note: the product had to undergo a recertification despite having a valid certificate on the same product version, due to two changes in operational conditions:

- Change of algorithms to use;
- Change of underlying HSM.

These changes are reflected in the updated accompanying documentation of the TOE, without changing its release name (11.5.23). See section 4 Scope of delivery for more details

1.2 Target of evaluation

The product is Smart-ID SecureZone, version 11.5.23

1.3 Patch management

Patch management is not part of the security target.

1.4 Evaluation activities

The evaluation activities were performed by TÜVIT. They took place between

- 2026-02-26 (date of the kick-off meeting)
- 2026-04-17 (date of the ETR)

Evaluators from TÜVIT were:

- Arzu Sarial
- Alexander Bobel
- Ludger Knobel
- Natalie Tupitzin

Designated contacts from the sponsor/developer side were:

- Rasmus Kukk,
- Meelis Kukk.

1.5 Additional requirements to the operating environment

The report summary includes the list of requirements to the operating environment.

1.6 Sponsor and developers

Sponsor and developer:
SK ID Solutions AS
Pärnu mnt 141, 11314 Tallinn, Estonia

2 Security Target

The security target provided with this certification report has the following reference: Smart-ID SecureZone Security Target, version 3.1.1, date 2026-03-18

2.1 Assumptions

The HSM shall:

- protect the confidentiality of the components of the Signature Creation Data.
- ensure cryptographic quality of generated keys.
- generate the D.serverShare and the corresponding D.serverModulus securely. It shall not be possible to derive D.serverShare from D.serverModulus and probability of equal D.serverShares shall be negligible.
- generate electronic signatures (D.serverSignatureShare) that cannot be forged without knowledge of the private key (D.serverShare), through robust cryptographic techniques. The D.serverShare cannot be reconstructed from the digital signatures.
- prevent or resist physical tampering with HSM device and components.
- provide the share of the signature (D.serverSignatureShare) creation function for the TOE only and protects the D.serverShare against attempts by other users to create a digital signature using it.
- ensure that the data to be signed cannot be altered when processed by the HSM.
- provide the cryptographically secure random number generator for the TOE.

The TSE shall

- generate D.applicationSignaturePart, that cannot be forged without knowledge of the D.clientPart, through robust cryptographic techniques. The TSE shall not allow the private key to be reconstructed from the digital signatures.
- ensure cryptographic quality of generated keys. TSE shall generate the D.clientShare and the correspond-ing D.clientModulus securely. It shall not be possible to derive D.clientShare from D.clientModulus and probability of equal D.clientShares shall be negligible.
- protect the confidentiality of the components of the Signature Creation Data
- protect the confidentiality and integrity of the communications between the TSE and TOE
- be run in isolated mobile app process, protected from other apps.

The TSP deploying the TOE is a qualified TSP and audited to be compliant with the requirements for TSP's given by reg. (EU) 910/2014. The audit of the qualified TSP shall cover the security objectives for the operational environment specified in this clause.
The operational environment shall

- ensure that the qualified TSP that issues qualified certificates is compliant with the relevant requirements for qualified TSP's as defined in reg. (EU) 910/2014.
- use a process for requesting a certificate, including Signature Verification Data and signer information, and CA signature in a way, which demonstrates the signer is in

control of the signing key associated with the Signature Verification Data presented for certification. The integrity of the request shall be protected.

- provide a J2EE application server which ensures that the TOE is the only application deployed in a container of the J2EE application server.
- limit physical and logical access to the components in the TOE environment to authorised admins. The TOE software, hardware environment and backup datasets shall be maintained by admins in a secure state, including protection against unauthorised software and configuration changes.
- provide trusted timestamps.
- ensure the Signature Verification Data integrity during transmit outside the TOE to the CA.
- ensure the integrity of the Signature Verification Data exported by the TOE to the CGA. The CGA shall verify the correspondence between the Signature Creation Data of the Signer and the Signature Verification Data in the input provided to the certificate generation function of the CGA.
- allow the verification of the integrity of the digest of the data to be signed (generated by the Signature Creation Application or SCA), so that the Signer can be sure he is signing the same document he intends to sign.
- ensure that the digest of the data to be signed cannot be altered in transit between physically separated components of the TOE environment.
- ensure that the data to be signed may practically have only one unique representation as a digest and that the probability for existence of two different data to be signed having identical digests is negligible.
- protect the integrity of the audit log and protect the audit log from unauthorized deletion.

The admin, who has unrestricted physical and logical access to the TOE and the TOE environment shall be well-trained and trusted and shall perform his duties.
The CGA shall generate qualified certificate and thus confirm that the Signature Creation Data, corresponding to the certified Signature Verification Data, is under the control of Signer. The CGA shall include identifying information of the Signer in the certificate and therefore enable to identify the Signer by the signature.
The signer’s management of authentication factors data outside the TOE shall be carried out in a secure manner

2.2 Threats

The product provides security functionality to cover the following threats:

- Create one or more forged signatures of fresh data to be signed under the name of the legitimate signer
- Decrease the trust in the signatures created with the service Smart-ID Trust Service Provider (TSP) and in the security of the TOE.

2.3 Organisational security policies

The product provides security functionality to cover the following OSPs:

- The confidentiality of Signature Creation Data must be reasonably assured (from reg. (EU) 910/2014, Annex II, point 1.(a)).
- Any given instance of a Signature Creation Data shall occur only once (from reg. (EU) 910/2014, Annex II, point 1.(b)).
- An electronic signature shall be reliably protected against forgery using currently available technology. It shall not be possible, with reasonable assurance, to derive an electronic signature from data other than the Signature Creation Data (from reg. (EU) 910/2014, Annex II, point 1.(c)).
- Signature Creation Data of a legitimate Signer shall be reliably protected against use by others (from reg. (EU) 910/2014, Annex II, point 1.(d) and Article 26, point (c)).
- The TOE and its environment shall not alter the data to be signed nor its actually signed representation (digest). The TOE and its environment shall not prevent such data from being presented to the Signer prior to signing (from reg. (EU) 910/2014, Annex II, point 2).

2.4 Security services

The product provides the following security functionality:

- Access Control separating anonymous users from key pair owners (Signers) and privileged users
- Key generation using the underlying hardware HSM
- Destruction of cryptographic keys after they are no longer used.
- Trusted path implementing JSON Web Encryption (JWE) messages for the communication between the TOE and the Smart-ID App TSE.
- Secure channel ensuring that vendor-specific proprietary communication channel is used, when connecting with HSM or database.
- Support functions: cryptographic support, management functions

3 Assumptions and clarification of scope

No clarification is needed.

4 Scope of delivery

The TOE consists solely of software as well as its associated guidance documentation that comprises the following parts:

- Administration Guide for SecureZone [AGD_Admin],
- Installation Guide for SecureZone [AGD_Inst],
- Smart-ID SecureZone Monitoring Guide [AGD_Mon], and
- Signer User Guidance information for SecureZone and TSE library operators [AGD_User].

The following TOE deliverables are provided to the user/administrator:

No.	Type	Item / Identifier	Evaluator's comments	Form of Delivery
1.	SW	SecureZone binary package (file name: sz-11.5.23_RELEASE-all.jar) 5cfcafdd4ed4dfbd9c414b615985abbb7310bc74b47211c3b541389cbe7b1086eb146a41b39a541b92ed1efd500c94a7	TOE software part	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	TOE software part	Secure file transfer system
3.	SW	SecureZone Admin CLI binary package (file name: secure-zone-cli.jar) 2b46995d8fc7b05af99214dbf9a26be935ff6768ac5b5276124bb19b21fcf043f5ac0be1b4833886de73b4a9b84347aa	TOE software part	Secure file transfer system
4.	SW	Liquibase changesets and scripts for initializing and updating the database schema (file name: liquibase.tar) 619252e50b20900cc7e8295b13127903a21407cf98c37ab1b43bd9b4ce687b9fefd14e5c8bf1739672398e05afc96170	TOE software part	Secure file transfer system
5.	DOC	Installation Guide for SecureZone 2.35_v142.pdf 750b5206517c559bba9fd0b4a954ab40a076727a6294246a8722b886892200ada996d7c54c711c1c7a4b2227f825bbc7	Part of Guidance documentation	Secure file transfer system

No.	Type	Item / Identifier	Evaluator's comments	Form of Delivery
6.	DOC	Administration Guide for SecureZone 2.17_v85.pdf fd8f8ce4ad49e165914efa64db5cec5ed74d977ee50fe9ab0f066ce268c3239baec75c8f470c92b08bc820c357e4573a	Part of Guidance documentation	Secure file transfer system
7.	DOC	monitoring_guide 1.6_v19.pdf 2dac8a1f63952a00759febb0b868556218861857a1b28eda1172debfebcb4a0661da35e33a4d26e1121e71107f39e844	Part of Guidance documentation	Secure file transfer system
8.	DOC	signers_guide 2.10_v13.pdf d48f4608e18081ad9eb5549fbf36d3c67885db9d40a541f64da620fb2b7bba7184c364567a7df8358ad53ec1c819a7fe	Part of Guidance documentation	Secure file transfer system
9.	DOC	Release Notes document (smartid-sz-release-notes_checksums-11.5.25.asice) *11.5.25 is the release package version here, which is not the TOE version*	Delivered in digitally signed container containing overview of changes and checksums of all delivered components	Secure file transfer system
10.	DOC	Checksums txt (file name: smartid-sz-checksums-11.5.25.txt) *11.5.25 is the release package version here, which is not the TOE version*	Delivered in digitally signed container containing checksums found from smartid-sz-release-notes-<version_number>.asice	Secure file transfer system

Table 1: TOE Deliverables

5 Architectural information

Based on the evaluation evidence described in the CC assurance family entitled TOE design (ADV_TDS) the TOE consists solely of six modules. A subsystem-level decomposition is not necessary because of the simple TOE structure. These are defined in [ADV]; the following table provides an overview:

Module	Description
TSSP module	*Contains implementation of Threshold Signature Scheme Protocol (TSSP).*
Configuration module	*Administrative command line tool, contains all the logic for system key (KTK et al.) generation and other administrative operations.*
Command line interface module	*Is responsible for configuration file loading and verification.*
JSON-RPC controller module	*A glue module for converting JSON-RPC calls to Java calls.*
Audit logging module	*Called by all the modules above to create audit log records.*
Support functionality module	*A support module for non-security-critical operations.*

Table 2: TOE modules

The following figure provides a graphical overview of the TOE architecture in consideration of the subsystems and modules:

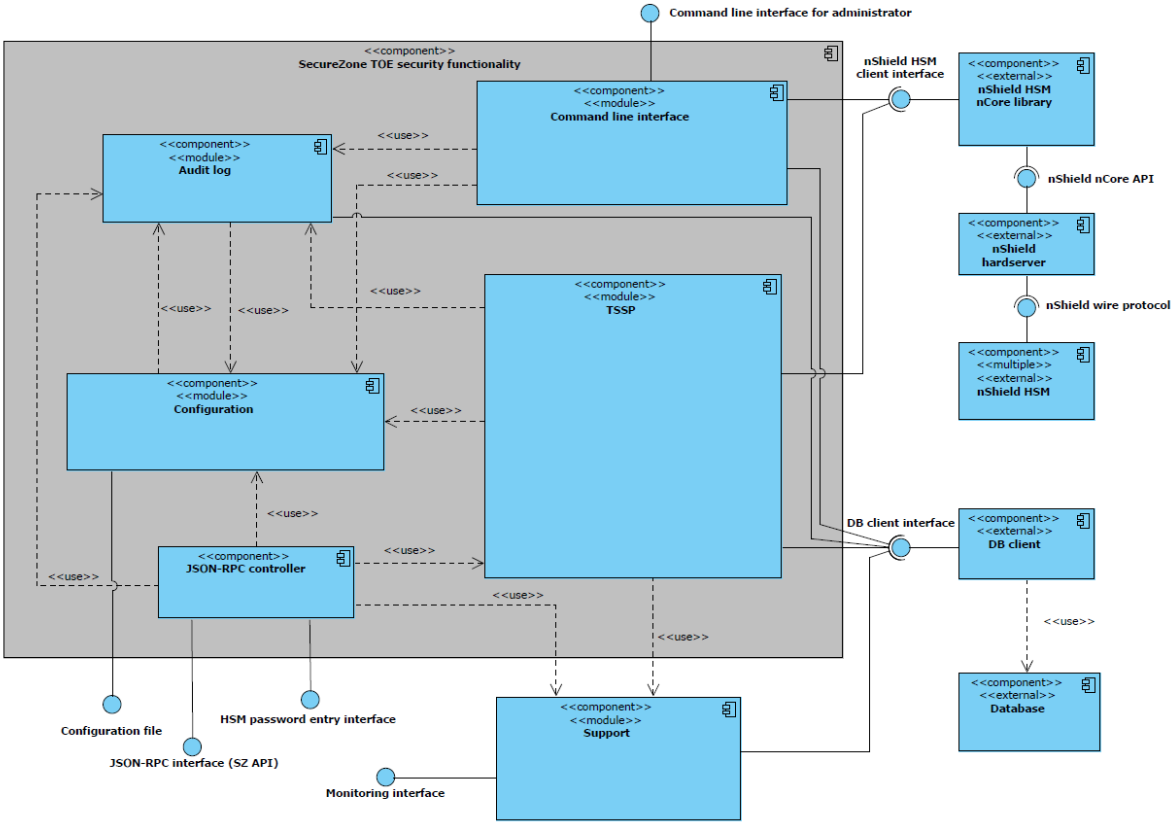

Figure 1: TOE architecture

6 Lifecycle management processes and production facilities

The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1. ALC_TAT.1) are fulfilled for the development and production site of the TOE listed below:

Name of site / Company name	Address	Type of site	Date of last audit	New audit / reused audit / N/A
Tallin, Estonia	SK ID Solutions AS Pärnu mnt 141, 11314 Tallinn, Estonia	• TOE development (implementation and testing), • TOE production and delivery initiation (TOE distribution), • Development of CC evaluation evidence documentation.	2026-04-08	New audit
	Server room in data center Vae 14, Laagri Harju country, Estonia	• Hosting all relevant development servers.	2023-04-05 / 06	New audit during first evaluation, not audited for re-evaluation
	Server room in data center, Sõpruse pst. 193, Tallinn, Estonia	• Hosting all relevant development servers (mirror).	2023-04-05 / 06	New audit during first evaluation, not audited for re-evaluation

Table 3: Relevant development/production sites

7 Evaluation and testing

7.1 Certification body

CERTIFICATION BODY - TÜV NORD CERT GmbH
Business Entity IT – Data Center
Am TÜV 45307 Essen

7.2 ITSEF

TÜV Informationstechnik GmbH
Am TÜV 1
45307 Essen

TÜVIT applied the following state-of-the-art documents and further security evaluation criteria during the evaluation:

- [ENISA-ITSEF-EUCC-ACCRED]

7.3 Assurance components

Standard version: CC 3.1r5
Assurance components: EAL4 augmented with AVA_VAN.5.

7.4 Evaluation configuration

The TOE under evaluation has been tested in its unique configuration. According to the operational environment of the TOE as specified in principle in the ST and outlined in Section 3.1 the developer's and evaluator's tests have been performed in the test configuration specified in the following table:

Tested Aspect	**Security Objectives on the Operational Environment according to [ST, 2.4] and [AGD_Inst, 7.2]**	**Operational Environment used for testing**
Operating system (OS)	*While being a Java application the SecureZone service and the SecureZone CLI can be executed on any platform, a Linux based environment is recommended, including Linux based container environments*	AlmaLinux
Java Version	*Java 17 64bit JRE JVM*	Java 17
Application server	*Apache Tomcat application server*	Apache Tomcat 64bit version 10.1.8
Database server	*PostgreSQL*	PostgreSQL version 16
HSM	*nShield Connect XC or nShield5s*	nCipher nShield Solo XC for nShield Connect XC with part number NH2075,

Tested Aspect	Security Objectives on the Operational Environment according to [ST, 2.4] and [AGD_Inst, 7.2]	Operational Environment used for testing
		Entrust nShield5s with firmware v13.5.1
TOE version	*11.5.23*	11.5.23

Table 4 : Operational Environment used for testing

7.5 Protection Profile

The ST does not claim conformance to a Protection Profile.

7.6 Evaluation results reuse

The evaluation reused results from one previous site audit (see section 6).

7.7 Base TOE results reuse (composite evaluation)

Not applicable

8 Results

8.1 Results of the evaluation

The product matches the assurance requirements defined in section 7.3
The verdicts for the CC components are summarised in the following table:

Assurance classes and components			**Verdict**
Development		**ADV**	**PASS**
	Security architecture description	ADV_ARC.1	PASS
	Complete functional specification	ADV_FSP.4	PASS
	Implementation representation of the TSF	ADV_IMP.1	PASS
	Basic modular design	ADV_TDS.3	PASS
Guidance documents		**AGD**	**PASS**
	Operational user guidance	AGD_OPE.1	PASS
	Preparative procedures	AGD_PRE.1	PASS
Life-cycle support		**ALC**	**PASS**
	Production support, acceptance procedures and automation	ALC_CMC.4	PASS
	Problem tracking CM coverage	ALC_CMS.4	PASS
	Delivery procedures	ALC_DEL.1	PASS
	Identification of security measures	ALC_DVS.1	PASS
	Developer defined life-cycle model	ALC_LCD.1	PASS
	Well-defined development tools	ALC_TAT.1	PASS
Security Target evaluation		**ASE**	**PASS**
	Conformance claims	ASE_CCL.1	PASS
	Extended components definition	ASE_ECD.1	PASS
	ST introduction	ASE_INT.1	PASS
	Security objectives	ASE_OBJ.2	PASS
	Derived security requirements	ASE_REQ.2	PASS
	Security problem definition	ASE_SPD.1	PASS
	TOE summary specification	ASE_TSS.1	PASS
Tests		**ATE**	**PASS**
	Analysis of coverage	ATE_COV.2	PASS
	Testing: security enforcing modules	ATE_DPT.1	PASS
	Functional testing	ATE_FUN.1	PASS
	Independent testing - sample	ATE_IND.2	PASS
Vulnerability Assessment		**AVA**	**PASS**
	Advanced methodical vulnerability analysis	AVA_VAN.5	PASS

Table 5: List of all verdicts

a

8.2 Information regarding the certificate

The corresponding certificate 9805.26 was issued on 20.05.2026 and is valid until 19.05.2031 (validity of the certificate is 5 years)

9 Attachments

9.1 Glossary and Abbreviations

abbreviation	Meaning
BSI	Federal Office for Information Security
TN CERT	TÜV NORD CERT GmbH As part of a partial business transfer (spin-off) that took place on August 22, 2024, the data center services of the TÜVIT IT Infrastructure business unit will be continued with the existing staff at TÜV NORD CERT GmbH, TN CERT for short, as the legal successor in the Business Entity IT, Datacenter Group.
TÜVIT	TÜV Informationstechnik GmbH (a company of TÜV NORD GROUP) see also TN CERT
TSE	Threshold Signature Engine – Smart-ID App TSE is the software component, which works within the Signer's environment and helps and assists Signer to follow the Threshold Signature Scheme Protocol (TSSP) and to use the Smart-ID SecureZone services for the key enrolment and signature creation.
D.serverShare and the corresponding D.serverModulus	Server-side component of the Signature Creation Data and the corresponding Signature Verification Data
D.clientShare and the corresponding D.clientModulus	Component of the Signature Creation Data created at client-side and the corresponding Signature Verification Data

10 References

10.1 Bibliography

reference	detail
[ENISA-CB-EUCC-ACCRED]	Accreditation of CBs for EUCC, 9 January 2025, European Union Agency for Cybersecurity, v1.6b
[CC 3.1r5]	CC:3.1 revision 5, Parts 1 through 3, published by the participants of the Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security Any reference to these documents will implicitly include • The CC and CEM addenda - Exact Conformance - CCDB-013-v2.0 • the Evaluation Methodology CEM:3.1 revision 5.
[ETR]	TUVIT-TSZ-CC-9265-2026, Version 2, 20.05.2026, TÜV