Certificate

TÜVNORD
TÜV NORD CERT GmbH
eIDAS
QSCD
tuev-nord.de ID: 9805.26

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

SK ID Solutions AS
Pärnu avenue 141
11314 Tallinn, Estonia

to confirm that the product

Smart-ID SecureZone 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.

Certificate ID: 9805.26

valid from 2026-05-20 until 2031-05-19

To Certificate

Essen, 2026-05-20

Guillaume Tetu
Digitally signed by Guillaume Tetu
Date: 2026.05.26 09:44:51 +02'00'

Certification Body of TÜV NORD CERT GmbH

TÜV NORD CERT GmbH
Am TÜV 1, 45307 Essen
tuev-nord-cert.de

TÜV®

Certification program

The certification body of TÜV NORD CERT 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:

- Beschreibung des Zertifizierungsverfahrens eIDAS QSCD, D502-01F300 Rev. 00/02.26

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

Certification and evaluation reports

- Certification report: **TNCERT-eIDAS-9805-2026, Version 1, 20.05.2026, TN CERT**
- Evaluation report: **TUVIT-TSZ-CC-9265-2026, Version 2, 20.05.2026, TÜVIT**

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

Subject of evaluation

The Target of Evaluation (TOE) defined as Smart-ID SecureZone version 11.5.23 is the server-side software implementation of the Smart-ID system, developed to provide alternative solution for the digital signature creation.
In detail, the TOE is a software archive composed by source code and scripts as well as supporting binaries. It is a software component, which implements the server-side functions of the Threshold Signature Scheme Protocol (TSSP) to activate a signature. The TOE as well as the Guidance documentation are delivered using a secure file transfer system to the Smart-ID operator.
The TOE implements the following security functionality:

Identifier	Security functionalities and features
SF.Authentication	SF.Authentication authenticates users with different methods. It also locks the authentication procedure in case of consecutive unsuccessful authentication tries.
SF.AccessControl	SF.AccessControl ensures that all three main groups of users are only allowed to perform operations, which are intended to be able for their role. The three main groups are:

Identifier	Security functionalities and features
	1. Anonymous users, 2. Key pair owners (Signers), 3. Privileged users (Admins and CA).
SF.Audit	SF.Audit generates audit records of the important system events by using standard Java toolset.
SF.KeyGen	SF.KeyGen ensures the use of the Common Criteria HSM to perform the most of the key generation operations. In case the HSM does not support generation and management of particular key type, TOE is generating that by himself. 1. TOE implements the TSSP and generates the compound modulus of the key pair (D.SVD). 2. TOE uses the HSM to generate the regular RSA key pair (D.KTK). The private key will be encrypted by HSM. 3. TOE implements the Diffie-Hellman key agreement protocol (D.TEK). 4. TOE uses the HSM to generate the regular AES key (D.KWK). key will be encrypted by HSM. 5. The TOE uses the RNG provided by the HSM to generate the regular AES key (D.DEK).
SF.CryptoAlgorithms	SF.CryptoAlgorithms ensures the use of the Common Criteria certified HSM to perform most of the key usage operations. In cases the HSM doesn't support operations with the particular key type, TOE is implementing this by himself. 1. Computation of signatures, 2. Creation and verification of RSA signatures, 3. Encryption/decryption of JSON Web Encryption (JWE) messages for transmission and database storage.
SF.KeyZer	SF.KeyZer enforces the TOE to destroy cryptographic keys after they are no longer used.
SF.TrustedPath	SF.TrustedPath implements JSON Web Encryption (JWE) messages for the communication between the TOE and the Smart-ID App TSE.
SF.SecureChannel	SF.SecureChannel ensures that vendor-specific proprietary communication channel is used, when connecting with HSM or database, such as nCipher impath and PostgreSQL connections.

Table 1: TOE security services

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.

Validity period of the certificate

The validity period of the QSCD certificate is five years, provided that vulnerabilities assessments are carried out every two years.

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.

Further information

The evaluation was carried out in accordance with the provisions of the TÜV NORD CERT GmbH certification scheme. The conclusions of the testing body contained in the evaluation report are consistent with the evidence provided.

This certificate is not a general recommendation of the IT product by TÜV NORD CERT GmbH or any other organization that recognizes this certificate or has had influence on it. A guarantee for the IT product by TÜV NORD CERT GmbH or any other organization that recognizes this certificate or has had influence on it is neither included nor expressed.