ZERTIFIKAT ★ сертификат ★ CERTIFICATE ★ CERTIFICADO ★ 證明書 ★ CERTIFICAT

# CERTIFICATE

SRC Security Research & Consulting GmbH
Emil-Nolde-Straße 7
D-53113 Bonn
Germany

**confirms hereby, pursuant to**
**Article 29 (1) and Annex II of the Regulation (EU) No. 910/2014**
**that the**

Qualified Signature Creation Device
MaskTech eSign Applet Secora$^{TM}$ ID S v1.1

**fulfils the following referred Requirements of the Regulation (EU) No. 910/2014[1].**

Certificate is valid until

**31.12.2029**

SRC Certificate Registration Number

**SRC.00056.QSCD.12.2022**

This certificate is only valid with the certification report and under consideration of the restrictions listed therein.

Bonn, 6 December 2022

Gerd Cimiotti

SRC Security Research & Consulting GmbH is a Designated Body notified to the EU commission for the certification of qualified electronic signature creation devices to be conformant with the Regulation (EU) No. 910/2014.

[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 Directive1999/93/EC.

## Description of the Qualified Signature Creation Device (QSCD):

## 1. Product Name and Scope of Delivery

### 1.1 Product Name

Signature Creation Device MaskTech eSign Applet on Secora™ ID S v1.1 from MaskTech International GmbH.

The product is referred to in the following as „MaskTech eSign Applet Card“ for short.

### 1.2 Delivery

The „MaskTech eSign Applet Card“ is implemented as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. It can be configured as contactless only, contact only or dual interface by the personalization agent. „MaskTech eSign Applet Card“ is based on the hardware platform Infineon Security Controller IFX_CCI_000005 by Infineon Technologies AG including the firmware, symmetric crypto library (SCL) and asymmetric cryptographic library (ACL). The hardware is CC certified (BSI-DSZ-CC-1110-V5-2022) and provides protection against side channel attacks and fault attacks.

The smart card embedded software contains the operating system Java Card Platform Secora™ ID S v1.1 (SLJ52GxxyyyzS) [COS ST], which too is CC certified (NSCIB-CC-22-175887).

The „MaskTech eSign Applet Card“ consists of three applets. The MaskTech eSign Applet provides the QSCD functionality and will be in the following denoted as *eSign application*. The MaskTech Helper Applet provides functionality for Secure Messaging as well as buffer handling and the MaskTech PACE Applet provides functionality for the PACE protocol. In addition, the MaskTech TLV-Library provides functionality for TLV-handling during communication with the device.

The three applets are packaged in cap files and can be loaded onto the chips in three ways:

- The cap files are pre-loaded onto the chips by the IC manufacturer Infineon Technology AG. In this case, the cap files are transferred to Infineon Technologies AG using their proprietary certified delivery procedures.
- The applet loading is performed by MaskTech International GmbH.
- The applet loading is performed by a certified third party in which case the cap files are transferred via encrypted and signed email or via a certified proprietary delivery process provided by the receiver.

After the applets are loaded onto the chips, the pre-personalized electronic document along with the IC Identifier and the relevant guidance documents are securely delivered to the QSCD-provisioning service provider or a subject acting on behalf of the QSCD provisioning service provider. In the latter case, the delivery process is supervised by the QSCD-provisioning service provider.

During the preparation of the device, the QSCD-provisioning service provider or a subject acting on behalf of the QSCD-provisioning service provider performs the following tasks:

- Initialize the security functions in the device for the identification as QSCD, for the protected export of the SVD, and for the proof of this QSCD identity to external entities.
- Links the identity of the device as QSCD and the identity of the legitimate user as potential applicant for certificates for SVD generated by the device.
- Obtain information on the intended recipient of the device.
- Set the PUK and prepare information about the PUK for deliver to the legitimate user.
- In case of key import: The initialization of the device.
- Optionally: Generate a certificate for at least one SCD, with RSA or ECDSA key with key length of up to 2K or 4K bits (depending on configuration) and 521 bits, respectively.
- Optionally: Present certificate info to the QSCD.

Once the device is fully prepared by the QSCD-provisioning service provider, the QSCD-provisioning service provider delivers the device and the accompanying PUK value information to the legitimate user.

The authenticity and integrity of a card or an applet can be authenticated during personalization using the correct personalization key.

The authenticity and integrity of the applets / cards can be verified as follows:

The used Java Card Platform Secora™ ID S v1.1 (SLJ52GxxyyyzS) can be uniquely identified by the “GET TOE INFO” command. A successful authentication against the Global Platform Security Domain must be done before the command “GET TOE INFO”. The expected values are defined in the public security target of the operating system [COS ST], chapter 1.4.2 (see Table 1). The applet ID of the currently loaded cap file can be verified by personalizing the Helper applet or by selecting the Helper applet before completing the personalization following [AGD_eSign], chapter 8.3. This is only possible during personalization.

**Table 1: COS identification data**

| Component | Reference value |
|---|---|
| CC Identifier of underlying platform | IFX_CCI_000005 |
| Embedded OS version | 1442 |
| ACL version | 2.07.003 |

| | |
|---|---|
| SCL version | 2.04.002 |
| HSL version | 03.12.8812 |

## 1.3 Delivery Items

The scope of the delivery for the product consists of the following items:

**Table 2: Delivery items**

| No. | Delivery item | Description / Additional Information | Type | Delivery method |
|---|---|---|---|---|
| 1 | IFX Secure Smart Card Controller including its IC Dedicated Support Software embedded into cards | Hardware platform Infineon Security Controller IFX_CCI_000005<br>(Refer to the Certification Report BSI-DSZ-CC-1110-V5-2022) | HW / FW | The IC and the Embedded Software are providing self-protection mechanisms, ensuring confidentiality and integrity during delivery. The delivery does not need additional security measures and can be considered as normal transport. |
| 2 | Operating System | Embedded Software<br>IC Embedded Software<br>Java Card Platform<br>Secora™ ID S v1.1 (SLJ52GxxyyyzS) | SW | The software part of the product is implemented in the Flash Memory of the IC. |
| 3 | Applets | Applets provided by MaskTech packed in cap-files:<br>eSign Applet<br>Helper Applet<br>PACE Applet<br>TLV-Library | SW | The cap-files can be delivered in three ways:<br>- Pre-loaded onto the chip by the IC manufacturer Infinion Technologies AG using their proprietary verified delivery procedures<br>- Loaded onto the chip by MaskTech<br>- Transferred to a certified third party electronically using the certified delivery procedures of MaskTech International GmbH |

| No. | Delivery item | Description / Additional Information | Type | Delivery method |
|---|---|---|---|---|
| 4 | Associated guidance documentation | MASKTECH eSign Applet on SECORA™ ID S v1.1, User Manual, MASKTECH eSign v1.00 (0013h), Version 1.08, 08.09.2022, [AGD_eSign] | DOC | The guidance documents of the product can be downloaded by the customer from the MaskTech web site. The necessary access data are sent to the customer upon request via encrypted email. |

## 1.4 Manufacturer

Manufacturer of the product is MaskTech International GmbH, Nordostpark 45, D-90411 Nuernberg.

## 2. Functional Description

### 2.1 Functionality and Architecture

The „MaskTech eSign Applet Card“ is implemented as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. It can be configured as contactless only, contact only or dual interface by the personalization agent. The hardware of „MaskTech eSign Applet Card“ consists of Infineon Security Controller IFX_CCI_000005 including the firmware, symmetric crypto library (SCL) and asymmetric cryptographic library (ACL). The Infineon security controller has been evaluated and certified according to CC Version 3.1 (BSI-DSZ-CC-1110-V5-2022) and provides protection against side channel attacks and fault attacks. In addition, the hardware provides co-processors supporting cryptographic standards AES, RSA, EC, and 3DES.

The software consists of the operating system Java Card Platform Secora™ ID S v1.1 (SLJ52GxxyyyzS) as well as the *eSign application* for the generation of qualified signatures.

The Java Card Platform Secora™ ID S v1.1 (SLJ52GxxyyyzS) is an operating system compliant with Java Card Specifications (Classic Edition) version 3.0.5 ([JCAPI3], [JCRE3], [JCVM3]) and GlobalPlatform Specification v.2.3.1 ([GP v23], [GPv23 Amd D]) and the GlobalPlatform Card ID Configuration v1.0 [GP-ID] and is CC certified (NSCIB-CC-22-175887).

Moreover, the operating system provides among others the following functionality:

- Cryptographic ciphers (AES, TDES)
- Signature algorithms (ECDSA, RSA)
- Key agreement algorithms (ECDH, PACE)
- Key pair generation (EC, RSA)
- Message digest algorithms (SHA-1, SHA-2 family)
- Random number generation (PTG.3 according to [AIS 31])
- Secure channel SCP03 from [GPv23 Amd D]
- Content management provided by [GP v23]
- LDS-API according to [ICAO_9303]
- PACE API, a proprietary API for the PACE cryptographic protocol which is especially hardened against side channel attacks.

In summary „MaskTech eSign Applet Card“ consists of the following components:

- Infineon Security Controller IFX_CCI_000005 including symmetric crypto library (SCL), asymmetric cryptographic library (ACL) and dedicated firmware from Infineon Technologies AG,
- Card Operating System Java Card Platform Secora™ ID S v1.1 (SLJ52GxxyyyzS)

- Three applets:
  - MaskTech eSign Applet: provides the QSCD functionality
  - MaskTech Helper Applet: provides functionality for Secure Messaging as well as buffer handling
  - MaskTech PACE Applet: provides functionality for the PACE protocol
- MaskTech TLV-Library: provides functionality for TLV-handling during communication with the device (The device only makes use of the BERTLV and PrimitiveBERTLV classes from the TLV-Library to parse incoming data.)

The „MaskTech eSign Applet Card“ supports PACE for the identification and authentication of the user as the legitimate card holder, for the protection against tracking and eavesdropping and for the establishment of a trusted channel between terminal and card. Additionally, it supports chip authentication version 1 to proof the authenticity of the chip to the terminal and establish a trusted channel between the terminal and card, as well as terminal authentication version 1 to restrict the service provisions to authorized Signature Creation Applications (SCAs) and Certificate Generation Authorities (CGAs). Terminal authentication version 1 is optional.

As the device is a dual-interface product, there are various interface options of the „MaskTech eSign Applet Card“, namely contact, contactless or dual interface, which are decided and configured by the personalization agent during personalization. If the personalization agent choses to configure the device as contact only interface to have an easy access without PACE authentication when the device is in a secure environment (i.e. preparation environment, signing environment and management environment), the trusted channel communication is optional except for key import. To support key import, Chip Authentication must be enabled and used to establish a trusted channel. If the „MaskTech eSign Applet Card“ is configured as contactless only or dual interface by the personalization agent, each interaction with the device requires user authentication using the PACE protocol.

Before the *eSign application* can be used, it must be completed. The signature key can either be generated in the card or securely personalized into the card before the card is delivered. In the latter case the signature key is generated by the trust service provider (TSP) (or a commissioned third party). As part of this completion of the *eSign application*, the CAN and PUK are set in the card and optionally, the public key certificate is inserted. Once personalization is complete, it is not possible to change the programme code.

In order to be able to generate a signature with the completed *eSign application*, the legitimate user must authenticate himself against the RAD, which consists of one or more secrets stored on the chip. In the preparation phase CAN and PUK are set in the personalization step and delivered to the signatory. The RAD PIN and $\mathrm{PIN}_{\mathrm{QES}}$ are not set in the personalization step, i.e. the QSCD is in non-operational state, and the signatory must set the initial PINs to switch the QSCD into an operational state. To set the RAD, the signatory must use the command “Activate Set PIN”. The creation of a qualified electronic signature is additionally protected by the secret $\mathrm{PIN}_{\mathrm{QES}}$ (signature PIN), which is a password with a minimum length of 6 digits stored on the chip in the OwnerPIN object.

After the *eSign application* has been activated, „MaskTech eSign Applet Card“ may be used for generation of qualified electronic signatures. A successful authentication of the owner of the signature key with correct entry of the signature PIN is a prerequisite for the generation of a qualified electronic signature.

The generation of multiple qualified signatures is not supported by the „MaskTech eSign Applet Card“. After successful entry of the $\text{PIN}_{\text{QES}}$ only one qualified signature can be generated and a further signature cannot be generated without a new entry of the $\text{PIN}_{\text{QES}}$. The authentication state of the $\text{PIN}_{\text{QES}}$ is reset to „not verified“ after each qualified signature creation. For the generation of further signatures a new entry of the $\text{PIN}_{\text{QES}}$ is necessary.

The *eSign application* can be administrated by the owner of the signature key. The administration comprises the following functions:

- changing a PIN (after successful user authentication with the currently valid PIN),

- changing a PUK (after successful user authentication with the currently valid PIN),

- changing a $\text{PIN}_{\text{QES}}$ (after successful user authentication with the currently valid signature $\text{PIN}_{\text{QES}}$)

For access relevant to the signature application, the „MaskTech eSign Applet Card“ supports the use of secure messaging. For (mutual) authentication of the external world and the card as well as for establishing a secure communication channel, the authentication protocols Password Authentication Connection Establishment (PACE), Asymmetric Role Authentication or Proof of Authorisation, Internal Authentication and Mutual Authentication with/without issuance of session keys are supported. Access rights of the external world are verified within the scope of the authentications.

The security properties of „MaskTech eSign Applet Card“ are explained in more detail together with the description of the security functions.

The Java Card operating system allows the card manufacturer a range of configuration options. Before initialization, the card manufacturer has defined the configuration by creating the file system and specifying further data. The installation data for loading the file system are delivered by the card manufacturer to the initiator of the card. Confidentiality and integrity of the data as well as their authentic origin are ensured by cryptographic mechanisms.

The installation of the file system is done during the initialization of the chip (completion of the operating system code and loading of the file system) by the initializer. The installation of the file system can only take place after the initialization system has been authenticated against the card. The keys used for cryptographically securing the loading data are only known to the card manufacturer. In this sense one can speak of an end-to-end security between card manufacturer and chip. This prevents the loading of incorrectly changed initialization data. The „MaskTech eSign Applet Card“ does not support the subsequent introduction of further software. The initializer must take into account the initialization requirements described in the guidance documents.

„MaskTech eSign Applet Card“ supports the following cryptographic algorithms for the generation of signature key pairs as well as of qualified electronic signatures:

- Asymmetric RSA algorithm according to [PKCSv2.2] (cf. [RFC 8017]) with a key length of up to 2048 bit or 4069 bit depending on the configured RSA library (2K or 4K respectively).

- DSA based on elliptic curves (ECDSA) using the groups E(Fp) (cf. [TR-03111]) with key lengths of 224 – 521 bit.

- Random number generation based on a hybrid Physical True Random Number Generator (hybrid PTRNG) of the underlying hardware. The hybrid PTRNG is a random number generator with a PTG.3 classification according to [AIS 31], implementing a true physical random source. The random numbers are subjected to statistical tests during operation ("online tests"). These properties were tested within the scope of the CC evaluation of the hardware of Infineon (cf. [HW ST], [IFX_Cert]).

Furthermore the following algorithms are supported. They are not used for signature generation by the card and are therefore **not** subject to this certification.

- Asymmetric operations with RSA (key lengths from 512 to 2048 bits for RSA 2K library or from 512 to 4096 bits for RSA 4K library; cf. [PKCSv1.5], [PKCSv2.2]) for encryption/decryption.

- Asymmetric operations on the basis of elliptic curves (cf. [TR-03111]) for chip and terminal authentication.

- Hash function SHA-1 according to [FIPS 180-4], where SHA-1 is used only for derivation of symmetric session keys,

- Hash functions SHA-224, SHA-256, SHA-384 and SHA-512 according to [FIPS 180-4] used only for internal operations,

- Diffie-Hellman (ECDH) according to [TR-03110-1], [TR-03111] and key length of 192, 224, 256, 384, 512 (brainpool) and 521 (NIST) for authentication (PACE) and key agreement for the secure messaging channel.

- Symmetric Triple-DES algorithm according to NIST SP800-67 [SP800-67] with an effective key length of 112 bits (CBC mode, retail MAC according to [SP 800-38A], [ISO 9797-1]).

- Symmetric AES algorithm according to [FIPS 197] with an effective key length of 128, 192 or 256 bits (CBC mode, CMAC according to [SP 800-38A], [ISO 9797-1])

„MaskTech eSign Applet Card“ supports the ECC Brainpool curves P192r1 (only for authentication and PACE), P224r1, P256r1, P384r1 and P512r1 according to [RFC 5639] and NIST curves P-192 (only for authentication and PACE), P-224, P-256, P-384 and P-521 from the NIST curve family according to [FIPS 186-3], Appendix D.1.2.

„MaskTech eSign Applet Card“ was successfully evaluated with the Common Criteria in version 3.1 (cf. [Cert Report]). The assurance level is EAL 5+ with the augmentations ALC_DVS.2 and AVA_VAN.5.

Furthermore, the „MaskTech eSign Applet Card“ takes into account the Protection Profiles „Protection profiles for Secure signature creation device", Part 2: "Device with key generation", BSI-CC-PP-0059-2009-MA-02 [PP SSCD Part 2], Part 3: “Device with key import”, BSI-CC-PP-0075-2012-MA-01 [PP SSCD Part 3], Part 4: "Extension for device with key generation and trusted communication with certificate generation application", BSI-CC-PP-0071-2012-MA-01 [PP SSCD Part 4], Part 5: “Extension for device with key generation and trusted communication with signature creation application”, BSI-CC-PP-0072-2012-MA-01 [PP SSCD Part 5] and Part 6: “Extension for device with key import and trusted communication with signature creation application”, BSI-CC-PP-0076-2013-MA-01 [PP SSCD Part 6].

The evaluation and certification of the product was performed pursuant to Regulation (EU) No. 910/2014, Article 30 (3) a [Reg No. 910/2014] and the Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 [CID (EU) 2016/650] that lists the Protection Profiles to be used for the evaluation and certification of local qualified signature creation devices. The protection profile EN 419 211 is listed in the Commission Implementing Decision (EU) 2016/650.

Products certified to be conformant to the requirements laid down in Annex II of Regulation (EU) No. 910/2014 are published by the Commission in a list of certified qualified electronic signature creation devices [EU QSCD list] (cf. Regulation (EU) No. 910/2014, Article 31 (2)).

## 2.2 Security Functions and Security Properties of „MaskTech eSign Applet Card“

Among others „MaskTech eSign Applet Card“ provides the subsequently listed security functions and security properties. They are described in the security target [ST] and were verified in the evaluation.

### „Access Control“

„MaskTech eSign Applet Card“ uses a role based access control which distinguishes among others between the roles "Administrator" and "Signatory". Furthermore, the following security attributes are used:

- For an authenticated role: „SCD / SVD Management“ (values: „authorized“, „not authorized“)

- For the data object Signature Creation Data (SCD, the i.e. signature key): „SCD operational“ (values: „yes“, „no“) and „SCD identifier“ (arbitrary value)

The QSCD-provisioning service provider, who performs the process of activating the *eSign application* and who has special access rights for this purpose, acts in the role of an administrator. To use these rights, he must authenticate himself to the card and prove his access rights to the card.

A user authenticates himself to the „MaskTech eSign Applet Card“ by knowing a secret key as an administrator (e.g. initializer, personalizer or card management system) or by entering the PIN or $\text{PIN}_{\text{QES}}$ as a signer.

In the usage phase, the application of a secure channel is supported by the „MaskTech eSign Applet Card“ both when using the contact and contactless interface. When using the contact interface, the connection between the „MaskTech eSign Applet Card“ and the signature application can optionally be cryptographically secured. The contactless interface can only be used with a secure channel.

The session keys can be negotiated by different methods. The „MaskTech eSign Applet Card“ provides both symmetric and asymmetric authentication protocols. In summary, the following authentication methods are used for mutual authentication and to establish a secure communication channel:

- **PACE protocol** for mutual authentication and for establishing a secure channel to protect the over the air communication between card and terminal.

- **Chip authentication** to establish a trusted channel between the terminal and the card (only required if key import shall be supported in contact only configuration).

- **Terminal authentication** (optional) to restrict service provisions to authorized Signature Creation Applications (SCAs) and Certificate Generation Authorities (CGAs).

Furthermore, the access control is implemented using access conditions, which are stored as security attributes in „MaskTech eSign Applet Card“. Access to a DF, an EF, a key or a PIN is only allowed, if the corresponding access conditions are satisfied. To this end, the security function checks before command execution, if especially the specific requirements concerning user authentication and secure communication are fulfilled.

Among others the following rules hold:

- The generation of the Signature Creation Data (SCD) and the Signature Verification Data (SVD) can only be performed via a trusted channel and only if the security attribute “SCD/SVD Management” has the value “authorized”.
- The PUK protection may only be set during personalization.
- Due to well defined access rules, sensitive data such as signature key, card PIN and signature PIN cannot be read out using the commands of the *eSign application*.
- The initial setting of a signature PIN by the designated owner of the signature key is only possible in the initial state (for the data object SCD the attribute “SCD operational” has the value “no”, i.e. especially the signature key is not usable) of the „MaskTech eSign Applet Card“ and after a successful user authentication.
- The change of an existing signature PIN to a new signature PIN may only be performed after a successful user authentication with the old signature PIN.

- Only the owner of the signature key can generate signatures. For this, a previous successful user authentication is required.

### „Password Authenticated Connection Establishment (PACE) Protocol“

„MaskTech eSign Applet Card“ supports the execution of the Password Authenticated Connection Establishment (PACE) protocol. The PACE protocol is a password based protocol for key agreement using the Diffie-Hellman algorithm (DH). It includes the proof, that „MaskTech eSign Applet Card“ and terminal have the same start value (value stored in the card and transmitted to the terminal by the card owner) and establishes a secure channel between „MaskTech eSign Applet Card“ and terminal to protect the contactless interface (air communication interface). In addition, a binding to the cardholder is achieved by using specific secrets as start values.

The successful execution of the PACE protocol as a necessary condition for the use of „MaskTech eSign Applet Card“ supports the owner of the signature key in controlling the sig-nature creation device when using the card for communication over the air. Here, the CAN is printed on the card body and therefore is no secret for anyone who has physical access to „MaskTech eSign Applet Card“. By inserting the CAN, the cardholder starts the communication with the contactless card. This procedure is an equivalent to the insertion of a contact card into a reader and makes the uncontrolled communication with „MaskTech eSign Applet Card“ more difficult.

### „Chip Authentication“

„MaskTech eSign Applet Card“ supports the execution of a chip authentication to proof the authenticity of the chip and secure messaging based on (mutual) authentication with elliptic curves and 3DES/AES according to [TR-03110-1] (cf. [AGD_eSign]).

The protocol for internal authentication is based on authenticated key agreement. For this, the „MaskTech eSign Applet Card“ makes use of a private/public key pair in the course of chip authentication. The private key is stored on the card. The corresponding public key must be made available to the terminal somehow. For example, this public key can be stored on the „MaskTech eSign Applet Card“. Generally, it is recommended to authenticate this public key e.g. by verifying an additional document signer signature stored on the card by the personalizer.

In the contact only configuration, chip authentication must be enabled to support key import. For the contactless / dual interface configuration, chip authentication is mandatory.

### „Terminal Authentication“

„MaskTech eSign Applet Card“ supports the execution of a mutual terminal authentication with the establishing of a secure channel with asymmetric cryptography based on elliptic curves according to [TR-03110-1].

The protocols for external and internal authentication use challenge-and-response protocols on the basis of suitable random numbers. Within the protocols, Country Verifying Certificate Authority (CVCA) certificates are used to proof the authenticity of public keys. The CVCA certificate is stored on the card during personalization. The CVCA then generates signed Document Verifier (DV) certificates for specified parties. During terminal authentication the personalized CVCA certificate is used to verify the certificate chain and thus, assigned access rights can be verified.

Terminal authentication is only supported for contactless configurations and is optional.

**„Administration of the MaskTech eSign Applet Card or the *eSign application***

This security function is used within the processes of initialization and personalization of the „MaskTech eSign Applet Card". For initialization and personalization of the „MaskTech eSign Applet Card", the related requirements defined by the manufacturer have to be considered (cf. 3.2).

In particular, the security function enforces the following rules:

- Initialization and personalization of the „MaskTech eSign Applet Card" can only be performed after a successful authentication with a secret key.
- At the end of the initialization and personalization phase, the access for a further initialization or personalization is blocked.
- The initialization with the loading of the initialization scripts and the subsequent checking of the loaded data is carried out according to the guidance documentation [AGD_eSign]. The loading of the initialization script is protected by security measures to ensure security and confidentiality.

**„Processes with PIN based Authentication to generate Qualified Signatures (Signature PIN)"**

The security function comprises the PIN based user authentication in the role „signer”. It may be used only after successful setting of the signature PIN. User authentication is performed by comparing a signature PIN provided by the user with the reference value (RAD) secretly stored in „MaskTech eSign Applet Card" (in the *eSign application*).

After a successful, finalized personalization, the „MaskTech eSign Applet Card" has a PUK (eight characters). Before signature generation, a signature PIN must be set with a minimum length of six characters (cf. [ST], table 3.1). For this, the designated owner of the signature key must authenticate himself to the „MaskTech eSign Applet Card" by a successful entry of the PUK. The generation of a signature after entry of the PUK is not possible. This is enforced by the „MaskTech eSign Applet Card".

The signature PIN has a PIN Try Counter (PTC) with the initial value three set during initialization, which is decremented by one after each wrong PIN entry. Thus, after repeated entries of a wrong PIN, the PTC is zero and the signature PIN is blocked. In this state, neither a further verification of a signature PIN can be performed, nor a qualified digital signature can be generated. After a successful entry of the signature PIN, the PTC is set to its initial value three provided that the signature PIN is not blocked.

The PTC of a blocked signature PIN may be reset by use of a resetting code (PUK). The „MaskTech eSign Applet Card" supports resetting codes with a minimum length of eight characters (cf. [ST], table 3.1). The resetting code can be used up to ten times. After entering the resetting code a maximum of ten times (incorrect or correct), it can no longer be used and it is no longer possible to reset a blocked signature PIN.

For the PIN reset, the command RESET RETRY COUNTER has to be used. With this command, a simultaneous change of a signature PIN is not possible. The security status of a signature PIN is not set, i.e. the reset of a blocked signature PIN does not enable the generation of a qualified signature without a preceding verification of the signature PIN.

A signature PIN can be changed by the owner of the signature key. To this end, he must authenticate himself towards „MaskTech eSign Applet Card“ by successfully inserting the currently valid signature PIN. Thus, changing a signature PIN to a new signature PIN is only possible after a successful user authentication using the currently valid signature PIN (command CHANGE REFERENCE DATA with old and new PIN).

After successful user authentication, a maximum of one qualified signature can be generated. Then, the PIN must be successfully entered again to generate signatures. This is controlled by the „MaskTech eSign Applet Card“.

**„Integrity of Stored Data“**

This security function shall guarantee the integrity of stored data. This concerns all DFs, EFs as well as safety-critical data in the RAM that are used for the generation of qualified signatures. This especially includes the signing key and the signature verification key as well as the reference value for verification of the signature PIN.

The operating system guarantees the integrity of stored data using a check value. When accessing a data object, this value is computed and compared to the value that has been generated and stored during storage of the data object. If both values differ, the corresponding data object will not be processed and the current command will abort.

**„Secure Data Exchange“**

„MaskTech eSign Applet Card“ supports the encrypted and integrity protected data exchange with the external world based on Secure Messaging according to the ISO Standard [ISO 7816-4] or the requirements defined in the specification of the card operating system according to [COS ST].

For this purpose, symmetric keys which have been agreed by a mutual authentication (e.g. PACE, chip authentication and terminal authentication) with the external world are employed.

**„Memory Processing“**

„MaskTech eSign Applet Card“ ensures, that safety-critical information (e.g. signature key, PIN) are removed with the deallocation of memory. This includes all temporary and permanent parts of the memory that store safety-critical data. For a recycling, these parts of the memory are overwritten.

### „Protection against Error Situations in Hardware and Software“

This security function shall guarantee a secure operation state in case of an error in the hardware or in the software. For instance, this includes the following error situations and attacks:

- inconsistencies when generating signatures and
- fault injection attacks.

If „MaskTech eSign Applet Card“ detects an error situation, it transits to a secure operating state. Then at least all processes are aborted that are related to the error situation. In serious error situations „MaskTech eSign Applet Card“ closes the session.

### „Resistance against Side Channel Attacks“

„MaskTech eSign Applet Card“ provides appropriate mechanisms implemented in hardware and software to resist side channel attacks as

- simple power analysis (SPA),
- differential power analysis (DPA),
- differential fault analysis (DFA),
- timing analysis (TA) and
- simple electromagnetic analysis (SEMA).

All safety-critical operations of „MaskTech eSign Applet Card“, especially the cryptographic functions, are protected by these mechanisms. Information about power consumption, electromagnetic emanation and execution times for commands do not allow to draw conclusions about safety-critical data as a signature key or a signature PIN.

This security function is active in all operation phases of „MaskTech eSign Applet Card“ (initialization, personalization and use).

### „Self-Test“

The operating system provides several kinds of self-tests which run during initial start-up to demonstrate the correct operation of the devices security functionality.

Furthermore, the integrity of stored data is verified during operation phase. This is described in the security function „Integrity of Stored Data”.

### „Cryptographic Algorithms“

This security function of „MaskTech eSign Applet Card“ provides the cryptographic functions. It is based on the cryptographic functions of the evaluated and certified semiconductor and its dedicated software.

„MaskTech eSign Applet Card“ supports the algorithms listed in chapter 2.1.

**„Generation of Key Pairs“**

„MaskTech eSign Applet Card“ supports the generation of RSA and ECDSA key pairs in the card for generating qualified signatures with a length up to 2048 bits or up to 4096 bits (depending on the configured RSA library of 2K or 4K respectively) for RSA keys and 224-521 bits for ECDSA keys.

The security function guarantees that, among others, the following requirements are fulfilled:

- RSA keys are generated with a length of up to 2048 bits (for configuration of 2K RSA library) or up to 4096 bits (for configuration with 4K RSA library). The acceptability deadline for the legacy use of a modulus of size above 1900 bits, but less than 3000 bits, is set to 31 December 2025 (cf. [SOG-IS], chapter 4.1). Keys below 1900 bits are not accepted anymore.

- The RSA key generation on board fulfils the requirements according to [SOG-IS], chapter 7.3 related to the distance of the two primes with $|p - q| \geq 2^{n/2-100}$. In addition, the size of d is close to the size of n by $d > 2^{n/2}$.

- ECDSA keys with E(Fp) are generated with a length of 224-521 bits. The supported curves ECC Brainpool P256r1, P384r1 and P512r1 according to [RFC 5639] and NIST P-256, P-384 and P-521 from the NIST curve family according to [FIPS 186-3], Appendix D.1.2 are recommended (cf. [SOG-IS], chapter 4.3). ECC curves Brainpool P224r1 and NIST P-224 are supported but not recommended by SOG-IS (cf. [SOG-IS], chapter 4.3).

- The generation of RSA keys is based on the Physical True Random Number Generator (PTRNG) of the underlying hardware with a PTG.3 classification pursuant to [AIS 31]. In addition, a pseudo random number generator (PRNG) of the underlying hardware (Deterministic Random Number Generator, DRG.3, cf. [HW ST]) is used for prime number tests.

- The key generation guarantees that the signature key cannot be derived from the signature verification key.

- After key generation the operating system verifies, if the signature key and the signature verification key are conform. Only valid key pairs are admitted.

- The key generation is resistant against side channel attacks.

The signature key pairs are generated in the card during initialization or personalization of the *eSign application*. Additionally, the life cycle of the „MaskTech eSign Applet Card“ allows the generation after the delivery to the signatory. „MaskTech eSign Applet Card“ fulfils the security requirements for the generation of RSA or ECDSA key pairs as listed above.

Alternatively, the signature key can be inserted into the card via a secure channel during personalization. According to [AGD_eSign], personalization must take place in a secure environment.

The designated signature key holder is not directly involved in the key generation process.

### „Generation of Qualified Signatures“

„MaskTech eSign Applet Card“ supports the generation of qualified electronic signatures with RSA and ECDSA signature keys with lengths of up to 2048 bits or up to 4096 bits (depending on the configured RSA library of 2K or 4K, respectively) for RSA keys and 224-521  bits for ECDSA keys. The security function has the following properties:

- Receipt of (already hashed) data (data to be signed, DTBS) to generate qualified digital signatures.
- Generation of RSA signatures with PSS and PKCS1-v1_5 according to chapter 8 and 9 of [PKCSv2.2] with a key length of 2048 bits (for configuration of 2K RSA library) or up to 4096 bits (for configuration with 4K RSA library).
- Computation of ECDSA signatures according to [TR-03111] with key lengths of 224-521 bits.
- The hybrid Physical True Random Number Generator (hybrid PTRNG) of the underlying hardware with a PTG.3 classification pursuant to [AIS 31] is used to generate random numbers for the generation of ECDSA signatures.
- The key generation is resistant against side channel attacks.
- The signature is generated in a manner that the signature key cannot be derived from the generated signature and that during signature generation no information about the signature key is revealed.
- A signature can only be generated, if the user has authenticated himself successfully with a signature PIN (command VERIFY) and if the security attribute „SCD operational“ of the data object SCD has the value „yes“.
- Using the contactless interface the card command for the generation of a qualified signature (PSO : Compute Digital Signature) must be sent to the card in a secure channel (established with PACE, optionally terminal authentication and chip authentication).

## 3. Fulfilment of the relevant Requirements of Regulation (EU) No. 910/2014

### 3.1 Fulfilled Requirements

The product fulfils the following requirements pursuant to the Regulation (EU) No. 910/2014.

**Table 3: Fulfilment of the requirements of the Regulation (EU) No. 910/2014**

| Reference | Requirement / Description / Result |
|---|---|
| **Article 29** | **Requirements for qualified electronic signature creation devices** |
| (1) | **Requirement**<br>Qualified electronic signature creation devices shall meet the requirements laid down in Annex II. |
| (2) | **Requirement**<br>The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48 (2). |
| **Annex II** | **Requirements for qualified electronic signature creation devices** |
| 1. | **Requirement**<br>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. | **Requirement**<br>Qualified electronic signature creation devices shall not alter the |

| Reference | Requirement / Description / Result |
|---|---|
| | data to be signed or prevent such data from being presented to the signatory prior to signing. |

Requirements Annex II, points 3, 4 (a) and 4 (b) concerning qualified trust service providers managing electronic signature creation data on behalf of the signatory are not relevant for the product.

## 3.2 Conditions of Use

**Requirements for the Responsible Initialization Party**

- The initialization data provided by MaskTech Intrenational GmbH (file system and further parameters) must be treated in a secure manner.
- Data integrity and data authenticity must be ensured during handling of the initialization data.
- The requirements of the card manufacturer to the initialization according to [AGD_eSign] must be taken into consideration.

**Requirements for the Responsible Personalization Party**

- The personalization party must ensure that the personalization data (especially of the *eSign application*) are treated in a secure way. The personalization data must be protected with respect to integrity, authenticity and confidentiality.
- The card manufacturer’s requirements to the personalization according to [AGD_eSign] must be adhered to.

**Requirements for the TSP**

- The TSP must ensure that the validity end date (attribute not after) of issued certificates for RSA keys does not exceed the suitability of RSA with a key length of 2048 bits. Currently, this is 31.12.2025.
- The TSP must ensure that the key length as implicitly chosen by him during key generation is appropriate from the beginning of key generation until the expiration date of the qualified certificate. Here the current version of [SOG-IS] must be considered.
- The TSP must ensure that after December 31, 2025, only 4K RSA library is configured.
- If the TSP distributes a product to generate qualified digital signatures with a product name that differs from the product name in the designation, then the TSP must point out the actual designated product in the documentation for the distributed product.
- Programs which a TSP provides to his clients for the transmission of reference data to „MaskTech eSign Applet Card“ (i.e. which are used by the owner of the signature key to set or change his card PIN or signature PIN)

must be configured such that reference data are inserted via the keyboard of the smart card reader as a default. In case that the program optionally allows to deactivate the keyboard of the smart card reader and to activate the keyboard of the PC, the program must output a warning note concerning a possible loss of security when changing the input mode.

**Requirements for the Owner of the Signature Key resp. for the Card Owner**

- The owner of the signature key must verify that the 8 digits PUK is still valid by setting a new signature PIN chosen by himself with a length of at least six digits. If the PUK is not valid the owner of the signature key must contact the issuing TSP.
- The owner of the signature key must treat the chosen signature PIN as confidential. The owner of the signature key must not confide his signature PIN and the resetting code to anybody and must keep it in a safe place.
- The owner of the signature key must change his signature PIN periodically.
- The owner of the signature key must use and keep „MaskTech eSign Applet Card“ such that misuse and manipulation are prevented.

**Requirements for the Manufacturer of Signature Application Components**

- The manufacturer of a signature application component must respect the interfaces of the smart card operating system [COS ST] as well as of the *eSign application* in an appropriate manner.
- When generating a digital signature on a hash value that has been computed by the external world and transmitted to the card, it must be guaranteed that the signature application component has chosen an appropriate hash function.
- The manufacturer of a signature application component used for the generation of qualified electronic signatures (Signature Creation Application, SCA) should consider the instructions for terminal developers pursuant to the Operational Guidance, [AGD_eSign].

## 3.3 Cryptographic Algorithms and Parameters

For the generation of digital signatures, „MaskTech eSign Applet Card“ provides RSA according to [PKCSv2.2] and ECDSA based on groups $E(F_p)$ according to [TR-03111]. Key lengths of up to 2048 bits or up to 4096 bits (depending on the configured RSA library of 2K or 4K respectively) for RSA and 224 – 521 bits for ECDSA with the ECC Brainpool curves P224r1, P256r1, P384r1 and P512r1 according to [RFC 5639] and NIST curves P-224, P-256, P-384 and P-521 from the NIST curve family according to [FIPS 186-3], Appendix D.1.2 are supported. For RSA signatures PSS and PKCS1-v1_5 according to chapter 8 and 9 of [PKCSv2.2] are supported as signature formats. Signatures are only generated with hash values that have been computed by the external world.

Random number generation based on a hybrid random number generator (hybrid PTRNG) of the underlying hardware is supported. The hybrid PTRNG of the underlying hardware from Infineon Technologies is a random number generator with a PTG.3 classification according to [AIS 31]. The random numbers are subjected to statistical tests during operation ("on line tests"). These properties were proven in the CC evaluation of Infineon's hardware (cf. [HW ST], [IFX_Cert]).

The cryptographic algorithms used by the product „MaskTech eSign Applet Card“ are classified by the algorithm catalogue SOG-IS [SOG-IS] as follows.

Among others, [SOG-IS] lists the following requirements for RSA:

- Legacy RSA: The acceptability deadline for the legacy use of a modulus of size above 1900 bits, but less than 3000 bits, is set to **31 December 2025**.
- RSA with modulus of size above 3000 bits, recommended.
- RSA PCKS#1_v1.5, legacy, acceptability deadline is **31 December 2027**
- RSA PSS (PKCS #1, v2.2), recommended.

Among others, [SOG-IS] lists the following elliptic curves:

- Brainpool Curve Family [RFC 5639] with brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, recommended
- NIST P-256, P-384, P-521, recommended

Recommended mechanisms fully reflect the state of the art in cryptography.

- The use of **ECDSA** with the parameters chosen by „MaskTech eSign Applet Card“ may only be used with a key length of 256 bits and above as recommended by the SOG-IS catalogue [SOG-IS].
- RSA signatures with the parameters chosen by „MaskTech eSign Applet Card“ may only be used until **31 December 2025** for the configuration of 2K RSA library.
- The use of RSA with parameters chosen by „MaskTech eSign Applet Card“ is not restricted by the algorithm catalogue SOG-IS [SOG-IS] if the 4K RSA library is configured.
- The TSP must ensure that in every case the validity end date (attribute not after) of issued certificates for RSA keys does not exceed the suitability of RSA with a key length of 2048 bits.
- In addition, RSA PCKS#1_v1.5 may only be used until **31 December 2027** regardless of the key length.

This certification of the „MaskTech eSign Applet Card“ is therefore valid until **31.12.2029**.

However, the validity may be extended if there are no impediments to the security of the products or the algorithms and parameters at this time, or shortened if new findings regarding the suitability of the algorithms are published in the algorithm catalogue SOG-IS [SOG-IS].

### 3.4 Assurance Level and Attack Potential

The product MaskTech eSign Applet on Secora™ ID S v1.1 was evaluated successfully according to the Common Criteria (CC) Version 3.1 with an assurance level **EAL 5+** (EAL 5 with augmentation ALC_DVS.2 and AVA_VAN.5).

The evaluation was performed against a **high** attack potential (augmentation AVA_VAN.5).

The underlying card operating system Java Card Platform Secora™ ID S v1.1 (SLJ52GxxyyyzS) was successfully evaluated according to Common Criteria (CC) Version 3.1 with assurance level EAL6 augmented ALC_FLR.1. The evaluation was performed against a **high** attack potential.

Neatherlands security certificate NSCIB-CC-22-175887 of 30. August 2022 is available for this.

For the evaluation of „MaskTech eSign Applet Card“ the protection profiles „Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation“, EN 419211-2:2013, [PP SSCD Part 2] and „Protection Profiles for Secure Signature Creation Device – Part 4: Extension for device with key generation and trusted communication with certificate generation application“, EN 419211-4:2013, BSI-CC-PP-0071-2012-MA-01, [PP SSCD Part 4], as well as „Protection profiles for Secure signature creation device – Part 3: Device with key import, Information Society Standardization System CEN/ISSS, EN419211-3:2013“ [PP SSCD Part 3], “Protection profiles for Secure signature creation device–Part 5: Extension for device with key generation and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN419211-5:2013” [PP SSCD Part 5] and “Protection profiles for Secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN419211-6:2014” [PP SSCD Part 6] were used (cf. [Cert Report]). So the requirements laid down in Regulation (EU) No. 910/2014 Article 30 (3) a as well as the Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 are fulfilled.

The evaluation was performed as a so-called composition evaluation, which takes into account the evaluation results of the CC evaluation of the Infineon Security Controller IFX_CCI_000005 from Infineon Technologies AG. This evaluation was performed with an assurance level **EAL 6+** (EAL 6 with augmentation ALC_FLR.1). The evaluation was performed against a **high** attack potential.

The semiconductor is listed under the Certification ID BSI-DSZ-CC-1110-V5-2022.

## 4. References

[Reg No. 910/2014] 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

[CID (EU) 2016/650] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[EU QSCD list] Compilation of: Member States' notifications on: Designated Bodies under Article 30 (2) and 39 (2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31 (1)-(2), and Certified Qualified Seal Creation Devices under Article 39 (3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51 (1) of Regulation 910/2014

[AIS 31] Anwendungshinweise und Interpretationen zum Schema, AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013

[Cert Report] TÜV Rheinland Nederland B.V., Certification Report, MaskTech eSign Applet on Secora™ ID S v1.1, Version 1, 18.10.2022, Report number NSCIB-CC-0299278-CR

[FIPS 180-4] Federal Information Processing Standards Publication FIPS PUB 180-4, Specifications for the Secure Hash Standard (SHS), March 2012

[FIPS 186-3] NIST: FIPS Publication 186-3: Digital Signature Standard (DSS), 2009.

[FIPS 197] NIST: FIPS Publication 197: Specification for the Advanced Encryption Standard (AES), 26. November 2001

[HW ST] Common Criteria Public Security Target, EAL6 / EAL6+, IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h, H13 , Resistance to attackers with HIGH attack potential, Revision 2.0, 2022-03-28, Infineon Technologies AG

[IFX_Cert] Certification Report, BSI-DSZ-CC-1110-V5-2022 for Infineon Security Controller IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies

AG, Bundesamt für Sicherheit in der Informationstechnik (BSI), Certification Report v1.0, 29. April 2022

[ISO 7816-4] ISO/IEC 7816-4: Integrated circuit(s) cards with contacts. Part 4: Interindustry commands for interchange, ISO/IEC 7816-4, First edition, September 1.1995

[ISO 9797-1] ISO/IEC 9797-1 Message Authentication Codes (MACs), ISO, 2011-03

[PKCSv2.2] PKCS #1 v2.2: RSA Cryptography Standard, RSA Laboratories, October 27, 2012

[PKCSv1.5] PKCS #1 v2.2: RSA Cryptography Standard, RSA Laboratories, November 1993

[PP SSCD Part 2] Protection Profiles for Secure Signature Creation Device - Part 2: De-vice with key generation, EN 419211-2:2013, Certified by Bundesamt für Sicherheit in der Informationstechnik under BSI-CC-PP-0059-2009-MA-02, 2016-06

[PP SSCD Part 3] Protection profiles for Secure signature creation device – Part 3: Device with key import, Information Society Standardization System CEN/ISSS, EN419211-3:2013, BSI-CC-PP-0075-2012-MA-01, 2016-06-30

[PP SSCD Part 4] Protection Profiles for Secure Signature Creation Device - Part 4: Extension for device with key generation and trusted communication with certificate generation application', EN 419211-4:2013, BSI-CC-PP-0071-2012-MA-01, 2016-06-30

[PP SSCD Part 5] Protection profiles for Secure signature creation device – Part5: Extension for device with key generation and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN419211-5:2013, BSI-CC-PP-0072-2012-MA-01, 2016-06-30

[PP SSCD Part 6] Protection profiles for Secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, Information Society Standardization System CEN/ISSS, EN419211-6:2014, BSI-CC-PP-0076-2013-MA-01, 2016-06-30

[RFC 5639] RFC 5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter, Johannes Merkle, Internet Engineering Task Force (IETF), 2010-03

[RFC 8017] RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2, K. Moriarty (Ed.), B. Kaliski, J. Johnson, and A. Rusch, 2016-11

[SOG-IS] SOG-IS Crypto Working Group; SOG-IS Crypto Evaluation Scheme; Agreed Cryptographic Mechanisms; Version 1.2 January 2020

[SP 800-38A] NIST: Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001

[SP800-67] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67, Revised January 2012, National Institute of Standards and Technology, 2012-01

[ST] Security Target Common Criteria Documents – MaskTech eSign Applet on Secora$^{TM}$ ID S v1.1, MaskTech International GmbH, Version 1.2

[COS ST] SECORA™ ID S v1.1 (SLJ52GxxyyyzS) – Security Target. Revision 2.1. NSCIB-CC-175887_3-stv2.1. Infineon Technologies AG. Aug. 2022

[AGD_eSign] MaskTech eSign Applet on SECORA\tm ID S v1.1, User Manual, MaskTech eSign v1.00 (0013h), version 1.08, 2022-09-08

[GP-ID] GlobalPlatform Card, ID Configuration, Version 1.0

[GP v23] GlobalPlatform Card Specification v2.3.1

[GPv23 Amd D] GlobalPlatform Technology - Secure Channel Protocol ’03’ - Card Speification v2.3 - Amendment D - Version 1.2, GlobalPlatform, April 2020

[ICAO_9303] ICAO Doc 9303, Machine Readable Travel Documents, ICAO, 2021

[JCAPI3] Java Card API version 3.0.5

[JCRE3] Java Card RTE version 3.0.5

[JCVM3] Java Card VM version 3.0.5

[TR-03110-1] BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, Technical Guideline, Feb. 2015

[TR-03111] BSI: Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC), Version 1.11, 17. April 2009

**End of certification report**