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
MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11)

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

Certificate is valid until

10.11.2029

SRC Certificate Registration Number

SRC.00063.QSCD.11.2024

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

Bonn, 11. November 2024

Gerd Cimiotti / Markus Schierack

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; last amended by Regulation No. 2024/1183.

Description of the Qualified Signature Creation Device (QSCD):

1. Product Name and Scope of Delivery

1.1 Product Name

Signature Creation Device MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11) from MaskTech International GmbH.

The product is referred to in the following as „MTCOS Pro 2.6 QSCD/SSCD / IFX" for short.

1.2 Delivery

The „MTCOS Pro 2.6 QSCD/SSCD / IFX" can be issued as contactless, contact based or as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. „MTCOS Pro 2.6 QSCD/SSCD / IFX" is based on the hardware platform SLC37GDA512 (V11) by Infineon Technologies AG with IC Dedicated Software and Crypto Library. The IC integrates functionality for symmetric encryption and a Public Key Crypto Coprocessor (Crypto@2304T) to support the implementation of asymmetric cryptographic algorithms. The hardware is CC certified (BSI-DSZ-CC-1107-V5-2024) and provides protection against side channel attacks and other attacks, e.g. fault attacks.

The smart card embedded software contains the operating system MTCOS Pro V2.6 and the application that provides the QSCD functionality which will be in the following denoted as *QSCD/SSCD application*. The product uses three derivatives with sales code (standard module "SLC37GDA512", coil on module "SLC37GDA512A2" and customer specific module "SLC37GDA512AA" variant) of SLC37GDA512 (V11), which differ only in the antenna capacity (input capacitance of the RF interface) of the module. Furthermore, two of them provide Very High Bit Rate (VHBR) support. However, these differences are not security relevant, thus all derivatives are taken as one configuration.

The product is provided in four configurations differing in

- Terminal Authentication Version 1 for the communication between the product and the signature generation application (SCA) or the certificate generation application (CGA), respectively, as well as for key import.

- Inclusion of an additional decryption key which is beyond the scope of this certification.

Thus, the following product configurations are available:

- SSCD-Std: Standard Configuration

- SSCD-TA: Standard Configuration with additional Terminal Authentication

- SSCD-DEC: Standard Configuration with an additional RSA key for decryption

- SSCD-DEC-TA: Standard Configuration with an additional RSA key for decryption and Terminal Authentication

The configurations SSCD-TA and SSEC-DEC-TA support key import. The selection of the layout and all configuration operations are performed before delivery to the signatory. The configuration of the initialised card can be retrieved during personalisation by reading the project-id (EF.PROJID) from the card. Project identifications are defined in [AGD], section 3.4. After personalisation, the file is rendered unusable (due to possible tracking of the ePassport), the configuration is then revealed by the available functionality.

Manufacturing of the chip is performed by Infineon Technologies AG who also writes the embedded software and deactivates the Flash Loader. The initialisation and / or pre-personalisation step is conducted by MaskTech International GmbH, one of the contracted service providers or Infineon Technologies AG. In the initialisation step the chip is configured, the MF is created, and the personalisation keys are written. In the pre-personalisation step, the *QSCD/SSCD application* including all files is created.

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:

- Initialise 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: Generation of the SCD/SVD pair and loading the SCD into the QSCD.
- Optionally: Generate a certificate for at least one SCD, with RSA or ECDSA key, 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.

Identification of the certified Product

For the Personalisation Agent to be able to check the correct delivery visually, a delivery note together with the hardware stating the product type and certification reference number is provided.

Further checks by the Personalisation Agent can be done as following:

- The labelling of the pre-personalised chip,
- the correct working of the personalisation key (EF.PERS),

- the product identifier stored in EF.PROJID; unless it has been changed along with the production keys by the Initialisation/Pre-personalisation Agent, it must be:

Table 1: Product identifier in EF.PROJID

Configuration	Product Identifier
MRTD-LayoutA-SSCD-Std	b80aca3c631034b2
MRTD-LayoutFlex-SSCD-Std	0ce4f789fd56b78f
MRTD-LayoutFlex-SSCD-TA	684a4bae8c4d7d37
MRTD-LayoutFlex-SSCD-DEC-DUALUSE	34d959a8a360a356
MRTD-LayoutFlex-SSCD-DEC-TA-DUALUSE	d87c332a00a28180

- the option byte of the ROM-key identifier that can be retrieved by the GET CHIP INFORMATION command
  - Option byte (DO E0 -> A1h -> 85h); the first nibble of the option byte must be a 'C'.
  - ROM-key identifier (DO E0 -> A1h -> 86h); the first byte has the same value as the option byte; the first nibble of the option byte must be a 'C'.

In addition, the authenticity and integrity of the cards can be verified as follows:

The commands "GET CHIP ID" and "GET CHIP INFORMATION" allow the identification of „MTCOS Pro 2.6 QSCD/SSCD / IFX". While "GET CHIP ID" returns the ten byte serial number, "GET CHIP INFORMATION" returns the chip identifier respectively additional information about the platform, the operating system and patch level. Whether the chip contains the correct file system layout can be verified by checking the product identifier stored in the file EF.PROJID (see [AGD], section 3.4).

For the certified version of MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11), the manufacturer provides specific values to the operating system parameters (Tag A1) „Manufacturer", „OS Identifier", „OS Version" and „Build Date" as well as "Version" and "Build Date" of the last patch level (Tag A2). For the hardware the parameters (Tag A0) „Manufacturer" and „Chip identifier" are provided. These values can be read from the card during production with the command „GET CHIP INFORMATION" according to [AGD], Annex G.

The following table describes the operating system parameters for the evaluated and certified configuration:

Table 2: Operating system parameters for the certified product

Data type	Tag in the protocol data DO	Data
Manufacturer	5F4D	24 (MaskTech GmbH)
OS Identifier	82	4d 54 43 4f 53 20 50 (MTCOS P)
OS Version	83	02 06 (2.6)
Build date	84	20 24 07 18 (2024-07-18)

Data type	Tag in the protocol data DO	Data
Option Byte	85	C… (1 Byte)
Init-key identifier	86	C... (8 Byte)

The following table describes the patch level info parameters for the evaluated and certified configuration:

Table 3: Patch level parameters for the certified product

Data type	Tag in the protocol data DO	Data
Patch Version	83	00 (0)
Build date	84	20 24 07 18 (2024-07-18)

The following table describes the hardware parameters for the evaluated and certified configuration:

Table 4: Hardware parameters for the certified product

Data type	Tag in the protocol data DO	Data
Manufacturer	5F4D	05 (Infineon Technologies AG)
Chip identifier	82	52 76 01 e0 ff ff ff Byte 1 - 2: Platform Byte 3: Hardware derivative 01h: SLC37GDA512 03h: SLC37GDA512AA 05h: SLC37GDA512A2 Byte 4: Commercial Cut Information Byte 5 – 7: -

The authenticity and integrity of a card can be authenticated during operational phase if the card is under control of the user by using the correct chip authentication key that is only personalised for this certified product.

1.3 Delivery Items

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

Table 5: Delivery items

No	Type	Description / Additional Information	Release	Form of Delivery
1	HW / SW	MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11) An IC module including the necessary basic software (OS) and SSCD application (file system)		SW is implemented in NVM memory; chip is initialised and tested before delivery to Personalisation Agent. Delivery type: The OS and application software is flashed on the IC Platform
		1. Hardware platform SLC37GDA512 (V11) secure dual-interface controller of Infineon Technologies AG (BSI-DSZ-CC-1107-V4-2023 [HW ST]. Chip including cryptographic library are certified according to CC EAL6 augmented with ALC_FLR.1 compliant to the Protection Profile BSI-CC-PP-0084-2014 [PP-0084].	SLC37GDA512 (V11) - IFX_CCI_000039h, Design Step T11 - firmware 80.306.16.0 - HSL v3.52.9708 - UMSLC v01.30.0564 - ACL v3.35.001	
		2. TOE Embedded Software IC Embedded Software (the operating system MTCOS Pro V2.6, implemented in NVM of the IC)	MTCOS Pro Version 2.6 Build date: 18.07.2024	
		3. TOE Embedded Applications IC Embedded Software / Part Application Software (containing the SSCD Application implemented in the NVM of the IC with the file system)	MTCOS Pro 2.6 QSCD/SSCD	
2	DOC	1. User Guidance MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11), MaskTech International GmbH	[AGD] 1.3, 02.10.2024	Password protected Secure Webserver
		2. MTCOS Pro 2.6 / SLC37 (V11) - Manual – MaskTech GmbH	[MT_Manual] Version 1.1, 27.09.2024	

Delivery items and associated delivery methods

Sensitive electronic documents: Delivery of sensitive electronic data is performed PGP encrypted via email. The guidance documentation can be obtained by password-protected download from MaskTech International GmbH website (http://www.masktech.com).

Flash image production: Confidentiality, integrity and authenticity are guaranteed by Infineon Technologies AG. SecureX webserver via an SSL-protected web access.

Product for Personalisation: Chip card hardware is securely shipped to the Personalisation Agent.

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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" can be issued as contactless, contact based or as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. The product is based on the hardware platform SLC37GDA512 (V11) by Infineon Technologies AG with IC Dedicated Software and Crypto Library. The IC integrates functionality for symmetric encryption (Triple-DES and AES) and a Public Key Crypto Coprocessor (Crypto@2304T) to support the implementation of asymmetric cryptographic algorithms like RSA and Elliptic Curve cryptography (cf. [IFX_Cert], chapter B.3). The hardware is CC certified (BSI-DSZ-CC-1107-V5-2024) and provides protection against side channel attacks and other attacks, e.g. fault attacks.

The smart card embedded software contains the operating system MTCOS Pro V2.6 and the application that provides the QSCD functionality which will be in the following denoted as *QSCD/SSCD application* (cf. [AGD_FSL]).

The operating system MTCOS Pro V2.6 provides a fully interoperable, multi-application platform compliant to ISO/IEC 7816 [ISO 7816] which is appropriate for cards used in applications with high level security requirements. The comprehensive offer of different technical and functional properties as well as security mechanisms of the MTCOS operating system especially supports the *QSCD/SSCD application*. Further applications may exist on the „MTCOS Pro 2.6 QSCD/SSCD / IFX" besides the dedicated *QSCD/SSCD application* for the generation of qualified digital signatures. But these applications are **not** subject to the certification at hand.

Moreover, the „MTCOS Pro 2.6 QSCD/SSCD / IFX" provides among others the following security functionalities:

- Initialising the Reference Authorisation Data (RAD),
- Secure Storage of the Reference Authorisation Data (RAD),
- Cryptographic ciphers (AES, TDES),
- Signature algorithms (ECDSA, RSA),
- Key agreement algorithms (DH, ECDH, PACE),
- Generation, importing and storage of key pairs (EC, RSA),
- Message digest algorithms (SHA-1, SHA-2 family),
- Random number generation (PTG.3 according to [AIS 31]),
- Application's file system follows the PKCS#15 structure [ISO 7816-15],
- Access control,
- User authentication before signature creation,
- PACE according to BSI TR-03110-1 [TR-03110-1] and TR-03110-2 [TR-03110-2] as well as ICAO-SAC [ICAO_SAC],

- Chip Authentication Version 1 according to BSI TR-03110-1 [TR-03110-1],
- Optionally Terminal Authentication Version 1 according to BSI TR-03110-1 [TR-03110-1].

In summary „MTCOS Pro 2.6 QSCD/SSCD / IFX", which is realised by a smartcard, consists of the following components:

- SLC37GDA512 (V11) secure dual-interface controller of Infineon Technologies AG (BSI-DSZ-CC-1107-V5-2024). Chips including cryptographic library are certified according to CC EAL6 augmented with ALC_FLR.1 compliant to the Protection Profile BSI-CC-PP-0084-2014 [PP-0084].
- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software.
- IC Embedded Software, i.e. the Card Operating System MTCOS Pro V2.6 and
- *QSCD/SSCD application*.

The „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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 authorised Signature Creation Applications (SCAs) and Certificate Generation Authorities (CGAs). Terminal authentication version 1 is optional.

To support key import in general or card internal key generation if the card is already under control of the signatory, a trusted channel to the card must be established. For key import Terminal Authentication is always required. For key generation, Terminal Authentication is required only if the card configuration supports Terminal Authentication and for other card configurations Chip Authentication is sufficient. In operational state, beside the selection of the *QSCD/SSCD application* each further interaction with the *QSCD/SSCD application* requires user authentication using the PACE protocol and trusted channel communication. For personalisation a successful authentication with the personalisation key is necessary.

Before the *QSCD/SSCD application* can be used, it must be completed. The signature key can either be generated in the card or securely personalised 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 *QSCD/SSCD application*, the CAN and PUK are set in the card and optionally, the public key certificate is inserted. In principle, the change of the programme code is not possible and once personalisation is completed, configurations cannot be changed anymore.

In order to be able to generate a signature with the completed *QSCD/SSCD 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 personalisation step and delivered to the signatory. The RAD PIN and PIN_{QES} are not set in the personalisation 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 protected by the secret PIN_{QES} (signature

PIN), which is a password with a minimum length of 6 digits stored on the chip in EF.PIN.QES.

After the *QSCD/SSCD application* has been activated, „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX". After successful entry of the PIN_{QES} only one qualified signature can be generated and a further signature cannot be generated without a new entry of the PIN_{QES}. The authentication state of the PIN_{QES} is reset to „not verified" after each qualified signature creation.

The PIN_{QES} stored in EF.PIN.QES of *QSCD/SSCD application* can be administrated by the owner of the signature key. The administration comprises the following functions:

- changing a PIN_{QES} (after successful user authentication with the currently valid signature PIN_{QES}) and
- reset the retry counter for PIN_{QES} (after successful user authentication with the currently valid PUK).

For access relevant to the *QSCD/SSCD application*, the „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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), Chip Authentication and optionally Terminal Authentication are supported. Access rights of the external world are verified within the scope of the authentications.

The security properties of „MTCOS Pro 2.6 QSCD/SSCD / IFX" are explained in more detail together with the description of the security functions.

The operating system allows the card manufacturer a range of configuration options. Before initialisation, 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 initialisation of the chip (completion of the operating system code and loading of the file system) by the initialiser. The installation of the file system can only take place after the initialisation system has been authenticated against the card. The keys used for cryptographically securing the loading data are only known by MaskTech International GmbH as software developer. In this sense one can speak of an end-to-end security between card manufacturer and chip. This prevents the loading of incorrectly changed initialisation data. The „MTCOS Pro 2.6 QSCD/SSCD / IFX" does not support the subsequent introduction of further software. The initialiser must take into account the initialisation requirements described in the guidance documents.

„MTCOS Pro 2.6 QSCD/SSCD / IFX" supports the following cryptographic algorithms for the generation of signature key pairs as well as of qualified electronic signatures:

- Asymmetric RSA algorithm with a key length of at least 2048 bit up to 4096 bit and the signature format RSASSA-PSS according to [PKCSv2.2] (cf. [RFC 8017]).

- DSA based on elliptic curves (ECDSA) using the groups $E(F_p)$ with key lengths of 256, 384, 512 or 521 bit (cf. [TR-03111], [ANSI X9.62]).

- 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 Technologies AG (cf. [HW ST], [IFX_Cert]).

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

- Asymmetric operations with RSA with key lengths from 2048 to 4096 bits and signature formats RSASSA-PSS, RSA-PKCS1-v1_5 and raw RSA (cf. [PKCSv2.2], [RFC 8017]) for generation of advanced signatures.

- Asymmetric operations with ECDSA with cryptographic key sizes brainpool(r1) 224, 256, 320, 384, 512 bits, NIST 224, 256, 384, 521 bits (cf. [TR-03111], [ANSI X9.62]) for generation of advanced signatures.

- Verification of digital signatures with RSA with SHA-1 and SHA-256 and cryptographic key sizes 1536 to 4096 bits (cf. [RFC 8017], [FIPS 180-4]).

- Verification of digital signatures with ECDSA with SHA-224, SHA-256, SHA-384 and SHA-512 and cryptographic key sizes brainpool(r1) 224, 256, 320, 384, 512 bits, NIST 224, 256, 384, 521 bits (cf. [TR-03111], [ANSI X9.62], [FIPS 180-4]).

- Asymmetric operations on the basis of elliptic curves (cf. [TR-03111]) for PACE, 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 (cf. [TR-03110-1]).

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

- Diffie-Hellman (ECDH) according to [TR-03111] and key length of 224, 256, 320, 384, 512 (brainpool) and 224, 256, 384, 521 (NIST) (cf. [ICAO_SAC]) for authentication (PACE) and key agreement for the secure messaging channel.

- Diffie-Hellman (DH) according to [SP 800-56A], [TR-03110-1] and cryptographic key sizes 2048 bit MODP with 224 bit prime order subgroup and 2048 MODP with 256 bit prime order subgroup for chip authentication.

- Symmetric Triple-DES algorithm according to NIST SP800-67 [SP800-67], [ISO 10116] with an effective key length of 112 bits; CBC mode according to NIST SP800-67 [SP800-67], [ISO 10116] and retail MAC according to [SP 800-67], [ISO 9797-1] compliant to [ICAO_SAC].

- Symmetric AES algorithm according to [FIPS 197], [ISO 10116] with an effective key length of 128, 192 or 256 bits; CBC mode according to [FIPS 197], [ISO 10116] and CMAC according to [FIPS 197], [SP 800-38B] compliant to [ICAO_SAC].

„MTCOS Pro 2.6 QSCD/SSCD / IFX" supports the ECC Brainpool curves P224r1, P256r1, P320r1, P384r1 and P512r1 according to [TR-03111] and NIST curves P-224, P-256, P-384 and P-521 from the NIST curve family according to [ANSI X9.62].

„MTCOS Pro 2.6 QSCD/SSCD / IFX" was successfully evaluated with the Common Criteria in version 3.1 (cf. [ETR]). The assurance level is EAL 5+ with the augmentations ALC_DVS.2, ALC_FLR.3 and AVA_VAN.5.

Furthermore, the „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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].

2.2 Security Functions and Security Properties of „MTCOS Pro 2.6 QSCD/SSCD / IFX"

Among others „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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"

„MTCOS Pro 2.6 QSCD/SSCD / IFX" 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: „authorised", „not authorised")

- 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 *QSCD/SSCD 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" by knowing a secret key as an administrator (e.g. initialiser, personaliser or card management system) or by entering the PIN or PIN_{QES} as a signer. The generation of qualified signatures is only possible after entering the PIN_{QES}.

In the usage phase, the application of a secure channel is supported by the „MTCOS Pro 2.6 QSCD/SSCD / IFX" both when using the contact and contactless interface. The authentication methods PACE, Chip Authentication and optionally Terminal Authentication are supported for both interfaces.

The session keys can be negotiated by different methods. The „MTCOS Pro 2.6 QSCD/SSCD / IFX" provides 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.
- **Terminal authentication** (optional) to restrict service provisions to authorised Signature Creation Applications (SCAs) and Certificate Generation Authorities (CGAs). Terminal authentication is required if key import shall be supported in operational state and the card is already under control of the signatory. For key generation in this scenario Terminal Authentication is required only if the card configuration supports Terminal Authentication, otherwise Chip Authentication is sufficient.

Furthermore, the access control is implemented using access conditions, which are stored as security attributes in „MTCOS Pro 2.6 QSCD/SSCD / IFX". 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 "authorised".
- 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 *QSCD/SSCD 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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“

„MTCOS Pro 2.6 QSCD/SSCD / IFX” supports the execution of the Password Authenticated Connection Establishment (PACE) protocol according to [TR-03110-1], [TR-03110-2] and [ICAO_SAC]. This security function includes PACEv2 (Generic Mapping), PACE-CAM (Chip Authentication Mapping) and PACE with key agreement and authentication. The PACE protocol is a password based protocol for key agreement using the Diffie-Hellman algorithm based on elliptic curve cryptography (ECDH) according to [TR-03111]. It includes the proof, that „MTCOS Pro 2.6 QSCD/SSCD / IFX” 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX” and terminal to protect the contactless (air communication interface) or contact based interface. In addition, a binding to the cardholder is achieved by using the specific secrets PIN, PUK and CAN as start values.

PACE-CAM may be used to perform Chip Authentication within the scope of the PACE authentication. Key generation and key import as well as certificate import in the operational use phase require Chip Authentication using the key stored on the card (EF.CA.SSCD). Also Terminal Authentication provided in the according layouts can only be performed, if a Chip Authentication using this key in EF.CA.SSCD has been performed beforehand.

PIN and PUK are protected by denial-of-service attacks by setting the chip into a suspended state, before the retry counter of the secret in question is exhausted after consecutive failed authentication attempts. Before the very last retry to authenticate against PIN or PUK, respectively can be done, an authentication against CAN must be performed.

The successful execution of the PACE protocol as a necessary condition for the use of „MTCOS Pro 2.6 QSCD/SSCD / IFX” supports the owner of the signature key in controlling the signature creation device especially 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX”. 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX” more difficult.

„Chip Authentication“

„MTCOS Pro 2.6 QSCD/SSCD / IFX” supports the execution of Chip Authentication Version 1 according [TR-03110-1], [ICAO_9303] to proof the authenticity of the chip to the terminal and to establish a trusted channel between the terminal and the card. For secure messaging based on (mutual) authentication with elliptic curve cryptography (ECDH) according to [TR-03111] or based on cryptographic key generation algorithms Diffie-Hellman (DH) and cryptographic key sizes 2048 bit MODP

with 224 bit prime order subgroup and 2048 bit MODP with 256 bit prime order subgroup according to [SP 800-56A] and [TR-03110-1] (cf. [ST], [AGD]) is used. Thus, DH as well as ECDH are supported for key agreement and authentication. For secure messaging 3DES, AES-128, AES-192 or AES-256 can be used.

The protocol for internal authentication is based on authenticated key agreement. For this, the „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" or in a central database. Generally, it is recommended to authenticate this public key e.g. by verifying an additional document signer signature stored on the card by the personaliser.

„Terminal Authentication"

„MTCOS Pro 2.6 QSCD/SSCD / IFX" supports the execution of mutual Terminal Authentication Version 1 according to [TR-03110-1] with the establishing of a secure channel with asymmetric cryptography based on elliptic curves according to [TR-03110-1] to restrict the service provisions to authorised signature creation applications and certificate generation applications. For terminal authentication signature verification using ECDSA with SHA-224, SHA-256, SHA-384 or SHA-512 or RSA with SHA-1 or SHA-256 is applied.

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 personalisation. The CVCA then generates signed Document Verifier (DV) certificates for specified parties that issues certificates for legitimate terminals. During terminal authentication the personalised CVCA certificate is used to verify the certificate chain and thus, assigned access rights can be verified.

Terminal authentication is usable only in a secure messaging session with chip authentication key.

If the card is already under control of the signatory, Terminal Authentication is always required for key import. For key generation Terminal Authentication is required only if the card configuration supports Terminal Authentication and for other card configurations Chip Authentication is sufficient.

„Administration of the „MTCOS Pro 2.6 QSCD/SSCD / IFX" or the QSCD/SSCD application "

This security function is used within the processes of initialisation and personalisation of the „MTCOS Pro 2.6 QSCD/SSCD / IFX". For initialisation and personalisation of the „MTCOS Pro 2.6 QSCD/SSCD / IFX", the related requirements defined by the manufacturer have to be considered (cf. 4.2).

In particular, the security function enforces the following rules:

- Initialisation and personalisation of the „MTCOS Pro 2.6 QSCD/SSCD / IFX" can only be performed after a successful authentication with a secret key.

- At the end of the initialisation and personalisation phase, the access for a further initialisation or personalisation is blocked.

- The initialisation with the loading of the installation scripts and the subsequent checking of the loaded data is carried out according to the guidance documentation [AGD], [MT_Manual]. The loading of the installation 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, i.e. PIN_{QES}. User authentication is performed by comparing a signature PIN provided by the user with the reference value (RAD) secretly stored in „MTCOS Pro 2.6 QSCD/SSCD / IFX” (in the *QSCD/SSCD application*).

After a successful, finalised personalisation, the „MTCOS Pro 2.6 QSCD/SSCD / IFX” has a PUK (at least 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX” 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX”.

The signature PIN has a PIN Try Counter (PTC) with the initial value three set during initialisation, 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX” 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 to reset the signature PIN. After using the resetting code a maximum of ten times for reset of the PTC, it can no longer be used for resetting the signature PIN and it is no longer possible to reset a blocked signature PIN. The PUK has a Retry Counter (RTC) with the initial value three set during initialisation, which is decremented by one after each wrong PUK entry. The secret is set in a suspended state, when the RTC is down to the value one. PACE authentication using PACE-CAN is required before the very last authentication attempt can be done. Finally, after the third repeated entry of a wrong PUK, the RTC is zero and the PUK is blocked. A reset of RTC is not possible.

For reset of the signature PIN, 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX” 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX".

„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"

„MTCOS Pro 2.6 QSCD/SSCD / IFX" supports the encrypted and integrity protected data exchange with the external world based on Secure Messaging according to the ISO Standard [ISO 7816] or the requirements defined in the specification of the card operating system [MT_Manual].

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"

„MTCOS Pro 2.6 QSCD/SSCD / IFX" ensures, that safety-critical information (e.g. signature key, PINQES) 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX” closes the session.

„Resistance against Side Channel Attacks“

„MTCOS Pro 2.6 QSCD/SSCD / IFX” 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 or differential electromagnetic analysis (SEMA / DEMA).

All safety-critical operations of „MTCOS Pro 2.6 QSCD/SSCD / IFX”, 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX” (initialisation, personalisation 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX” provides the cryptographic functions. It is based on the cryptographic functions of the evaluated and certified semiconductor and its dedicated software.

„MTCOS Pro 2.6 QSCD/SSCD / IFX” supports the algorithms listed in chapter 2.1.

„Generation of Key Pairs“

„MTCOS Pro 2.6 QSCD/SSCD / IFX” supports the generation of RSA and ECDSA key pairs in the card for generating qualified signatures with a length from 2048 bits up to 4096 bits for RSA keys and 256, 384, 512 and 521 bits for ECDSA keys.

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

- RSA keys are generated with a key length of at least 2048 bit up to 4096 bit and the signature format RSASSA-PSS according to [PKCSv2.2] (cf. [RFC

8017]). 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 sufficiently large by $d > 2^{n/2}$., where n denotes the bit length of the modulus.

- ECDSA keys with $E(F_p)$ are generated with a length of 256, 384, 512 and 521 bits. The supported curves ECC Brainpool P256r1, P384r1 and P512r1 according to [TR-03111] and NIST P-256, P-384 and P-521 from the NIST curve family according to [ANSI X9.62] are recommended (cf. [SOG-IS], chapter 4.3). (In addition, ECC curves Brainpool P224r1, P320r1 and NIST P-224 are also supported, but only for advanced electronic signatures.)

- 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. [ST], [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 personalisation of the *QSCD/SSCD application*. Additionally, the life cycle of the „MTCOS Pro 2.6 QSCD/SSCD / IFX" allows the generation after the delivery to the signatory. „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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 personalisation or after the delivery to the signatory. In the latter case the loading of the signature key can only be performed after a successful Terminal Authentication, hence when Terminal Authentication is supported. According to [AGD], personalisation must take place in a secure environment.

„Generation of Qualified Signatures"

„MTCOS Pro 2.6 QSCD/SSCD / IFX" supports the generation of qualified electronic signatures with RSA and ECDSA signature keys with a length from 2048 bits up to 4096 bits for RSA keys and 256, 384, 512 and 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 RSASSA-PSS according to chapter 8 and 9 of [PKCSv2.2] with a key length of at least 2048 bit up to 4096 bit.

- Computation of ECDSA signatures according to [TR-03111] with key lengths of 256, 384, 512 or 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 und 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“.
- 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 or 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** Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.
(1a)	**Requirement** Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes shall be carried out only on behalf of the signatory, at the request of the signatory, and by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.
(2)	**Requirement** 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** 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

Reference	Requirement / Description / Result
	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** 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.

3.2 Conditions of Use

Requirements for the Responsible Initialisation Party

- The initialisation data provided by MaskTech International 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 initialisation data.
- The requirements of the card manufacturer to the initialisation according to [AGD] must be taken into consideration.

Requirements for the Responsible Personalisation Party

- The personalisation party must ensure that the personalisation data (especially of the *QSCD/SSCD application*) are treated in a secure way. The personalisation data must be protected with respect to integrity, authenticity and confidentiality.
- The card manufacturer's requirements to the personalisation according to [AGD] 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 less than 3000 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 RSA keys with length of at least 3000 bits up to 4096 bits are used.
- 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" (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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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 [MT_Manual] as well as of the *QSCD/SSCD 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 Guidance, [AGD].

3.3 Cryptographic Algorithms and Parameters

For the generation of digital signatures, „MTCOS Pro 2.6 QSCD/SSCD / IFX" provides RSA according to [PKCSv2.2] (cf. [RFC 8017]) and ECDSA based on groups $E(F_p)$ (cf. [TR-03111], [ANSI X9.62]). Asymmetric RSA algorithm with a key length of at least 2048 bit up to 4096 bit and 256, 384, 512 and 521 bits for ECDSA with the ECC Brainpool curves P256r1, P384r1 and P512r1 according to [TR-03111] and NIST curves P-256, P-384 and P-521 from the NIST curve family according to [ANSI X9.62] are supported.

For RSA signatures RSASSA-PSS according to [PKCSv2.2] (cf. [RFC 8017]) is supported as signature format. 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 AG 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 Technologies AG hardware (cf. [HW ST], [IFX_Cert]).

The cryptographic algorithms used by the product „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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.
- RSASSA-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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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 „MTCOS Pro 2.6 QSCD/SSCD / IFX" may only be used until **31 December 2025** for the configuration of RSA keys with key length less than 3000 bits.
- The use of RSA with parameters chosen by „MTCOS Pro 2.6 QSCD/SSCD / IFX" is not restricted by the algorithm catalogue SOG-IS [SOG-IS] if the configuration of RSA keys with key length of at least 3000 bits up to 4096 bits is applied.
- 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 less than 3000 bits.

Due to Regulation (EU) No 910/2014 [Reg No. 910/2014], Article 30 (3a) the validity of the certification shall not exceed five years. Therefore, this certification of the „MTCOS Pro 2.6 QSCD/SSCD / IFX" is with issuing date **11.11.2024** valid until **10.11.2029**. In addition, the algorithm RSA with key lengths less than 3000 bits may only be used until **31.12.2025**.

However, the validity may be shortened if new findings regarding the suitability of the algorithms are published in the algorithm catalogue SOG-IS [SOG-IS]. In addition, in accordance with Article 30 (3a), a vulnerability analysis must be carried out every two

years. Where vulnerabilities are identified and not remedied, the certification shall be cancelled.

3.4 Assurance Level and Attack Potential

The product MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11) 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, ALC_FLR.3 and AVA_VAN.5).

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

For this the German Common Criteria Certificate with registration number BSI-DSZ-CC-1221 will be available.

For the evaluation of „MTCOS Pro 2.6 QSCD/SSCD / IFX" 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 Standardisation 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 Standardisation 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 Standardisation System CEN/ISSS, EN419211-6:2014" [PP SSCD Part 6] were used (cf. [ETR]). 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 SLC37GDA512 (V11) from Infineon Technologies. 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-1107-V5-2024. It shall be noted that meanwhile the semiconductor was re-certified under BSI-DSZ-CC-1107-V5-2024. In regard to BSI-DSZ-CC-1107-V4-2023, a new asymmetric Crypto Library "ACL v3.35.001" was included, targeting security issues concerning modular inversion explained in [EUCLEAK].

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; last amended by Regulation (EU) No 2024/1183

[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

[ANSI X9.62] ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-11-16.

[ETR] SRC, Evaluation Report, Evaluation Technical Report Summary (ETR Summary), MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11), Version 1.2, 25.10.2024

[EUCLEAK] EUCLEAK, Side Channel Attack on the YubiKey 5 Series, Thomas Roche, NinjaLab, Montpellier, France, September 3rd, 2024

[FIPS 180-4] Federal Information Processing Standards Publication FIPS PUB 180-4, Specifications for the Secure Hash Standard (SHS), 2015-08

[FIPS 186-5] NIST: FIPS Publication 186-5: Digital Signature Standard (DSS), February 3rd, 2023.

[FIPS 197] NIST: FIPS Publication 197: Specification for the Advanced Encryption Standard (AES), published 26. November 2001, updated May 9th, 2023

[HW ST] Infineon Technologies AG, IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11, Security Target Lite, Revision v6.5, 2024-08-20

[IFX_Cert] Certification Report, BSI-DSZ-CC-1107-V5-2024 for IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000044h, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000048h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Ch, IFX_CCI_00004Dh, IFX_CCI_00004Eh design step T11 with firmware 80.306.16.0, 80.306.16.1 or 80.312.02.0, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 or v2.11.003, optional ACL v3.35.001, v3.34.000, v3.33.003 or v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik (BSI), Certification Report V1.0, 4. September 2024

[ISO 7816] ISO/IEC 7816: Identification cards - Integrated circuit cards - Multipart Standard, ISO/IEC, 2008

[ISO 7816-15] ISO/IEC 7816-15: Identification cards – Integrated circuit cards – Part 15: Cryptographic Information Application, ISO/IEC, 2016-05

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

[ISO 10116] ISO/IEC 10116-2017, Information Technology – Security Techniques – Modes of operation for an n-bit block cipher, 2017-07

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

[PP-0084] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13.01.2014, Certification-ID: BSI-CC-PP-0084-2014

[PP SSCD Part 2] Protection Profiles for Secure Signature Creation Device - Part 2: Device 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 1.3, February 2023

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

[SP 800-38B] NIST: Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2016-10

[SP 800-56A] NIST: Special Publication 800-56A Rev. 3: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2018-04

[SP800-67] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67, National Institute of Standards and Technology, 2017-11

[ST] Security Target Common Criteria Documents – MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11), Secure signature creation device with key generation and key import, MaskTech International GmbH, Version 0.10, 26.09.2024

[AGD] User Guidance, MTCOS Pro 2.6 QSCD/SSCD / SLC37 (V11), MaskTech International GmbH, Version 1.3, 02.10.2024

[AGD_FSL] File System Layout, MTCOS Pro 2.6 / SLC37 (V11), MaskTech International GmbH, Version 0.3, 04.10.2023

[MT_Manual] MTCOS 2.6 / SLC37 (V11) - Manual, MaskTech GmbH, Version 1.1, 27.09.2024

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

[ICAO_SAC] ICAO: Technical Report: Supplemental Access Control for Machine Readable Travel Documents, TR-SAC V1.1, 2014-04-15

[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-03110-2] BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2 – Protocols for electronic Identification, Authentication and Trust Services (eIDAS), Version 2.21, Technical Guideline, Dec. 2016

[TR-03111] BSI: Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC), Version 2.10, 01.06.2018

End of certification report