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
TCOS Health Professional Card Version 2.1
Release 1 / SLC52

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

Certificate is valid until

31.12.2027

SRC Certificate Registration Number

SRC.00043.QSCD.07.2021

This certificate is only valid with the certification report.

Bonn, 23 July 2021

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 TCOS Health Professional Card Version 2.1 Release 1/SLC52 from Deutsche Telekom Security GmbH.

The product is a health professional card (HPC) of the German health telematics and is referred to in the following as „HPC Signature Card“ for short.

1.2 Delivery

The „HPC Signature Card“ is implemented as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. „HPC Signature Card“ is based on the hardware platform Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 by Infineon Technologies AG and including optional software libraries and dedicated firmware from Infineon Technologies AG. The hardware provides the crypto coprocessors "Crypto@2304T" (Cryptography with elliptic curves) and "Symmetric Crypto Processor" (Encryption and decryption with the AES).

The smart card embedded software contains the operating system TCOS Flexcert Version 2.0 Release 2/SLC52. This platform is an ISO-7816 compatible, multifunctional platform, that fulfils the requirements for the card operating system generation 2 of the German Health Care system pursuant to [eHC-COS]. The „HPC Signature Card“ fulfils the requirements to the related object system according [HPC-ObjSys]. It has the application for creating qualified electronic signatures, referred to below as the *QES application*, and is generally provided with further applications, such as the *health professional application* and the *ESIGN application*. However, the other applications are **not** the subject of this certification.

The „HPC Signature Card“ is delivered as a card with *QES application* from the trust service provider (TSP) to the end customer. For this purpose, the TSP obtains the cards from the chip manufacturer and initialises them with the scripts provided by Deutsche Telekom Security GmbH. The initialization / pre-personalisation script prepared by the manufacturer is sent to the card in a secure manner. Alternatively, the TSP can obtain cards that have already been initialised.

The card is also personalised by the trust service provider (or a commissioned third party), who loads the specific data into the card and then delivers it to the end customer. Personalisation involves the on-board generation of the signature key pair or its insertion and the setting of a specific transport PIN as transport protection when the card is delivered to the customer. When the card is delivered to the end customer, it has all the other data, i.e. the signature key and the corresponding signature key certificate are already in the card.

The authenticity and integrity of a card can be authenticated during personalisation by the correct personalisation key.

Furthermore, the product „HPC Signature Card“ can be identified as a certified product as follows:

For the certified version of the TCOS Health Professional Card Version 2.1 Release 1/SLC52, the manufacturer-specific values for the parameters "Chip Manufacturer (IFX)", "Chip Type", "Card Type", "OS Version (ROM mask version)" and "(Pre-)Completion Code Version" are specified in [TCOSPERG], Appendix C.1.1.2. They can be read from the card during production with the command "Format" using the option "Reading of Chip Information" or during the usage phase with the command GET CARD INFO. Thus, the operating system version of the „HPC Signature Card“ can be determined.

The file system / object system can be uniquely identified by reading out the EF.ATR (cf. [TCOSPERG], Appendix F). The version of the object system is coded in the data object with tag 'D4'.

1.3 Delivery Items

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

Table 1: Delivery items

No.	Delivery item	Description / Additional Information	Type	Delivery method
1	IFX Secure Smart Card Controller SLC52 including its IC Dedicated Support Soft-ware embedded into cards	Hardware platform Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12. Module types: - M8.8 (SLC52GDA600A8) - COM10.8 (SLC52GDA600A9) Embedded into card body and delivered as smart card	HW / SW	The hardware part of the product is delivered in an insured parcel to the Personaliser. In the life cycle of the product the hardware is always protected by an authentication procedure. Two module types are used for the product, they only differ in antenna capacitance.

No.	Delivery item	Description / Additional Information	Type	Delivery method
2	Operating System	Embedded Software IC Embedded Software (the operating system and completion data) TCOS Flexcert Version 2.0 Release 2/SLC52 ROM Masks: TCOS30_SLC52_ROM_And_NVM_GDA600A8.hex TCOS30_SLC52_ROM_And_NVM_GDA600A9.hex OS Version: 01 B8 Completion Code Version: 00	SW	The software part of the product is implemented in Flash Memory of the IC. For each module type a separate flash image exists, the fingerprint does not change between these images.
3	Application	Embedded Application Health Professional Card Application according to [HPC-ObjSys].	SW	The application software part of the product is implemented in Flash of the IC.
4	Associated guidance documentation	TCOS Health Professional Card Version 2.1 Release 1, Operation and Personalization Guidance, Guidance Documentation of TCOS Health Professional Card Version 2.1 Release 1, Deutsche Telekom Security GmbH, Version 1.1, 19.07.2021, [TCOSPERG].	DOC	The guidance documents of the product are always delivered in an encrypted and signed form. Therefore the integrity and authenticity (key validation) can be ensured during the delivery.

No.	Delivery item	Description / Additional Information	Type	Delivery method
5	Activation command APDUs to open phases 6.2 and 7 and authentication key	Activation command to open lifecycle phase 6.2 or 7 and corresponding authentication key. The activation commands are FORMAT-Command APDUs to open the corresponding production phases as described in [TCOSADM], sec. 6.1.1.4 (in particular sec. 6.1.1.4.3).	Text files	The authentication keys and command APDUs of the product are always delivered in an encrypted and signed form. Therefore the integrity, authenticity and confidentiality can be ensured during the delivery.

1.4 Manufacturer

Manufacturer of the product is Deutsche Telekom Security GmbH, Untere Industriestrasse 20, D-57250 Netphen.

2. Functional Description

2.1 Functionality and Architecture

The „HPC Signature Card“ is implemented as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. The hardware of „HPC Signature Card“ consists of Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG. The hardware provides the crypto coprocessors "Crypto@2304T" (Cryptography with elliptic curves) and "Symmetric Crypto Processor" (Encryption and decryption with the AES). The Infineon security controller has been evaluated and certified according to CC 3.1 (BSI-DSZ-CC-1079-V2-2020).

The software consists of the operating system TCOS Flexcert Version 2.0 Release 2/SLC52 as well as of the *QES application* for the generation of qualified electronic signatures.

The operating systems TCOS Flexcert Version 2.0 Release 2/SLC52 provides an interoperable, multifunctional platform conform to 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 TCOS operating system especially supports the *QES application*. Further applications may exist on the „HPC Signature Card“ (e.g. application for the health professional) besides the dedicated *QES application* for the generation of qualified digital signatures. But these applications are **not** subject to the certification at hand.

Moreover the operating system provides among others the following functionality:

- file system according to ISO 7816,
- access control of the file system,
- authentication of components,
- secure messaging for a secure communication with the external world,
- key management and PIN management,
- PIN based user authentication,
- generation of RSA keys and
- generation of electronic signatures (RSA).

In summary „HPC Signature Card“ consists of the following components:

- Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG,
- TCOS Operating System „TCOS Flexcert Version 2.0 Release 2/SLC52“ and
- *QES application*.

Before the *QES application* can be used, it must be completed. The signature key is generated by the trust service provider (TSP) (or a commissioned third party) before

the card is delivered. The signature key can either be generated in the card or securely personalised into the card. As part of this completion of the *QES application*, the public key certificate is also inserted and the transport PIN is set in the card. Once personalisation is complete, it is not possible to change the programme code.

In order to be able to generate a signature with the completed *QES application*, the designated signature key holder must activate the „HPC Signature Card“ as a signature generation device (QSCD). To do this, he or she must replace the preset and maximum five-digit transport PIN with a valid signature PIN.

After the *QES application* has been activated, „HPC Signature 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.

„HPC Signature Card“ is a so-called multi-signature qualified signature creation device (multi-signature QSCD) enabling the generation of either exactly one, or a limited number of qualified signatures after successful entry of the signature PIN. The number is determined during initialisation (value n of the signature counter with n = 250) and cannot be changed afterwards. „HPC Signature Card“ checks the signature counter limit, i.e. after generation of n signatures no further signatures can be generated without a new entry of the signature PIN. The security state "Successful PIN Entry" is cancelled in „HPC Signature Card“ with a reset of the card. For the generation of further signatures a new entry of the signature PIN is necessary. The use of a multi-signature QSCD is bound to specific usage conditions (cf. conditions for the use of the signature counter).

The use of the multi-signature capability requires that the „HPC Signature Card“ is operated in a special security mode (Security Environment #2), which requires that the data to be signed is transferred to the card via a secure channel. The establishment of the secure channel by the card only takes place if a successful mutual authentication with the external world has taken place. For the secure transmission of the data to be signed, the external world must authenticate itself under the role "SAC for stack or comfort signatures". This enables the use of the batch signatures according to [TR-03114] and [TR-03115].

Individual signatures can be generated in Security Environment #1 without these additional security mechanisms.

In Security Environment #2, the „HPC Signature Card“ also supports the transfer of the signature PIN via a secure channel established by means of mutual authentication and the external world has authenticated itself under the role of "remote PIN sender". This supports the concept of "remote PIN entry" (cf. [TR-03114], [TR-03115]), whereby the eHealth card terminal used by the signature key holder for PIN entry and the eHealth card terminal in which the „HPC Signature Card“ is inserted are differentiated. Here, secure end-to-end communication takes place between the „HPC Signature Card“ and a security module of the card terminal used for PIN entry. Special conditions of use apply for the use of this scenario.

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

- changing a signature PIN (after successful user authentication with the currently valid signature PIN) and
- resetting the PIN try counter of signature PIN without setting a new signature PIN (after successful user authentication with resetting code).

For access relevant to the signature application, the „HPC Signature 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 according to [eHC-COS] are supported. Access rights of the external world are verified within the scope of the authentications. This includes in particular the right of a signature application component to generate multi-signatures or as a "remote PIN sender".

The security properties of „HPC Signature Card“ are explained in more detail together with the description of the security functions.

The TCOS 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 (cf. Table 1, No. 3, Script file with Load Application APDUs) is performed during initialisation of the chip (completion of OS code and loading of the file system) by the initialiser. The installation of the file system may only be performed after an authentication of the initialisation system to the card. The cryptographic keys used for the secure loading of data are only known by the card manufacturer. In this sense there exists an end-to-end security between card manufacturer and chip. By this measure the loading of initialisation data that have been modified without authorisation can be prevented. A subsequent loading of further software is not supported by „HPC Signature Card“.

„HPC Signature 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 [PKCS#1] with a key length of 2048 bits.
- DSA based on elliptic curves (ECDSA) using the groups $E(F_p)$ (cf. [TR-03111]) with key lengths of 256 bits. For this, „HPC Signature Card“ supports the ECC Brainpool curve P256r1 according to [RFC 5639].
- Generation of random numbers based on a random number generator of the underlying hardware from IFX. The random number generator is a Physical True Random Number Generator (PTRNG) with a PTG.2 classification pursuant to [AIS 31]. The random numbers are subject to statistical tests

performed in the operation phase („online tests“). These properties were checked in a CC evaluation of the Infineon hardware (cf. [HW ST]). This PTRNG is also used with a cryptographic post-processing based on the recommendations in TR-02102 (cf. [TR-02102]). In the process of RSA key generation, 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.

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

- DSA based on elliptic curves (ECDSA) using the groups $E(F_p)$ (cf. [TR-03111]) with key lengths of 256, 384 and 512 bits.
- Asymmetric operations with RSA (key lengths 2048 and 3072 bits; (cf. [PKCS#1]) and on the basis of elliptic curves (cf. [TR-03111]) for authentication and encryption/decryption.
- Hash functions SHA-1, SHA-256, SHA-384 and SHA-512 according to [FIPS 180-4].
- Diffie-Hellman (ECDH) according to [TR-03110], [TR-03111] 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 168 bits (CBC mode, retail MAC according to [eHC-COS]).
- Symmetric AES algorithm according to [FIPS 197] with an effective key length of 128, 192 or 256 bits (CBC mode, CMAC according to [TR-03110], [SPUB 800-38B]).
- Random number generation based on a hybrid deterministic random number generator (DRNG) whose seed is generated by the underlying hardware (PTG.2). The DRNG was evaluated as a DRG.4 generator with resistance to high attack potential according to [AIS 20].
- Generation of random numbers based on a random number generator of PTG.3 classification pursuant to [AIS 31] that uses the outputs of the HW generator PTRNG. A cryptographic post-processing is used to achieve the conformity with the class PTG.3.

„HPC Signature Card“ supports the ECC Brainpool curves P256r1, P384r1 und P512r1 according to [RFC 5639] and the ANSI curves ansix9p256r1 and ansix9p384r1, which are identical to P-256 and P-384 according to [FIPS 186-4].

„HPC Signature Card“ was successfully evaluated with the Common Criteria in version 3.1 (cf. [ETR]). The assurance level is EAL 4+ with the augmentations ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

Furthermore, the „HPC Signature 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] und 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] as well as "Common Criteria Protection Profile Card Operating System Generation 2 (PP COS G2)", BSI-CC-PP-0082-V2-2014, Version 1.9 [BSI-CC-PP-0082].

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 „Sig Card“

Among others „HPC Signature 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“

„HPC Signature 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: „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)

A user authenticates himself to the „HPC Signature Card“ by knowing a secret key as an administrator (e.g. initialiser, personaliser or card management system) or by entering the signature PIN as a signer.

In the usage phase, the application of a secure channel is supported by the „HPC Signature Card“ both when using the contact and contactless interface. When using the contact interface, the connection between the „HPC Signature Card“ and the signature application can optionally be cryptographically secured, but only if single signatures are generated. The creation of signatures using the multi-signature capability always requires communication via a secure channel. The contactless interface can only be used with a secure channel.

The session keys can be negotiated by different methods. The „HPC Signature Card“ provides both symmetric and asymmetric authentication protocols according to [eHC-COS]. 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.

- **Role authentication** or **proof of authorisation** with asymmetric keys for (mutual) authentication without establishing a secure channel.

- **Device authentication** with asymmetric keys for mutual authentication and establishing a secure channel which is especially used for the secure transmission of the signature PIN in the case of a remote PIN entry.

- **CMS authentication** with symmetric or asymmetric keys for mutual authentication and establishing a secure channel to the card management system.

If the communication via the contactless interface is already protected by a secure channel established after a device authentication or CMS authentication, an additional secure channel established by the PACE protocol can be omitted. The secure channel built up after successful device authentication or CMS authentication replaces the secure channel of the PACE protocol.

Furthermore, the access control is implemented using access conditions, which are stored as security attributes in „HPC Signature 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:

- A key generation on board or the loading of the signature key into the card can only be performed during personalisation and only if the security attribute “SCD/SVD Management” has the value “authorised”.
- The PIN for transport protection may only be set during personalisation.
- 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 operating system.
- The substitution of the transport PIN by 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 „HPC Signature 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.
- The use of the multi-signature capability is only possible in Security Environment #2. In this case, signatures can only be generated if a successful user authentication has taken place, a mutual authentication with the establishment of a secure channel has taken place and the further accesses for signature generation take place using secure messaging. The external world must have authenticated itself under the role "SAC for stack or comfort signatures".

„Password Authenticated Connection Establishment (PACE) Protocol“

„HPC Signature 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 „HPC Signature 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 „HPC Signature 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 „HPC Signature Card“ supports the owner of the signature key in controlling the signature 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 „HPC Signature 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 „HPC Signature Card“ more difficult.

„Role Authentication and Proof of Authorisation“

„HPC Signature Card“ supports the execution of a role authentication or a proof of authorisation based on (mutual) authentication with RSA or elliptic curves pursuant to [eHC-COS].

The protocols for external and internal authentication use challenge-and-response protocols on the basis of suitable random numbers. Within the protocols, CV certificates are used to proof the authenticity of public keys. These certificates contain role and authorisation information and thus assigned access rights can be verified. For internal authentication, the „HPC Signature Card“ has related private keys for role authentication as well as proof of authorisation. In addition, root keys are stored in the „HPC Signature Card“ to enable the verification of CV certificates.

„Device Authentication“

„HPC Signature Card“ supports the execution of a mutual device authentication with the establishing of a secure channel with asymmetric cryptography based on elliptic curves pursuant to [eHC-COS].

The protocols for external and internal authentication use challenge-and-response protocols on the basis of suitable random numbers. Within the protocols, CV certificates are used to proof the authenticity of public keys. These certificates contain authorisation information and thus, assigned access rights can be verified. Device authentications are used especially for the communication with a signature application component that has the access right of a so-called “SAC for stack or comfort signatures” and/or “remote PIN sender”. With this, the signature PIN as well as data to be signed in case of using the multi-signature capability can be securely transmitted to the card.

For internal authentication, the „HPC Signature Card“ has a specific private key for device authentication. In addition, the necessary root key is stored in the „HPC Signature Card“ to enable the verification of related CV certificates.

„CMS Authentication“

The „HPC Signature Card“ supports the execution of a mutual authentication with the establishing of a secure channel by means of asymmetric algorithms based on elliptic curve cryptography or by means of symmetric mechanisms based on the algorithm AES with a card management system (CMS) according to [eHC-COS].

The protocols for external and internal authentication use challenge-and-response protocols on the basis of suitable random numbers.

Asymmetric protocols are based on the use of CV certificates to proof the authenticity of public keys assigned to the card management system. These certificates contain authorisation information and thus assigned access rights can be verified. For internal authentication, the „HPC Signature Card“ has a specific private key for CMS authentication. In addition, the specific root key for CMS authentication is also stored in the „HPC Signature Card“ to enable the verification of related CV certificates.

In principle, for symmetric protocols the „HPC Signature Card“ may contain AES key pairs, one AES key for encryption and decryption operations and one AES key for the generation of message authentication codes (MAC). For these, AES keys of length 128 and/or 256 bits may be used. By the chosen conditions these keys are not personalised and the use of symmetric CMS authentications is not possible.

„Administration of the „HPC Signature Card“ or the *QES application*“

This security function is used within the processes of initialisation and personalisation of the „HPC Signature Card“. For initialisation and personalisation of the „HPC Signature Card“, the related requirements defined by the manufacturer have to be considered (cf. 4.2).

Moreover, the data stored in the *QES application* (e.g. certificates) may be administrated by a card management system after the delivery of the card to the designated user.

In particular, the security function enforces the following rules:

- Initialisation and personalisation of the „HPC Signature Card“ 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 initialisation scripts and the subsequent checking of the loaded data is carried out according to the guidance documentation [TCOSPERG]. The loading of the initialisation script is protected by security measures to ensure security and confidentiality.
- Accesses of the card management system to the „HPC Signature Card“ are only possible after a successful CMS authentication with the establishment of

a secure channel. All further accesses in this session must use secure messaging based on the established secure channel.

„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 „HPC Signature Card“ (in the *QES application*).

After a successful, finalised personalisation, the „HPC Signature Card“ has a transport PIN (five characters) that is used only for transport protection. Before signature generation, a signature PIN must be set with a minimum length of six characters and a maximum length of eight characters (cf. [TCOSPERG], section A.1.1). For this, the designated owner of the signature key must authenticate himself to the „HPC Signature Card“ by a successful entry of the transport PIN. The generation of a signature after entry of the transport PIN is not possible. This is enforced by the „HPC Signature Card“.

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 „HPC Signature Card“ supports resetting codes with a minimum length of eight characters and maximum length of twelve characters. 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 „HPC Signature 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).

The number of signatures that can be generated after a signature PIN has been successfully entered depends on the security environment set in the card. After a successful user authentication, exactly one signature can be generated in Security Environment #1 and up to 250 signatures in Security Environment #2. „HPC Signature Card“ internally checks if the maximum value has been reached or has

been exceeded. Once the maximum value has been exceeded, a signature PIN must be inserted again in order to generate signatures.

„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 technical implementation uses 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“

„HPC Signature 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 [eHC-COS].

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

„Memory Processing“

„HPC Signature Card“ ensures, that safety-critical information (e.g. signature key, signature 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“

These 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 „HPC Signature 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 „HPC Signature Card“ closes the session. Depending from the error „HPC Signature Card“ either will be blocked or can be used in further sessions after a reset.

„Resistance against Side Channel Attacks“

„HPC Signature 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 „HPC Signature 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 „HPC Signature Card“ (initialisation, personalisation and use).

„Self-Test“

„HPC Signature Card“ provides several kinds of self-tests. After each reset as well as periodically during running time a self-test is performed automatically.

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 „HPC Signature Card“ provides the cryptographic functions. It is based on the cryptographic functions of the evaluated and certified semiconductor and its dedicated software.

„Sig Card“ supports the algorithms listed in chapter 2.1.

„Generation of Key Pairs“

„HPC Signature Card“ supports the generation of RSA and ECDSA key pairs in the card for generating qualified signatures with a length of 2048 bits for RSA keys and 256 bits for ECDSA keys.

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

- RSA keys are generated with a length of 2048 bits. 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).

- 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 $E(F_p)$ are generated with a length of 256 bits. The applied curve brainpoolP256r1 is recommended (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.2 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 generation of ECDSA keys is based on the PTRNG used with a cryptographic post-processing based on the recommendations in TR-02102 (cf. [TR-02102]), Annex B.
- The key generation guarantees that the signature key cannot be derived from the signature verification key.
- After key generation „HPC Signature Card“ 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 key generation is only possible, if the security attribute „SCD operational“ of the data object SCD has the value „no“.

The signature key pairs are generated exclusively in the card during initialisation or personalisation of the *QES application*. „HPC Signature Card“ fulfils the security requirements for the generation of RSA or ECDSA key pairs as listed above. In the use phase, the card command GENERATE ASYMMETRIC KEY PAIR is only usable to read the public key from the card. A renewed key generation is not possible.

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

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

„Generation of Qualified Signatures“

„HPC Signature Card“ supports the generation of qualified electronic signatures with RSA and ECDSA signature keys with lengths of 2048 bits for RSA keys and 256 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 digital signatures with RSA according to the PKCS #1 standard in version 2.1 [PKCS#1] with the RSASSA-PSS formatting procedure as well as the ISO standard 9796-2 [ISO 9796-2] with the ISO9796-2 DS2 formatting procedure with a key length of 2048 bits.
- Generation of ECDSA signatures according to [eHC-COS], signECDSA (cf. [TR-03111]) with a key length of 256 bits.

- The Physical True Random Number Generator (PTRNG) of the underlying hardware with a PTG.2 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“.
- 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).
- The use of the multi signature capability is only possible in the security environment SE#2. In this case, signatures can only be generated after a successful user authentication and a mutual authentication with the establishment of a secure channel. All accesses for the generation of a signature are performed with secure messaging. The external world must have authenticated itself under the role “SAC for stack or comfort signatures”.

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 1: 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.
(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 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

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 Initialisation Party

- The initialisation data provided by Deutsche Telekom Security 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 [TCOSPERG] must be taken into consideration.

Conditions of Use for the Signature Counter

During initialisation the number n of signatures (value of the signature counter, Security Environment #1: n = 1, Security Environment #2: n = 250) that may be generated after one entry of the signature PIN is determined. Generally, a number greater than one is only allowed if the following conditions are satisfied:

The TSP is obliged to inform the applicator about the special security requirements for the operational environment of the QSCD with the possibility to generate several or an indefinite number of signatures (multi-signature QSCD) according to [Reg No. 910/2014]. The information must be performed before issuing the qualified certificate and shall list the special security requirements resulting from the high potential of attacks in a detailed way. Especially but not exclusively, all security requirements for the environment must be indicated that are part of the designation.

Considering the given circumstances and the planned purpose of use, the operational environment must be protected by the owner of the signature key in a physical and logical way such that misusing the signature functionality of the multi-signature QSCD and spying of the identification data (signature PIN) by attackers with a high potential of attack can be practically excluded and such that the owner of the signature key alone controls the process of signature generation. The TSP is obliged to name at least one operational environment fulfilling these requirements.

The physical security requirements include the protection from an unauthorised access to the QSCD, especially in an unattended mode of operation. In this context the TSP shall inform specifically about the attribution of the qualified digital signatures [Reg No. 910/2014].

The logical measures of protection include that only designated products according to [Reg No. 910/2014] or products sufficiently verified with manufacturer's declaration may be used and that the following additional conditions are satisfied:

- properly installed product and observance of the scheduled operational environment according to the security notes in the corresponding manuals and designations,
- regular verification of the integrity of the product and of the platform it is based upon (hardware and operating system),
- protection of the IT platform against malware,
- trust worthy security administration,
- trust worthy network infrastructure, if the QSCD is used in an IT network and
- trust worthy connection to external communication networks, if the QSCD is operated within an IT network that is connected to external communication interfaces.

The TSP should inform the owner of the signature key in a multi-signature QSCD that in case of any doubts on a sufficient security of his operational environment a conformity and designation department according to [Reg No. 910/2014] should be contacted.

Requirements for the Responsible Personalisation Party

- The personalisation party must ensure that the personalisation data (especially of the *QES 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 [TCOSPERG] must be adhered to.
- The value one for the signature counter as provided by the card manufacturer during personalisation may only be changed under observation of the conditions of use for the signature counter.

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.
- 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.
- The TSP must inform the owner of the signature key about designated card terminals and corresponding signature application components where the owner can activate his signature PIN.

  This aspect must be considered in the TSP's security concept.

- Programs which a TSP provides to his clients for the transmission of reference data to „HPC Signature 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 – depending from the personalisation model – verify that the 5 digits transport PIN is still valid by setting a new signature PIN chosen by himself with a length of at least six digits. If the transport PIN 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 „HPC Signature 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 TCOS Flexcert Version 2.0 Release 2/SLC52 as well as of the *QES 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, [TCOSPERG], chapter 4.4.

3.3 Cryptographic Algorithms and Parameters

For the generation of digital signatures, „HPC Signature Card“ provides RSA according to [PKCS#1] and ECDSA based on groups $E(F_p)$ according to [TR-03111]. Key lengths of 2048 bits for RSA and 256 bits for ECDSA with the Brainpool curve P256r1 according to [RFC 5639] are supported. The key length is set by the considered initialisation scripts during initialisation and cannot be changed afterwards. For RSA signatures RSASSA-PSS according to [PKCS#1] and ISO9796-2 DS2 according to [ISO 9796-2] 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 random number generator (PTRNG) of the underlying hardware is supported. The PTRNG of the underlying hardware from Infineon Technologies is a random number generator with a PTG.2 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]). This generator is used for RSA key generation and for ECDSA signature generation. In the process of RSA key generation, 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. For the generation of ECDSA keys PTRNG is used with a cryptographic post-processing based on the recommendations in TR-02102 (cf. [TR-02102]), Annex B.

The cryptographic algorithms used by the product „HPC Signature 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 PSS (PKCS #1, v2.1), recommended
- ISO 9796-2, recommended

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

- Brainpool Curve Family [RFC 5639] with brainpoolP256r1, recommended

Recommended mechanisms fully reflect the state of the art in cryptography. So, the use of ECDSA with the parameters chosen by „HPC Signature Card“ is not restricted by the algorithm catalogue SOG-IS [SOG-IS]. RSA signatures with the parameters chosen by „HPC Signature Card“ may only be used until 31 December 2025. 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.

This certification of the „HPC Signature Card“ is therefore valid until **31.12.2027**.

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 TCOS Health Professional Card Version 2.1 Release 1/SLC52 was evaluated successfully according to the Common Criteria (CC) Version 3.1 with an assurance level **EAL 4+** (EAL 4 with augmentation ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5).

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

The underlying card operating system TCOS Flexcert Version 2.0 Release 2/SLC52 was successfully evaluated according to Common Criteria (CC) Version 3.1 with

assurance level **EAL4+** (EAL4 with augmentations ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5). The evaluation was performed against a **high** attack potential.

The German security certificate BSI-DSZ-CC-0904-V2 of 24. June 2021 is available for this.

For the evaluation of „HPC Signature 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] (cf. [ETR]) 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] were used. 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_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 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-1079-V2-2020.

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

[VDV] Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung – VDV) vom 15. Februar 2019

[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 20] Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitätsklassen und Evaluierungsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013

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

[ANSI X9.63] American National Standard X9.63-2001, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2005-11

[BSI-CC-PP-0082] BSI, Common Criteria Protection Profile – Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082-V4, Version: 2.1, Date: 10 July 2019

[eHC-COS] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.13.1 vom 01.11.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[EGK-Wrap] Einführung der Gesundheitskarte, Spezifikation Wrapper, Version 1.8.0, 24.08.2016, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), TCOS Health Professional Card Version 2.1 Release 1/SLC52, Version 1.0, 16.07.2021, SRC.00043.QSCD.07.2021

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

[FIPS 186-4] NIST: FIPS Publication 186-4: Digital Signature Standard (DSS), 2013.

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

[HPC-ObjSys] Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem, Version 5.0.0 vom 10.09.2020, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[HW CR] Certification Report of the underlying hardware platform, BSI-DSZ-CC-1079-V2-2020 for IFX_CCI_00000Fh, IFX_CCI_000010h,IFX_CCI_000026h, IFX_CCI_000027h,IFX_CCI_000028h, IFX_CCI_000029h,IFX_CCI_00002Ah, IFX_CCI_00002Bh,IFX_CCI_00002Ch in the design step G12 and including optional software libraries and dedicated firmware from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020-06-16

[HW ST] Security Target of the underlying hardware platform, Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+, IFX_CCI_00000Fh, IFX_CCI_000010h,IFX_CCI_000026h, IFX_CCI_000027h,IFX_CCI_000028h, IFX_CCI_000029h,IFX_CCI_00002Ah, IFX_CCI_00002Bh,IFX_CCI_00002Ch G12, Date 2020-04-03, Version 0.8

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

[ISO 9796-2] ISO/IEC 9796-2:2010 Information technology - Security techniques - Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, ISO, 2010-12

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

[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 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

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

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

[SPUB 800-38B] NIST: Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

[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] Specification of the Security Target TCOS Health Professional Card Version 2.1 Release 1/SLC52, Deutsche Telekom Security GmbH, Version: 2.0.2, 07.07.2021

[TCOSADM] TCOS FlexCert Version 2.0 Release 2, Administrator's Guidance, Guidance Documentation of TCOS FlexCert Version 2.0 Release 2/SLC52, Deutsche Telekom Security GmbH, Version 1.0, 26.05.2021

[TCOSPERG] TCOS Health Professional Card Version 2.1 Release 1, Operation and Personalization Guidance, Guidance Documentation of TCOS Health Professional Card Version 2.1 Release 1, Deutsche Telekom Security GmbH, Version 1.0, 09.07.2021

[TCOSWRG] TCOS FlexCert Version 2.0 Release 2, Guidance, Guidance Documentation of the Wrapper to TCOS FlexCert Version 2.0 Release 2/SLC52, Deutsche Telekom Security GmbH, Version 1.0, 26.05.2021

[TR-02102] BSI: Technische Richtlinie TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2013.02, Stand: 09.01.2013

[TR-03106] Technische Richtlinie BSI TR-03106, eHealth – Zertifizierungskonzept für Karten der Generation G2, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.2, 27.07.2017

[TR-03110] BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, 24. März 2010

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

[TR-03114] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03114, Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007

[TR-03115] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03115, Komfortsignatur mit dem Heilberufsausweis, Version 2.0, 19.10.2007

[TR-03143] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03143, eHealth G2-COS Konsistenz-Prüftool, Version 1.1, 18.05.2017

[TR-03144] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03144, eHealth – Konformitätsnachweis für Karten-Produkte der Kartengeneration G2, Version 1.2, 27.07.2017

End of certification report