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
Articles 29 (1) and Annex II of the Regulation (EU) No. 910/2014
that the

Qualified Signature Creation Device
STARCOS 3.6 QES C1

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

Certificate is valid until

31.12.2025

SRC Certificate Registration Number

SRC.00048.QSCD.05.2022

This certificate is only valid with the certification report.

Bonn, 30 May 2022

Gerd Cimiotti

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

[1] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive1999/93/EC.

Description of the Qualified Signature Creation Device (QSCD):

1. Product Name and Scope of Delivery

1.1 Product Name

Signature Creation Device STARCOS 3.6 QES C1 from Giesecke+Devrient Mobile Security GmbH (G+D MS).

The product is a health professional card of the German Health Care Infrastructure. The product is sold by the manufacturer under the sales name STARCOS 3.6 QES C1. The product is a smart card usable for the generation of qualified signatures and will be denoted as „HPC Signature Card“ in the following.

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. The hardware of the „HPC Signature Card“ consists of the Chip M7893 B11 with the provided Crypto Co-Processors "Crypto@2304T" (Cryptography with RSA and elliptic Curves) and "Symmetric Crypto Processor" (Encryption and Decryption with AES), where the crypto library provided by Infineon is not used.

The smart card embedded software contains the operating system STARCOS 3.6 COS C1. 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 [EGK-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“ will be delivered as smart card with the *QES application* by the Trust Service Provider (TSP) to the customer. For this, the TSP obtains the cards from Giesecke+Devrient Mobile Security GmbH. The manufacturer loads the card operating system and, if applicable, the *QES application* into the card.

The personalisation of the card is also conducted by the trust service provider (or by a commissioned third party), who loads the specific data into the card and then delivers it to the end customer. With the personalisation, the signature key pair is generated internally on the card and a specific transport PIN is set 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 included, i.e. the signature key and the corresponding signature key certificate are already on the card.

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

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

For the certified version of STARCOS 3.6 QES C1 the manufacturer provides in [AGD_Ini] and [AGD_Pers] specific values to the parameters „Chip Manufacturer

Data“, „Version of the Operating System“, „Fabkey Key Material Identification“ and „OS Completion Level / Initialisation Table Identifier“. These values can be read from the card during production with the command „GET PROTOCOL DATA“ (CLA = A0; INS = CA). During the usage phase, the “Chip Manufacturer Data”, the “Completion Status” and the “Operating System Version” can be read.

The following commands can be used to retrieve identification data:

Table 1: TOE Identification “GET PROTOCOL DATA” command

Command parameters	Identifier length	Description
P1 = ‘9F’, P2 = ‘6B’	8 bytes	Chip manufacturer data
P1 = ‘9F’, P2 = ‘6A’	7 bytes	Version of the operating system
P1 = ‘9F’, P2 = ‘6F’	7 bytes	Fabkey key material identification
P1 = ‘9F’, P2 = ‘67’	20 bytes	OS completion level / Initialisation table identifier

The following table describes the evaluated and certified configuration:

Table 2: Evaluated and certified TOE identifier

Data type	Tag in the protocol data DO	Data
Chip manufacturer data	9F6B	05 78 00 04 00 0D 00 00
OS Version	9F6A	47 44 00 B6 02 01 00
Fabkey key material	9F6F	Second byte = ‘12’
OS completion level	9F67	First three bytes = ’02 00 00’

To distinguish test cards and productive cards, the Fabkey key material is used (table 2, row 3). The second byte in the answer data of GET PROTOCOL DATA command with tag ‘9F6F’ has to be ‘12’ for productive cards. Otherwise, response ‘F8’ is shown in the second byte.

Different versions of initialisation tables may result in identical versions of the TOE. Therefore no fixed reference values can be provided for the remaining bytes of tag ‘9F67’. The response data deliver a unique reference value for every initialisation table. All references for valid initialisation tables are published on G&D website: https://certificates.gi-de.com/.

The parameters and the command are described in [AGD_Pers], section 5.7.

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	Dual interface module with hardware for contact-based and contactless interface (inlays) of completed card with or without antenna This part of the TOE consists of	**Hardware platform** M7893 B11 by Infineon Technologies (incl. its IC Dedicated Test Software) Module type: T-M8.4-8-1 (Certification under BSI-DSZ-CC-0879-V4-2020)	HW/ FW	The IC and the Embedded Software are providing self-protection mechanisms, ensuring confidentiality and integrity during delivery. The delivery does not need additional security measures and can be considered as normal transport.
2		**TOE Embedded Software** IC Embedded Software (the operating System) STARCOS 3.6 (implemented in Flash of IC)	SW	
3	Application	TOE Embedded Application Qualified Signature Application according to [HPC-ObjSys]).	SW	The application software part of the TOE is implemented in the NVM of the IC
4	Wrapper	Interface to support the reading of object information from the TOE.	SW	Item in electronic form
5	Cryptographic Keys	Cryptographic keys for personalisation, securing the TOE from personalisation by illegal entities, e.g. during transport	-	Item in electronic form, encrypted and signed to protect against disclosure or modification.
6	Main Guidance	Guidance Documentation STARCOS 3.6 – Main Document, [AGD_Main]	DOC	Document in electronic form.
7	Initialisation Guidance	Guidance Documentation for the Initialisation Phase for STARCOS 3.6 QES C1, [AGD_Ini]	DOC	Document in electronic form.

No.	Delivery item	Description / Additional Information	Type	Delivery method
8	Personalisation Guidance	Guidance Documentation for the Personalisation Phase for STARCOS 3.6 QES C1, [AGD_Pers]	DOC	Document in electronic form.
9	Usage Guidance	Guidance Documentation for the Usage Phase for STARCOS 3.6 QES C1, [AGD_Use]	DOC	Document in electronic form.
10	Internal Design Specification	Internal Design Specification for STARCOS 3.6 QES C1, [AGD_internal]	DOC	Document in electronic form.
11	Interface Specification	STARCOS 3.6 Functional Specification of the TOE interfaces for STARCOS 3.6 COS C1, [FSP_IF_COS]	DOC	Document in electronic form.
12	Wrapper Guidance	Guidance Documentation for the Wrapper, [AGD_Wrapper]	DOC	Document in electronic form.
13	Guidance for Inlay Production	Guidance Documentation for the Inlay Production, STARCOS 3.6 QES C1, [AGD_Inlay]	DOC	Document in electronic form.

1.4 Manufacturer

Manufacturer of the product is Giesecke+Devrient Mobile Security GmbH, Prinzregentenstraße 159, 81677 München, Germany.

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 the „HPC Signature Card“ consists of the Chip M7893 B11 with the provided Crypto Co-Processors "Crypto@2304T" (Cryptography with RSA and elliptic Curves) and "Symmetric Crypto Processor" (Encryption and Decryption with AES), where the crypto library provided by Infineon is not used. The chip M7893 B11 has been evaluated and certified according to CC 3.1. The base evaluation of the product has been performed based on documents of the underlying platform M7893 B11, BSI-DSZ-CC-0879-V2-2015. The IC product was undertaken a successful re-certification under BSI-DSZ-CC-0879-V4-2020, where the certificate was issued on 12.02.2020.

The software consists of the operating system STARCOS 3.6 COS C1 as well as of the *QES application* for the generation of qualified electronic signatures.

The operating system STARCOS 3.6 COS C1 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 STARCOS operating system especially supports the *QES application*. In addition to the dedicated *QES application* for generating qualified electronic signatures, there are other applications on the „HPC Signature Card“ in accordance with the specifications for the file system of the health professional card [HPC-ObjSys]. But these applications are **not** subject to the designation 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 digital signatures (RSA).

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

- The hardware platform Infineon M7893 B11 with dedicated software,
- STARCOS 3.6 COS C1 (Certificate BSI-DSZ-CC-0916-2015) and
- *QES application* with the corresponding data structures for storing and managing data of the holder of the Qualified Signature Creation Device (signature PIN, signature key).

Before the *QES application* can be used, it must be completed. This involves the generation of the signature keys by the trust service provider (TSP) (or an authorised third party) before the card is delivered. Within the scope of this completion of the *QES application*, the public key certificate is also inserted and the transport PIN is set in the card. After completion of the personalisation, it is not possible to change the programme code.

To be able to generate a signature with the completed *QES application*, the designated key holder must activate the „HPC Signature Card“ as a qualified signature creation device (QSCD). To do this, he must replace the pre-set transport PIN with a maximum of five digits with a valid 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 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 stack 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 PIN after successful user authentication with the currently valid PIN and
- resetting the PIN try counter without setting a new PIN after successful user authentication with the unblocking code (PUK).

Up to three attribute certificates can be stored in the *QES application*. These can be subsequently deleted or overwritten after the card has been issued, provided the signature key holder authorises this process by means of a specific user PIN (PIN.CH).

The „HPC Signature Card“ supports the use of secure messaging for accesses relevant to the *QES application*. For the (mutual) authentication of the external world and the card as well as for the establishment of a secure communication channel authentication protocols like asymmetric role authentication, internal authentication and mutual authentication with/without negotiation of session keys according to [EGK-COS] are supported. Within the scope of the authentications, access rights of the external world are verified. This includes in particular the right of a signature application component to generate multi-signatures or to act as a "remote PIN sender".

The security properties of „HPC Signature Card“ are explained in more detail in chapter 2.2, together with the description of the security functions.

The STARCOS operating system allows the card manufacturer a number of configuration options. Prior to initialisation, the card manufacturer has defined the configuration by creating the file system and defining further data. The installation data for loading the file system are delivered by the card manufacturer to the initialiser of the card. Confidentiality and integrity of the data and their authentic origin are ensured by cryptographic procedures.

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 to the card manufacturer. In this sense one can speak of an end-to-end security between card manufacturer and chip. This prevents the loading of incorrectly changed initialisation data. The „HPC Signature Card“ does not support the subsequent introduction of further software. Approved initialisation tables, which also have a successful certification according to [TR-03144], as well as associated identification data are given on the web pages of Giesecke+Devrient Mobile Security GmbH. The initialiser must take into account the initialisation requirements described in the guidance documents.

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

- Asymmetric RSA algorithm according to [PKCS#1] with key length of 2048 bits.
- Hash function SHA-256 according to [FIPS 180-4].
- Random number generation based on a deterministic random number generator (DRNG), whose seed is generated by the True Random Number Generator (TRNG) of the underlying hardware. The DRNG was evaluated as a DRG.4 generator with resistance to high attack potential according to [AIS 20]. The TRNG is a random number generator with a PTG.2 classification according to [AIS 31]. The random numbers are subjected to statistical tests during operation ("online tests"). These properties were tested within the scope of the CC evaluation of the hardware of Infineon (cf. [STHW], [STHW_V4], [IFX_Cert_V2], [IFX_Cert_V4]).

The generation of hash values can either be carried out within the „HPC Signature Card“ with the command PSO:HASH or completely outside the card. The command PSO:HASH can also be used for a mixed mode. For this, the first part of the data to be signed is first hashed outside the card and then the intermediate value calculated in this way and the rest of the data are passed to the card in order to calculate the final hash value in the card. In principle, the command PSO:HASH allows a so-called chaining in order to calculate the hash value of data to be signed whose length exceeds the maximum possible input length of the command by iteratively applying the command PSO:HASH.

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

- DSA based on elliptic curves (ECDSA) based on groups $E(F_p)$ (cf. [TR-03111]),
- 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 and decryption,
- Hash functions SHA-1, 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 AES algorithm according to [FIPS 197] with effective key length of 128, 192 and 256 bits (CBC-Mode, CMAC according to [TR-03110], [SPUB 800-38B]).

The „HPC Signature Card“ supports the ECC Brainpool curves P256r1, P384r1 and P512r1 according to [RFC 5639] as well as 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 augmentation 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] and Part 4: "Extension for device with key generation and trusted communication with certificate generation application", BSI-CC-PP-0071-2012 [PP SSCD Part 4]. The evaluation also strongly reuses the results of the COS platform evaluation, STARCOS 3.6 COS C1 certified under BSI-DSZ-CC-0916-2015.

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 qualified signature creation devices where the electronic signature creation data or electronic seal creation data is held in an entirely but not necessarily exclusively user-managed environment (cf. [CID (EU) 2016/650], Art. 1).

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)). Currently, this list is implemented by a dashboard administrated by the EU Commission.

2.2 Security Functions and Security Properties of „HPC Signature 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 between the roles "Administrator" (Administrator or „R.Admin“) and "Signatory" (Signatory or „R.Sigy“). 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, i.e. the signature key): „SCD operational“ (values: „yes“, „no“)

The TSP, who performs the process of activating the *QES 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 with a secret key.

A user authenticates himself to „HPC Signature Card“ as a signer by inserting his PIN.

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 [EGK-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 the establishment of a secure channel for the transmission of the data to be signed when using the multi-signature capability or with a secure transmission of the signature PIN.
- **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 can only be performed during personalisation and only if the security attribute “SCD/SVD Management” has the value “authorised”.
- The PIN for transport protection can only be set during personalisation.
- An export of sensitive information (e.g. private signature keys, transport PIN, signature PIN) via the commands of the operating system is not possible due to the access rules set.
- The substitution of the transport PIN by a real PIN by the designated signature key holder can only take place in the initial state (for the data object SCD the attribute „SCD operational“ has the value „no“, i.e. in particular the

signature key on the card cannot be used) of the „HPC Signature Card“ after a successful user authentication.

- The change of an existing PIN to a new PIN may only be performed after a successful user authentication with the old 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 based card into a reader and makes the uncontrolled communication with „HPC Signature Card“ more difficult.

„Role Authentication and Proof of Authorisation“

The „HPC Signature Card“ supports the execution of role authentication or proof of authorisation by means of (mutual) asymmetric authentication based on RSA or elliptic curves in accordance with [EGK-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, necessary 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 [EGK-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 symmetrical procedures based on the AES with a card management system (CMS) according to [EGK-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.

For the protocol based on symmetric algorithms, the „HPC Signature Card“ can basically have AES key pairs, a key for encryption and decryption operations and a key for MAC generation, of length 128 bits and 256 bits. However, due to the chosen conditions of use, these keys are not personalised and the application of a symmetric CMS authentication is therefore 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. 3.2).

Moreover, the data Signature Key Certificate and Attribute Certificates stored in the *QES application* 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 [AGD_Ini]. 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 „signatory”. It may be used only after successful setting of the PIN. User authentication is performed by comparing a PIN provided by the user with the reference value (RAD) secretly stored in „HPC Signature Card“ (in the *QES application*).

Once personalisation has been successfully completed, the „HPC Signature Card“ is equipped with a transport PIN (specific PIN), which is used exclusively for transport protection. Before generating a signature, a signature PIN must be set with a minimum length of six digits. For this purpose, the user must authenticate himself to the „HPC Signature Card“ by successfully entering the transport PIN. It is not possible to generate a signature after entering the transport PIN; this is prevented 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 electronic 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 PIN Try Counter (PTC) of a blocked PIN can be reset by using a reset code (PUK). The „HPC Signature Card“ supports a reset code with a length of at least four digits and a maximum length of twelve digits. The reset code can be used a maximum of 10 times. After entering the reset code a maximum of 10 times (incorrect or correct), it can no longer be used and it is no longer possible to reset a blocked PIN. Due to the conditions of use of the personaliser (see chapter 3.2), the minimum length of the resetting code is eight digits.

To reset the PTC, use the command RESET RETRY COUNTER. It is not possible to change a PIN. The security status of a PIN is not set, i.e. resetting a blocked PIN does not enable the generation of a qualified electronic signature.

A PIN can be changed by the key holder. To do this, he must authenticate himself against the „HPC Signature Card“ by successfully entering the current PIN, i.e. changing a PIN to a new PIN is only possible after successful user authentication using the current 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 security-critical data in the RAM that are used for the generation of qualified electronic signatures. This especially includes the signing key and the signature verification key as well as the reference value for verification of the 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] respectively the requirements to the card operating system according [EGK-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 security-critical information (e.g. signature key, PIN) are removed with the deallocation of memory. This includes all temporary and permanent parts of the memory that store security-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 on 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 such as

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

All security-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 security-critical data as a signature key or a 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.

„HPC Signature Card“ supports the algorithms listed in chapter 2.1.

„Generation of Key Pairs“

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

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 sufficiently large, that is to say $d > 2^{n/2}$.
- The high quality of the random number generation for the generation of the prime numbers ensures that the signature key and the signature verification key are not predictable and are unique with high probability. The prime numbers are generated independently of each other.
- The deterministic random number generator (DRNG) of the „HPC Signature Card“ is used for key generation.
- The key generation guarantees that the key cannot be derived from the public 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 key pairs as listed above. In the usage 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.

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 keys with lengths of 2048 bits. The security function has the following properties:

- Receipt of (already hashed) data (data to be signed, DTBS) to generate qualified signatures.

- Receipt of intermediate values of a hash value calculation or data to be hashed completely in the card with the final calculation of the hash value to generate a qualified electronic signature.

- When using the contactless interface, each hash value transferred to the „HPC Signature Card“ must be secured with a MAC.

- Generation of digital signatures with RSA according to the PKCS #1 standard in version 2.1 [PKCS#1] with the RSASSA-PSS signature format as well as the ISO standard 9796-2 [ISO 9796-2] with the ISO9796-2 DS2 format.

- The generation of signatures is resistant against side channel attacks.

- The signature is generated in a manner that the key cannot be derived from the generated signature and that during signature generation no information about the key is revealed.

- A signature can only be generated, if the user has authenticated himself successfully with a PIN (command VERIFY) and if the security attribute „SCD operational“ of the data object SCD has the value „yes“.

- 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 2: 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.

Reference	Requirement / Description / Result
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.

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 Giesecke+Devrient Mobile 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 [AGD_Ini] must be taken into consideration.
- The security notices according to [AGD_Use], 5.5.7 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 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,
- trustworthy security administration,
- trustworthy network infrastructure, if the QSCD is used in an IT network and
- trustworthy 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 designated body 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 [AGD_Pers] must be adhered to.
- The PUK for the signature PIN must be selected with a minimum length of eight digits.
- The security notices according to [AGD_Use], 5.5.7 must be taken into consideration.

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. The current version of [SOG-IS] limits their eligibility to the period until 31.12.2025.
- If the TSP distributes a product to generate qualified electronic 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 „HPC Signature Card“ (i.e. which are used by the owner of the signature key to set or change his 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.

- The security notices according to [AGD_Use], 5.5.7 must be taken into consideration.

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

- The owner of the signature key must verify that the 5 digits transport PIN is still valid by setting a new PIN chosen by himself with a length of at least six digits. If the transport PIN is not valid the owner of the key must contact the issuing TSP.

- The owner of the signature key must treat the chosen PIN as confidential. The owner of the key must not confide his PIN as well as his PUK to anybody and must keep them in a safe place.

- The owner of the key must change his PIN periodically.

- The owner of the key must use and keep „HPC Signature Card“ such that misuse and manipulation are prevented.

- When using "remote PIN entry", the „HPC Signature Card“ must be in an eHealth card terminal in a secure area and the signature key holder must use an eHealth card terminal under his control for PIN entry. The secure area must have sufficient protection to ensure the sole physical control of the signature key holder over the „HPC Signature Card“. In particular, it must not be possible to steal the „HPC Signature Card“.

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 STARCOS 3.6 COS C1 as well as of the *QES application* in an appropriate manner.

- When generating a qualified electronic signature on a hash value that has been computed by the external world and transmitted to the card, it must be guaranteed that the signature application component has chosen an appropriate hash function.

- The manufacturer of a signature application component used for the generation of qualified electronic signatures (Signature Creation Application, SCA) should consider the instructions for terminal developers pursuant to the Operational Guidance, [AGD_Use]. Especially the restrictions and

requirements for the use of cryptographic keys according [AGD_Use], section 5.5.6 have to be taken into consideration. To ensure secure use of the product's functionality, the limits on command usage according [AGD_Use], section 5.5.6 shall be applied. It must be ensured by the signature application component that these requirements are fulfilled. In addition, the security notices according [AGD_Use], section 5.5.7 must be taken into account.

3.3 Cryptographic Algorithms and Parameters

The „HPC Signature Card" provides the RSA algorithm for the generation of electronic signatures. The RSA algorithm is used with a key length of 2048 bits. The key length is set by the considered initialisation scripts during initialisation and cannot be changed afterwards. RSASSA-PSS according to [PKCS#1] and ISO9796-2 DS2 according to [ISO 9796-2] are supported as signature formats.

For the generation of electronic signatures, a card-internal or a partially card-internal hash value calculation with the hash function SHA-256 according to [FIPS 180-4] or an exclusively external hash value calculation can be used. For the use of hash functions, the conditions of use for the manufacturers of signature application components in particular must be taken into account.

The generation of random numbers is based on a deterministic random number generator (DRNG), whose seed is generated by the True Random Number Generator (TRNG) of the underlying hardware. The DRNG was evaluated as a DRG.4 generator with resistance to high attack potential according to [AIS 20]. The TRNG 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 ("online tests"). These properties were tested within the scope of the CC evaluation of the hardware of Infineon (cf. [STHW], [STHW_V4], [IFX_Cert_V2], [IFX_Cert_V4]).

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.
- ISO9796-2 DS2 (ISO 9796-2), recommended.
- Hash functions: SHA-256, SHA-512/256, SHA-384, SHA-512, recommended.

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

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 **31.12.2025**.

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 STARCOS 3.6 QES C1 was evaluated successfully according to the Common Criteria (CC) Version 3.1 with an assurance level **EAL 4+** (EAL 4 with augmentation AVA_VAN.5).

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

For the evaluation of „HPC Signature Card“ the protection profile „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 419211-4:2014“, [PP SSCD Part 4] were used.

Please note, that the base evaluation was conducted based on the protection profiles [BSI-CC-PP-0059] and [BSI-CC-PP-0071]. The protection profiles [PP SSCD Part 2] and [PP SSCD Part 4] are identical in content. They have been provided by the Technical Committee CEN/TC 224 and are referenced by 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 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [CID (EU) 2016/650]. The changes to the Protection Profile only comprises editorial aspects resulting from the standardisation of the Protection Profile by the Technical Committee CEN/TC 224. So the requirements laid down in Regulation (EU) No. 910/2014 Articles 30 (3) a, 39 (2) as well as the Commission Implementing Decision (EU) 2016/650 are fulfilled.

The evaluation of the product STARCOS 3.6 QES C1 was performed in the form of a so-called "Composition Evaluation", which takes into account the evaluation results of the CC evaluation of the M7893 B11 of the manufacturer Infineon Technologies. This evaluation was performed with assurance level **EAL 6+** (EAL 6 with augmentation ALC_FLR.1). The evaluation was performed against a **high** attack potential.

The German security certificate BSI-DSZ-CC-0879-V4-2020 of 12 February 2020 is available for this.

The underlying card operating system STARCOS 3.6 COS C1 was successfully evaluated according to the Common Criteria (CC) version 3.1 with the assurance level **EAL 4+** (EAL 4 with the augmentations ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5). The evaluation was carried out against a **high** attack potential.

The German security certificate BSI-DSZ-CC-0916-2015 dated 7 August 2015 is available for this. For this, two maintenance reports BSI-DSZ-CC-0916-2015-MA01

dated 28 January 2016 and BSI-DSZ-CC-0916-2015-MA02 dated 2 August 2018 are available. In both cases the product, the COS, was not changed.

4. References

[Reg No. 910/2014] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

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

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

[AIS 20] Bundesamt für Sicherheit in der Informationstechnik, Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitätsklassen und Evaluierungsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, 15.05.2013

[AIS 31] Anwendungshinweise und Interpretationen zum Schema, AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, 15.05.2013

AIS20/ AIS31 Common accompanying document:

A proposal for: Functionality classes for random number generators, Version 2.0, September 18, 2011, W. Killmann, W. Schindler

[BSI-CC-PP-0059] CC Protection profile: Protection profiles for secure signature creation device, Part 2: Device with key generation, Version 2.0.1, BSI-CC-PP-0059-2009-MA-01, Information Society Standardization System (CEN/ISSS), 2012-01-23

[BSI-CC-PP-0071] CC Protection profile: Protection profiles for secure signature creation device, Part 4: Extension for device with key generation and trusted communication with certificate generation application, Version 1.0.1, BSI-CC-PP-0071-2012, Information Society Standardization System (CEN/ISSS), 2012-11-14

[BSI-CC-PP-0082] BSI, Common Criteria Protection Profile – Card Operating System Generation 2 (PP COS G2), BSI-CC-PP-0082-V2, Version: 1.9, Date: 18 November 2014

[EGK-COS] Einführung der Gesundheitskarte, Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.7.0 vom

26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH, inklusive der normativen Errata

[EGK-Wrap] Einführung der Gesundheitskarte, Spezifikation Wrapper, Version 1.6.0, 26.08.2014, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), STARCOS 3.6 QES C1, Version 1.2, 06.05.2022, SRC.00048.QSCD.05.2022

[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

[FSP_IF_COS] STARCOS 3.6 Functional Specification – Part 1: Interface Specification, Version 1.19, 31.07.2015

[HPC-ObjSys] Spezifikation des elektronischen Heilberufsausweis HBA-Objektsystem, Version 3.8.1, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, 30.09.2015

[IFX_Cert_V2] Certification Report of the underlying hardware platform, BSI-DSZ-CC-0879-V2-2015 for Infineon Security Controller M7893 B11 with optional RSA2048/4096 v1.03.006, EC v1.03.006, SHA-2 v1.01 libraries and Toolbox v1.03.006 and with specific IC dedicated software (firmware), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015-11-13

[IFX_Cert_V4] Certification Report of the underlying hardware platform, BSI-DSZ-CC-0879-V4-2020 for Infineon Security Controller M7893 B11 with optional RSA2048/4096 v2.03.008, EC v2.03.008,SHA-2 v1.01 libraries and Toolbox v2.03.008 and with specific IC dedicated software (firmware), Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020-02-12

[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, 2016-06-30, BSI-CC-PP-0059-2009-MA-02

[PP SSCD Part 4] Protection Profiles for Secure Signature Creation Device - Part 4: Extension for device with key generation and trusted communication to certificate generation application, EN 419211-4:2013, BSI-CC-PP-0071-2012-MA01, 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

[ST] Security Target STARCOS 3.6 QES C1, Giesecke & Devrient GmbH, Version 1.1/10.05.16

[STHW] Security Target Lite M7893 B11 Including optional Software Libraries RSA - EC - SHA-2 - Toolbox, Version 0.2, Infineon Technologies AG, Chipcard and Security, 2015-08-31

[STHW_V4] Public Security Target M7893 B11, Version 3.7, Infineon Technologies AG, Chipcard and Security, 2020-02-03

[AGD_Main] Guidance Documentation STARCOS 3.6 – Main Document, Version 1.7/29.07.2015

[AGD_Ini] Guidance Documentation for the Initialization Phase STARCOS 3.6 QES, Version 1.2/ Status 10.05.2016

[AGD_Inlay] STARCOS 3.6 COS C1/2 Guidance Documentation for Inlay Production, Version 1.1/Status 13.07.2015

[AGD_internal] STARCOS 3.6 Internal Design Specification, Version 1.3, Status 31.07.2015

[AGD_Pers] Guidance Documentation for the Personalization Phase STARCOS 3.6 QES, Version 1.1 / Status 07.10.2015

[AGD_Use] Guidance Documentation for the Usage Phase STARCOS 3.6 QES, Version 1.2/Status 16.03.2022

[AGD_Wrapper] STARCOS 3.6 COS C1/2 Guidance Documentation for the Wrapper, Version 1.3/Status 29.07.2015

[TR-03106] Technische Richtlinie BSI TR-03106, eHealth – Zertifizierungskonzept für Karten der Generation G2, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.1, 22.05.2015

[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 2.10, 20.03.2012

[TR-03111] BSI: Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC), Version 2.0, 2013-03

[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 1.1, 22.05.2015

End of certification report