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

# AMENDMENT

Amendment 1 to the Certification
SRC.00046.QSCD.08.2021 of 16.08.2021

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 for the**

Qualified Signature Creation Device
STARCOS 3.7 HBA G2.1

**the above mentioned Certification has been amended as follows**
**and is valid until**

**31.12.2027**

This certificate is only valid with the certification report.

Bonn, 19. November 2025

Markus Schierack
21.11.2025 09:07 Uhr

Markus Schierack

Christoph Sesterhenn
19.11.2025 10:01 Uhr

Christoph Sesterhenn

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

[1] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive1999/93/EC, last amended by Regulation (EU) No. 2024/1183.

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

## 1. Product Name and Scope of Delivery

### 1.1 Product Name

Signature Creation Device STARCOS 3.7 HBA G2.1 from Giesecke+Devrient Mobile Security GmbH (G+D MS).

The product is sold by the manufacturer under the sales name STARCOS 3.7 HBA G2.1. 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. „HPC Signature Card“ is based on the Infineon Security Controller IFX_CCI_000005h (incl. its IC Dedicated Test Software). The software consists of the STARCOS 3.7 COS HBA-SMC operating system and of the application for generating qualified electronic signatures, in the following denoted as *QES application*.

The smart card embedded software contains the STARCOS 3.7 COS HBA-SMC operating system. 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 operating system developer (i.e. G+D MS) delivers the product either as card (dual interface card) or as module. It contains the operating system at delivery and may already contain the file system for the *QES application* or it contains secret data allowing secure loading of initialisation data containing the file system of the *QES application*.

The Card Initialising Facility performs the initialisation and production of the cards possibly at different sites. Afterwards the cards are delivered to the personalising facility. The delivery of the product to the QSCD provision service happens either at the delivery to the initialisation site, or the card production site or the personalisation site.

With the initialisation data secret data is imported into the product allowing secure loading of personalisation data. This secret data is sent by G+D MS to the card issuer who uses it to secure the personalisation data and then send the secured personalisation data to the personalising facility which performs the personalisation before issuance of the product. The initialisation can be done completely by G+D MS. The personalisation process as well as the generation of the personalisation data can be done partly or completely by G+D MS.

The operating system is implemented in the Flash area of the IC. The file system containing the application data is also installed in the Flash memory of the IC. Beside

the files for the *QES application* there may be additional files for other applications, e.g. for a health professional application, which do not belong to the designation of the product. The file system part of the „HPC Signature Card“ is represented by the Guidance Documentation that define the security relevant parts of the file system.

Each application, in particular the *QES application*, defines access rules to protect itself against misuse and unauthorised access. Usually the data structures for applications are loaded onto the card during initialisation and personalisation. Nevertheless, it is still possible to add some data structures in the usage phase to the signature application. Furthermore, the complete data structures of additional applications may be loaded during the usage phase. These data structures do not include any executable code, therefore application functionality is always limited to the functionality of the operating system.

The authenticity and integrity of a card or a module 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 3.7 HBA G2.1 [AGD_init] provides the manufacturer specific values to the parameters „Chip Manufacturer Data“ and „Version of the Operating System“. These values can be read from the card during production with the command „GET PROTOCOL DATA“ according to [AGD_init], chapters 4.2.4 and 4.6.2 or [AGD_pers], chapter 5.7.2. During the usage phase the parameters „Chip Manufacturer Data“ and the „Version of the Operating System“ can be read from the card according to [AGD_use], chapter 4.1.1.2.

## 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 | Completed card with hardware for contact-based and contact-less interface. | **Hardware platform**<br><br>IFX_CCI_000005h Infineon Technologies (incl. its IC Dedicated Test Software).<br><br>(Refer to the Certification Report BSI-DSZ-CC-1110-V3-2020) | HW/ FW | The IC and the Embedded Software are providing self-protection mechanisms, ensuring confidentiality and integrity |

| No. | Delivery item | Description / Additional Information | Type | Delivery method |
|---|---|---|---|---|
| 2 | | **TOE Embedded Software**<br><br>IC Embedded Software STARCOS 3.7 HBA G2.1 (the operating system STARCOS 3.7 HBA-SMC including the *QES Application* [Appl_Spec] implemented in Flash of the IC) | SW | during delivery. The delivery does not need additional security measures and can be considered as normal transport. |
| 3 | 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 and modification. |
| 4 | Main Guidance | Guidance Documentation STARCOS 3.7 HBA G2.1 – Main Document, [AGD_main]. | DOC | Document in electronic form. |
| 5 | Initialisation Guidance | Guidance Documentation for the Initialisation Phase for STARCOS 3.7 HBA G2.1, [AGD_init]. | DOC | Document in electronic form. |
| 6 | Personalisation Guidance | Guidance Documentation for the Personalisation Phase for STARCOS 3.7 HBA G2.1, [AGD_pers]. | DOC | Document in electronic form. |
| 7 | Usage Guidance | Guidance Documentation for the Usage Phase for STARCOS 3.7 HBA G2.1, [AGD_use]. | DOC | Document in electronic form. |
| 8 | Internal Design Specification | Internal Design Specification for STARCOS 3.7, [AGD_internal] | DOC | Document in electronic form. |
| 9 | Interface Specification | Functional Specification STARCOS 3.7 HBA G2.1, [FSP] | 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 smart card product „STARCOS 3.7 HBA G2.1“ is intended for the use as a card for the generation of qualified signatures. 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 Infineon Security Controller IFX_CCI_000005h (incl. its IC Dedicated Test Software). The Infineon Security Controller IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h in design step H13 including optional software libraries and dedicated firmware was evaluated CC EAL 6+ (CC Version 3.1) and is listed under the Certification ID BSI-DSZ-CC-1110-V3-2020.

The software consists of the operating system STARCOS 3.7 COS HBA-SMC operating system as well as of the *QES application* for the generation of qualified signatures (cf. [Appl_Spec]).

The STARCOS 3.7 COS HBA-SMC operating system 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*. Further applications may exist on the „HPC Signature Card“ besides the dedicated *QES application* for the generation of qualified signatures. 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 and elliptic curve keys and
- generation of digital signatures (RSA and elliptic curves).

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

- The hardware platform Infineon IFX_CCI_000005h (Certificate BSI-DSZ-CC-1110-V3-2020).

  The hardware platform has the following features:

  - Flash: 448 kByte
  - RAM: 12 kByte
  - Symmetric Co-Processor for DES/AES (SCP): Accessible
  - Asymmetric Co-Processor for RSA/ECC (Crypto2304T): Accessible

- STARCOS 3.7 COS HBA-SMC operating system (Certificate BSI-DSZ-CC-0976-V4-2021) and

- *QES application*.

Before the *QES application* can be used, it must be completed. This involves the generation of the signature keys by the certification service provider (CSP) (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. The „HPC Signature Card“ supports one RSA key with key length of 2048 bit and one ECDSA key with key length 256 bit.

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).

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 authentication, internal authentication and mutual authentication with/without negotiation of session keys accordingly are supported. Within the scope of the authentications, access rights of the external world are verified.

The security properties of „HPC Signature Card“ are explained in more detail 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. 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.
- DSA based on elliptic curves (ECDSA) using the groups $E(F_p)$ (cf. [TR-03111]) with key length of 256 bits,
- 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. [HW ST], [IFX_Cert]).

„HPC Signature Card“ supports the ECC curve brainpoolP256r1 according to [RFC 5639].

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

- Asymmetric operations on the basis of elliptic curves (cf. [TR-03111]) for authentication and encryption/decryption.
- Hash function SHA-1 according to [FIPS 180-2], where SHA-1 is used only for derivation of symmetric session keys,
- Hash functions SHA-224, SHA-256, SHA-384 and SHA-512 according to [FIPS 180-2] used only for internal operations,
- 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 is used for the encryption of communicated data. „CMAC Mode for Authentication“ is used to ensure data integrity (cf. [SPUB 800-38B]).

„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 5: "Extension for device with key generation and trusted channel to signature generation application", BSI-CC-PP-0072-2012 [PP SSCD Part 5]. The evaluation also strongly reuses the results of the COS platform evaluation, STARCOS 3.7 COS HBA-SMC operating system certified under BSI-DSZ-CC-0976-V4-2021.

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)).

## 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 between the roles "Administrator" and "Signatory". Furthermore, the following security attributes are used:

- For an authenticated role: „SCD / SVD Management“ (values: „authorised“, „not authorised“)
- For the data object Signature Creation Data (SCD, the i.e. signature key): „SCD operational“ (values: „yes“, „no“) and „SCD identifier“ (arbitrary value)

The CSP, 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.

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 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 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.

- 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.

- Due to well defined access rules, sensitive data such as signature key and PIN cannot be read out using the commands of the operating system.

**„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 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 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 [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 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.

**„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 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 [AGD_init]. 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 and a maximum length of eight 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 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 eight 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.

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

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

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 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 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 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 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 $d > 2^{n/2}$.
- 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 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.
- An import of key pairs is not possible.
- 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.

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 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 signatures.
- Generation of RSA signatures with PSS according to chapter 8 and 9 of [PKCS#1] with a key length of 2048 bits.
- Computation of ECDSA signatures according to [TR-03111] with key length of 256 bits.
- The deterministic random number generator (DRNG) of the „HPC Signature Card“ is used to generate random numbers for the generation of ECDSA signatures.
- 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“.
- 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 role authentication and device 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 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**<br><br>Qualified electronic signature creation devices shall meet the requirements laid down in Annex II. |
| (2) | **Requirement**<br><br>The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48 (2). |
| **Annex II** | **Requirements for qualified electronic signature creation devices** |
| 1. | **Requirement**<br><br>Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least: |
| (a) | the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured; |
| (b) | the electronic signature creation data used for electronic signature creation can practically occur only once; |
| (c) | the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology; |
| (d) | the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others. |
| 2. | **Requirement** |

| Reference | Requirement / Description / Result |
|---|---|
| | 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. |

Article 29 (1a) concerning qualified trust service providers managing electronic signature creation data on behalf of the signatory is not relevant for the product.

## 3.2 Conditions of Use

**Requirements for the Responsible Initialisation or Pre-Personalisation Party**

- The initialisation data (pre-personalisation) 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_init] 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 CSP 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 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 personalisation party must ensure that cryptographic keys used to protect the personalisation data must be treated in a secure way.
- The card manufacturer's requirements to the personalisation according to [AGD_pers] must be adhered to.

**Requirements for the CSP**

- The CSP 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 (cf. section 3.3).
- If the CSP distributes a product to generate qualified electronic signatures with a product name that differs from the product name in the designation, then the CSP must point out the actual designated product in the documentation for the distributed product.
- The CSP must ensure that the key length as implicitly chosen by him during key generation is appropriate from the beginning of key generation until the expiration date of the qualified certificate (cf. section 3.3).
- Programs which a CSP 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.

**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 CSP.
- The owner of the signature key must treat the chosen PIN as confidential. The owner of the key must not confide his PIN to anybody and must keep it 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.

**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 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].

## 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 are supported. Signatures are only generated with hash values that have been computed by the external world.

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 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. [HW ST], [IFX_Cert]).

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.

  Though SOG-IS has the RSA 2048 with legacy until 31.12.2025, as the exchange of the product is more time consuming as expected due to the large amount of cards in the field it is acceptable to extend the usage of RSA 2048 until 30.06.2026. This extension is regarded as acceptable in the light of RSA 2048 set to legacy until 31.12.2028 according to the recommended end dates for key sizes defined by ETSI TS 119 312 [ETSI TS 119 312], section 8.4. In addition, the suitability of RSA 2048 was set to end of 2030 by NIST according to NIST SP 800-78-5 [SPUB 800-78-5], section 3.1 which also supports the defined extension.
- RSA PSS (PKCS #1, v2.1), recommended.

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

- brainpoolP256r1 according to [RFC 5639], recommended

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

- 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“ (key length of 2048 bits) may only be used until **30 June 2026**. The CSP 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.

### 3.4 Assurance Level and Attack Potential

The product STARCOS 3.7 HBA G2.1 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 Part 5: "Extension for device with key generation and trusted channel to signature generation application", BSI-CC-PP-0072-2012 [PP SSCD Part 5] (cf. [ETR]) were used. 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 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_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h in design step H13 including optional software libraries and dedicated firmware. This evaluation was performed with an assurance level **EAL 6+** (EAL 6 augmented with ALC_FLR.1). The evaluation was performed against a **high** attack potential.

The semiconductor is listed under the Certification ID BSI-DSZ-CC-1110-V3-2020.

## 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, last amended by Regulation No 2024/1183

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

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

[AIS 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

[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

[ETSI TS 119 312] ETSI TS 119 312 V1.5.1 (2024-12), Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites, Version 1.5.1, Date: 2024-12

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), STARCOS 3.7 HBA G2.1, Version 1.0, 03.08.2021, SRC.00046.QSCD.08.2021

[EGK-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

[FIPS 180-2] NIST: FIPS Publication 180-2: Secure Hash Standard (SHS), August 2002 und Change Notice 1, February 2004.

[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

[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

[HW ST] Common Criteria Public Security Target, EAL6 / EAL6+, IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h, H13 , Resistance to attackers with HIGH attack potential, Revision 1.8, 2020-04-22, Infineon Technologies AG

[IFX_Cert] Certification Report, BSI-DSZ-CC-1110-V3-2020 for Infineon Security Controller IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik (BSI), 13 May 2020

[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 5] Protection Profiles for Secure Signature Creation Device - Part 5: Extension for device with key generation and trusted channel to signature creation application, EN 419211-5:2014, BSI-CC-PP-0072-2012, 2012-11-14

[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

[SPUB 800-78-5] NIST Special Publication 800, NIST SP 800-78-5: Cryptographic Algorithms and Key Sizes for Personal Identity Verification, July 2024

[ST] G+D Mobile Security, Security Target, STARCOS 3.7 HBA G2.1, Version 1.8, 02.08.2021, Company Confidential

[AGD_main] G+D Mobile Security, Guidance Documentation, STARCOS 3.7 HBA G2.1, Main Document, Version 1.0, 21.04.2021, G+D Business Confidential

[AGD_init] G+D Mobile Security, Guidance Documentation for the Initialisation Phase STARCOS 3.7 HBA G2.1, Version 1.1, 29.04.2021, G+D Business Confidential

[AGD_pers] G+D Mobile Security, Guidance Documentation for the Personalisation Phase STARCOS 3.7 HBA G2.1, Version 1.0, 21.04.2021, G+D Business Confidential

[AGD_use] G+D Mobile Security, Guidance Documentation for the Usage Phase STARCOS 3.7 HBA G2.1, Version 1.0, 21.04.2021, G+D Business Confidential

[AGD_internal] G+D Mobile Security, STARCOS 3.7 COS Internal Design Specification, Version 1.0, 04.04.2018

[AGD_Wrapper] STARCOS 3.7 COS Guidance Documentation for the Wrapper, Version 1.3/Status 10.02.21, G+D Business Confidential

[Appl_Spec] G+D Mobile Security, STARCOS 3.7 HBA G2.1, Application Information, Monday, June 7, 2021 2:41:30 PM, html-file

[FSP] G+D Mobile Security, Functional Specification STARCOS 3.7 HBA G2.1, Version 1.1, 21.07.2021, G+D Business Confidential

[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 2.10, 01.06.2018

[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 amendment 1**