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

Qualified Signature Creation Device
IDEMIA_HC_Germany_NEO_G2.1_HBA, V1

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.00036.QSCD.09.2020

This certificate is only valid with the certification report.

Bonn, 29 September 2020

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

Qualified Signature Creation Device IDEMIA_HC_Germany_NEO_G2.1_HBA, V1 from IDEMIA.

The product is a Health Professional Card (HPC) of the German health telematics and is referred to in the following briefly as “HPC Signature Card”.

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 “HPC Signature Card” consists of an integrated circuit (IC) family H13 with Crypto Libraries ACL v2.08.007, SCL v02.04.002 and Hardware Support Library (HSL) v03.12.8812 provided by Infineon Technologies AG. For cryptographic support “HPC Signature Card” uses SCL v02.04.002 for AES and CMAC and ACL v2.08.007 for RSA incl. key generation as well as ECDSA incl. key generation. The hybrid random number generation that meets AIS31 PTG.3 is used by the “HPC Signature Card” as well.

The smart card embedded software contains the operating system IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1. This platform is an ISO-7816 compatible, multifunctional platform, that fulfils the requirements for the card operating system generation 2 of the German Health Care system pursuant to [eHC-COS]. The “HPC Signature Card” fulfils the requirements to the related object system according [HPC-ObjSys]. It has the application for creating qualified electronic signatures, referred to below as the QES application, and is generally provided with further applications, such as the health professional application and the ESIGN application. However, the other applications are not the subject of this certification.

The “HPC Signature Card” is delivered as a card with QES application by the Certificate Service Provider (CSP) to the end customer. The CSP purchases the cards from IDEMIA GmbH. The manufacturer loads the card operating system and the QES application into the card.

The card is personalised by the CSP (or an authorised third party) before he delivers it to the end customer. Personalisation is also used to generate the signature key pair within the card and to set a specific transport PIN as transport protection for the delivery to the customer. When the card is delivered to the end customer, it contains all data. That is, the signature key and the corresponding signature key certificate are already in the card.

The product is a flash product so that the loading of the operating system can be its own step separated from the manufacturing of the IC. The card preparation consists of the OS flashing (loading of the COS on the flash memory), the product pre-personalisation and the personalisation phase.

- The OS Flashing phase can be done by the IC Manufacturer after the IC Pre-Personalisation or it is postponed after the delivery of the ICs to IDEMIA. An additional aspect of the OS Flashing phase is that initial key material is

loaded into the card and stored. This key material is used for authentication purposes during the following life cycle phases. After the OS Flashing phase, the flash-loader is effectively blocked upon first start of the COS.

- In the Product Pre-Personalisation phase, the object system together with non-individual card data (e.g. file system) are loaded onto the card. After the phase has been successfully completed, the product enters the personalisation mode in which individual data may be stored but no further extensions of the object system are possible.
- During Product Personalisation, the card individual data can be stored by the Product Personaliser. The product supports the secure Product Personalisation via a secured channel.

The product is delivered by IDEMIA in different variants. The variants non-pre-personalised smartcard or module, pre-personalised smartcard or module or pre-personalised and personalised smartcard may apply. The product is delivered

- to an external Pre-Personaliser as a non-pre-personalised smartcard or module with the dedicated load files, the product data sheet, and the guidance for the Pre-Personaliser and the Personaliser. Furthermore, the delivery contains key material required for conducting the Product Pre-Personalisation/Personalisation. This is the case if IDEMIA does not conduct the Product Pre-Personalisation and the Product Personalisation.
- to an external Product Personaliser as a pre-personalised smartcard or module, the product data sheet and the guidance for the Product Personaliser. Furthermore, the delivery contains key material required for conducting the Personalisation. This is the case if IDEMIA conducts the Product Pre-Personalisation.
- to the smartcard issuer as a pre-personalised and personalised smartcard. In this case, only the operational guidance is shipped additionally to the issuer. This is the case if IDEMIA also conducts the Product Personalisation.

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

[Idemia_AGD_PRE], section 8.7 describes the data objects that contain the specific values of the product. The data object “CPLC information” contains among others “IC Fabricator”, “IC Type”, “Operating System Identifier”, “Operating System Release Date”, “Operating System Release Level”, “Serial Number”, “Product Configuration”, “IC Personaliser”, “IC Personalisation Date” and “IC Personalisation Equipment Identifier”. The data object “Card Configuration” contains “Family Identifier”, “Configuration Identifier”, “Mask Identifier”, “Mask Date”, “Mask Identifier”, “IC Manufacturer” and “IC Type”.

All these values can be read from the card during personalisation with the command “GET DATA”.

During personalisation, the authenticity and integrity of a card or module can be verified using the correct personalisation key by a mutual authentication between the card and the personalisation system.

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	TOE_IC	Integrated Circuit (IC) family H13 with Crypto Libraries ACL v2.08.007, SCL v02.04.002 and Hardware Support Library (HSL) v03.12.8812 provided by Infineon Technologies AG contact based / contactless module	HW / SW	Delivery of not-pre-personalised / pre-personalised smart-cards
2	TOE_ES	Smartcard Embedded Software comprising the IDEMIA_HC_Germany_NEO_G2.1_COS, V1 as Card Operating System Card (designed as flash implementation) for the German Health Care System provided by Idemia Version V1 ES Revision/Release 2.2.4 Variants: 0x10 or 0x11	SW	Delivery of OS Flashing image (implemented in EEPROM/Flash of the microcontroller)
3	Wrapper	Wrapper for interpretation of the exported TSF data. Version 2.2.6 The Wrapper software is delivered as 7z archive. The 7z archive file must have the following SHA256 checksum: A1BC338E1B4F40E2F0334DBB2643160020505B929E23C1F391FA47E69202E5C6 The 7z archive consists of Wrapper.jar iwrapper.jar jdom-2.0.5.jar bcprov-ext-jdk15on-150.jar For the corresponding SHA256 checksums, see [Idemia_Wrapper], chap. 1.1.	SW	Delivery as electronic file

No.	Delivery item	Description / Additional Information	Type	Delivery method
4	OS-PrePerso sequence	Command sequence used by the OS Pre-Personalizer to configure the Card Operating System. Signed by the developer. The signature is verified by the TOE_ES.	SW	Delivery as electronic file
5	Associated guidance documentation	IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 – Preparative Guidance, [Idemia_AGD_PRE], IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 – Operational User Guidance, [Idemia_AGD_OPE], IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 –Wrapper Guidance, [Idemia_Wrapper] IDEMIA_HC_Germany_NEO_G2.1_COS V1 – Data Sheet Data Sheet with information on the actual identification data and configuration of the gHC Card	DOC	Document in paper / electronic form
6	Aut-Key K_MORPHO_AUT	Public part of the authentication key pair relevant for the authenticity of the TOE	KEY	Document in paper form / electronic file[1]
7	Perso-Key K_OBJ_PERS	Personalisation key relevant for the product personalisation of the TOE	KEY	Document in paper form / electronic file
8	Object System Signature Key K_OBJ_VERIFICATION	Object System Signature Key, needed for calculation of the Signature over an Object System.	KEY	Document in paper form / electronic file
9	OS PrePersonaliser Master Key K_OS_PREPERS_MK	Key for derivation of card individual authentication keys	KEY	Document in paper form / electronic file
10	K_OPE_DEC	Key needed for encryption of secrets in Load Application sequences. Used for encryption and integrity check of key data imported during the Operational phase	KEY	Document in paper form / electronic file

[1] The Public Key Part is delivered as part of the data sheet

No.	Delivery item	Description / Additional Information	Type	Delivery method
11	K_OPE_VERIFICATION	Key needed to calculate a Signature over Load Application sequences. Used for generation of the signature calculated during the creation of the LOAD APPLICATION commands for a possible In-Field update	KEY	Document in paper form / electronic file

Note: The PrePersoScript is also part of the TOE delivery, although it is not part of the TOE. The PrePersoScript is a specific command sequence sent to the card by the Product Pre-Personaliser of the Card to create internally the non-card individual data. It is signed by the developer and the signature is verified by the TOE_ES. It is delivered as electronic file.

Deliverables in paper form require a personal passing on or a procedure of at least the same security. Deliverables in electronic form have to be submitted integrity and authenticity protected. For Key material also confidentiality has to be ensured.

The commercial numbering of the TOE by Infineon Technologies AG is as follows:

H13 chip family

Product Type: SLC32GDA

By executing the GET DATA command, the following product identifications of the foundry are given:

IC Manufacturer: 81 00

IC Type: 13 2A

OS Version: 02 02

Mask Date: 00 62

OS Subversion: 04 00

1.4 Manufacturer

Manufacturer of the product is IDEMIA, 18, Chaussée Jules César, 95520 Osny, FRANCE.

2. Functional Description

2.1 Functionality and Architecture

The “HPC Signature Card” is implemented as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. The hardware of “HPC Signature Card” consists of an integrated circuit (IC) family H13 with Crypto Libraries ACL v2.08.007, SCL v02.04.002 and Hardware Support Library (HSL) v03.12.8812 provided by Infineon Technologies AG. For cryptographic support “HPC Signature Card” uses SCL v02.04.002 for AES and CMAC and ACL v2.08.007 for RSA incl. key generation as well as ECDSA incl. key generation. The hybrid random number generation that meets AIS31 PTG.3 is used by the “HPC Signature Card” as well. The hardware was evaluated according to CC 3.1 and certified (BSI-DSZ-CC-1110-V3-2020).

The software consists of the operating system IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 (flash) as well as of the QES application for the generation of qualified electronic signatures as part of the product’s file system. The card operating system was evaluated according to CC 3.1 and certified (BSI-DSZ-CC-1098-2020).

The operating system IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 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 card’s operating system supports in particular the QES application. Further applications (e.g. Health Professional Application) may exist on the “HPC Signature Card” besides the dedicated QES application for the generation of qualified digital signatures. But these applications are not subject to the designation at hand.

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

- On-card-generation of RSA and EC key pairs of high quality
- Different signature schemes (RSA and EC)
- Different encryption schemes (based on AES and RSA with appropriate key lengths and padding schemes)
- Key derivation schemes
- PIN based authentication scheme
- Different key based authentication schemes (based on AES, EC and RSA, with / without session key agreement)
- Hash value calculation
- Random number generation of high quality
- Calculation and verification of cryptographic checksums
- Verification of Card Verifiable certificates (CV certificates)
- Protection of the communication between the product and the external world against disclosure and manipulation (Secure Messaging)
- Protection of files and data by access control functionality
- Life-cycle state information related to the Operating System itself as well as to all objects processed by the card

- Confidentiality of cryptographic keys, PINs and further security critical data
- Integrity of cryptographic keys, PINs and further security critical data
- Confidentiality of operating system code and its internal data
- Resistance of crypto functionality against Side Channel Analysis (SPA, DPA, TA, DFA)
- Card management functionality
- Channel management (with separation of channel related objects).

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

- integrated circuit (IC) family H13 with Crypto Libraries ACL v2.08.007, SCL v02.04.002 and Hardware Support Library (HSL) v03.12.8812 provided by Infineon Technologies AG,
- Card Operating System IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 and
- *QES application* with the correspondent data files to store and manage the card holder data of the Qualified Signature Creation Device (signature PIN).

Before it’s usage, the QES application has to be completed. For this, the card internal generation of the signature key is initiated by the CSP (or an authorised third party) before the card is issued to the end user, the health professional. By this, the public key certificate is also personalised and the transport PIN is set in the QES application. After personalisation, a modification of the program code is not possible.

In order to generate a signature with the completed QES application, the designated signature key holder must activate the “HPC Signature Card” as a qualified signature creation device (QSCD). To do this, he must replace the transport PIN with a valid signature PIN.

After the QES application has been activated, “HPC Signature Card” may be used for generation of qualified digital signatures. A successful authentication of the owner of the signature key with correct entry of the signature PIN is a prerequisite for the generation of a qualified digital 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 (250 at a maximum) of qualified signatures after successful entry of the signature PIN. The number is determined during personalisation (value n of the signature counter) 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. 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 ability is not restricted to any security environment (SE). However, a different signature counter may be personalised for the security environments SE#1 and SE#2 (e.g. value 1 for SE#1 and 250 for SE#2).

The specific security environment SE#2 requires that the data to be signed are 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 “SAK for batch signature”. This enables the batch signature to be used in accordance with [TR-03114].

In the security environment SE#2, the “HPC Signature Card” supports also the transfer of the signature PIN via a trusted channel that has been established by a successful mutual authentication with the external world in the role “remote PIN sender”. This supports the concept of “remote PIN entry” (see [TR-03114]) where the eHealth card terminal used by the signature key holder for PIN entry and the eHealth card terminal containing the “HPC Signature Card” are different. 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 operating conditions apply to the use of this scenario.

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

- changing a *signature* PIN (after successful user authentication with the currently valid signature PIN),
- resetting the PIN try counter of signature PIN (after successful user authentication with PUK).

The “HPC Signature Card” supports the use of secure messaging for access relevant to the signature application. The authentication protocols Password Authentication Connection Establishment (PACE), Asymmetric Role Authentication or Authorization Proof, Internal Authentication and Mutual Authentication with or without negotiation of session keys according to [eHC-COS] are supported for the (mutual) authentication of external world and card as well as for the establishment of a secure communication channel. Access rights of the external world are verified in the context of authentications. This includes in particular the right of a signature application component to generate multi-signatures or as a “remote PIN sender”.

The security properties of “HPC Signature Card” are explained in more detail together with the description of the security functions (see section 2.2).

The installation of the file system proceeds in the product pre-personalisation phase where the object system is loaded together with the non-individual card data (e.g. file system) onto the card. After the phase has been completed successfully, the product enters the personalisation mode in which individual data may be stored but no further extensions of the object system are possible. This means that card management (deletion, loading of objects in the object system etc.) is not possible during the personalisation phase.

IDEMIA (Idemia R&D) ships the qualified object system to the product pre-personaliser in a way which effectively prevents the modification of the object system during the loading process. This process ensures that only those object systems issued by IDEMIA (Idemia R&D) can be loaded onto the card operating system.

During product personalisation, the card individual data can be stored by the product personaliser. The product supports the secure product personalisation via a secured channel.

Depending on the chosen production variant of the TOE, the OS pre-personalisation is done as intermediate step before the product pre-personalisation. In this case, the product pre-personaliser can exchange the initial key material for personalisation with its own.

"HPC Signature Card" supports the following cryptographic algorithms for the generation of signature key pairs as well as of qualified digital signatures:

- RSA with key length of 2048 bits pursuant to [TR-03116-1].
- DSA based on elliptic curves (ECDSA) using the groups $E(F_p)$ (cf. [TR-03111]) with key length of 256 bits and domain parameter brainpoolP256r1.
- Generation of random numbers based on a random number generator of the underlying hardware from IFX. The random number generator is a hybrid physical random number generator with a PTG.3 classification pursuant to [AIS 31]. The random numbers are subject to statistical tests performed in the operation phase ("online tests"). These properties were subject of the CC evaluation of the Infineon hardware (cf. [HW ST]).

Furthermore, the following algorithms are supported (cf. [Idemia_Crypt_Discl]). They are not used for signature generation by the card and are therefore **not** subject to this designation.

- DSA based on elliptic curves (ECDSA) using the groups $E(F_p)$ (cf. [TR-03111]) with key lengths of 384 and 512 bits.
- Asymmetric operations with RSA algorithm (key lengths 2048 and 3072 bits; cf. [PKCS#1]) and on the basis of elliptic curve cryptography (cf. [TR-03111]) for authentication as well as encryption and decryption.
- Hash functions SHA-1, SHA-256, SHA-384 and SHA-512 according to [TR-03116-1] and [FIPS 180-4], where SHA-1 and SHA-256 are used for derivation of symmetric session keys,
- Diffie-Hellman based on elliptic curves (ECDH) according to [TR-03110], [TR-03111] with key lengths of 256, 384 and 512 bits for authentication (PACE) and for key agreement for the secure messaging channel.
- Symmetric AES algorithm according to [TR-03116-1] and [FIPS 197] with effective key lengths 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" supports the ECC Brainpool curves brainpoolP256r1, brainpoolP384r1 and brainpoolP512r1 according to [RFC 5639] as well as the ANSI curves ansix9p256r1 and ansix9p384r1 according to [ANSI X9.62].

"HPC Signature Card" was successfully evaluated with the Common Criteria in version 3.1, Revision 5 as well as with the protection profiles „Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation", [PP SSCD Part 2], „Part 4: Extension for device with key generation and trusted channel to certificate generation application" [PP SSCD Part 4], and „Part 5: Extension for device with key generation and trusted channel to signature creation application" [PP SSCD Part 5] (cf. [ETR]). The assurance level is EAL 4+ with augmentations ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5.

In addition, "HPC Signature Card" claims strict conformance to the protection profile „Common Criteria Protection Profile – Card Operating System Generation 2 (PP COS G2)", [BSI-CC-PP-0082].

The evaluation and certification of the product was performed pursuant to Regulation (EU) No. 910/2014, Article 30 (3) a [Reg No. 910/2014] and the Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the

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

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

2.2 Security Functions and Security Properties of „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 among others between the roles "Administrator" and "Signatory". Furthermore, the following security attributes are used:

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

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 (terminal authentication) and prove his access rights to the card.

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

In the use phase, the “HPC Signature Card” supports the application of a secure channel for the communication via the contact based as well as the contactless interface. If the contact based interface is used, the communication between “HPC Signature Card” and a signature application may be optionally secured by cryptographic mechanisms. The use of the contactless interface requires that a successful PACE protocol has been performed. Nevertheless, in the security environment SE#2, a secure channel must be used for the generation of qualified signatures regardless of whether the access happens via the contact based or contactless interface.

For mutual authentication and for establishing a secure communication between terminal and “HPC Signature Card”, the following authentications are used:

- **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 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 may only be set during personalisation.
- Due to well defined access rules, sensitive data such as signature key, card PIN and signature PIN cannot be read out using the commands of the operating system.
- The substitution of the transport PIN by a signature PIN by the designated owner of the signature key is only possible in the initial state (for the data object SCD the attribute “SCD operational” has the value “no”, i.e. especially the signature key is not usable) of the “HPC Signature Card” and after a successful user authentication.
- The change of an existing signature PIN to a new signature PIN may only be performed after a successful user authentication with the old signature PIN.
- Only the owner of the signature key can generate signatures. For this, a previous successful user authentication is required.
- The use of the multi signature capability is possible in both security environments, i.e. in security environment SE#2 as well as in SE#1. The Security Status Evaluation Counter (SSEC) is limited to 250 for SE#1 and SE#2.

„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 the 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 the 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 [eHC-COS].

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

„Device Authentication“

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

The protocols for external and internal authentication use challenge-and-response protocols on the basis of suitable random numbers. Within the protocols, CV certificates are used to proof the authenticity of public keys. These certificates contain authorisation information and thus, assigned access rights can be verified. Device authentications are used especially for the communication with a signature application component that has the access right of a so-called “SAC for stack or comfort signatures” and/or “remote PIN sender”. So, the signature PIN and also the data to be signed can be securely transmitted to the card. In the security environment SE#2, a device authentication and the secure transmission of the data to be signed is enforced by the card if single or multi signatures are generated.

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“

“HPC Signature Card” supports the execution of a mutual authentication with the establishing of a secure channel on the basis of elliptic curve cryptography or the symmetric algorithm AES with a card management system (CMS) pursuant to [eHC-COS].

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

Asymmetric protocols are based on the use of CV certificates to proof the authenticity of public keys assigned to the card management system. These certificates contain authorisation information and thus assigned access rights can be verified. For internal authentication, the “HPC Signature Card” has a specific private key for CMS authentication. In addition, the specific root key for CMS authentication is also stored in the “HPC Signature Card” to enable the verification of related CV certificates. The asymmetric card administration shall be used and is not optional (cf. [Idemia_OBJ], 3.1.1).

In principle, for symmetric protocols the “HPC Signature Card” may contain AES key pairs, one AES key for encryption and decryption operations and one AES key for the generation of message authentication codes (MAC). For these, AES keys of length 128 and/or 256 bits may be used. By the chosen conditions these keys are not personalised and the use of symmetric CMS authentications is not possible (cf. [Idemia_OBJ], 3.1.1).

„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 process ensures that only those object systems issued by IDEMIA (Idemia R&D) can be loaded onto the card operating system.

- 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 of the role “signer”. It may be used only after successful setting of the signature PIN. User authentication is performed by comparing a signature PIN provided by the user with the reference value (RAD) secretly stored in “HPC Signature Card” (in the *QES application*).

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

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

The PTC of a blocked signature PIN may be reset by use of a resetting code (PUK). The “HPC Signature Card” supports resetting codes with a minimum length of eight characters and maximum length of twelve characters. The resetting code can be used up to ten times. After entering the resetting code a maximum of ten times (incorrect or correct), it can no longer be used and it is no longer possible to reset a blocked signature PIN.

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

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

The number of signatures, that may be generated after a successful entry of the signature PIN, can be configured. A value between 1 and 250 may be configured. “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. In general, however, the

value of the signature counter can be modified by the personaliser (card manufacturer; cf. chapter 3.2, Requirements for the Responsible Personalisation Party).

„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 which are used for the generation of qualified signatures. This especially includes the signing key and the signature verification key as well as the reference value for verification of the signature PIN.

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

„Secure Data Exchange“

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

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

„Memory Processing“

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

„Protection against Error Situations in Hardware and Software“

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

- inconsistencies when generating signatures and
- fault injection attacks.

If “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.

„Resistance against Side Channel Attacks“

“HPC Signature Card” provides appropriate mechanisms implemented in hardware and software to resist side channel attacks as

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

All 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 such as a signature key or a signature PIN.

This security function is active in all operation phases of “HPC Signature Card” (initialisation, personalisation and use).

„Self-Test“

“HPC Signature Card” provides several kinds of self-tests. After each reset a self-test is performed automatically.

Furthermore, the integrity of stored data is verified during the 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 2.1.

„Generation of Key Pairs“

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

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

- RSA keys are generated with a length of 2048 bits. The acceptability deadline for the legacy use of a modulus of size above 1900 bits, but less than 3000 bits, is set to 31 December 2025 (cf. [SOG-IS], chapter 4.1).

- The RSA key generation on board fulfils the requirements according to [SOG-IS], chapter 7.3 related to the distance of the two primes with |p - q| ≥ 2n/2-100. In addition, the size of d is close to the size of n by d > 2n/2.
- ECDSA keys with E(Fp) are generated with a length of 256 bits. The applied curve brainpoolP256r1 is recommended (cf. [SOG-IS], chapter 4.3).
- The hybrid random number generator of the underlying Infineon hardware is used for key generation.
- The key generation guarantees that the signature key cannot be derived from the signature verification key.
- The key generation process ensures that the private and public key part are consistent with each other.
- The key generation is resistant against side channel attacks.
- After key generation, 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 digital signatures with RSA and ECDSA signature keys with lengths of 2048 bits for RSA keys and 256 bits for ECDSA keys. The security function has the following properties:

- Receipt of (already hashed) data (data to be signed, DTBS) to generate qualified digital signatures.
- Every hash value transmitted via the contactless interface is protected by a message authentication code.
- Generation of RSA signatures according to [eHC-COS], signPSS (RSASSA-PSS according to [PKCS#1]) with a key length of 2048 bits.
- Generation of ECDSA signatures according to [eHC-COS], signECDSA (cf. [TR-03111]) with a key length of 256 bits.
- The hybrid random number generator of the underlying Infineon hardware is used to generate random numbers for the generation of RSA signatures (signature format RSASSA-PSS) and ECDSA signatures.
- The key generation is resistant against side channel attacks.
- The signature is generated in a manner that the signature key cannot be derived from the generated signature and that, during signature generation, no information about the signature key is revealed.
- A signature can only be generated if the user has authenticated himself successfully with a signature PIN (command VERIFY) and if the security attribute “SCD operational” of the data object SCD has the value “yes”.

- Using the contactless interface, the card command for the generation of a qualified signature (PSO : Compute Digital Signature) must be sent to the card via a secure channel (established with PACE, optionally device authentication).
- The use of the multi signature capability in the security environment SE#2 is only possible after a successful user authentication and a mutual authentication with the establishment of a secure channel. All accesses for the generation of a signature are performed with secure messaging. The external world must have authenticated itself under the role “SAC for stack or comfort signatures”.

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

3.1 Fulfilled Requirements

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

Table 1: Fulfilment of the requirements of the Regulation (EU) No. 910/2014

Reference	Requirement / Description / Result
Article 29	**Requirements for qualified electronic signature creation devices**
(1)	**Requirement** Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.
(2)	**Requirement** The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48 (2).
Article 39	**Qualified electronic seal creation devices**
(1)	**Requirement** Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.
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;

Reference	Requirement / Description / Result
(d)	the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
2.	**Requirement** Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

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 or Pre-Personalisation Party

- The initialisation (pre-personalisation) data provided by IDEMIA (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 [Idemia_AGD_PRE] must be adhered to.

Conditions of Use for the Signature Counter

During initialisation, the number *n* of signatures that may be generated after one entry of the signature PIN is determined (value of the signature counter). 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 provided 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 that are part of the designation must be indicated.

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 out 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 CSP is obliged to name at least one operational environment fulfilling these requirements.

The physical security requirements include the protection against unauthorised access to the QSCD, especially in an unattended operation mode. In this context, the CSP shall inform specifically about the assignment of the qualified digital signatures to the designated owner of the signature key [Reg No. 910/2014].

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

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

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

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 [Idemia_AGD_PRE] must be adhered to.
- The value one for the signature counter in security environment SE#1 may only be changed (during personalisation) under observation of the conditions of use for the signature counter.

Requirements for the CSP

- If the CSP distributes a product to generate qualified digital 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 inform the owner of the signature key about designated card terminals and corresponding signature application components where the owner can activate his signature PIN.

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

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

Requirements for the Owner of the Signature Key / Card Owner

- The owner of the signature key must verify that the 5 digits transport PIN is still valid by setting a new signature PIN chosen by himself with a length of at least six digits. If the transport PIN is not valid, the owner of the signature key must contact the issuing CSP.
- The owner of the signature key must treat the chosen signature PIN as confidential. The owner of the signature key must not confide his signature PIN to anybody and must keep it in a safe place.
- The owner of the signature key must change his signature PIN periodically.
- The owner of the signature key must use and keep “HPC Signature Card” such that misuse and manipulation are prevented.

Requirements for the Manufacturer of Signature Application Components

- The manufacturer of a signature application component must respect the interfaces of the smart card operating system as well as of the *QES application* (cf. [Idemia_AGD_OPE]) in an appropriate manner.
- When generating a digital signature on a hash value that has been computed by the external world and transmitted to the card, it must be guaranteed that the signature application component has chosen an appropriate hash function.

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(Fp) 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 random number generator of the underlying hardware from IFX. The random number generator is a Hybrid Random Number Generator (HRNG) with a PTG.3 classification pursuant to [AIS 31]. The random numbers are subject to statistical tests performed in the operation phase („online tests“). These properties were checked in a CC evaluation of the Infineon hardware (cf. [HW ST]).

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

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

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

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

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 IDEMIA_HC_Germany_NEO_G2.1_HBA, V1 was evaluated successfully according to the Common Criteria (CC) Version 3.1, Revision 5 with an assurance level EAL 4+ (EAL 4 with augmentation ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5).

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

For the evaluation of “HPC Signature Card”, the protection profiles “Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation”, [PP SSCD Part 2], “Part 4: Extension for device with key generation and trusted channel to certificate generation application” [PP SSCD Part 4], and “Part 5: Extension for device with key generation and trusted channel to signature creation application” [PP SSCD Part 5] (cf. [ETR]) were used. So, the requirements laid down in Regulation (EU) No. 910/2014 Article 30 (3) a as well as the Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 are fulfilled.

The evaluation was performed as a so-called composition evaluation, which takes into account the evaluation results of the CC evaluation of the semiconductor “Infineon smart card IC (Security Controller), design step H13” from the semiconductor manufacturer Infineon Technologies AG. This evaluation was performed with an assurance level EAL 6+ (EAL 6 with augmentations 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

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

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

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

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

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

[eHC-COS] Spezifikation des Card Operating System (COS), Elektrische Schnittstelle, Version 3.12.0 vom 15.05.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Errata zu Release 3.1.1 Online-Produktivbetrieb (Stufe 3), Version 1.0.0 vom 27.08.2019, gematik Gesellschaft für Telematik-anwendungen der Gesundheitskarte mbH

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR) – Summary, IDEMIA_HC_Germany_NEO_G2.1_HBA, V1, Version 1.0, 22.09.2020, SRC.00036.QSCD.09.2020

[FIPS 180-4] Federal Information Processing Standards Publication 180-4 (FIPS PUB 180-4), SECURE HASH STANDARD (SHS), 5 August 2015, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology (NIST)

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

[ISO 7816-4] ISO/IEC 7816-4:2013 (3rd edition), Identification cards – Integrated circuit cards – Part 4: Organisation, security and commands for interchange

[HPC-ObjSys] Elektronische Gesundheitskarte und Telematikinfrastruktur, Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem, Version: 4.5.0, 15.05.2019, gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH

[HW ST] Security Target Lite of the underlying hardware platform, Common Criteria Public Security Target 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, Revision 1.8, Infineon Technologies AG, 2020-04-22

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

[PP SSCD Part 2] Protection Profiles for Secure Signature Creation Device - Part 2: Device with key generation, EN 419 211-2:2013, resp. DIN EN 419 211-2:2013-12

[PP SSCD Part 4] Protection Profiles for Secure Signature Creation Device - Part 4: Extension for device with key generation and trusted channel to certificate generation application, EN 419 211-4:2013, resp. DIN EN 419 211-4:2014-03

[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 419 211-5:2013, resp. DIN EN 419211-5:2014-03

[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] IDEMIA_HC_GERMANY_NEO_G2.1_HBA, V1, Security Target, Idemia GmbH, Version V1.15, 21.09.2020, filename: 20200728_IDEMIA_ASE_eIDAS_GHC_SecurityTarget_V115.pdf

[Idemia_AGD_PRE] IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 – Preparative Guidance, Version: 1.10, 03.07.2020, filename: IDEMIA_HC_Germany_NEO_G2.1_COS_V1_PreparativeGuidance_V1.10.pdf

[Idemia_AGD_OPE] IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 – Operational User Guidance V2.0, Version: 2.1, 16.07.2020, file name: IDEMIA_HC_Germany_NEO_G2.1_COS_V1_OperationalUserGuidance_V2.1.pdf

[Idemia_Wrapper] IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 –Wrapper Guidance, Version: V1.7, 03.07.2020, filename: IDEMIA_DEV_MAN_GHC_V1_Wrapper_V1.7

[Idemia_OBJ] HPC (Health Professional Card) – Object System eGK_DI HPC9000, V1 Functional Specification 1.0.1-0, Version 1.0.1, 28.07.2020, file name: HPC9000 Object System FSP 1.0.1.pdf

[Idemia_Crypt_Discl] IDEMIA, Crypto Disclaimer, IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1, Version 2.0, Date 2020-06-26

[TR-03110] Technical Guideline BSI TR-03110:

Technical Guideline TR-03110-1: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, BSI, 2015

Technical Guideline TR-03110-2: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 – Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.21, BSI, 2016

Technical Guideline TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications, Version 2.21, BSI, 2016

Technical Guideline TR-03110-4: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 4 – Applications and Doc-ument Profiles, Version 2.21, BSI, 2016

[TR-03111] BSI: Technische Richtlinie TR-03111, Elliptic Curve Cryptography (ECC), Version 2.10, 1. Juni 2018

[TR-03114] BSI: Technische Richtlinie TR-03114: Stapelsignatur mit dem Heilberufsausweis, Version 2.0, 22.10.2007

[TR-03116-1] BSI: Technische Richtlinie BSI TR-03116-1: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur, Version 3.20, 21.09.2018

End of certification report