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 / Seal Creation Device
STARCOS 3.7 eIDAS C2

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

Certificate is valid until

31.12.2029

SRC Certificate Registration Number

SRC.00057.QSCD.11.2022

This certificate is only valid with the certification report.

Bonn, 25 November 2022

Gerd Cimiotti

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

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

Description of the Qualified Signature Creation Device (QSCD):

1. Product Name and Scope of Delivery

1.1 Product Name

Signature and Seal Creation Device STARCOS 3.7 eIDAS C2 from Giesecke+Devrient Mobile Security GmbH (G+D MS).

The product is sold by the manufacturer under the sales name STARCOS 3.7 eIDAS C2. The product is a smart card usable for the generation of qualified signatures as well as qualified seals and will be denoted as „Sig & Seal Card“ in the following.

1.2 Delivery

The „Sig & Seal Card“ is implemented as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. The product „Sig & Seal Card“ is based on the hardware platform IFX_CCI_000005h by Infineon Technologies. The software consists of the STARCOS 3.7 COS HBA-SMC operating system and of the application for generating qualified electronic signatures and seals according to [Appl_Spec], in the following denoted as *eSign&Seal application*.

The smart card embedded software contains the STARCOS 3.7 COS HBA-SMC operating system. This is an ISO-7816 compatible, multifunctional platform, which is appropriate for cards to be used in applications fulfilling high security requirements. The card possesses the *eSign&Seal application* and may in general contain further applications. However, these applications are not part of the designation at hand.

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 *eSign&Seal application* or it contains secret data allowing secure loading of initialisation data containing the file system of the *eSign&Seal 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 *eSign&Seal application* there may be additional files for other applications, which do not belong to the designation of the product. The file system part of the „Sig & Seal Card“ is represented by the Guidance Documentation that define the security relevant parts of the file system.

Each application, in particular the *eSign&Seal 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 *eSign&Seal 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 eIDAS C2 [AGD_init], the manufacturer provides 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], chapters 5.2.9 and 5.5.2. During the usage phase the parameters „Chip Manufacturer Data“, the „Version of the Operating System“ and the “Image ID” can be read from the card according to [AGD_use], chapter 4.1.1.2.

The following commands can be used to retrieve identification data:

Table 1: TOE Identification “GET PROTOCOL DATA” command

Command parameters	Identifier length	Description
P1 = ‘9F’, P2 = ‘6B’	8 bytes	Chip manufacturer data
P1 = ‘9F’, P2 = ‘6A’	7 bytes	Version of the operating system
P1 = ‘9F’, P2 = ‘67’	4 bytes	Image ID

The following table describes the evaluated and certified configuration:

Table 2: Evaluated TOE identifier for productive TOE (COS) version

Data type	Tag in the protocol data DO	Data
Chip manufacturer data	9F6B	05 16 00 13 00 02 00 00
OS Version	9F6A	47 44 00 B7 04 01 01
Image ID	9F67	06 00 00 30

1.3 Delivery Items

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

Table 3: Delivery items

No.	Delivery item	Description / Additional Information	Type	Delivery method
1	Completed card with hardware for contact-based and contactless interface.	**Hardware platform** IFX_CCI_000005h by Infineon Technologies (incl. its IC Dedicated Test Software). (Refer to the Certification Report BSI-DSZ-CC-1110-V5-2022-MA-01)	HW/ FW	The IC and the Embedded Software are providing self-protection mechanisms, ensuring confidentiality and integrity during delivery. The delivery does not need additional security measures and can be considered as normal transport.
2		**TOE Embedded Software** IC Embedded Software STARCOS 3.7 eIDAS C2 (the operating system STARCOS 3.7 COS HBA-SMC including the QES Application [Appl_Spec] implemented in Flash of the IC)		
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 eIDAS C2 – Main Document, [AGD_main].	DOC	Document in electronic form.
5	Initialisation Guidance	Guidance Documentation for the Initialisation Phase for STARCOS 3.7 eIDAS C2, [AGD_init].	DOC	Document in electronic form.
6	Personalisation Guidance	Guidance Documentation for the Personalisation Phase for STARCOS 3.7 eIDAS C2, [AGD_pers].	DOC	Document in electronic form.

No.	Delivery item	Description / Additional Information	Type	Delivery method
7	Usage Guidance	Guidance Documentation for the Usage Phase for STARCOS 3.7 eIDAS C2, [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 eIDAS C2, [FSP]	DOC	Document in electronic form.

1.4 Manufacturer

Manufacturer of the product is Giesecke+Devrient Mobile Security GmbH, Prinzregentenstraße 161, 81677 München, Germany.

2. Functional Description

2.1 Functionality and Architecture

The smart card product „STARCOS 3.7 eIDAS C2“ is intended for the use as a card for the generation of qualified signatures or qualified seals. From a technical point of view „Sig & Seal Card“ is implemented as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface, with an ISO 7816 conformant operating system and an application layer which directly accesses the operating system layer.

The product „Sig & Seal Card“ is based on the hardware platform IFX_CCI_000005h (incl. its IC Dedicated Test Software) by Infineon Technologies. 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 in several versions was evaluated CC EAL 6+ (CC Version 3.1) and is listed under the Certification ID BSI-DSZ-CC-1110-V5-2022-MA-01.

The software consists of the STARCOS 3.7 COS HBA-SMC operating system as well as of the *eSign&Seal application* for the generation of qualified signatures or qualified seals (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 *eSign&Seal application*. Further applications may exist on the „Sig & Seal Card“ besides the dedicated *eSign&Seal 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 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 „Sig & Seal Card“ consists of the following components:

- The hardware platform Infineon IFX_CCI_000005h (Certificate BSI-DSZ-CC-1110-V5-2022-MA-01),
- STARCOS 3.7 COS HBA-SMC operating system (Certificate BSI-DSZ-CC-0976-V4-2021) and
- *eSign&Seal application.*

After issuance „Sig & Seal Card“ is in one of the states as explained in chapter 1.2.

Before the *eSign&Seal application* can be used, it must be completed. This involves the generation of the signature or seal key by the certification service provider (CSP) (or an authorised third party) before the card is delivered. At least one signature or seal key is generated in the card. Within the scope of this completion of the *eSign&Seal application*, the public key certificate is also inserted and the transport PINs are set in the card. After completion of the personalisation, it is not possible to change the programme code. The „Sig & Seal Card“ supports a maximum of ten keys, 4 RSA keys with key length of 2048 bits, 2 RSA keys with key length of 4096 bits and 4 ECDSA keys with key length 384 bits.

To be able to generate a signature or seal with the completed *eSign&Seal application*, the designated key holder must activate the „Sig & Seal Card“ as a qualified signature / seal creation device (QSCD). To do this, he must replace the pre-set transport Signature PIN with a maximum of five digits with a valid Signature PIN (PIN.CH.DS).

After the *eSign&Seal application* has been activated, „Sig & Seal Card“ may be used for generation of qualified electronic signatures or qualified electronic seals. A successful authentication of the owner of the signature key with correct entry of the Signature PIN is a prerequisite for the generation of a qualified electronic signature or a qualified electronic seal.

The generation of multiple qualified signatures or seals is not supported by the „Sig & Seal Card“. After successful entry of the Signature PIN only one qualified signature or qualified seal can be generated and a further signature or seal cannot be generated without a new entry of the Signature PIN. The security state "Successful Signature PIN Entry" is cancelled in „Sig & Seal Card“ with a reset of the card. For the generation of further signatures or seals a new entry of the Signature PIN is necessary.

The *eSign&Seal application* can be administrated by the owner of the „Sig & Seal Card“. The administration comprises the following functions:

- generation of a signature or seal key pair and obtaining a certificate for the public key exported from the card,
- key pair destruction by overwriting the previous value with newly generated value,
- 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).

A signature generation requires prior successful authentication of the Signatory with the Signature PIN. The generation of a signature or seal key pair is an administrative function and requires prior successful authentication of the card holder with an Admin PIN (PIN.CH.ADMIN) and the Card Issuer or CSP with a symmetric authentication scheme and the admin authentication key (“Mutual Authenticate ESignK” with K.CA.AUT). Before the first use of the Admin PIN, the card holder must replace the pre-set transport Admin PIN with a valid Admin PIN.

The „Sig & Seal Card“ supports the use of secure messaging for accesses relevant to the *eSign&Seal 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 „Sig & Seal 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 „Sig & Seal Card“ does not support the subsequent introduction of further software. The initialiser must take into account the initialisation requirements described in the guidance documents.

„Sig & Seal Card“ supports the following cryptographic algorithms for the generation of signature or seal key pairs as well as of the generation of qualified electronic signatures or qualified electronic seals:

- Asymmetric RSA algorithm according to [PKCS#1] with key length of 2048 or 4096 bits.
- DSA based on elliptic curves (ECDSA) using the groups E(Fp) (cf. [TR-03111]) with key length of 384 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]).

„Sig & Seal Card“ supports NIST Curve P-384 from the NIST curve family according to [FIPS 186-4], Appendix D.1.2 or secp384r1 according to [SEC 2].

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

- Hash function SHA-1 according to [FIPS 180-4], 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 180-4] used only for internal operations,
- Symmetric AES algorithm according to [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]).

„Sig & Seal Card“ was successfully evaluated with the Common Criteria in version 3.1 as well as with 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 creation 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 (cf. [ETR]). The assurance level is EAL 4+ with augmentation AVA_VAN.5.

2.2 Security Functions and Security Properties of „Sig Card“

Among others „Sig & Seal 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“

„Sig & Seal Card“ uses a role based access control which distinguishes among others between the roles "Administrator" and "Signatory". Furthermore, the following security attributes are used:

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

The CSP, who performs the process of activating the *eSign&Seal 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 „Sig & Seal Card“ as a signer or seal creator by inserting his Signature PIN.

In the usage phase, the application of a secure channel is supported by the „Sig & Seal Card“ both, when using the contact and contactless interface. When using the contact interface, the connection between the „Sig & Seal Card“ and the signature application can optionally be cryptographically secured. The contactless interface can only be used with a secure channel.

The session keys can be negotiated by different methods. The „Sig & Seal 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.
- **Mutual Authenticate ESignK** with symmetric keys for mutual authentication and establishing a secure channel to the card issuer or CSP.

If the communication via the contactless interface is already protected by a secure channel established after a Mutual Authenticate ESignK authentication, an additional secure channel established by the PACE protocol can be omitted. The secure channel built up after such a successful 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 „Sig & Seal 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:

- The activation of the *eSign&Seal application* may only be performed by an authorised CSP using a secure channel which he has established before. The secure channel is established with mutual authentication. For an activation the CSP has to prove his access rights (in this case the security attribute „SCD / SVD Management“ for the accessing role has the value „authorised“).
- PINs for transport protection can only be set during personalisation.
- The replacement of the transport Signature PIN by a real Signature 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 or seal key on the card cannot be used) of the „Sig & Seal Card“ after a successful user authentication.
- The setting of a real Admin PIN requires the authentication with the transport Admin PIN.
- The change of an existing PIN to a new PIN may only be performed after a successful user authentication with the old PIN.
- Signatures or seals can only be generated by the key holder. This requires a previous successful user authentication with the Signature PIN.

- After personalisation signature key pairs can only be generated by the card issuer or the CSP. This requires a previous successful authentication of the card issuer of CSP with a symmetric authentication scheme and the admin authentication key and successful user authentication with the Admin PIN.

- Sensitive data as signature key, and PIN cannot be read using the commands of the operating system.

„Password Authenticated Connection Establishment (PACE) Protocol“

„Sig & Seal 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 „Sig & Seal 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 „Sig & Seal 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 „Sig & Seal 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 „Sig & Seal 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 „Sig & Seal Card“ more difficult.

„Mutual Authenticate ESignK“

The „Sig & Seal Card“ supports the execution of a mutual authentication with the establishing of a secure channel by means with a symmetric authentication scheme and the admin authentication key (K.CA.AUT) with the card issuer or the CSP according to [EN 419212-3]. For this the Mutual Authentication command offered by the operating system of the card has to be used.

„Processes with PIN based Authentication to generate Qualified Signatures or Qualified Seals (PIN)“

The security function comprises the PIN based user authentication in the role „signatory”. It may be used only after successful setting of the Signature PIN. User authentication is performed by comparing the Signature PIN provided by the user with the reference value (RAD) secretly stored in „Sig & Seal Card“ (in the *eSign&Seal application*).

Once personalisation has been successfully completed, the „Sig & Seal Card“ is equipped with a transport Signature PIN (specific PIN), which is used exclusively for transport protection. Before generating a signature or seal, a Signature PIN must be set which has at least six digits. For this purpose, the user must authenticate himself to the „Sig & Seal Card“ by successfully entering the transport Signature PIN. It is not possible to generate a signature after entering the transport Signature PIN; this is prevented by the „Sig & Seal Card“.

The PIN Try Counter (PTC) of a blocked Signature PIN can be reset by using a reset code (PUK). The „Sig & Seal Card“ supports a reset code with a length of at least six

digits, and the reset code can be used a maximum of 20 times. After entering the reset code a maximum of 20 times (incorrect or correct), it can no longer be used and it is no longer possible to reset a blocked Signature PIN. Due to the conditions of use at the personaliser (see chapter 3.2), the minimum length of the reset code is six digits. The reset code is protected by a retry counter with value three, i.e. after three consecutive erroneous PUK entries the PUK mechanism itself is blocked.

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

A Signature PIN can be changed by the key holder. To do this, he must authenticate himself against the „Sig & Seal Card“ by successfully entering the current Signature PIN, i.e. changing a Signature PIN to a new Signature PIN is only possible after successful user authentication using the current Signature PIN (command CHANGE REFERENCE DATA with old and new PIN).

After successful user authentication, a maximum of one qualified signature or qualified seal can be generated. Then, the Signature PIN must be successfully entered again to generate signatures or seals. This is controlled by the „Sig & Seal Card“.

„Processes with PIN based Authentication to generate Signature or Seal Key Pairs“

The security function comprises the PIN based user authentication in the role „Administrator”. It may be used only after successful setting of the Admin PIN. User authentication is performed by comparing the Admin PIN provided by the user with the reference value (RAD) secretly stored in „Sig & Seal Card“.

Once personalisation has been successfully completed, the „Sig & Seal Card“ is equipped with a transport Admin PIN (specific PIN), which is used exclusively for transport protection. Before generating a signature or seal key after delivery of the card to the card holder, an Admin PIN must be set which has at least six digits. For this purpose, the user must authenticate himself to the „Sig & Seal Card“ by successfully entering the transport Admin PIN. It is not possible to generate a signature or seal key after entering the transport Admin PIN; this is prevented by the „Sig & Seal Card“.

The PIN Try Counter (PTC) of a blocked Admin PIN can be reset by using the reset code (PUK). The „Sig & Seal Card“ supports a reset code with a length of at least six digits, and the reset code can be used a maximum of 20 times. After entering the reset code a maximum of 20 times (incorrect or correct), it can no longer be used and it is no longer possible to reset a blocked Admin PIN. Due to the conditions of use at the personaliser (see chapter 3.2), the minimum length of the reset code is six digits. The reset code is protected by a retry counter with value three, i.e. after three consecutive erroneous PUK entries the PUK mechanism itself is blocked. Both PIN objects, Signature PIN and Admin PIN, reference the same PUK.

To reset the PTC, use the command RESET RETRY COUNTER. It is not possible to change an Admin PIN using this command. The security status of an Admin PIN is not set, i.e. resetting a blocked Admin PIN does not enable the generation of a signature or seal key.

An Admin PIN can be changed by the key holder. To do this, he must authenticate himself against the „Sig & Seal Card“ by successfully entering the current Admin PIN, i.e. changing an Admin PIN to a new Admin PIN is only possible after successful user authentication using the current Admin PIN (command CHANGE REFERENCE DATA with old and new PIN).

„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“

„Sig & Seal 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].

To this purpose, symmetric keys are employed, that have been agreed by a mutual authentication with the external world.

„Memory Processing“

„Sig & Seal Card“ ensures, that safety-critical information (e.g. signature or seal 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 „Sig & Seal 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 „Sig & Seal Card“ closes the session. Depending on the error „Sig & Seal Card“ either will be blocked or can be used in further sessions after a reset.

„Resistance against Side Channel Attacks“

„Sig & Seal 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),
- electromagnetic analysis (EMA) and
- differential electromagnetic analysis (DEMA).

All safety-critical operations of „Sig & Seal 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 such as a signature or seal key or a PIN.

This security function is active in all operation phases of „Sig & Seal Card“ (initialisation, personalisation and use).

„Self-Test“

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

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

„Generation of Key Pairs“

„Sig & Seal Card“ supports the generation of RSA and ECDSA key pairs in the card for generating qualified signatures or qualified seals with a length of 2048 bits or 4096 bits for RSA keys and 384 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 or 4096 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). RSA keys with a modulus size equal or greater than 3000 bits are recommended.

- 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 384 bits. The applied curve NIST P-384 or secp384r1 is recommended (cf. [SOG-IS], chapter 4.3).

- The deterministic random number generator (DRNG) of the „Sig & Seal Card“ is used for key generation.

- The key generation guarantees that the key cannot be derived from the public verification key.

- After key generation „Sig & Seal 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.

- During initialisation or personalisation key generation is only possible after a successful authentication of the initialiser or personaliser. In the usage phase the successful authentication of the card holder with Admin PIN and of the card issuer or CSP by a symmetric authentication is required.

The signature key pairs are generated exclusively in the card during initialisation or personalisation of the *eSign&Seal application* or during the usage phase. „Sig & Seal Card“ fulfils the security requirements for the generation of RSA or ECDSA key pairs as listed above. With the delivery of the „Sig & Seal Card“ to the designated card holder at least one signature key is already available. However, the „Sig & Seal Card“ attribute operational has to be set to “yes” by the card holder before a signature or seal can be generated.

„Generation of Qualified Signatures and Seals“

„Sig & Seal Card“ supports the generation of qualified electronic signatures or qualified electronic seals with RSA and ECDSA keys with lengths of 2048 bits or 4096 bits for RSA keys and 384 bits for ECDSA keys. The security function has the following properties:

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

- Generation of RSA signatures with PSS and PKCS1-v1_5 according to chapter 8 and 9 of [PKCS#1] with a key length of 2048 bits or 4096 bits.

- Computation of ECDSA signatures according to [TR-03111] with key lengths of 384 bits.

- The deterministic random number generator (DRNG) of the „Sig & Seal Card“ is used to generate random numbers for the generation of ECDSA signatures.

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

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

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

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

3.1 Fulfilled Requirements

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

Table 2: Fulfilment of the requirements of the Regulation (EU) No. 910/2014

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

Requirements for the Responsible Personalisation Party

- The personalisation party must ensure that the personalisation data (especially of the *eSign&Seal 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

- If the CSP distributes a product to generate qualified electronic signatures or qualified electronic seals 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. Here the current version of [SOG-IS] must be considered.

- Programs which a CSP provides to his clients for the transmission of reference data to „Sig & Seal Card“ (i.e. which are used by the owner of the signature or seal key to set or change his Signature PIN or Admin 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 or Seal Key resp. for the Card Owner

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

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

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

- The owner of the key must use and keep „Sig & Seal 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 *eSign&Seal application* in an appropriate manner.

- When generating a qualified electronic signature or qualified electronic seal 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 or qualified electronic seals (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 or seals, „Sig & Seal Card“ provides RSA according to [PKCS#1] and ECDSA based on groups $E(F_p)$ according to [TR-03111]. Key lengths of 2048 bits and 4096 bits for RSA and 384 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 „Sig & Seal 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.
- The use of a modulus of size greater or equal to 3000 bits is recommended.
- RSA PCKS#1_v1.5, legacy, acceptability deadline is 31 December 2027.
- RSA PSS (PKCS #1, v2.1), recommended.

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

- NIST P-384, recommended.

Recommended mechanisms fully reflect the state of the art in cryptography. So, the use of ECDSA with the parameters chosen by „Sig & Seal Card“ is not restricted by the algorithm catalogue SOG-IS [SOG-IS]. The algorithm RSA may only be used until 31 December 2025 for RSA keys with modulus size of 2048 bits. For keys with modulus size 4096 bits the use is restricted until 31 December 2027 if the format RSA PCKS#1_v1.5 is used. The use of such keys with the format RSA PSS is not restricted.

This certification of the „Sig & Seal Card“ is therefore valid until **31.12.2029**.

However, the validity may be extended if there are no impediments to the security of the products or the algorithms and parameters at this time, or shortened if new findings regarding the suitability of the algorithms are published in the algorithm catalogue SOG-IS [SOG-IS].

3.4 Assurance Level and Attack Potential

The product STARCOS 3.7 eIDAS C2 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 „Sig & Seal Card“ the protection profiles „Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation“, EN 419211-2:2013, [PP SSCD Part 2] and „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, [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 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 from the manufacturer Infineon Technologies AG. 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-V5-2022-MA-01.

4. References

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

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

[EU QSCD list] Compilation of: Member States' notifications on: Designated Bodies under Article 30 (2) and 39 (2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31 (1)-(2), and Certified Qualified Seal Creation Devices under Article 39 (3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51 (1) of Regulation 910/2014; Currently, this list is realised by a so-called “Dashboard” and is publicly available (https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD).

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

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

[EN 419212-3] Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 3: Device authentication protocols; English version EN 419212-3:2017

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), STARCOS 3.7 eIDAS C2, Version 1.0, 08.11.2022, SRC.00057.QSCD.11.2022

[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

[FIPS 180-4] NIST: FIPS Publication 180-4: Secure Hash Standard (SHS), August 2015.

[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

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

[ISO 7816-8] ISO/IEC 7816-8: 2016 (3rd edition) Identification cards – Integrated circuit cards – Part 8: Commands and mechanisms for security operations

[ISO 7816-9] ISO/IEC 7816-9: 2004 (2nd edition) Identification cards – Integrated circuit cards – Part 9: Commands for card management

[HW ST] Common Criteria Public Security Target, EAL6 augmented / 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 2.0, 2022-03-28, Infineon Technologies Connected Systems S CERT

[IFX_Cert] Certification Report, BSI-DSZ-CC-1110-V5-2022 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), Certification Report v1.0, 29 April 2022

[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, DIN EN 419211-2:2013, BSI-CC-PP-0059-2009-MA-02, 2016-06-30

[PP SSCD Part 5] Protection Profiles for Secure Signature Creation Device - Part 2: Extension for device with key generation and trusted channel to signature creation application, EN 419211-2:2014, BSI-CC-PP-0072, 2012-11-14

[SEC 2] Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, January 27, 2010, Version 2.0

[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] G+D Mobile Security, Security Target to SSCD PP, Security Target STARCOS 3.7 eIDAS C2, Version 1.2, 02.11.2022, Business Confidential

[AGD_main] G+D Mobile Security, STARCOS 3.7 eIDAS C2, Guidance Documentation STARCOS 3.7 eIDAS C2 - Main Document, Version 1.0, 21.12.2021, Business Confidential

[AGD_init] G+D Mobile Security, STARCOS 3.7 eIDAS C2, Guidance Documentation for the Initialisation Phase, Version 1.0, 21.12.2021, Business Confidential

[AGD_pers] G+D Mobile Security, STARCOS 3.7 eIDAS C2, Guidance Documentation for the Personalisation Phase, Version 1.0, 21.12.2021, Business Confidential

[AGD_use] G+D Mobile Security, STARCOS 3.7 eIDAS C2, Guidance Documentation for the Usage Phase, Version 1.1, 04.07.2022, Business Confidential

[AGD_internal] G+D Mobile Security, Internal Design Specification STARCOS 3.7, Business Confidential

[Appl_Spec] G+D Mobile Security, Application Specification STARCOS 3.7 eIDAS ICA ESIGN, Date Monday, February 7, 2022, 4:05:03 PM, html-file

[FSP] G+D Mobile Security, Functional Specification STARCOS 3.7 eIDAS C2, Version 1.2, 21.12.2021, Business Confidential

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

End of certification report