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

Approved Security

SRC
security consulting

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
TCOS 3.0 Signature Card Version 2.0
Release 2/SLE78CLX1440P

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.00032.QSCD.12.2018

This certificate is only valid with the certification report.

Bonn, 18 December 2018

Gerd Cimiotti

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

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

Description of the Qualified Signature Creation Device (QSCD):

1. Product Name and Scope of Delivery

1.1 Product Name

Signature Creation Device TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P from T-Systems International GmbH.

The product is sold by the manufacturer in the product variant TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P. The product is a signature card and will be denoted as „Sig Card“ in the following.

1.2 Delivery

The „Sig Card“ is implemented as a so-called Dual Interface Card, i.e. the card possesses a contact and a contactless interface. Depending from its configuration the card can be used either as an only contact card or as an only contactless card or as an dual interface card. The hardware of „Sig Card“ consists of an IFX Secure Smart Card Controller SLE78CLX1440P. The software consists of the operating system TCOS 3.0 Signature Card Version 2.0 Release 2 (ROM, possibly in parts in EEPROM) and of the application for generating qualified electronic signatures, in the following denoted as *eSign application*.

The smart card embedded software contains the operating system TCOS 3.0 Signature Card Version 2.0 Release 2. 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 application* and may in general contain further applications (as for instance the already installed Netkey application). However these applications are not part of the designation at hand.

The product can be delivered in the states „initialised”, „pre-personalised” and „personalised”.

- An <u>initialised</u> „Sig Card“ provides all functions, however signature key and certificate are yet missing. Key generation is initiated after card delivery by the designated owner of the signature creation device. Key generation as well as loading of the certificate into the card is performed by a certification service provider (CSP). This activation procedure is similar to the activation procedure of the *eSign application* as used in an electronic identity card.
- A <u>pre-personalised</u> „Sig Card“ contains all necessary keys and can be transferred by the signer from state "not ready for use" to state "ready for use" using authentication data. To this purpose, the certificate to the public signature key must be generated by an authorised CSP and be stored in the „Sig Card“.
- A <u>personalised</u> „Sig Card“ contains beside all card owner data and the signature key pair also the certificate to the public signature key for signature verification. Thus this „Sig Card“ is already bound to the end customer.

Beyond the requirements of regulations [Reg No. 910/2014], production and delivery to the end customer, who is the designated owner of the signature creation device „Sig Card“, are subject to specific factors. Above all this applies to the embedding of

ICs for the final delivery at the production sites of the embedders which have been audited and certified during evaluation of the „Sig Card“.

At least the following data are stored in the card by the card manufacturer during initialisation and personalisation of the „Sig Card“:

- Master File (MF), among others with the following data
  - a signed chip authentication key and
  - authentication data of the card owner (Card Access Number (CAN); card PINs)
- *eSign application*

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

[TCOSADM], Appendix E provides the manufacturer specific values to the parameters „Chip Manufacturer (IFX)“, „Chip Type“, „Card Type (TCOS 3.0 Signature Card)“, „OS Version (ROM Mask Version)“, „(Pre-)Completion Code Version“, „File System Version“ and „Authentication Key Identifier“ for the designated version of TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P with respect to the underlying hardware (Infineon SLE78CLX1440P). These values can be read from the card during production with the command „Format“ using option „Reading of Chip Information“.

1.3 Delivery Items

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

Table 1: Delivery items

No.	Type	Description	Version	Date	Delivery
1	Hardware / Software	IFX Secure Smart Card Controller SLE78CLX1440P including its IC Dedicated Support Software embedded into modules Delivered as smart card (Module Package Type M8.4)			The hardware part of the TOE is delivered in an insured parcel to the Installation Agent. In the life cycle of the product the hardware is always protected by an authentication procedure

No.	Type	Description	Version	Date	Delivery
2	Software (Operating System)	IC Embedded Software (the operating system and completion data) TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P ROM Mask: TCOS30_Infineon_78xxx_ROM_And_NVM_AES_KV00_WI01.hex OS Version: 01 B6 Completion Code Version: 02			The software part of the product is implemented in ROM/EEPROM of the IC
3	Software (File System)	*eSign application* (dedicated files for the application in a file system), File System Version: 02			The software part of the product is implemented in ROM/EEPROM of the IC
4	Documentation	Operational Guidance, Guidance Documentation of TCOS 3.0 Signature Card Version 2.0 Release 2 with the application Netkey [TCOSOPG]	1.2	27.11.2018	The guidance document of the product is delivered always in an encrypted and signed form. Therefore the integrity and authenticity (key validation) can be ensured during the delivery

No.	Type	Description	Version	Date	Delivery
5	Documentation	TCOS 3.0 Signature Card Version 2.0 Release 2, Administrator’s Guidance, Guidance Documentation of TCOS 3.0 Signature Card Version 2.0 [TCOSADM]	0.3	27.11.2018	The guidance document of the product is delivered always in an encrypted and signed form. Therefore the integrity and authenticity (key validation) can be ensured during the delivery
6	Text Files	Activation command to open lifecycle 6 and 7 and corresponding authentication keys			The authentication keys and command APDUs of the product are delivered always in an encrypted and signed form. Therefore the integrity, authenticity and confidentiality can be ensured during the delivery

1.4 Manufacturer

Manufacturer of the product is T-Systems International GmbH, Untere Industriestrasse 20, D-57250 Netphen.

2. Functional Description

2.1 Functionality and Architecture

The smart card product „TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P“ is intended for the use as a signature card. From a technical point of view „Sig Card“ is implemented as a dual interface smart card with a proprietary operating system and an application layer which directly accesses the operating system layer.

The „Sig Card“ is based on the semiconductor „Infineon SLE78CLX1440P" with proprietary dedicated software of Infineon Technologies AG. The semiconductor family SLE78CLX1440P including the dedicated software was evaluated CC EAL 5+ (CC Version 3.1) and is listed under the Certification ID BSI-DSZ-CC-0829-V3.

The software consists of the operating system TCOS 3.0 Signature Card Version 2.0 Release 2 (ROM, possibly in part EEPROM) as well as of the *eSign application* for the generation of qualified digital signatures.

The operating systems TCOS 3.0 Signature Card Version 2.0 Release 2 provides an interoperable, multifunctional platform conform to ISO 7816 which is appropriate for cards used in applications with high level security requirements. The comprehensive offer of different technical and functional properties as well as security mechanisms of the TCOS operating system especially supports the *eSign application*. Further applications (e.g. the already installed Netkey application) may exist on the „Sig Card“ besides the dedicated *eSign 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 elliptic curve keys and
- generation of digital signatures (elliptic curves).

In summary „Sig Card“ consists of the following components:

- semiconductor (IC) from Infineon (SLE78CLX1440P) with proprietary software,
- TCOS Operating System „TCOS 3.0 Signature Card Version 2.0 Release 2“ and
- *eSign application*.

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

In the state „personalised” the card already contains both the signature verification key and the certificate to the signature verification key. In order to activate „Sig Card“

as a secure signature creation device the cardholder must replace the preset transport PIN with a valid signature PIN.

In the state „pre-personalised” „Sig Card“ contains all necessary keys and can be transferred from the state "not ready for use" to the state "ready for use" with authentication data by the card holder. In order to activate „Sig Card“ as a secure signature creation device the card-holder must replace the preset transport PIN with a valid signature PIN. After that a certificate to the signature verification key must be generated and loaded into „Sig Card“ by a CSP (compare with state „initialised”).

In state „initialised” the card holder may activate „Sig Card“ as a secure signature creation device supervised by the CSP who has generated the certificate. For this purpose, the designated owner of the signature key must at first set the signature PIN in the card using a signature terminal. Only after that an authorised CSP may initiate the generation of the signature key in the card. The CSP must authenticate himself to the card. Only if a CSP has authenticated himself successfully to the card, he may initiate key generation. During the activation phase the CSP initiates key generation in the card using a secure channel between CSP and „Sig Card“ and the public signature verification key is read from the card. The CSP may generate the qualified certificate only if he is convinced that „Sig Card“ is controlled by the owner of the signature key. Thereafter the qualified signature key certificate generated by the CSP may be loaded into the card with integrity protection using the secure channel.

The secure channel guarantees confidentiality as well as authenticity of the communicated data (Secure Messaging).

After the *eSign application* has been activated, „Sig 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.

„Sig 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 (2^{16}-2 at a maximum) or an unlimited number of qualified signatures after successful entry of the signature PIN. The number is determined during initialisation (value n of the signature counter) and cannot be changed afterwards. „Sig 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 „Sig Card“ with a reset of the card. For the generation of further signatures a new entry of the signature PIN is necessary. The use of a multi-signature QSCD is bound to specific usage conditions (cf. conditions for the use of the signature counter).

„Sig Card“ uses a PIN mechanism (PIN-PIN mechanism) that enables the optional use of a second signature PIN (signature PIN2 or PIN2.QES) by the owner of the signature key. Signature PIN PIN2 consists of at least 8 characters and therefore can be distinguished from the proper signature PIN. It can be used as a resetting code for the signature PIN as well as for the generation of qualified signatures. In the same manner signature PIN can be used as a resetting code for signature PIN2.

The *eSign 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 with or without setting a new signature PIN (after successful user authentication with signature PIN2 (PIN2.QES))
- resetting the PIN try counter of signature PIN2 with or without setting a new signature PIN2 (after successful user authentication with signature PIN (PIN1.QES))
- abandoning the signature function by terminating the signature key. In this case the signature key must be terminated. A successful user authentication is a prerequisite for the abandonment.

After an abandonment the *eSign application* may be reactivated, i.e. with supervision of a CSP a new signature key may be generated in the card, a qualified certificate to this key may be issued and loaded into the card. The reactivation of the *eSign application* is performed in the same way as its activation which corresponds to the status of delivery (state „initialised”).

All accesses using the contactless interface of „Sig Card“ which are relevant for the signature application must be performed with secure messaging at a signature terminal. For the mutual authentication between terminal and card as well as for establishing a secure communication channel the authentication protocol PACE (contactless interface), terminal authentication and chip authentication (both for contactless and contact interfaces) are used. During terminal authentication the access rights of the terminal are verified. These include the rights

- of a CSP to activate the *eSign application*, that must be encoded in a CV certificate specific for the CSP, and
- of a signature terminal to generate qualified digital signatures and to manage the signature PIN.

Accesses over the contact interface for the generation of qualified signatures and for the administration of the signature PIN may be performed without secure messaging. However accesses of a CSP (e.g. for key generation) must always be performed with secure messaging.

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

The installation of the file system (file system '02’) is performed during initialisation of the chip (completion of OS code and loading of the file system) by the initialiser. The installation of the file system may only be performed after an authentication of the initialisation system to the card. The cryptographic keys used for the secure loading of data are only known by the card manufacturer. In this sense there exists an end-to-end security between card manufacturer and chip. By this measure the loading of initialisation data that have been modified without authorisation can be prevented. A subsequent loading of further software is not supported by „Sig Card“.

„Sig Card“ supports the following cryptographic algorithms for the generation of signature key pairs as well as of qualified digital signatures:

- Generation of random numbers based on a random number generator of the underlying hardware from IFX. A cryptographic post-processing is used to achieve the conformity with the class PTG.3. The random number generator is a True Random Number Generator (TRNG) with a PTG.2 classification pursuant to [AIS 31]. The random numbers are subject to statistical tests performed in the operation phase („online tests“). These properties were checked in a CC evaluation of the Infineon hardware (cf. [HW ST]).
- DSA based on elliptic curves (ECDSA) using the groups $E(F_p)$ (cf. [TR-03111]) with key lengths of 256, 320, 384 and 512 bits.

„Sig Card“ supports the standardised domain parameters according to [RFC 5639] (Brainpool curve family) as well as the NIST P-256 curve, as specified in [TR-03110], appendix A.2.1.1.

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

- Hash functions SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 according to [FIPS 180-2], where SHA-1 and SHA-256 are used for derivation of symmetric session keys,
- Diffie-Hellman based on elliptic curves (ECDH) according to [TR-03111] with key lengths of 192, 224, 256, 320, 384 and 512 bits for authentication (PACE, terminal authentication and chip authentication) and for key agreement for the secure messaging channel.
- 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 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] (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 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 Card“ uses a role based access control which distinguishes among others between the roles "Administrator" and "Signatory". Furthermore, the following security attributes are used:

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

The CSP, who performs the process of activating the *eSign 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 „Sig Card“ as a signer by inserting his signature PIN.

All accesses over the contact interface or the contactless interface of „Sig Card“ which are relevant for the signature application must be performed at a signature terminal. For mutual authentication and for establishing a secure communication between terminal and „Sig 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.
- **Terminal authentication** to authenticate the terminal towards the card and to prove the associated access rights for the terminal (e.g. the right to generate a new qualified signature key).
- **Chip authentication** to authenticate the chip towards the terminal and to establish a secure channel for the encrypted and integrity protected communication between card and terminal.

With contactless communication terminal authentication and chip authentication must be performed using the secure channel, which has been built up with the successful execution of the PACE protocol. The secure channel, subsequently built up with the successful chip authentication, replaces the secure channel of the PACE protocol.

In a contact based communication a secure channel can be established with terminal authentication and chip authentication.

Especially, this procedure is necessary for a CSP’s accesses to generate a key and to load a qualified certificate into the card. In case of a contactless access at first the local air communication interface between signature terminal and „Sig Card“ is protected by the PACE protocol. After terminal authentication and chip authentication, the CSP can perform remote accesses to the card protected by the secure channel which has been established based on these authentications. In case of a contact access a secure channel is implemented using chip authentication and terminal authentication. In this way an end-to-end security can be implemented between CSP and chip.

Furthermore, the access control is implemented using access conditions, which are stored as security attributes in „Sig 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 application* (generation of the signature key pair, reading the public key and loading the qualified signature key certificate) 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 (PACE, terminal authentication and chip 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“). In case of a „Sig Card“ which already has been personalised this only holds for the state "terminated".
- In the „Sig Card“ states „initialised” or „terminated” (the attribute „SCD operational“ for the data object SCD has the value „no“, i.e. especially no usable signature key is present on the card), the setting of the signature PIN by the designated owner of the signature key pair may only be performed after successful user authentication (card PIN resp. transport PIN after „Sig Card“ delivery in state „personalised” or „pre-personalised”).
- The setting of signature PIN2 by the designated owner of the signature key may only be performed after a successful user authentication (with signature PIN) and after signature PIN has already been set.
- 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.
- The abandonment of the signature function presumes a successful user authentication (card PIN). After a successful abandonment the *eSign application* may not be used further for the generation of qualified signatures, i.e. the *eSign application* is not in state „ready for use“. Signatures may only be generated by the owner of the signature key. To this end, a user authentication with the signature PIN must have been performed successfully before.
- Sensitive data as signature key, card PIN and signature PIN cannot be read using the commands of the operating system.

„Password Authenticated Connection Establishment (PACE) Protocol“

„Sig 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 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 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 Card“ supports the owner of the signature key in controlling the signature creation device when using the card for communication over the air.

Depending from the function to be performed the following start values must be distinguished for the PACE protocol. Here the CAN may be printed on the card body and therefore is no secret for everybody, who has physical access to „Sig Card“. By inserting the CAN, the card-holder starts communication with the contactless card. This procedure is an equivalent to the introduction of a contact card into a reader and makes the uncontrolled communication with „Sig Card“ more difficult.

The execution of the respective function may depend from additional security functions (e.g. successful entry of the signature PIN during signature PIN change). The list merely describes which parameters shall be used in the PACE protocol.

- Card Access Number (CAN, randomly generated number with 6 decimal digits)
    - PACE protocol
- Card PIN
    - generation of a signature key pair controlled by the CSP who generates the certificate,
    - setting a new signature PIN and
    - deleting the signature key

„Sig Card“ supports the execution of the PACE protocol using the contact interface.

„Terminal Authentication“

„Sig Card“ supports the execution of the terminal authentication. This protocol is used for an authentication of the terminal towards „Sig Card“ (challenge-and-response protocol). Furthermore the protocol provides a proof for the access rights of the signature terminal towards „Sig Card“. For contactless communication these rights are bound to the secure channel which subsequently will be established with chip authentication.

For authentication, the terminal generates an authentication token using its private key and an input consisting of a random number generated by „Sig Card“ and further data (e.g. identity of „Sig Card“, ephemeral public terminal keys). The authentication token is verified by „Sig Card“ with the public key of the terminal. The algorithm ECDSA serves as a cryptographic base.

„Chip Authentication“

„Sig Card“ supports the execution of chip authentication. This protocol is used for authentication of the chip towards the terminal as well as for the establishment of a secure channel for the encrypted and integrity protected communication between terminal and card.

The protocol is based on a hybrid algorithm derived from the Diffie-Hellman protocol for key agreement. This algorithm uses the ephemeral DH key pair of the terminal (from terminal authentication) as well as the static DH key pair of „Sig Card“. However, the computation of the authentication token is performed with message authentication codes (MAC) based on the symmetric keys agreed with DH. The cryptographic base is the Diffie-Hellman algorithm with elliptic curves according to [TR-03111].

The chip authentication uses the ephemeral public terminal keys of the preceding terminal authentication. Thus a mutual authentication between terminal and card is achieved.

For chip authentication „Sig Card“ possesses a chip authentication key (static DH key pair). The public key is stored in „Sig Card“ as a signed data object in EF.CardSecurity of the MF. The signature has been generated by the manufacturer using his key.

The manufacturer only signs public keys of authentic signature cards. Using this mechanism the validity of the data personalised in EF.CardSecurity may be proven (passive authentication). Finally, with successful chip authentication and the proof, that the card possesses the respective private key, the authenticity of the chip is ensured. Thus it may be demonstrated, that „Sig Card“ is an evaluated and designated signature card.

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

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

After delivery to the designated owner of the signature key „Sig Card“ does not contain a valid signature PIN. Especially, no valid qualified signature can be generated.

If „Sig Card“ is in state „initialised“, the signature PIN must be set with a minimum length of m characters (the default value for the minimum length is six) before activation of the *eSign application* by the designated owner of the signature key. If „Sig Card“ is in state „pre-personalised“ or „personalised“ the owner of the signature key must replace the transport PIN by a valid signature PIN.

In order to set signature PIN2, a successful (implicit or explicit) user authentication with signature PIN is necessary. Furthermore, signature PIN2 may only be set, after signature PIN has been set.

Both signature PINs have separate PIN Try Counters (PTC) with initial values (sigad), which are decremented by one after a wrong PIN entry. Thus after repeated entries of a wrong PIN (with sigad repeats) the PTC is zero and the corresponding signature PIN is blocked. If both signature PINs are blocked, „Sig Card“ 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 a signature PIN the corresponding PTC is set to its initial value sigad, however only if the corresponding signature PIN resp. „Sig Card“ is not blocked. The initial value sigad is set during card initialisation and has default value three for both signature PINs.

The (re)set of a signature PIN by the command CHANGE REFERENCE DATA does not lead to a re-initialisation of the corresponding PTC. Furthermore a signature PIN may only be (re)set by the command CHANGE REFERENCE DATA, if this signature PIN is not blocked.

Together with the initialisation data, provided by the card manufacturer, the default values minimum length of signature PIN (six bytes), minimum length of signature PIN2 (eight bytes) and minimum length of a PTC (three) are valid. The values can be modified during personalisation by the card manufacturer (cf. chapter 4.2, Requirements for the Responsible Personalisation Party).

The PTC of signature PIN can be reset using (the second) signature PIN2 (PIN2.QES). „Sig Card“ supports signature PIN2 with a length of at least eight characters, which may be used as a resetting code for signature PIN. In an analogous way, the PTC of signature PIN2 may be reset using 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 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 „Sig Card“ by successfully inserting the currently valid signature PIN. Thus changing a signature PIN into 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. The values from 1 to 2^{16}-2 and „unlimited“ may be configured. „Sig Card“ internally checks, if the maximum value has been reached or has been exceeded. Afterwards in order to generate signatures, a signature PIN must be inserted again. With the file system provided by the card manufacturer the signature counter is set to the value „1“, i.e. after each generation of a signature a new verification of the signature PIN is necessary. But generally, the value of the signature counter can be modified by the personaliser (card manufacturer; cf. chapter 4.2, Requirements for the Responsible Personalisation Party).

With abandonment of the *eSign application* the signature key can be „terminated“. A precondition for this termination is a successful user authentication with the card PIN. After termination no further qualified signature can be generated.

Using contactless communication, the execution of administration functions for a signature PIN is bound to a successful execution of the PACE protocol. The corresponding parameter, which must be provided for the PACE protocol by the cardholder, depends on the administration function to be executed (cf. security function „Password Authenticated Connection Establishment (PACE) Protocol“).

„User Authentication with the Card PIN“

The security function comprises the cardholder’s PIN based authentication. It is only available after a successful initialisation and personalisation. The authentication with a card PIN is performed by the cardholder with inserting the correct card PIN. In order to perform card operations, the card PIN is stored in the MF of the card with read protection.

The card PIN may be used to activate the authentication function of „Sig Card“. Especially, it serves as a security feature for administration functions of the *eSign application* (e.g. abandonment of the *eSign application*).

After successful personalisation „Sig Card“ contains for the card PIN - depending from the personalisation model - either a transport PIN with five characters or no reference value. The transport PIN enables the cardholder only to set a card PIN of at least six characters chosen by himself. Thus before the first administration of the *eSign application* the transport PIN must be modified to a card PIN. To this end, the cardholder must authenticate himself towards „Sig Card“ by successfully inserting the transport PIN. After setting the card PIN, the transport PIN cannot be used any longer. User authentication with the transport PIN does not enable a terminal authentication.

The card PIN possesses a PIN Try Counter (PTC). After a predefined number of subsequent wrong PIN entries the card PIN will be blocked. In this state a new entry of the card PIN is only possible, if a successful entry of card PIN2 has been performed before (state „unblock – reset retry counter“).

The PTC is set to 3 during initialisation. This ensures that at a maximum 3 subsequent trials are possible to guess the card PIN.

The card PIN (card PIN2) can be changed by the cardholder. To this end, he must authenticate himself towards „Sig Card“ by inserting the currently valid card PIN (card PIN2), i.e. changing the card PIN (card PIN2) into a new card PIN (card PIN2) is only possible after a successful user authentication with the currently valid card PIN (card PIN2).

„Integrity of Stored Data“

This security function shall guarantee the integrity of stored data. This concerns all DFs, EFs as well as safety-critical data in the RAM, that are used for the generation of qualified signatures. This especially includes the signing key and the signature verification key as well as the reference value for verification of the signature PIN.

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

„Secure Data Exchange“

„Sig 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].

To this purpose, symmetric keys are employed, that have been agreed by a mutual authentication (PACE, terminal authentication and chip authentication) with the external world.

„Memory Processing“

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

„Protection against Error Situations in Hardware and Software“

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

- inconsistencies when generating signatures and
- fault injection attacks.

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

„Resistance against Side Channel Attacks“

„Sig Card“ provides appropriate mechanisms implemented in hardware and software to resist side channel attacks as

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

All safety-critical operations of „Sig Card“, especially the cryptographic functions, are protected by these mechanisms. Information about power consumption, electromagnetic emanation and execution times for commands do not allow to draw conclusions about safety-critical data as a signature key or a signature PIN.

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

„Self-Test“

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

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

„Generation of ECDSA Key Pairs“

„Sig Card“ supports the generation of ECDSA key pairs in the card for generating qualified signatures with lengths of 256, 320, 384 and 512 bits.

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

- Keys for ECDSA with $E(F_p)$ are generated with lengths of 256, 320, 384 and 512 bits.
- The key generation fulfils the requirements according to [SOG-IS], chapter 5.2.
- The 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.
- After key generation „Sig Card“ verifies, if the signature key and the signature verification key are conform. Only valid key pairs are admitted.
- An import of ECDSA key pairs is not possible.
- The key generation includes a physical deletion of the old private key before the new key pair is generated.
- The key generation is resistant against side channel attacks.
- The key generation is only possible, if the security attribute „SCD operational“ of the data object SCD has the value „no“.
- The key generation is only possible, if the CSP has authenticated himself towards „Sig Card“ and has proved his access rights which are necessary for

key generation. In this case the security attribute SCD / SVD management has the value „authorised“. The card command for key generation (GENERATE ASYMMETRIC KEY PAIR) is only executed in a secure channel (established after terminal authentication and chip authentication), to which access rights are bound that have been proved in terminal authentication.

The signature key pair is generated exclusively in the card during activation of the *eSign application*. In this process „Sig Card“ fulfils the security requirements for the generation of ECDSA key pairs as listed above.

In a not personalised „Sig Card“ the command GENERATE ASYMMETRIC KEY PAIR to generate the key pair can only be executed by an authorised CSP in the secure channel between CSP and „Sig Card“ which has been established using terminal authentication and chip authentication.

Parameters of elliptic curves are loaded into „Sig Card“ during card initialisation. The guidance documents [TCOSADM] and [TCOSOPG] list the admitted curves. When using the command for key generation, the key length is not directly provided by the CSP, but an elliptic curve is chosen the key generation is based on. This implicitly defines the key length since curve parameters are stored in the card. Thus only such curves resp. key lengths can be used, whose parameters either are already stored in the card or are transmitted to the card by the command GENERATE ASYMMETRIC KEY PAIR.

With key generation the CSP must ensure that a curve resp. key length is chosen, that is appropriate beginning with the time of key generation, until expiration of the qualified signature key certificate. Here the list of currently admitted cryptographic algorithms according to [SOG-IS] has to be used.

The owner of the signature key pair must authorise the key generation process with a successful user authentication using the card PIN.

„Generation of Qualified Signatures“

„Sig Card“ supports the generation of qualified digital signatures with ECDSA signature keys with lengths of 256, 320, 384 and 512 bits. The security function has the following properties:

- Receipt of (already hashed) data (data to be signed, DTBS) to generate qualified digital signatures.
- Computation of ECDSA signatures according to [TR-03111] with key lengths of 256, 320, 384 and 512 bits.
- The random number generator of the underlying Infineon hardware is used to generate random numbers for the generation of ECDSA signatures.
- The key generation is resistant against side channel attacks.
- The signature is generated in a manner that the signature key cannot be derived from the generated signature und that during signature generation no information about the signature key is revealed.

- A signature can only be generated, if the user has authenticated himself successfully with a signature PIN (command VERIFY) and if the security attribute „SCD operational“ of the data object SCD has the value „yes“.
- Using the contactless interface the card command for the generation of a qualified signature (PSO : Compute Digital Signature) must be sent to the card in a secure channel (established with PACE, optionally terminal authentication and chip authentication).

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 Party

- The initialisation data provided by T-Systems International 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 [TCOSADM] and [TCOSOPG] must be taken into consideration.

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 performed before issuing the qualified certificate and shall list the special security requirements resulting from the high potential of attacks in a detailed way. Especially but not exclusively, all security requirements for the environment must be indicated that are part of the designation.

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

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

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

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

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

Requirements for the Responsible Personalisation Party

- The card manufacturer must ensure that the personalisation data (especially of the *eSign application*) are treated in a secure way. The personalisation data must be protected with respect to integrity, authenticity and confidentiality.
- The card manufacturer 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 [TCOSADM] und [TCOSOPG] must be taken into account.
- Concerning the personalisation of parameters for the data objects signature PIN and signature PIN2, the indications according to [TCOSADM] and [TCOSOPG] must be taken into account. Especially the minimum length m of the signature PIN must not be less than six. Furthermore the PTC of the signature PIN may be personalised with the value m/2 (rounded down) at a maximum and must not exceed the value 20. The minimum length for the signature PIN2 must be greater or equal than 8. The default values provided by the card manufacturer already fulfil these requirements.
- The value one for the signature counter as provided by the card manufacturer during personalisation may only be changed under observation of the conditions of use for the signature counter.

Requirements for the CSP

- The component used to generate qualified certificates (application) (certificate generation application, CGA) should consider the instructions for CSPs pursuant to the Operational Guidance, [TCOSADM], chapter 8.
- The CSP must describe the process to activate the *eSign application* in his security concept. It has to be explained how the CSP can make sure that the designated owner of the signature key possesses a qualified signature creation device - here „Sig Card“ - and that this device is completely controlled by him alone.
- If the CSP distributes a product to generate qualified digital signatures and if its product name differs from the product name in the designation, then the CSP must point out to the actually designated product in the documentation for the distributed product.

  In this case the CSP must add a supplement to the designated product at the responsible supervisory body. In the supplement at the least the CSP, the name of the designated product as well as the distribution name of the product have to be listed.
- The CSP must inform the owner of the signature key about designated card terminals and corresponding signature application components where he can activate his signature PIN.

  This aspect must also be considered in the CSP’s security concept.
- 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 Card“ (i.e. which are used by the owner of the signature key to set or change his card PIN or signature PIN) must be configured such that reference data are inserted via the keyboard of the smart card reader as a default. In case that the program optionally allows to deactivate the keyboard of the smart card reader and to activate the keyboard of the PC, the program must output a warning note concerning a possible loss of security when changing the input mode.

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

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

- When using signature PIN2 the owner of the signature key must choose different values for both signature PINs.
- The owner of the signature key must use and keep „Sig Card“ such that misuse and manipulation are prevented.
- In order to generate qualified digital signatures the owner of the signature key uses „Sig Card“ only together with a lawful signature application component.

Requirements for the Manufacturer of Signature Application Components

- The manufacturer of a signature application component must respect the interfaces of the smart card operating system TCOS as well as of the *eSign application* (cf. [TCOSADM] and [TCOSOPG]) in an appropriate manner.
- When generating a digital signature on a hash value that has been computed by the external world and transmitted to the card, it must be guaranteed that the signature application component has chosen an appropriate hash function.
- The manufacturer of a signature application component used for the generation of qualified digital signatures (Signature Creation Application, SCA) should consider the instructions for terminal developers pursuant to the Operational Guidance, [TCOSADM], chapter 8.

3.3 Cryptographic Algorithms and Parameters

For the generation of digital signatures „Sig Card“ provides ECDSA based on groups $E(F_p)$ according to [TR-03111]. Key lengths of 256, 320, 384 and 512 bits 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. A cryptographic post-processing is used to achieve the conformity with the class PTG.3. The random number generator is a True Random Number Generator (TRNG) with a PTG.2 classification pursuant to [AIS 31]. The random numbers are subject to statistical tests performed in the operation phase („online tests“). These properties were checked in a CC evaluation of the Infineon hardware (cf. [HW ST]).

The cryptographic algorithms used are based on the algorithm catalogue SOG-IS [SOG-IS].

Among others [SOG-IS] lists the following suitable hash functions:

- SHA-2 [FIPS 180-2] with hash value lengths of 256 (SHA-256), 384 (SHA-384) and 512 (SHA-512) bits

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

- Brainpool Curve Family [RFC 5639] with BrainpoolP256r1, BrainpoolP384r1 and BrainpoolP512r1
- NIST P-256 from the NIST Curve Family [FIPS 186-4]

3.4 Assurance Level and Attack Potential

The product TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P 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 Card“ the protection profile „Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation“, EN 419211-2:2013, [PP SSCD Part 2] (cf. [ETR]) was used. So the requirements laid down in Regulation (EU) No. 910/2014 Articles 30 (3) a, 39 (2) as well as the Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 are fulfilled.

The evaluation was performed as a so-called composition evaluation, which takes into account the evaluation results of the CC evaluation of the semiconductor SLE78CLX1440P from the semiconductor manufacturer Infineon Technologies AG. This evaluation was performed with an assurance level **EAL 5+** (EAL 5 with augmentations ALC_DVS.2, AVA_VAN.5). The evaluation was performed against a **high** attack potential.

The semiconductor is listed under the Certification ID BSI-DSZ-CC-0829-V3.

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

[ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P, Version 1.1, 12.12.2018, SRC.00032.QSCD.12.2018

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

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

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

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

[HW ST] Security Target of the underlying hardware platform, Security Target BSI-DSZ-CC-0829-V3-2017, Version 2.3, 2017-09-28, “Security Target M7820 A11 including the optional SHA-2 Software Library”, Infineon Technologies AG (confidential document)

[PP SSCD Part 2] Protection Profiles for Secure Signature Creation Device - Part 2: Device with key generation, EN 419211-2:2013, 2016-06-30, BSI-CC-PP-0059-2009-MA-02

[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 1.1 June 2018

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

[ST] Specification of the Security Target TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P, T-Systems International GmbH, Version 2.0.2, 29.11.2018

[TCOSADM] TCOS 3.0 Signature Card Version 2.0 Release 2, Administrator’s Guidance, Guidance Documentation of TCOS 3.0 Signature Card Version 2.0, Version 0.3, 27.11.2018

[TCOSOPG] Operational Guidance, Guidance Documentation of TCOS 3.0 Signature Card Version 2.0 Release 2 with the application Netkey, 1.2, 27.11.2018

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

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

End of certification report