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

AMENDMENT

Amendment 2 to the Certification
SRC.00032.QSCD.12.2018 of 18.12.2018

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 for the

Qualified Signature / Seal Creation Device
TCOS 3.0 Signature Card Version 2.0
Release 2/SLE78CLX1440P

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

31.12.2026

Bonn, 9 September 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

No changes compared to the previous certification status.

1.2 Delivery

No changes compared to the previous certification status.

1.3 Delivery Items

No changes compared to the previous certification status.

1.4 Manufacturer

No changes compared to the previous certification status.

2. Functional Description

2.1 Functionality and Architecture

No changes compared to the previous certification status.

2.2 Security Functions and Security Properties of „Sig Card“

No changes compared to the previous certification status.

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

3.1 Fulfilled Requirements

No changes compared to the previous certification status.

3.2 Conditions of Use

No changes compared to the previous certification status.

3.3 Cryptographic Algorithms and Parameters

The information in this section is replaced as described below:

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, recommended

Among others [SOG-IS] lists the following suitable digital signature schemes:

- ECDSA, recommended

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

- Brainpool Curve Family [RFC 5639] with BrainpoolP256r1, BrainpoolP384r1 and BrainpoolP512r1, recommended

- NIST P-256 from the NIST Curve Family [FIPS 186-4], recommended

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

- The use of **ECDSA** with the parameters chosen by „Sig Card“ is **not restricted** by the algorithm catalogue SOG-IS [SOG-IS].

Due to the suitability of ECDSA with the parameters chosen by „Sig Card“, the certification of the „Sig Card“ is extended until **31.12.2026**.

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

No changes compared to the previous certification status.

4. References

The indicated references are extended or changed as follows:

[ETR_Comp]	Evaluation Technical Report for Composite Evaluation (ETR Comp), BSI-DSZ-CC-0829-V3-2017, M7820 A11, Version 2, 2017-10-02
[IFX_Cert]	Certification Report of the underlying hardware platform, BSI-DSZ-CC-0829-V3-2017 for Infineon Technologies Smart Card IC (Security Controller) M7820 A11, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017
[SOG-IS]	SOG-IS Crypto Working Group; SOG-IS Crypto Evaluation Scheme; Agreed Cryptographic Mechanisms; Version 1.2 January 2020

End of amendment 2