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

AMENDMENT

Amendment 1 to the Certification
SRC.00043.QSCD.07.2021 of 23.07.2021

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 Creation Device
TCOS Health Professional Card Version 2.1
Release 1 / SLC52

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

31.12.29

Bonn, 24 May 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 reference certificate.

1.2 Delivery

No changes compared to the reference certificate.

1.3 Delivery Items

No changes compared to the reference certificate.

1.4 Manufacturer

No changes compared to the reference certificate.

2. Functional Description

2.1 Functionality and Architecture

The following is added to the first paragraph:

In the meantime, the hardware platform has been re-certified under the certification number BSI-DSZ-CC-1079-V3-2021.

2.2 Security Functions and Security Properties of „Sig Card“

No changes compared to the reference certificate.

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

3.1 Fulfilled Requirements

No changes compared to the reference certificate.

3.2 Conditions of Use

No changes compared to the reference certificate.

3.3 Cryptographic Algorithms and Parameters

As stated in the original certification report the cryptographic algorithms used by the product „HPC Signature Card“ are classified by the algorithm catalogue SOG-IS [SOG-IS] as follows.

Among others, [SOG-IS] lists the following requirements for RSA:

- Legacy RSA: The acceptability deadline for the legacy use of a modulus of size above 1900 bits, but less than 3000 bits, is set to 31 December 2025.
- RSA PSS (PKCS #1, v2.1), recommended
- ISO 9796-2, recommended

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

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

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

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

- **RSA** signatures with the parameters chosen by „HPC Signature Card“ may only be used until **31 December 2025**. The CSP must ensure that the validity end date (attribute not after) of issued certificates for RSA keys does not exceed the suitability of RSA with a key length of 2048 bits.

Due to the suitability of ECDSA with the parameters chosen by „HPC Signature Card“, the certification of the „HPC Signature Card“ is extended 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 last paragraph is replaced by:

The semiconductor is listed under the Certification ID BSI-DSZ-CC-1079-V2-2020. In the meantime, the hardware platform has been re-certified under the certification number BSI-DSZ-CC-1079-V3-2021.

For the purpose of issuing this amendment, the CC Evaluation Laboratory of SRC has verified that the vulnerability assessment conducted as part of the certification with the registration number SRC.00043.QSCD.07.2021 and the associated penetration tests and test statements are still currently valid [Statement Letter].

4. References

The indicated references are extended or changed as follows:

[Statement Letter] SRC, Statement Letter, Re-Assessment von TCOS Health Professional Card Version 2.1 Release 1 / SLC 52 (SRC.00043.QSCD.07.2021), 27.04.2022

[HW CR] Certification Report of the underlying hardware platform, BSI-DSZ-CC-1079-V2-2020 for IFX_CCI_00000Fh, IFX_CCI_000010h,IFX_CCI_000026h, IFX_CCI_000027h,IFX_CCI_000028h, IFX_CCI_000029h,IFX_CCI_00002Ah, IFX_CCI_00002Bh,IFX_CCI_00002Ch in the design step G12 and in-cluding optional software libraries and dedicated firmware from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020-06-16

Certification Report of the underlying hardware platform, BSI-DSZ-CC-1079-V3-2021, 2021-11-12

[HW ST] Security Target of the underlying hardware platform, Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+, IFX_CCI_00000Fh, IFX_CCI_000010h,IFX_CCI_000026h, IFX_CCI_000027h,IFX_CCI_000028h, IFX_CCI_000029h,IFX_CCI_00002Ah, IFX_CCI_00002Bh,IFX_CCI_00002Ch G12, Date 2020-04-03, Version 0.8,

Security Target of the underlying hardware platform, Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+, 2021-11-05, Revision 1.5

End of amendment 1