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

AMENDMENT

Amendment 2 to the Certification
SRC.00036.QSCD.09.2020 of 29.09.2020

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
IDEMIA_HC_Germany_NEO_G2.1_HBA, V1

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

31.12.2027

Bonn, 5 June 2023

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):

The current certification consists of the referenced certificate and amendment 1.

1. Product Name and Scope of Delivery

1.1 Product Name

No changes compared to the current certification.

1.2 Delivery

No changes compared to the current certification.

1.3 Delivery Items

No changes compared to the current certification.

1.4 Manufacturer

No changes compared to the current certification.

2. Functional Description

2.1 Functionality and Architecture

No changes compared to the current certification.

2.2 Security Functions and Security Properties of „Sig Card“

No changes compared to the current certification.

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

3.1 Fulfilled Requirements

No changes compared to the current certification.

3.2 Conditions of Use

The requirements for the CSP are changed to:

Requirements for the CSP

- 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. The current version of [SOG-IS] limits their eligibility to the period until 31.12.2025.
- If the CSP distributes a product to generate qualified digital signatures with a product name that differs from the product name in the designation, then the CSP must point out the actual designated product in the documentation for the distributed product.
- The CSP must inform the owner of the signature key about designated card terminals and corresponding signature application components where the owner can activate his signature PIN.

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

- Programs which a CSP provides to his clients for the transmission of reference data to "HPC Signature Card" (i.e. which are used by the owner of the signature key to set or change his card PIN or signature PIN) must be configured such that reference data are inserted via the keyboard of the smart card reader as a default. In case that the program optionally allows to deactivate the keyboard of the smart card reader and to activate the keyboard of the PC, the program must output a warning note concerning a possible loss of security when changing the input mode.

3.3 Cryptographic Algorithms and Parameters

For the generation of digital signatures, "HPC Signature Card" provides RSA according to [PKCS#1] and ECDSA based on groups $E(F_p)$ according to [TR-03111]. Key lengths of 2048 bits for RSA and 256 bits for ECDSA are supported. Signatures are only generated with hash values that have been computed by the external world.

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

The cryptographic algorithms used by the product "HPC Signature Card" are classified by the algorithm catalogue SOG-IS [SOG-IS] as follows.

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

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

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

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

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

- 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 TSP 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.

This certification of the „HPC Signature Card" is therefore valid until **31.12.2027**.

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 current certification.

4. References

No changes compared to the current certification.

End of amendment 2