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

AMENDMENT

Amendment 1 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.

Bonn, 20 October 2021

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

The scope of the delivery for the product consists of the following items. Compared to the reference certificate only the delivery items 2 TOE_ES (ES Revision/Release 2.2.4) and 3 Wrapper (Version and SHA 256 check sum of the 7z archive).

Table 1: Delivery items

No.	Delivery item	Description / Additional Information	Type	Delivery method
1	TOE_IC	Integrated Circuit (IC) family H13 with Crypto Libraries ACL v2.08.007, SCL v02.04.002 and Hardware Support Library (HSL) v03.12.8812 provided by Infineon Technologies AG contact based / contactless module	HW / SW	Delivery of not-pre-personalised / pre-personalised smart-cards
2	TOE_ES	Smartcard Embedded Software comprising the IDEMIA_HC_Germany_NEO_G2.1_COS, V1 as Card Operating System Card (designed as flash implementation) for the German Health Care System provided by Idemia Version V1 ES Revision/Release 2.2.6 Variants: 0x10 or 0x11	SW	Delivery of OS Flashing image (implemented in EEPROM/Flash of the microcontroller)

No.	Delivery item	Description / Additional Information	Type	Delivery method
3	Wrapper	Wrapper for interpretation of the exported TSF data. Version 2.2.7 The Wrapper software is delivered as 7z archive. The 7z archive file must have the following SHA256 checksum: 62D76A73DB6FFC71F5942A5CE4D1890765C803016AEB6D61F6187E0841878BDF The 7z archive consists of Wrapper.jar iwrapper.jar jdom-2.0.5.jar bcprov-ext-jdk15on-150.jar For the corresponding SHA256 checksums, see [Idemia_Wrapper], chap. 1.1.	SW	Delivery as electronic file
4	OS-PrePerso sequence	Command sequence used by the OS Pre-Personalizer to configure the Card Operating System. Signed by the developer. The signature is verified by the TOE_ES.	SW	Delivery as electronic file
5	Associated guidance documentation	IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 – Preparative Guidance, [Idemia_AGD_PRE], IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 – Operational User Guidance, [Idemia_AGD_OPE], IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 –Wrapper Guidance, [Idemia_Wrapper] IDEMIA_HC_Germany_NEO_G2.1_COS V1 – Data Sheet Data Sheet with information on the actual identification data and configuration of the gHC Card	DOC	Document in paper / electronic form
6	Aut-Key K_MORPHO_AUT	Public part of the authentication key pair relevant for the authenticity of the TOE	KEY	Document in paper form / electronic file[1]

[1] The Public Key Part is delivered as part of the data sheet

No.	Delivery item	Description / Additional Information	Type	Delivery method
7	Perso-Key K_OBJ_PERS	Personalisation key relevant for the product personalisation of the TOE	KEY	Document in paper form / electronic file
8	Object System Signature Key K_OBJ_VERIFICATION	Object System Signature Key, needed for calculation of the Signature over an Object System.	KEY	Document in paper form / electronic file
9	OS PrePersonaliser Master Key K_OS_PREPERS_MK	Key for derivation of card individual authentication keys	KEY	Document in paper form / electronic file
10	K_OPE_DEC	Key needed for encryption of secrets in Load Application sequences. Used for encryption and integrity check of key data imported during the Operational phase	KEY	Document in paper form / electronic file
11	K_OPE_VERIFICATION	Key needed to calculate a Signature over Load Application sequences. Used for generation of the signature calculated during the creation of the LOAD APPLICATION commands for a possible In-Field update	KEY	Document in paper form / electronic file

Note: The PrePersoScript is also part of the TOE delivery, although it is not part of the TOE. The PrePersoScript is a specific command sequence sent to the card by the Product Pre-Personaliser of the Card to create internally the non-card individual data. It is signed by the developer and the signature is verified by the TOE_ES. It is delivered as electronic file.

Deliverables in paper form require a personal passing on or a procedure of at least the same security. Deliverables in electronic form have to be submitted integrity and authenticity protected. For Key material also confidentiality has to be ensured.

The commercial numbering of the TOE by Infineon Technologies AG is as follows:

H13 chip family

Product Type: SLC32GDA

By executing the GET DATA command, the following product identifications of the foundry are given:

IC Manufacturer: 81 00

IC Type: 13 2A

OS Version: 02 02

Mask Date: 00 62

OS Subversion: 06 00

1.4 Manufacturer

No changes compared to the reference certificate.

2. Functional Description

2.1 Functionality and Architecture

No changes compared to the reference certificate.

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

No changes compared to the reference certificate.

3.4 Assurance Level and Attack Potential

No changes compared to the reference certificate.

4. References

The indicated references are extended or changed as follows:

[Idemia_AGD_PRE]	IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 – Preparative Guidance, Version: 1.11, 02.08.2021, filename: IDEMIA_HC_Germany_NEO_G2.1_COS_V1_PreparativeGuidance_V1.11.pdf
[Idemia_AGD_OPE]	IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 – Operational User Guidance V2.2, 02.08.2021, file name: IDEMIA_HC_Germany_NEO_G2.1_COS_V1_OperationalUserGuidance_V2.2.pdf
[Idemia_Wrapper]	IDEMIA_HC_GERMANY_NEO_G2.1_COS, V1 –Wrapper Guidance, Version: V1.8, 02.08.2021, filename: IDEMIA_DEV_MAN_GHC_V1_Wrapper_V1.8
[Idemia_IAR]	Auswirkungsanalyse, Management Version, Patch IDEMIA Health Card Germany G2.1 COS NEO V1, Version 1.3

End of amendment 1