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

AMENDMENT

Amendment 1 to the Certification
SRC.00076.QSCD.02.2026 of 10.02.2026

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[1]
that for the

Qualified Signature / Seal Creation Device
LuxTrust Crypto Box device V2

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

09.02.2031

This amendment is only valid with the following report and the original certification.

Markus Schierack
03.08.2026 21:29 Uhr

Christoph Sesterhenn
03.08.2026 14:24 Uhr

Bonn, 03 August 2026

Markus Schierack / Christoph Sesterhenn

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; last amended by Regulation (EU) No 2024/1183.

Description of the Qualified Signature Creation Device (QSCD):

1. Product Name and Scope of Delivery

A trustworthy system supporting server signing is a system that offers remote digital signatures as a service. It ensures that Signer's signing keys are only used under the sole control of the Signer for the intended purpose.

The LuxTrust Crypto Box device V2 uses the CryptoServer CP5 for key generation and for creating the digital signature values. The system consists of a local and remote environment. The Signer is in the local environment and interacts using a device (e.g. laptop, tablet or smart phone) with the Server Signing Application (SSA) in the remote environment.

The signature operation is performed using a Signature Activation Protocol (SAP), which requires that Signature Activation Data (SAD) be provided at the local environment. The SAD binds together three elements: Signer authentication with the signing key and the representation of the data to be signed (DTBS/R(s)).

To ensure the Signer has sole control of his signing keys, the signature operation needs to be authorised. This is carried out by a Signature Activation Module (SAM), which can handle one endpoint of SAP, verify SAD and activate the signing key within a Cryptographic Module. Both, the Cryptographic Module and the SAM are to be located within a tamper protected environment. SAD verification means that the SAM checks the binding between the three SAD elements as well as checking that the Signer is successfully authenticated.

The logical scope of the LuxTrust Crypto Box device V2 itemizing the security services being in scope of the evaluation:

- Signer management and
- Signature operation.

After the certification of the LuxTrust Crypto-Box SAM version 2.0.0.1, the developer found a flaw that affected the long-term availability of the deployed device: The developer fixed the flaw and submitted the LuxTrust Crypto-Box SAM version 2.0.0.2 to the evaluation lab. The evaluator assessed the change and found no impact on the security functionality, and that the evaluation results from version 2.0.0.1 still hold for version 2.0.0.2 (cf. [ETR LuxTrust-SAM], [Statement Letter]). Based on these results, the designation body concludes that the following statements of the original certification report still hold for the LuxTrust Crypto-Box SAM 2.0.0.2, with the interchange of LuxTrust Crypto-Box SAM 2.0.0.1 into LuxTrust Crypto-Box SAM 2.0.0.2, or are updated as indicated.

1.1 Product Name

No changes compared to the original certification report.

1.2 Delivery

No changes compared to the original certification report.

1.3 Delivery Items

No changes compared to the original certification report.

1.4 Identification and initialisation by the User

The second to last paragraph is updated as followed.

For this purpose, the subsequent command can be used. The LuxTrust Crypto-Box SAM 2.0.0.2 firmware module has the name CISA and the hexadecimal module identifier 11A.The firmware module of the LuxTrust Crypto-Box SAM 2.0.0.2 has now the version 1.4.6.2 as shown in the example of the command readout below.

Example:

```
csadm dev=<hsm port>@<hsm ips address> ListFirmWare
  ID name          type version        initialization level
-------------------------------------------------------------
   0 SMOS          SDK  5.6.6.1        INIT_OK
   4 POST          SDK  1.0.0.2        INIT_OK
  68 CXI           SDK  2.2.3.7        INIT_OK
  81 VDES          SDK  1.0.9.4        INIT_OK
  83 CMDS          SDK  3.6.0.13       INIT_OK
  84 VRSA          SDK  1.3.6.5        INIT_OK
  86 UTIL          SDK  3.0.5.3        INIT_OK
  87 ADM           SDK  3.0.25.5       INIT_OK
  88 DB            SDK  1.3.2.4        INIT_OK
  89 HASH          SDK  1.0.12.1       INIT_OK
  8b AES           SDK  1.4.1.7        INIT_OK
  8e LNA           SDK  1.2.4.4        INIT_OK
  8f ECA           SDK  1.1.12.4       INIT_OK
  91 ASN1          SDK  1.0.3.8        INIT_OK
  96 MBK           SDK  2.3.0.0        INIT_OK
  9c ECDSA         SDK  1.1.16.2       INIT_OK
 11a CISA          SDK  1.4.6.2        INIT_OK
 1a0 CXIAL         SDK  1.0.0.1        INIT_OK
```

1.5 Manufacturer and Applicant

No changes compared to the original certification report.

2. Functional description

No changes compared to the original certification report.

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

3.1 Fulfilled Requirements

No changes compared to the original certification report.

3.2 Conditions of Use

No changes compared to the original certification report.

3.3 Cryptographic Algorithms and Parameters

No changes compared to the original certification report.

3.4 Assurance Level and Attack Potential

The fifth paragraph now reads the following.

The LuxTrust Crypto-Box SAM 2.0.0.1 was successfully evaluated according “ISO/IEC 15408 Evaluation criteria for IT-Security” Version 3.1 of the Common Criteria (see [ISO/IEC 15408-1], [ISO/IEC 15408-2] and [ISO/IEC 15408-3]) Revision 5 and the Common Evaluation Methodology (see [CEM]) with assurance level **EAL 4+** (EAL4 with augmentation AVA_VAN.5). The evaluation was carried out against a **high attack potential**. After the certification of the LuxTrust Crypto-Box SAM version 2.0.0.1, the developer found a flaw that affected the long-term availability of the deployed device. The developer fixed the flaw and submitted the LuxTrust Crypto-Box SAM 2.0.0.2 to the evaluation lab. The evaluator assessed the change and found no impact on the security functionality, and that the evaluation results from version 2.0.0.1 still hold for version 2.0.0.2 (cf. [ETR LuxTrust-SAM], [Statement Letter]).

4. References

The following references are updated or added:

[ETR LuxTrust-SAM] SRC, Evaluation Report, Evaluation Technical Report (ETR), LuxTrust Crypto Box SAM 2.0.0.2, Version 2.5.3, 30 July 2026

[Statement Letter] SRC, Statement Letter, Maintenance LuxTrust Crypto-Box SAM 2.0.0.2, SRC GmbH, 28.07.2026

[ST LuxTrust-SAM] LuxTrust Crypto Box SAM Security Target, LuxTrust S.A. & achelos GmbH, Version 0.2.8, 2026-04-14

End of amendment 1