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

CERTIFICATE

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 the

Qualified Signature / Seal Creation Device
LuxTrust Crypto Box device V2

fulfils the following referred Requirements of the Regulation (EU) No. 910/2014[1].

Certificate is valid until

09.02.2031

SRC Certificate Registration Number

SRC.00076.QSCD.02.2026

This certificate is only valid with the certification report.

Markus Schierack
10.02.2026 14:24 Uhr

Christoph Sesterhenn
10.02.2026 13:31 Uhr

Bonn, 10 February 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 SAM 2.0.0.1 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 SAM 2.0.0.1 itemizing the security services being in scope of the evaluation:

- Signer management and
- Signature operation.

1.1 Product Name

The product is a Qualified Signature Creation Device and Qualified Seal Creation Device with the product name **LuxTrust Crypto Box device V2** (short „Crypto Box“) for the generation of remote electronic signatures and remote electronic seals.

The CryptoServer Se-Series Gen2 CP5 (short “CryptoServer CP5”) is available in the versions CryptoServer CP5 Se12 5.1.2.0, CryptoServer CP5 Se52 5.1.2.0, CryptoServer CP5 Se500 5.1.2.0, CryptoServer CP5 Se1500 5.1.2.0. This certification at hand covers all these listed CryptoServer CP5 versions.

A basic requirement for such a service is that the key owner must ensure control of the seal or signature keys. In particular, the signature key must be under the sole control of the key owner. A Signature Activation Module (SAM) is provided to ensure sole control. The main purpose of LuxTrust Crypto-Box SAM 2.0.0.1 is to check the Signature Activation Data (SAD) and to use the correct signature key. The SAD binds together three elements: signer authentication with the signing key and the data to be signed (DTBS/R(s)). The SAD abstractly described in the corresponding standard [EN 419 241-1] and protection profile EN 419 241-2 [EN 419 241-2] are implemented within this project in form of an authentication assertion. This assertion binds the successful authentication of the key holder cryptographically to the Data to be Signed (DTBS).

The certified version of LuxTrust Crypto-Box SAM 2.0.0.1 is V 2.0.0.1. The firmware needs to be signed by Utimaco. The signed firmware will not include deviations compared to V 2.0.0.1, but receives a new version number due to the added signature information. The evaluation results and the certification are fully valid for the signed version also.

1.2 Delivery

The LuxTrust Crypto-Box SAM 2.0.0.1 is a firmware module for the Utimaco CryptoServer CP5. The delivery comprises the delivery of the LuxTrust Crypto-Box SAM 2.0.0.1 firmware module to the Trust Service Provider (TSP). The delivery of the LuxTrust Crypto-Box SAM 2.0.0.1 firmware module and LuxTrust Crypto-Box SAM 2.0.0.1 documentation has to follow strictly the secured delivery procedures. Especially, appropriate signing of the LuxTrust Crypto-Box SAM 2.0.0.1 is performed for preparing its delivery. The corresponding process requires involvement of Utimaco.

The LuxTrust Crypto-Box SAM 2.0.0.1 runs inside a CP5 device, which is a CP HSM in a production environment. For this, the compiled LuxTrust Crypto-Box SAM 2.0.0.1 must be signed by an appropriate code-signing key for being loaded into and executed on a CP5 device. In order to be loaded into a CP5 HSM for production, the LuxTrust Crypto-Box SAM 2.0.0.1 must be signed by Utimaco with the specific CryptoServer CP5 Module Signature Key (MSK). This MSK is only used for signing firmware modules that shall be loaded into CryptoServer CP5 devices. The process to complete this signing process between Utimaco and LuxTrust is described in [SAM-Sign-Proc]. The SAM firmware module can only be loaded into a CryptoServer CP5 under the in [SAM-Sign-Proc] defined circumstances. In addition, the complete signing process and its steps are described.

After finalising the code signing process between LuxTrust and Utimaco, the following steps are executed for delivering a LuxTrust Crypto-Box SAM 2.0.0.1 release package to a TSP:

- All artefacts of the to be delivered LuxTrust Crypto-Box SAM 2.0.0.1 version are extracted under dual control of the GIT repository. This also includes artefacts, which are built based on stored artefacts like the LuxTrust Crypto-Box SAM 2.0.0.1 binary.
- The prepared artefacts comprising the signed LuxTrust Crypto-Box SAM 2.0.0.1 binary are packed under dual control into a temporary folder on a laptop of the development team.
- The LuxTrust Crypto-Box SAM 2.0.0.1 binary (file name: cisa.mtc) has previously been signed as described in the procedure described above. Subsequently, the signed version replaces the original version in the folder containing the prepared delivery artefacts.
- The content of the folder containing the LuxTrust Crypto-Box SAM 2.0.0.1 delivery artefacts is packed as a ZIP container, which is encrypted with sufficiently long random password (at least 10 characters containing digits, upper and lower case letters and symbols).
- The encrypted ZIP is wrapped into another ZIP that is sealed using LuxTrust COSI Trust Services hub in ASIC-E with XAdES format (cf. section 4.4 of [ETSI EN 319 162-1]) in applying a Qualified Seal of LuxTrust Release Management with a Qualified Signature Timestamp. The signing tool implicitly uses the

LuxTrust Qualified Sealing service and the LuxTrust Qualified Timestamping service for this purpose.

The person on the TSP side, who is responsible for the acceptance check, later on validates ASIC-E container by using a trustworthy XAdES validation tool or service that uses the European Trusted Lists as the set of eligible trust anchors (e.g. cf. [EC DSS APP]). The validation must pass successfully and it must uniquely identify LuxTrust Release Management as the signer.

The packed ZIP file represents the delivery bundle, which is transferred via a secure channel to the TSP, a customer or any other relying party. For instance, transfer of the ZIP can be performed via signed email that directly contains the ZIP or that contains a download URL of the ZIP; or via securely sent postal package containing a USB stick. The password of the inner ZIP file is being sent via a different channel, e.g. a separate encrypted email or orally during a telephone call.

When using an email for delivering the release package, the corresponding mail contains a clear advice for the customer how the ZIP has to be validated and unpacked and with an explicit reference, that all complementary information including an unambiguous visible version indication of the contained LuxTrust Crypto-Box SAM 2.0.0.1 binary can be found in the also contained [AGD_PRE] PDF document. The advice also indicates that the LuxTrust Crypto-Box SAM 2.0.0.1 binary version can be identified and crosschecked upon loading it into a CP5 HSM by using the Utimaco csadm ListFirmware command (cf. section 7.8.1 of [CP5 MAN ADM]). When alternatively delivering the release package on a USB stick, the same advice is contained in the enclosed letter of the postal delivery package.

1.3 Delivery Items

The certified product consists of the Hardware Security Module (HSM) "CryptoServer CP5" and the Signature Activation Module LuxTrust Crypto-Box SAM 2.0.0.1. The LuxTrust Crypto-Box SAM 2.0.0.1 is implemented as a firmware module for the HSM "CryptoServer CP5". In particular, the LuxTrust Crypto-Box SAM 2.0.0.1 represents a so-called Internal SAM with regard to [ST HW]. Both modules together form the Qualified Signature/Seal Creation Device (QSCD) required for remote qualified signatures and remote qualified seals according to the Regulation (EU) No. 910/2014 [Reg No. 910/2014].

The scope of delivery for „Crypto Box“ consists of the following items:

Table 1: Delivery items and associated delivery methods

No.	Delivery item	Description	Type	Delivery method
1	LuxTrust Crypto Box SAM V 2.0.0.1 (see remark regarding the version)	The LuxTrust Crypto-Box SAM is a firmware module for the Utimaco CryptoServer CP5.	LuxTrust Crypto-Box SAM binary `cisa.mtc` in a crypto-graphically signed ZIP file	The content of the folder containing the LuxTrust Crypto-Box SAM binary (file name: `cisa.mtc`) is packed as a ZIP container, which is encrypted with sufficiently long random password (at least 10 characters). The password is sent via a different channel. The encrypted ZIP is wrapped into another ZIP that is sealed using LuxTrust COSI Trust Services hub in ASIC-E with XAdES format in applying a Qualified Seal of LuxTrust Release Management with a Qualified Signature Timestamp. The person who is responsible for the acceptance check validates the ASIC-E container by using a trustworthy XAdES validation tool or service that uses the European Trusted Lists as the set of eligible trust anchors. The validation must pass successfully and it must uniquely identify LuxTrust Release Management as the signer. The firmware needs to be signed by Utimaco. The signed firmware will not include deviations compared to V 2.0.0.1, but receives a new version number due to the added signature information. The evaluation results (and therefore the certification) are fully valid for the signed version also.

No.	Delivery item	Description	Type	Delivery method
2	LuxTrust Crypto Box SAM AGD_PRE, LuxTrust S.A, Version 0.4.0	Preparatory LuxTrust Crypto-Box SAM 2.0.0.1 guidance	PDF	Included in release package (see above)
3	LuxTrust Crypto Box SAM AGD_OPE, LuxTrust S.A, Version 0.3.9	Operational LuxTrust Crypto-Box SAM 2.0.0.1 guidance	PDF	Included in release package (see above)
4	LuxTrust Crypto Box JCA provider	Java JCA Provider enabling Java client applications to access Crypto-Box	JAR with accompanying JavaDoc HTML documentation	Included in release package (supporting software; not part of the certified product)
5	LuxTrust CBADM tool	Command line utility for administering LuxTrust Crypto-Box SAM	Executable JAR with accompanying JavaDoc HTML documentation	Included in release package (supporting software complementarily to the CP5 csadm and cxitool utilities; not part of the certified product)

Note: Hardware and Software components of the CryptoServer CP5, with the main components of the certified CryptoServer CP5 being stated in the certification report issued by the certification body (cf. [CR_CP5]; Chapter 2.1), are not part of the Crypto Box delivery. Moreover, those latter components must be procured separately from Utimaco as pre-requisite for using LuxTrust Crypto-Box SAM 2.0.0.1.

1.4 Identification and initialisation by the User

Besides the present documentation, the validation process is additionally described either in the letter accompanying the LuxTrust Crypto-Box SAM 2.0.0.1 media device or in the electronic message that references the LuxTrust Crypto-Box SAM 2.0.0.1 release bundle download URI, so that the relying party is informed regarding security provisions for acceptance.

The person responsible for the acceptance check validates the signature on the outer ZIP file by using a trustworthy ASiC-E validation tool or service that employs the European Trusted Lists as the set of eligible trust anchors. The validation must pass

successfully and it must uniquely identify LuxTrust Release Management as the signer.

The `cisa.mtc` file containing the LuxTrust Crypto-Box SAM 2.0.0.1 binary is code-signed with the UTIMACO MSK. However, validity of the code signature is checked and enforced automatically when loading the LuxTrust Crypto-Box SAM 2.0.0.1 into a CP5 HSM. The person responsible for the acceptance check does not need to validate the LuxTrust Crypto-Box SAM 2.0.0.1 code signature.

The process checking the authenticity and integrity of the CP5 HSM merely consists of checking the physical integrity of the packing seals and labels on the security bag that wraps the supplied device.

The preparative guidance [AGD_PRE] covers initializing the LuxTrust Crypto-Box SAM 2.0.0.1, including the following steps:

- Preparation
- Initial Device Settings Including IP Address
- Connecting HSM to The Setup Host
- Creating HSM Authentication Keys
- Creating User Administrators
- Creation of System Administrators
- Deletion of Default Administrator
- Creation of Master Backup Key
- Import of Master Backup Key
- Loading of the LuxTrust Crypto-Box SAM 2.0.0.1

After a restart of the HSM, the version number of the LuxTrust Crypto-Box SAM 2.0.0.1 can be checked to match with the version number indicated in the message that accompanies the delivery package.

For this purpose, the subsequent command can be used. The LuxTrust Crypto-Box SAM 2.0.0.1 firmware module has the name CISA and the hexadecimal module identifier 11A.

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  1.4.6.0        INIT_OK
 1a0 CXIAL         SDK  1.0.0.1        INIT_OK
```

The identification of the CryptoServer CP5 is described in certification report [CR_CP5], section 2.1.

1.5 Manufacturer and Applicant

Manufacturer of CryptoServer CP5 is Utimaco IS GmbH, Germanusstraße 4, D-52080 Aachen, Germany.

Manufacturer of LuxTrust Crypto-Box SAM 2.0.0.1 as well as developer, sponsor or applicant of the product is LuxTrust S.A., IVY Building 13-15, Parc d’activités, L-8308 Capellen, Luxembourg.

2. Functional description

2.1 Functionality and architecture

2.1.1 General Framework

A Trust Service Provider establishes an eIDAS compliant service that offers remote electronic signatures and seals. The service ensures that the signer's signing key is only used under the sole control of the signer for the intended purpose. A Signature Activation Module (SAM) is provided to ensure this control. For this, the product **LuxTrust Crypto Box device V2** is used as a Qualified Signature/Seal Creation Device (QSCD). The Signature Activation Module is realised by the firmware module LuxTrust Crypto-Box SAM 2.0.0.1 that resides inside the Hardware Security Module, the CryptoServer CP5.

The system providing the service for electronic signatures and seals consists of a local and a remote environment. The signer is in the local environment, the LuxTrust Crypto-Box SAM 2.0.0.1 is part of the remote environment. The signer interacts using a device (e.g. laptop, tablet or smart phone) with the Server Signing Application (SSA) in the remote environment which calls the external functions provided by LuxTrust Crypto-Box SAM 2.0.0.1.

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)). One of the three SAD elements is the signer authentication. The signer authentication is assumed to be conducted according to EN 419 241-1, SCAL.2 for qualified signatures. The other two elements are the assignment of the authenticated signer to the associated private key and the data to be signed. For the LuxTrust Crypto-Box SAM 2.0.0.1 SAD is represented in form of an authentication assertion. This assertion binds the successful authentication of the key holder cryptographically to the associated private key as well as to the Data to be Signed (DTBS).

To ensure the signer has sole control of his signing key, the signature operation needs to be authorised. This is carried out by LuxTrust Crypto-Box SAM 2.0.0.1, which can handle one endpoint of SAP, verify SAD and activate the signing key within a cryptographic module. This cryptographic module is the Utimaco CryptoServer Se-Series Gen2 CP5. The CryptoServer is used for key generation and for creating the digital signature values. LuxTrust Crypto-Box SAM 2.0.0.1 is a software component integrated into the CryptoServer.

The CryptoServer together with LuxTrust Crypto-Box SAM 2.0.0.1 forms the Qualified Signature/Seal Creation Device (QSCD). Within the QSCD, all external interfaces are provided by the LuxTrust Crypto-Box SAM 2.0.0.1. Only for administrative processes the QSCD provides an additional external interface provided by the CryptoServer CP5.

In order to support the service for the generation of remote electronic signatures a QSCD provides two eIDAS functions:

- eIDAS Key Generation
- Signature/Sealing

2.1.2 Overall Architecture

The LuxTrust Crypto-Box SAM 2.0.0.1 in conjunction with the CryptoServer CP5 version 5.1 represents the Qualified Signature Creation Device (QSCD) required for eIDAS compliant qualified server signing. The LuxTrust Crypto-Box SAM 2.0.0.1 adds various security functions to the built-in CP5 features. It is composed of a single sub-system, which is supposed to be installed and operated on the CryptoServer CP5. The subsystem is the LuxTrust Crypto-Box SAM 2.0.0.1, a CP5 firmware module that extends the CP5 standard firmware modules.

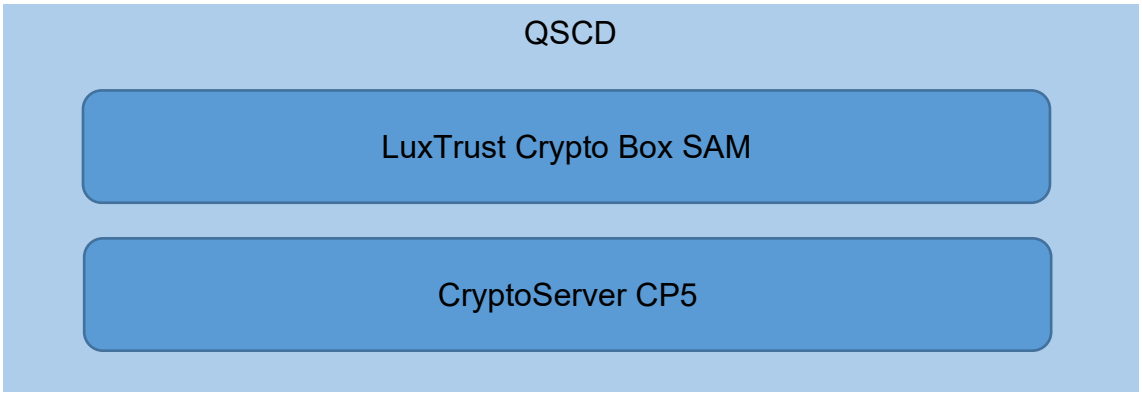

Figure 1: QSCD

The user (signer) interacts with the Server Signing Application (SSA) using a Signer interaction component (SIC) on a device (e.g. laptop, tablet or smart phone). The SSA calls the external functions provided by the subsystem LuxTrust Crypto-Box SAM 2.0.0.1. The LuxTrust Crypto-Box SAM 2.0.0.1 ensures appropriate control of the seal and signature keys of a key holder (in particular, the sole control of the signature keys of the key holder). The LuxTrust Crypto-Box SAM 2.0.0.1 is called via an external interface that can be reached from outside the CryptoServer CP5 through the CP5 communication protocol stack (cf. [ST HW]).

The task of the LuxTrust Crypto-Box SAM 2.0.0.1 is the examination of the Signature Activation Data (SAD) as well as securing that the correct signature key is used. It uses the CryptoServer CP5 to generate the signing key and to create the digital signature value. Therefore, the LuxTrust Crypto-Box SAM 2.0.0.1 communicates with the CXI abstraction layer (CXIAL) (cf. [CP5 API CXIAL]) to invoke the functionalities for qualified signature and seal creation and the functionalities for generation of the required signing keys.

In order to ensure that the signer has sole control over her signing keys, authorisation is compelling for performing the signature operation. Therefore, the LuxTrust Crypto-Box SAM 2.0.0.1 handles one endpoint of SAP and activates the signing key within a cryptographic module only upon successful verification of the SAD. Both, the cryptographic module and the LuxTrust Crypto-Box SAM 2.0.0.1 are located within a tamper-protected environment of the CryptoServer CP5. SAD verification means that the LuxTrust Crypto-Box SAM 2.0.0.1 checks the binding between the three SAD elements and verifies the signer’s proper authentication. For this purpose, the LuxTrust Crypto-Box SAM 2.0.0.1 does not itself authenticate the signer but has to assume (based on the environment) that a part of or the complete authentication has taken place and relies on an assertion.

The signer is located in the local environment with a user device (laptop, tablet, smartphone). The user interface can display documents for the signer. The device

uses a signer interaction component (SIC) to communicate with the SSA. The SSA forwards the communication from the SIC or from the SSA to the QSCD. Inside the QSCD, the LuxTrust Crypto-Box SAM 2.0.0.1 receives the messages. When the LuxTrust Crypto-Box SAM 2.0.0.1 has verified SAD, it can authorize the activation of the signing key within the cryptographic module and produce a digital signature value. The LuxTrust Crypto-Box SAM 2.0.0.1 returns the value to the SSA that may further deliver it to the SIC.

The operation environment consists of various service components that act together as an electronic signature or seal creation service under sole control of a natural or under control of a legal person signatory. The signature or seal creation service consists of an SSA, an identity Provider (IDP) and the QSCD. Depending on the chosen parametrisation, the LuxTrust Crypto-Box SAM 2.0.0.1 can support varying operation modes:

- **MULTI-USE issuance and SINGLE-USE issuance**

  Upon successful signatory authentication, an IDP can provide a template for the signatory public key certificate (PKC) as part of the signature or seal creation request. In this scenario, the LuxTrust Crypto-Box SAM 2.0.0.1 performs signatory key pair generation during signature or seal activation and thereby delegates issuance of the signatory PKC to a certification authority (CA) that resides in the internal LuxTrust Crypto-Box SAM 2.0.0.1 database within the CP5 security boundaries. Depending on whether the instantly generated PKC is intended for use during the current and during subsequent signature creation or seal creation requests or only for use during the current request, the generated signatory private key is either encrypted and authenticated for being returned with the signature result or it is immediately destroyed upon usage. The former scenario is denoted MULTI-USE issuance, the latter one SINGLE-USE issuance.

- **FOREIGN issuance**

  Alternatively, upon successful authentication, an IDP can provide a signatory PKC together with the corresponding encrypted private key as part of the signature or seal creation request. In this scenario, the LuxTrust Crypto-Box SAM 2.0.0.1 applies the provided PKC and key for signing data on behalf of the signatory. The provided PKC may either have been issued by a LuxTrust Crypto-Box SAM 2.0.0.1 embedded CA as a side effect of the previously described MULTI-USE issuance scenario, or by an external CA. The latter alternative scenario is denoted FOREIGN issuance. It requires a preceding request, during which LuxTrust Crypto-Box SAM 2.0.0.1 generates a key pair and supplies a certificate signing request (CSR) along with the encrypted and authenticated signatory private key. An external CA uses the supplied CSR for issuing a PKC to the signatory.

As specified in [EN 419 241-1], section 5.12, the outlined service components are managed by a Trust Service Provider (TSP) except for the user environment. Signature or seal creation must specifically take place in a tamper-proof environment. Note that the SSA and IDP are technical service components, which both are part of the TSP-managed environment, form together the Server Signing Application logical component in the sense of [EN 419 241-1]. The specific decomposition into two separate technical service components was motivated for achieving suitable modularity with regard to the generic signature creation transaction sequence. Alternatively, SSA and IDP can also be embodied as a single service component.

The genuine role of the IDP service component is taking signer authentication into account, while this is either realised by the IDP directly or indirectly in further delegating signer authentication to an external Identity Provider (cf. [EN 419 241-1], section 5.7.4.1). Therefore, the IDP service component particularly knows the outcome of a signer authentication and consequently also represents the natural supplier of signer identity data and of corresponding stored signing keys in protected form (cf. [EN 419 241-1], section 5.12.2) for the SSA service component, which in turn integrates that data into the prepared signature creation request for forwarding it to the QSCD.

In particular, the TSP-managed IDP service component should not be confused with an external Identity Provider, to which it can delegate signer authentication.

2.1.3 Cryptographic Algorithms

The following cryptographic algorithms are supported by the „Crypto Box“ (cf. [ST LuxTrust-SAM], section 7.4.2):

- RSA key pair generation with specified cryptographic key sizes 2048 up to 8192 bits modulus according to [SOG-IS] section 4.1
- ECC key pair generation with specified cryptographic key of minimum 224 bits that meet the following: ECC key pair generation for ECC domain parameters Curve P-224, Curve P-256, Curve P-384 or Curve P-521 as specified in [FIPS 186-4] appendix 6, or brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1 or brainpoolP512t1 as specified in [ECCBP] chapter 10, or curve FRP256v1, secp224r1, secp256r1, secp384r1, secp521r1 as specified in [ANSSI]
- Calculation of hash values with hash functions SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512 according to [FIPS 180-4], chapter 6 for SHA-2, and [FIPS 202] for SHA-3
- Digital signature generation and verification with RSA signature scheme with appendix according to [PKCS#1], RSASSA-PSS or RSASSA-PKCS-v1_5 and cryptographic key sizes of minimum 2048 bits modulus length that meet the following: [PKCS#1], chapters 8.1.1 or 8.2.1 (signature generation) and chapters 8.1.2 and 8.2.2 (signature verification)
- Digital signature generation and verification with ECDSA and cryptographic key sizes minimum 224 bits that meet the following: signature generation according to [ANSI-X9.62] with signature keys based on ECC domain parameters Curve P-224, Curve P-256, Curve P-384 or Curve P-521 as specified in [FIPS 186-4], appendix D, or brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1 or brainpoolP512t1 as specified in [ECCBP], chapter 10, or curve FRP256v1; Curves used only for signature generation: secp224r1, secp256r1, secp384r1, secp521r1 as specified in [ANSSI]
- HMAC calculation with algorithm HMAC and cryptographic key sizes between 4 and 1024 bytes according to [FIPS 198-1]
- Generation of random numbers with a hybrid deterministic random number generator that implements RNG class DRG.4 of [AIS 20/31], chapter 4.9

2.1.4 User Authentication and Authorisation

The LuxTrust Crypto Box device V2 provides several functions for service operations, i.e. functions GET, POST and PUT as well as a SETUP function used to modify configuration items that are permanently stored in the local trust store. However, calling an exposed function requires proper authentication and suitable permissions of the calling user. Authentication is entirely taken into account by the CryptoServer CP5, while this is enforced by the LuxTrust Crypto-Box SAM 2.0.0.1 by calling at each entry point of its TSFI (Security Functions Interfaces) functions the check_permission function that is exposed by a module of CryptoServer CP5. A check_permission call ensures that the user, who has invoked a LuxTrust Crypto-Box SAM 2.0.0.1 function, is properly authenticated by the CryptoServer CP5 and is member of the user group specified in the corresponding check_permission call and owns in that group the minimum permission level specified by the LuxTrust Crypto-Box SAM 2.0.0.1 as a pre-requisite for the invoked TSFI function.

The executing of some essential variants of the SETUP function requires dual control. For this, check_permission calls specify minimum permissions that cannot be satisfied by a single user alone, which means that the corresponding function can only be executed if several users jointly perform the call and achieve the required minimum permission level by adding there individually owned permission levels. This enforces dual control.

Users are equipped with suitable authentication means and with user accounts that have appropriate associated user groups and permissions assigned by authorised User Administrators of the CryptoServer CP5. The latter ones are equipped with suitable authentication means and administrative permissions during the setup process in using predefined User Administrator accounts. Predefined accounts are immediately destroyed after bootstrapping of new dedicated User Administrators.

Service requests (GET, POST or PUT) must be signed by the user with a private key that is assigned to the user and a correspondent service component certificate is available that has suitable extended key usages for the intended function call. The certificate has been imported into the local trust store of the LuxTrust Crypto-Box SAM 2.0.0.1 during the setup phase by means of the SETUP function. This mechanism ensures that a caller of a TSFI function owns a service role that is appropriate for carrying out the given call, namely acting as SSA, as IDP or as QSCD or as a service resource-managing component (SRM). In addition, this mechanism ensures authenticity and integrity of request and response messages during the operation.

Service roles may further be restricted by optionally specifying suitable certificate policies in service component certificates, while this is interpreted and enforced by the LuxTrust Crypto-Box SAM 2.0.0.1 when handling a TSFI function call. This design provides fine-grained access control regarding capabilities of service components and enables restrictions regarding use of cryptographic mechanisms, use of different certificate issuance modes, use of different signing modes and restriction of resources.

When importing service component certificates in the local trust store of the LuxTrust Crypto-Box SAM 2.0.0.1 during setup, all path validation checks that can be performed at that point in time are anticipated and role and policy information is parsed and redundantly stored for accelerating call handling during service operations.

The concept of using service component certificates for authenticating individual requests and responses of the communication protocol enables multi-tenancy by

segregating policies for disjoint sets of service components. This is achieved by the LuxTrust Crypto-Box SAM 2.0.0.1 only permitting communication between service components that are issued by the same CA. Each such isolated group of service components can be regarded a logical tenant of the LuxTrust Crypto-Box SAM 2.0.0.1 with its own set of certificate policies that is also called a Crypto Box domain. A Crypto Box domain can be represented by the CA that issues the service component certificates for the participants of that domain with their individual service roles.

For additionally ensuring segregation of management roles for different Crypto Box domains, another concept has been added. It consists in binding each Crypto Box domain to a so-called domain authorization key (DAK) during setup and by the LuxTrust Crypto-Box SAM 2.0.0.1 requiring that service managers for a given Crypto Box domain must prove possession of the corresponding DAK to obtain access for changing the configuration of a domain.

A DAK to domain binding is realised by calculating and maintaining a HMAC over the public part of the given DAK and each encrypted private key blob of the to be bound Crypto Box domain. The LuxTrust Crypto-Box SAM 2.0.0.1 holds exactly two private keys for each domain, namely the one, which pertains to the CA certificate of the domain, and the one, which pertains to the QSCD certificate of the domain. A DAK to domain binding is established when service managers trigger issuance of a CA or an QSCD certificate for a Crypto Box domain.

The secret key that is used for calculating a DAK to domain binding HMAC is derived from the CryptoServer CP5 Master Backup Key (MBK), which enables uniform message authentication of domain bindings across all devices of an HSM cluster without the need to deploy an extra secret.

Proof of possession of a given DAK is achieved by service managers having to sign SETUP function calls for changing domain configurations with the corresponding DAK.

2.1.5 Service Component Certificates

Each service component that access the QSCD must own a suitable component certificate and use the corresponding private key for signing requests, so that service-specific authorisations can be verified. A given component certificate may grant several roles for an actor. Roles are encoded as extended key usages (cf. [RFC 5280], section 4.2.1.12 and [ITU-T X.509], section 8.2.2.4). Service component constraints are encoded as certificate policies (cf. [RFC 5280], section 4.2.1.4 and of [ITU-T X.509], section 8.2.2.6) in service component certificates. Service roles have no default value and authorisations always have defaults that can be overwritten.

Service roles are identified by defined object identifiers that must be included in the extended key usage extension field of the certificate. Multiple extended key usages can be specified in a single service component certificate, except for the QSCD role that must not be combined with another role. Additionally, for each domain only one single certificate with QSCD role can be imported into the LuxTrust Crypto-Box SAM 2.0.0.1 trust store. Object identifiers are defined for the service roles QSCD, IDP, SSA and SRM.

Object identifiers are also used as a policy identifier for defining service component constraints for overwriting constraint defaults when issuing service component certificates. Constraints are only applicable to a service role when this is assigned to the role in question. A constraint must always have one or more appropriate policy

qualifiers. This means that the role is relevant for the respective authorisation. For example, based on the request syntax an IDP cannot determine a signing mode. In this respect, the restriction of a signing mode makes no sense for an IDP and is therefore not applicable to this role. Algorithm restrictions, on the other hand, are applicable to all service roles; the LuxTrust Crypto-Box SAM 2.0.0.1 ignores restrictions that make no sense for a role.

The following constraints are defined:

Table 2: Constraints

Constraints	Applicable to	Default Value
Cryptographic Suite	Any Role	Any supported algorithm
Issuance Mode	IDP, SCD	FOREIGN issuance
Signing Mode	SSA, SCD	HASHED DATA signing
Transaction Freshness	SSA, SCD	≤ 600 seconds deviation
Signing Load	SSA, SCD	≤ 250 tasks per request
Generation Load	SRM, SCD	≤ 1 Generation per Request
Caching Load	SRM, SCD	≤ 1024 key pairs per key type

- **Policy Qualifier for Constraining Cryptographic Suite**

  An individual policy qualifier has to be specified for each authorised key pair generation mechanism, while the corresponding policy qualifier is either RsaEncryption (OID 1.2.840.113549.1.1.1) or EcPublicKey (OID 1.2.840.10045.2.1). The corresponding parameter pertaining to a specified policy qualifier is of *RsaGrants* type in the former case and of *EcGrants* type in the latter case (cf. [RFC 5280], section 4.2.1.4).

- **Policy Qualifier for Constraining Issuance Mode**

  The constraint specifies eligible certificate issuance modes. Rules for signatory certificate issuance are enforced during POST and GET requests. When the present constraint is omitted, the defined default value becomes effective. For defining an issuance policy, a policy qualifier has to be specified for each authorised issuance mode, with eligible qualifications being defined by an object identifier. Multiple qualifiers can be specified for the present policy.

- **Policy Qualifier for Constraining Signing Mode**

  The constraint specifies eligible signing modes for signature or seal tasks. When the present constraint is omitted, the defined default value becomes effective. For defining a signing policy, a policy qualifier has to be specified for each authorised signing mode, with eligible qualifications being defined by an object identifier. Multiple qualifiers can be specified for the present policy.

- **Policy Qualifier for Constraining Transaction Freshness**

  The constraint specifies the maximum deviation, which is defined as the magnitude of the time difference in seconds between the transaction start time indicated in a POST request and the time indicated by the QSCD device clock when the request is received. The time difference comprises the corresponding IDP round trip for authorising the request. The maximum value is specified using a single perimeter grant qualifier using an object identifier and a non-negative maximum 32 bits INTEGER parameter. When the present constraint is omitted, the defined default value becomes effective.

- **Policy Qualifier for Constraining Signing Load**

  This constraint specifies the maximum number of authorised signature creation tasks per request using a perimeter grant qualifier. The present policy must not specify a signing load greater than 250. When the present constraint is omitted, the defined default listed value becomes effective.

- **Policy Qualifier for Constraining Key Generation Load**

  The present constraint specifies the maximum number of key pairs that can be generated and stored in the persistent cache per PUT request using a perimeter grant qualifier. The parameter value can be set to zero for solely authorising querying the number of cached key pairs for the specified key generation parameters. When the present constraint is omitted, the defined default value becomes effective.

- **Policy Qualifier for Constraining Caching Load**

  The constraint specifies maximum number of key pairs that can be cached in the key store for a given key specification using a perimeter grant qualifier. When the present constraint is omitted, the defined default value becomes effective.

2.1.6 Persistant Data

The LuxTrust Crypto-Box SAM 2.0.0.1 contains two distinct databases that are stored persistently:

- **Trust Store**

  The trust store contains configuration items of the specified Crypto Box domains. It comprises for each domain the following: The service component certificates that the domain CA issues directly, the domain CA certificate itself with its encrypted private key, and, when already available, the associated singleton QSCD certificate with its encrypted private key. Stored CA and SCD certificates must be bound to a domain authorization key (cf. section 4.2). The LuxTrust Crypto-Box SAM 2.0.0.1 ensures uniqueness of a domain CA certificate implicitly by means of the data structure. By contrast, it ensures uniqueness of an SCD certificate per domain explicitly during certificate import.

  The LuxTrust Crypto-Box SAM 2.0.0.1 exclusively uses the trust store database for verifying requests. This comprises checks of certificate validity, revocation status, roles and authorizations, as well as identification of the appropriate tenant. It uses the trust store also to sign responses with the QSCD private key. The private key corresponding to a CA domain certificate is used for certifying service component certificates and other artefacts during SETUP,

and for issuing multi-use or single-use signatory certificates during a POST transaction.

An entry of the trust store contains a certificate and optionally an encrypted private key in a structure with complementary information been added during the import. A trust entry can directly be looked up using the subject key identifier and the authority key identifier of the stored certificate, with both identifiers being mandatory for service component certificate.

- **Key Store**

  The key store contains cached key pairs that have not yet been associated with any certificate and that have been prefabricated using the PUT method. The stored key pairs have never ever left the Crypto Box device V2. Stored key pairs can consequently be regarded as freshly generated key pairs when required by the GET method or when required for issuing a certificate during a POST method call, or when calling the createItem variant of the SETUP method. LuxTrust Crypto-Box SAM 2.0.0.1 automatically generates a key pair when needed and when not being available in the cache.

  Prefabricated key pairs are generic artefacts that do not need to be bound to a domain. Moreover, domains can intentionally share such key pairs for maximizing effectiveness of the caching functionality.

The LuxTrust Crypto-Box SAM 2.0.0.1 creates its databases automatically when not yet existing during module start up or when being erased because of using a specific variant of the SETUP function. It drops databases implicitly when the CP5 operating system calls a specific method for ensuring resource clean up upon module removal.

2.1.7 Functions

The LuxTrust Crypto-Box SAM 2.0.0.1 offers four TSFI functions, the service functions named POST, GET and PUT, and the SETUP function with several variants for configuration tasks.

- **POST**

  The function POST *signs (batches of) data* on behalf of an identified remote signer under their sole control over the signing key and with optional issuance of signing key and certificate.

- **GET**

  The function GET *creates certificate signing requests (CSR) and corresponding key pairs* wrapped in key blobs for enabling an external CA to issue signing certificates.

- **PUT**

  The function PUT is an optional method that prefabricates virgin key pairs during idle times and keeps them in the internal key store for later use.

- **SETUP**

  The function SETUP configures LuxTrust Crypto-Box SAM 2.0.0.1 by issuing service component certificates and importing them into the internal trust store alongside with issuing CA certificates and optionally keys.

Method POST

The method POST performs creation of one or more signatures or seals (up to 250) on behalf of a remote signatory and under their sole control by using their private key and a corresponding public key certificate (PKC). The latter is either directly supplied as a parameter or created during the process using a supplied PKC template and signer identity. The actual choice made by the IDP regarding the representation of the signatory identity data is represented by a corresponding data structure in the signer authentication response syntax.

For preparing a call, SSA sends a signed signatory authentication (*SignedAuthRequest*) request to IDP. It subsequently validates the signed IDP response (*SignedAuthResponse*) and uses it to prepare a signed request addressed to QSCD. Upon reception of the response, the signature of the device (QSCD) is validated by SSA prior to process the content. For the authentication request SSA generates a unique signing transaction identifier and an optional challenge data that may contain a binding to the data to be signed (DTBS). SSA sends a Signer authentication request comprising the signing transaction identifier to the IDP in order to obtain an assertion that contains and confirms the identity of the Signer. The signed IDP response especially contains *IdentityData*, *TBSCertificateTemplate*, *KeySpecification* (RSA key or ECDSA key), and IDP signature with algorithm, value and key identifiers.

After verification of the signed IDP response SSA uses the IDP assertion confirming the signer identity and linked to the transaction challenge created by the SSA in order to assemble signature request (*SignedPostRequest*) sent to the QSCD. The response of the QSCD is the *SignedPostResponse*. The signed request contains the complete *SignedAuthResponse* as an evidence for the authenticated signer identity (*signerIdentity*). The *SignedPostResponse* contains the resulting signatures as well as a signature created by the QSCD for message authentication. The present SAM version also supports an alternative POST request syntax with a light-weight signature envelope in the case that an SSA does not delegate user authentication to an IDP subsystem [AGD_OPE].

The user must have a successfully passed CP5 authentication and belong to a specific user group with appropriate permission level. The *SignedPostRequest* must be signed, with the signer having the SSA role. The *SignedAuthRequest* must be signed by the same signer. The *SignedAuthResponse* must be signed, with the signer having the IDP role.

Method GET

The method GET creates a CSR by employing a fresh key pair. This method has to be called by an IDP in order to issue a signatory certificate via an external CA. It requires grant of foreign issuance permission. The *SignedGetRequest* is answered by the QSCD with *SignedGetResponse*.

The user must have a successfully passed CP5 authentication and belong to a specific user group with an appropriate permission level. The *SignedGetRequest* must be signed, with the signer having the IDP role. The *SignedGetResponse* contains the CSR, the wrapped encrypted and authenticated fresh private key matching CSR, and the signature of the device (QSCD) for message authentication.

Method PUT

The method PUT is optional in the sense that it is not needed from a purely functional point of view. It serves for prefabrication of key pairs during idle times for storing them as backup blobs in the internal key store that is used as a persistent cache in order accelerate key pair provisioning during subsequent POST or GET requests. Consequently, the present method serves for resource management with no semantic effect regarding signature creation or certificate issuance. The *SignedPutRequest* is answered by the QSCD with *SignedPutResponse*.

The user must have a successfully passed CP5 authentication and belong to a specific user group with an appropriate permission level. The *SignedPutRequest* must be signed, with the signer having SRM role. The message contains the key algorithm specification for to be pre-fabricated key pairs (*keySpec*) and the number of key pairs to be added (must be >= 0 with default value 1). The *SignedPutResponse* contains the total number of cached key pairs corresponding to *keySpec*, and the signature of the device (QSCD) for message authentication.

Method SETUP

The method SETUP is used for performing administrative tasks, which in contrast to the preceding methods are not automated and executed by authorised persons during a device setup ceremony. The purpose of the method is the administration of the domains. For each domain, a CA has to be issued and installed in the trust store of each HSM cluster member together with the required service component certificates signed by that CA and containing the required role and optional policy information. Otherwise, the signature or seal service for that domain is not operable.

Variants of the method that change a domain configuration in the trust store require that an authorised administrator additionally prove possession of the corresponding domain authorisation key (DAK). A proof of possession is performed by the key owner digitally signing a request with subsequent verification of that signature by the QSCD. This approach enables secure segregation of domain management rights. For this purpose, a binding between a fresh DAK and cryptographic keys pertaining to a domain, namely the domain CA and QSCD keys, is established when creating the corresponding cryptographic key pairs. The binding is achieved by calculating a secure message authentication code over the octets of the concerned key blobs followed by the octets of the public part of the DAK upon successful DAK ownership proof.

The same calculation is performed for verifying the binding between a cryptographic key and the presented DAK when a resource of the corresponding domain is managed, while this activity implicitly comprises access to cryptographic keys of that domain.

This calculation can be achieved for all members of a CryptoServer CP5 cluster without the need of specific secret sharing by deriving the message authentication key from the 256 bit AES master backup key residing in CryptoServer CP5. The master backup key is already shared between all members when setting up an HSM cluster.

Additionally, setup operations, which could create an impact when replayed, have to be called with a random challenge that must previously be requested using the subsequent challenge item SETUP variant. This approach effectively guarantees

replay prevention during configuration, while this is crucial for setup actions that could change the trust store configuration by reconstruction of a previous state.

The Method SETUP consists of the *SetupRequest* that is answered by the QSCD with *SetupResponse*.

The user must have a successfully passed CP5 authentication and belong to a specific user group with an appropriate permission level. Some SETUP variants require a specific permission level in order to ensure dual control. Calls for managing configuration items pertaining to a given domain must additionally be signed with the corresponding domain authorization key.

2.2 Security functions and security properties of the „Crypto Box“

Access Control

In order to employ exposed TSFI functions of the LuxTrust Crypto-Box SAM 2.0.0.1, a caller must be an authorised user of the CryptoServer CP5, possess suitable authentications means and be a member of an appropriate user group with an appropriate permission level. Such properties must be configured by a user administrator of the CryptoServer CP5 in the CXI database of the underlying HSM to equip a user with a specified security role for enabling them to execute LuxTrust Crypto-Box SAM 2.0.0.1 functions mapped to the given role. For this purpose, the LuxTrust Crypto-Box SAM 2.0.0.1 requires dedicated user groups, which are not reserved for standard CP5 functionality. This enables the LuxTrust Crypto-Box SAM 2.0.0.1 to segregate its user groups from the ones employed by CP5.

Additionally, a caller must have complementary service roles and authorisations, which are suitable for performing the intended request types as part of a signature or seal creation service via exposed LuxTrust Crypto-Box SAM 2.0.0.1 functions. Such properties must be issued by a LuxTrust Crypto-Box SAM 2.0.0.1 service manager as specific extensions of service component certificates. Component certificates are end entity certificates signed by the corresponding domain CA certificate. Granted service component roles are represented as extended key usages. Additional constraints for granted service components are encoded as certificate policies. This complementary certificate-based authorisation layer is not yet available during LuxTrust Crypto-Box SAM 2.0.0.1 setup and is therefore not applied when calling the SETUP method.

In summary, LuxTrust Crypto-Box SAM 2.0.0.1 access control consists in a stack of several complementary layers of control that require

- secure messaging between the device and a service component enforced by the CP5,
- suitable (multi-factor) user authentication enforced by CP5,
- suitable user group and permission level enforced by CP5 as requested by LuxTrust Crypto-Box SAM 2.0.0.1,
- suitable service component role and policy grants for method calls enforced by LuxTrust Crypto-Box SAM 2.0.0.1.

In order to segregate management of LuxTrust Crypto-Box SAM 2.0.0.1 users from other CP5 users, the LuxTrust Crypto-Box SAM 2.0.0.1 defines three new user groups in addition to the existing standard user groups by using unused CP5 user groups. The required user groups for calling exposed LuxTrust Crypto-Box SAM 2.0.0.1 functions are Service-User, Service-Manager and Device-Manager. In all cases, the

permission level 2 is needed, except for the request variants of the SETUP method, which require dual control and therefore augmented permission level 4. Additionally, execution of variant *ensureNoItem* requires a different role than other SETUP variants due to its global effect.

Table 1: User Group Mappings

Method	Variant	Required Group	Required Permission
POST	-	Service User	2
GET	-	Service User	2
PUT	-	Service User	2
SETUP	ensureNoItem	Device Manager	4
	rebindItem	Service Manager	4
	importItem	Service Manager	4
	Any other variant	Service Manager	2

Dual control for the above-cited three request types (with permission level 4) is motivated by the fact that execution of each of them can create a major trust change for the LuxTrust Crypto-Box SAM 2.0.0.1, thus requiring specific attention.

Each calling client component goes through the CP5 authentication, then through the CP5 role and permission check, with the LuxTrust Crypto-Box SAM 2.0.0.1 enforcing required roles and permission levels via corresponding calls at the beginning of each request processing. The LuxTrust Crypto-Box SAM 2.0.0.1 explicitly requests the calling client to belong to the required CP5 user group with sufficient permission level, while the corresponding check thereof is delegated to the underlying CryptoServer CP5.

User Authentication

The design and implemented security functions for user authentication are mainly based on user roles, their permissions and the use of asymmetric key pairs that are assigned to users by service components certificates. These aspects were described in detail in sections 3.1.4 to 3.1.7.

For registration within CryptoServer CP5, for every user a dedicated authentication mechanism has to be chosen. The CryptoServer CP5 provides two different user authentication mechanisms (cf. [ST HW]):

RSA Signature authentication mechanism: The authentication is performed with an RSA signature (RSA signature scheme RSASSA-PKCS1-v1_5 according to the standard [PKCS#1], chapter 8.2.1, with key lengths of minimum 2048 and maximum 8192 bits modulus lengths).

HMAC Password authentication mechanism: For this mechanism a password is used. First the host running the application software demands a 128 bit random value (challenge) from the CryptoServer CP5. Then the host calculates the HMAC value over this challenge and the command data block using the user's authentication password as the HMAC key.

Furthermore, for Internal SAM the following authentication mechanism is provided:

Module Signature authentication mechanism: The authentication is performed with the help of an RSA signature (PKCS#1 signature according to the standard [PKCS#1]), which has to be calculated over the firmware module with the dedicated CryptoServer CP5 Module Signature Key owned by the manufacturer.

After five unsuccessful user authentication attempts the corresponding user is blocked. Any additional attempt of this user to authenticate towards the CryptoServer CP5 will fail. A blocked user can only be unblocked by a User Administrator.

For exchanging sensitive data, a Secure Messaging session (trusted channel) can be set up between the CryptoServer CP5 and the (local non-internal or remote external) client application. Such a Secure Messaging session is mandatory for each command which requires user authentication. Here, although they may run in different environments, for local non-internal client applications and remote external client applications the identically same trusted communication mechanism is enforced by security functions.

CryptoServer CP5 supports the user authentication and secure messaging with RSA signature generation and verification, hash value calculation, key derivation, HMAC calculation, Diffie-Hellman key agreement, AES encryption, AES decryption, MAC-calculation and random number generation by hybrid RNG for the challenge value.

Key Authorisation

The SAM Authorised External Key (SAEK) signature interface allows an Internal SAM application to request usage of a signature key for which the CryptoServer will not check the key authorisation. As a consequence, the internal SAM calling the SAEK signature interface takes full responsibility on correct legitimation of this operation, including key authorisation as required by [EN 419 221-5]: As mandated by CryptoServer CP5 Guidance, an Internal SAM will only invoke the SAEK signature interface if it has completely validated key authorisation of the signature key before. Therefore, the CryptoServer CP5 can implicitly derive prior successful key authorisation of the signature key from each invocation of the SAEK signature interface.

Physical Access Control and Audit Logs

The LuxTrust Crypto-Box SAM 2.0.0.1 is a firmware module which implements the Signature Activation Protocol (SAP). It runs within the same physical boundary as the CryptoServer CP5 and therefore relies on the same physical security mechanisms for tamper detection and response as the CryptoServer CP5. Moreover in this case the creation of a trusted channel for the connection to the firmware modules of the CryptoServer CP5 is not necessary.

The LuxTrust Crypto-Box SAM 2.0.0.1 and the CryptoServer CP5 in combination or the CryptoServer CP5 on its own are able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions
- All auditable events for the not specified level of audit;
- Privileged User management;
- Privileged User authentication;
- Signer management;
- Signer authentication;
- Signing key generation;
- Signing key destruction;
- Signing key activation and usage, and
- Change of configuration.

Within each audit record at least the following information is contained:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.

For audit events resulting from actions of identified users, LuxTrust Crypto-Box SAM 2.0.0.1 is able to associate each auditable event with the identity of the user that caused the event.

The CryptoServer CP5 monitors the following events:

- Self-test error,
- Stored data integrity failure,
- Failure of user authentication or of key authorisation attempts and
- Results of the services performing Administration, Key Management and Software Updates of the CryptoServer.

Moreover it provides the corresponding audit records and a service to query the audit records. This service has to be authenticated by a user in Administrator, User Administrator, Key Manager or Security Officer role. The CryptoServer CP5 does not provide any possibility to modify the audit records except for entire clearance, whereby the service for the clearance of the audit data has to be authenticated by a user in Administrator or User Administrator role.

The CryptoServer CP5 preserves a secure operation state when the following types of failures and attacks occur:

- Power supply too high/too low,
- Temperature too high/too low,
- Integrity check of cryptographic keys and stored firmware modules, and
- Self-test fails.

The CryptoServer provides an alarm mechanism which detects physical environmental failure attacks and reacts by destroying all sensitive data. For this mechanism a sensory is implemented which watches temperature and voltage.

Furthermore, the CryptoServer CP5 with its tamper-evident enclosure (the heat sink and the potting material) implements the following physical security mechanisms against direct physical attacks:

- The hardware components of the CryptoServer are covered by hard, opaque potting material or the heat sink, which show evidence of tampering on the enclosure when a physical attack is attempted.
- The potting material is hard and opaque enough to prevent direct observation and easy penetration to the depth of the underlying hardware components. It is highly probable that anyone attempting to penetrate to the depth of the circuitry will break off large pieces of potting material and tear important hardware components off the module, causing serious damage to the CryptoServer CP5.

The tamper response and zeroisation circuitry is active while the module is in standby mode (powered down).

The implemented sensory and software parts of the CryptoServer CP5 react properly to all security relevant events being generated by the hardware in response to any physical attack attempts. The resistance of the hardware and sensory of the CryptoServer CP5 to physical and chemical attacks has been evaluated and successfully certified according to the requirements for level 3 of [FIPS 140-2]. This is equivalent to the physical security requirements as laid down for Security Level 3 in [ISO/IEC 19790], chapters 7.7.2 (Physical security general requirements) and 7.7.3 (Physical security requirements for each physical security embodiment). Therefore, the CryptoServer CP5 supplies effective hardware and software based mechanisms satisfying resistance to physical attack.

Due to the implemented alarm mechanism the CryptoServer CP5 preserves a secure state also if the power supply or temperature is outside of a well-defined operational range: If extreme power levels occur to the CryptoServer CP5 or if extreme temperature is monitored, an alarm is triggered, all data is deleted and the CryptoServer CP5 will be reset cleanly. The CryptoServer CP5 realises effective hardware and software based features to preserve a secure operational state in case of induced hardware or software failures or tampering.

For the protection of data and firmware integrity the CryptoServer implements various measures:

During the boot process after power-on or reset the boot loader of the CryptoServer CP5 and operating system SMOS performs further self-tests, like a memory RAM test. SMOS loads and initialises all remaining firmware modules and performs further self-tests.

It is only possible to execute any cryptographic or other security-relevant service after these power-on self-tests have been completed successfully. If one of these power-on self-tests fails, the CryptoServer CP5 enters the secure Error State.

The CryptoServer CP5 performs the following self-tests at specific conditions:

- Online Test of the digitised noise data of the PTRNG,
- Continuous DRNG tests (whenever random bytes are requested),
- ECDSA Key Pair-wise Consistency Test (sign/verify) for any newly generated or imported ECDSA key pair according to [FIPS 140-2], chapter 4.9.2,
- RSA Key Pair-wise Consistency Tests (encrypt/decrypt and sign/verify) for any newly generated RSA key pair according to [FIPS 140-2], chapter 4.9.2 and
- Firmware Load Test (via RSA signature verification) for every firmware module when being loaded.

If one of these conditional self-tests fails, the requested action is not performed (e.g. firmware module to be loaded is not loaded, generated key is not stored etc.), and the command is aborted with an error code. The successful completion of all self-tests or the secure Error State is indicated by the "Get State" command.

A secret or private key is deleted by overwriting it with zeros. This mechanism ensures that any previous information content is not available after deletion.

The CryptoServer monitors stored data, prohibits usage of altered data and notifies the user if integrity errors are detected.

Software Updates

The CryptoServer CP5 supports a secure software update by providing the "Load File" service. If the file is a firmware module (*.mtc), like the LuxTrust Crypto-Box SAM 2.0.0.1, the signature of the firmware module is checked. If it cannot be successfully verified, the loading of the module is rejected.

This service has to be authenticated by a user with the Administrator role.

The "Load File" service allows the download of firmware modules only in a dedicated format which contains also a signature calculated over the executable code (RSA signature according to [PKCS#1], with a key length of 4096 bits). The signature has to be calculated with a dedicated Module Signature Key owned by the manufacturer. If the signature cannot be verified, the download is prohibited and the "Load File" service will return an error code instead. If the set of loaded firmware modules is incomplete or in any way not compliant to the software that is released for this project, the CryptoServer CP5 will be set to a secure Error State.

In this Error State no cryptographic operations are available, only status requests can be performed.

Self Protection

The following security mechanisms prevent the manipulation of the security functions by a non-trusted, active external entity.

To ensure the integrity of the LuxTrust Crypto-Box SAM 2.0.0.1, it is signed with a code-signing key; the corresponding public key is available in every CryptoServer CP5 based on the HSM factory process. The CryptoServer CP5 verifies the signature

during the initialisation process. Long-living trust anchors are incorporated in the HSM memory that is protected against attacks (cf. [ST HW]).

The LuxTrust Crypto-Box SAM 2.0.0.1 runs inside the security boundaries of the CryptoServer CP5 as an ordinary firmware module. It therefore obtains the same comprehensive protection and resources like any built-in CP5 firmware module. This comprises protection against threats like tampering, physical attacks or side channel attacks, with those capabilities being stated for the CP5 due to its Common Criteria EAL4 augmented certification with AVA_VAN.5 based on [ST HW] according to [EN 419 221-5].

In addition, self-protection is supported by User Authentication, Message Authentication and Signatory Authentication.

Moreover, LuxTrust Crypto-Box SAM 2.0.0.1 also uses persistent databases via the CP5 DB module. Tampering with those data is prevented and access to persistent data by external entities is protected for similar reasons, namely due to LuxTrust Crypto-Box SAM 2.0.0.1 data using storage media residing inside the boundaries of the CP5 HSM and access paths that entirely rely on built-in firmware modules. No external access to the data is possible, unless it passes through exposed and authentication-protected TSFI functions and the checks implemented by the LuxTrust Crypto-Box SAM 2.0.0.1 when executing the invoked functions.

Cryptographic Algorithms

The CryptoServer CP5 provides cryptographic mechanisms and enables cryptographic services like signature generation and verification for the user of the CryptoServer.

It supports the following cryptographic operations:

- AES algorithm in CBC mode with a key length of 16, 24 or 32 bytes used for encryption or decryption ([NIST SP 800-38A], [FIPS 197]),
- AES algorithm in OFB mode with a key length of 16, 24 or 32 bytes used for encryption ([NIST SP 800-38A], [FIPS 197]),
- AES algorithm in ECB mode with a key length of 16, 24 or 32 bytes used for encryption or decryption (for internal use only, to support an internal SAM) ([NIST SP 800-38A], [FIPS 197]),
- AES algorithm in GCM mode with a key length of 16, 24 or 32 bytes used for authenticated encryption or decryption ([NIST SP 800-38A]),
- AES algorithm with a key length of 16, 24 or 32 bytes used for CMAC generation and verification ([NIST SP 800-38B]),
- ECDSA algorithm according to the standard [ANSI-X9.62] with key lengths of minimum 224 bits used for ECDSA signature generation or verification,
- RSA algorithm according to the standard [PKCS#1] with key lengths of minimum 2048 bits and maximum 8192 bits used for RSA encryption or decryption and RSA signature generation and verification,

- HMAC calculation in (HMAC key size shorter than 13 bytes for internal use only to support user authentication, key size 13 bytes and more also as cryptographic service),
- Hash algorithms SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384 and SHA3-512,
- Diffie-Hellmann key agreement (for internal use only to support the implementation of the trusted channel),
- Key Derivation (for internal use only to support the implementation of the trusted channel and the secure backup of keys) and
- Random number generation by a hybrid RNG.

Communication Protection

In order to communicate with the LuxTrust Crypto-Box SAM 2.0.0.1, a service component instance must successfully authenticate, possess suitable access permissions and employ secure messaging. In addition, it must possess a certificate that may contain complementary policy information as the right to use a specific signing mode and that must contain the roles that the component can take, such as acting as a SSA, an IDP or a SCD. A service component must digitally sign any sent message with the private key of that certificate. The signature is validated by the receiving component. This approach adds a complementary security layer to the ones exposed by the underlying CryptoServer CP5. It ensures payload authenticity and integrity. It particularly enables a receiving party to identify the sending party of each message or of each message part, when it originates from multiple parties, and to determine unambiguously the roles and capabilities granted to the sender.

In the case of a POST method, the request has a triply wrapped signature envelope in order to enforce a key security function of the SAP. It serves for checking the proper binding between signer authentication, DTBS(s) and signing key identifier and accurate sequencing of actions. The innermost payload signed by the originating SSA represents the unique signing transaction identifier. It consists of a unique time stamp, a sequence number, an arbitrary number of random octets and other optional content that may be imposed by a local service policy and it is created when the SSA initializes the request. This part of the payload is countersigned by the IDP, which is used to identify the signer and then adds the signer identity data prior to countersign the augmented payload when returning it to the originating SSA. Finally, the SSA adds the DTBS(s) to complement the signing request and to countersign the entire structure prior to send it to the LuxTrust Crypto-Box SAM 2.0.0.1.

Prior to carry out complementary validations like ensuring that the request has not been replayed, the LuxTrust Crypto-Box SAM 2.0.0.1 checks, whether all involved service components have valid and suitable service component certificates, belong to the same domain, i.e. have the same issuer, use granted algorithms and parameters only and have assembled the request with suitable payload data in the right order.

Key Management

A QSCD is not assigned to a particular client and can generate several keys for a customer. All keys are stored in the database of the SSA assigned to the customer.

The signing key is the private key of an asymmetric key pair used to create a digital signature under the Signer's sole control or to create a digital seal under the seal creator's control. The private key can only be used by the CryptoServer CP5. The LuxTrust Crypto-Box SAM 2.0.0.1 uses the asset R.Signing_Key_Id, which identifies a signing key in the Cryptographic Module. The binding of the R.Signing_Key_Id with the signatory or seal creator is protected in integrity. The integrity and confidentiality of the private key and the link between the R.Signing_Key_Id and the private key is the responsibility of the CryptoServer CP5. The LuxTrust Crypto-Box SAM 2.0.0.1 ensures that only the Signer can use the private key under their control or sole control.

During the key generation, the keys are assigned a unique key ID. It is initialised during key generation process. The CryptoServer CP5 ensures that the key identifier is sufficient to uniquely identify the key within the system the CryptoServer CP5 is part of.

The LuxTrust Crypto-Box SAM 2.0.0.1 uses the CryptoServer for key generation.

The LuxTrust Crypto-Box SAM 2.0.0.1 generates cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA key pair generation and specified cryptographic key sizes 2048 up to 8192 bits that meet the requirements of [SOG-IS], chapter 4.1.

The LuxTrust Crypto-Box SAM 2.0.0.1 generates cryptographic keys in accordance with a specified cryptographic key generation algorithm ECDSA key pair generation with given elliptic curve domain parameters and specified cryptographic keys of minimum 224 bits with ECC domain parameters

- Curve P-224, Curve P-256, Curve P-384 or Curve P-521 as specified in [FIPS 186-4], appendix 6,
- brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1 or brainpoolP512t1 as specified in [ECCBP], chapter 10 and
- curves FRP256v1, secp224r1, secp256r1, secp384r1, secp521r1 as specified in [ANSSI].

A process exists to ensure the confidentiality and integrity of private and secret keys when they are outsourced. If this is done using cryptographic mechanisms, algorithms and parameters must be selected that have at least the same level of security as the keys to be protected. Private and secret keys are encrypted by the CryptoServer in the QSCD with the Master Backup Key (256 bit, AES) before they are issued to the external storage. Backup keyblobs with integrity protected signature verification data and encrypted signing keys are stored in a database outside the LuxTrust Crypto-Box SAM 2.0.0.1. This process ensures that only one copy of the user's key pair is exported and stored in the data base.

Private and secret keys are generated and used in the CryptoServer CP5. This includes in particular the private keys of the "signers" and "seal issuers" hosted in the hardware component.

Key management cannot be done without user authentication. Only if a defined authentication status has been obtained then key management tasks can be executed. In addition to that, for some key management functions the key usage has to be authorised before. This security function is therefore closely related to the security

functions provided by CryptoServer CP5 related to authentication of users and key authorisation.

The CryptoServer CP5 provides the following services by means of the security function "Cryptographic Algorithms":

- Generation and export of the Master Backup Key (authenticated by an Administrator),
- Import of the Master Backup Key (authenticated by an Administrator, and under dual person control),
- Generation of keys (authenticated by a Key Manager or Internal SAM):
  - AES Keys,
  - ECDSA Keys and
  - RSA Keys,
- Deletion of keys (authenticated by a Key Manager or Internal SAM) and
- Modification of key attributes.

The CryptoServer CP5 enforces the key usage to authenticated users who are currently authorised to change attributes of secret key.

Plaintext secret and private keys are destroyed by overwriting them with zeros.

Encrypted secret and private keys are destroyed by deleting the logical address, and by zeroizing the encryption key in case of a physical attack. For permanent storage inside the CryptoServer CP5, the CryptoServer CP5 enforces all secret and private keys to be stored encrypted with the internal Master Key. The commands for key deletion delete the encrypted secret and private keys by deletion of the logical addresses, respectively. After that it is no longer possible to address the memory areas of the encrypted keys via the CryptoServer CP5 interface. Furthermore, there is no logical access from outside of the CryptoServer to the Master Key itself. In case of e.g. a physical attack, the Master Key is protected by the alarm mechanism of the CryptoServer CP5 and its hard, opaque tamper-evident enclosure. The Master Key will be actively zeroised in case of an alarm. The Master Key will also actively be erased in case of a Clear command (by actively overwriting it with a new Master Key). This ensures secure storage and destruction also for encrypted secret and private keys.

The ability to manage security attributes of general keys and assigned keys is restricted by the CryptoServer CP5 [ST HW] as follows:

- The use of permissive default values for security attributes shall be enforced. The Key Manager or Internal SAM shall be allowed to specify alternative initial values to override the default values when an object or information is created.
- For general keys the change of the security attribute "Assigned Flag" and the key export (“Export Flag”) is restricted to the role Key Manager. The change of authorisation data is restricted to the user, but only after representing the current authorisation data, or to the Key Manager. The security attributes "Key

ID", "Key Type", "Re-Authorisation conditions", "Key Usage" and "Integrity Protection Data" may not be changed.

- For assigned keys the change of authorisation data is restricted to the user or to the Key Manager, but only after representing the current authorisation data. The security attributes "Key ID", "Key Type", "Re-Authorisation conditions", "Key Usage", "Export Flag", "Assigned Flag" and "Integrity Protection Data" may not be changed.

Generation of qualified electronic signatures and qualified electronic seals

The data to be signed are transmitted to the LuxTrust Crypto-Box SAM 2.0.0.1 within a signed request of the method POST (SignedPostRequest). The LuxTrust Crypto-Box SAM 2.0.0.1 checks the integrity of the received request before signing them.

The LuxTrust Crypto-Box SAM 2.0.0.1 uses the CryptoServer to perform cryptographic operations for the generation of qualified electronic signatures and qualified electronic seals:

- The LuxTrust Crypto-Box SAM 2.0.0.1 is able to generate a digital signature with RSA signature schemes RSASSA-PSS or RSASSA-PKCS-v1_5 and cryptographic key sizes of minimum 2048 and maximum 8192 bits modulus length according to [PKCS#1], chapters 8.1.1 or 8.2.1.

- The LuxTrust Crypto-Box SAM 2.0.0.1 is able to generate a digital signature with ECDSA signature algorithm and cryptographic key sizes minimum 224 bits according to [ANSI-X9.62] with signature keys based on ECC domain parameters

    - Curve P-224, Curve P-256, Curve P-384 or Curve P-521 as specified in [FIPS 186-4], appendix D,

    - brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1 or brainpoolP512t1 as specified in [ECCBP], chapter 10 and

    - curve FRP256v1 as specified in [ANSSI].

- The LuxTrust Crypto-Box SAM 2.0.0.1 performs hash value calculation in accordance with a specified cryptographic algorithm SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384 or SHA3-512 according to [FIPS 180-4], chapter 6 for SHA-2 and according to [FIPS 202] for SHA-3.

Administration

Privileged users are entirely managed by CryptoServer CP5 in using HSM proprietary commands. LuxTrust Crypto-Box SAM 2.0.0.1 only manages complementary authorisation for automated privileged users that act as service components like SSA, IDP, QSCD, SRM, while human person administrators that perform setup operations and that can also create other privileged users do not need specific authorisation certificates. Instead, LuxTrust Crypto-Box SAM 2.0.0.1-specific authorisation is added to privileged users during SETUP via DAK binding and verification during subsequent requests for restricting administrative access of a privileged user to domains, for which

she possesses a DAK. Creation of such users is entirely performed with standard HSM functionality prior to SETUP of LuxTrust Crypto-Box SAM 2.0.0.1.

The LuxTrust Crypto-Box SAM 2.0.0.1 relies on the CryptoServer CP5 for authorisation and management of privileged users. Privileged users are created and authenticated by the Cryptographic module before administrative functions of the LuxTrust Crypto-Box SAM 2.0.0.1 can be used. At SETUP, the LuxTrust Crypto-Box SAM 2.0.0.1 checks the authentication state, i.e. checks if a user authentication with required user group membership and minimum required permission level have been performed by using an internal interface to the CryptoServer CP5.

Signer Creation is based on the methods POST and GET. Key pair generation for signers is triggered by LuxTrust Crypto-Box SAM 2.0.0.1, with the actual generation task being performed by the CryptoServer CP5, while identity management is taken into account by IDP outside LuxTrust Crypto-Box SAM 2.0.0.1, with id data and evidences provided to LuxTrust Crypto-Box SAM 2.0.0.1 for signing from IDP via SSA. Id data may be represented as an X.509 certificate when applied for multi-use or alternatively as an X.509 certificate template only with corresponding key pair creation performed together with the signature creation transaction in the case of single use ("on the fly") certificates. The method PUT may trigger creation of key pairs beforehand. In that latter case, they are not associated with any identity, i.e. they can be considered as "virgin". Those key pairs are cached in a LuxTrust Crypto-Box SAM 2.0.0.1 internal key store database and do never leave the boundary of the HSM prior to be assigned (once and only once) to a signer identity.

Signer private key is either destroyed immediately upon single use for signing (in the case of single-use certificate policy) or key and signer X.509 certificate are managed by an IDP (an automated privileged user from the LuxTrust Crypto-Box SAM 2.0.0.1 perspective), while this latter approach is used in the case of multi-use certificate policy.

Security-relevant administration of the CryptoServer CP5 cannot be done without user authentication. Only if a defined authentication status has been obtained then administration tasks can be executed. In addition to that, for some administration functions, related to key management, the key usage has to be authorised before. This security function is therefore related to the security functions "User Authentication" and "Key Authorisation".

The CryptoServer provides the following administrative services:

- Backup of keys and users,
- Unblock of user accounts due to authentication failures,
- Unblock of cryptographic keys due to key authorisation failures,
- Export of General (non-Assigned) keys,
- Modifications of key attributes by authorised subjects,
- System time setting,
- Export and deletion of the audit log and
- Software Update.

For the user administration typical functions are available. Basically, the service deals with administration of the user database (creation, deletion, changing). The commands for creation or deletion of a user have to be authenticated by a user in User Administrator role. The command for changing the user's authentication token (password or public key) has to be authenticated by the respective user himself.

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

3.1 Fulfilled Requirements

The product fulfils the following requirements pursuant to the Regulation (EU) No. 910/2014.

Table 4: Fulfilment of the requirements of the Regulation (EU) No. 910/2014

Reference	Requirement / Description / Result
Article 29	**Requirements for qualified electronic signature creation devices**
(1)	**Requirement** Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.
(1a)	**Requirement** Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes shall be carried out only on behalf of the signatory, at the request of the signatory, and by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.
Article 39	**Qualified electronic seal creation devices**
(1)	**Requirement** Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.
Annex II	**Requirements for qualified electronic signature creation devices**
1.	**Requirement** Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:
(a)	the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
(b)	the electronic signature creation data used for electronic signature creation can practically occur only once;
(c)	the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;

Reference	Requirement / Description / Result
(d)	the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.
2.	**Requirement** Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

3.2 Conditions of Use

Requirements for the operational environment

- The certified QSCD shall be used only by a qualified trust service provider conformant to the Regulation (EU) No. 910/2014 [Reg No. 910/2014].
- The security objectives for the operational environment as specified in the Security Target Lite for CryptoServer Se-Series Gen2 CP5 (cf. [ST HW], chapter 5.2) and for LuxTrust Crypto-Box SAM 2.0.0.1 (cf. [ETR LuxTrust-SAM], chapter 4.2) shall be considered.

3.3 Cryptographic Algorithms and Parameters

For the generation of digital signatures and digital seals LuxTrust Crypto Box device V2 provides ECDSA algorithm according to the standard [ANSI-X9.62] with key lengths of minimum 224 bits used for ECDSA signature generation, and RSA algorithm according to the standard [PKCS#1] with key lengths of minimum 2048 bits and maximum 8192 bits used for RSA. The used signature scheme is RSASSA-PSS or RSASSA-PKCS-v1_5. For ECDSA key lengths of 224, 256, 320, 384, 512 and 521 bits are supported.

For ECDSA the product „Crypto Box“ supports the use of the curves Curve P-224, Curve P-256, Curve P-384 and Curve P-521 as specified in [FIPS 186-4], appendix D, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1 and brainpoolP512t1 as specified in [ECCBP], chapter 10, and curve FRP256v1 as specified in [ANSSI].

Signatures and seals are generated with hash values that have been computed by the external world as well as generated internally by the „Crypto Box“ itself. For the internal generation of hash values the Hash algorithms SHA-224, SHA-256, SHA-384 and SHA-512 according to [FIPS 198-1], and SHA3-224, SHA3-256, SHA3-384 and SHA3-512 according to [FIPS 202] are available.

The generation of random numbers is based on a hybrid deterministic random number generator of the CryptoServer CP5. The RNG is a class DRG.4 generator (cf. [AIS 20/31], chapter 4.9). The internal state of the RNG is seeded by a PTRNG of class PTG.2 (cf. [ST HW], chapter 7.3.1).

All cryptographic algorithms are provided by the CryptoServer CP5 (cf. [ST HW], chapter 7.3.1). The following cryptographic algorithms used by the product „Crypto Box“ are classified as “recommended” by the algorithm catalogue SOG-IS [SOG-IS]:

Table 5: Recommended SHA-2/SHA-3 Hashfunctions

Recommended (R)
SHA-2: SHA-256, SHA-384, SHA-512, SHA-512/256 SHA-3: SHA3-256, SHA3-384, SHA3-512

Table 6: Recommended RSA primitive sizes

Recommended (R)
At least 3000 Bits

Table 7: Recommended Digital Signature Schemes

Recommended (R)
RSA PSS (PKCS #1, v2.1)

Table 8: Recommended Elliptic Curve Parameters

Recommended (R)
BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1 NIST P-256, NIST P-384, NIST P-521 FRP256v1

Recommended mechanisms fully reflect the state of the art in cryptography and the use of those algorithms and key lengths is not restricted. According to [SOG-IS] the following restrictions apply for cryptographic algorithms and key lengths provided by „Crypto Box“:

- The RSA padding scheme RSA-PKCS#1_v1.5 is evaluated by [SOG-IS] as legacy and its validity period ends by **December, 31st 2030**.
- RSA signature generation with key length of less than 3000 bits and ECDSA signature generation with a key length of 224 bits **may no longer** be used.
- The hashfunction SHA-224 **may no longer** be used.

Due to Regulation (EU) No 910/2014 [Reg No. 910/2014], Article 30 (3a) the validity of the certification shall not exceed five years. Therefore, this certification of the QSCD “LuxTrust Crypto Box device V2” with issuing date **February, 10th 2026** is valid until **February, 9th 2031**. The above restrictions apply and must be taken into consideration when using the QSCD.

However, the validity may be shortened if new findings regarding the suitability of the algorithms are published in the algorithm catalogue SOG-IS [SOG-IS]. In addition, in accordance with Article 30 (3a), a vulnerability analysis must be carried out every two years. Where vulnerabilities are identified and not remedied, the certification shall be cancelled.

3.4 Assurance Level and Attack Potential

The product was successfully evaluated according to Common Criteria (CC) Version 3.1 with an assurance level of **EAL 4+** (EAL4 with augmentation AVA_VAN. 5 and ALV_FLR.2 defined in CC Part 3, and with ALC_PAM.1 defined in [ISO/IEC 9569]). The evaluation was carried out against a **high attack potential** (Augmentation AVA_VAN.5).

Due to the absence of standards referred in Regulation (EU) No. 910/2014, Art. 30 (3) a the certification is based on a process other than referred to in Regulation (EU) No. 910/2014, Art. 30 (3) a. For this SRC's certification body (Designated Body) has defined an alternative certification process "Certification of the conformity of QSCDs for server-signing with the requirements laid down in Annex II of Regulation (EU) No. 910/2014" [SRC_Alt_Cert] that has been notified to the EU Commission (Art. 30 (3) b).

The security evaluation process notified to the Commission consists of a security evaluation according to the "ISO/IEC 15408 Evaluation criteria for IT-Security" (Common Criteria Evaluation, cf. [ISO/IEC 15408-1], [ISO/IEC 15408-2], [ISO/IEC 15408-3]) as already listed in the Commission Implementing Decision (EU) 2016/650 [CID (EU) 2016/650] and the use of the following two protection profiles (PP):

- „EN 419 221-5 PP Cryptographic Module for Trust Services" [EN 419 221-5], and
- „EN 419 241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing" [EN 419 241-2].

For this both PPs were used for the evaluation, EN 419 221-5 for the security evaluation of the "CryptoServer CP5" and EN 419 241-2 for the security evaluation of the signature activation module (LuxTrust Crypto-Box SAM 2.0.0.1). The alternative certification process refers to an older version of the PP EN 419 241-2 but there is no change in the certification process itself. This newer version is also used in an notified alternative certification process defined by TÜV Informationstechnik GmbH (TÜVIT) [TüViT_Alt_Cert]. Thus, the used certification process is compliant to [SRC_Alt_Cert] as well as [TüViT_Alt_Cert] where newer versions are stated.

The LuxTrust Crypto-Box SAM 2.0.0.1 was successfully evaluated (cf. [ETR LuxTrust-SAM]) 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**.

The "CryptoServer CP5" of Utimaco GmbH was successfully evaluated by Brightsight BV according to the Protection Profile EN 419 221-5. This evaluation was conducted 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 4 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**.

The "CryptoServer CP5" of Utimaco GmbH is certified by TrustCB B.V. under the certificate number **NSCIB-CC-2300142-02** (cf. [CR_CP5]). This certificate is valid until 05-12-2028 (cf. [CERT_CP5]).

4. References

[Reg No. 910/2014] 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 Directive 1999/93/EC; last amended by Regulation (EU) No 2024/1183

[CID (EU) 2016/650] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[EU QSCD list] Compilation of: Member States' notifications on: Designated Bodies under Article 30(2) and 39(2) of Regulation 910/2014 and Certified Qualified Signature Creation Devices under Article 31(1)-(2), and Certified Qualified Seal Creation Devices under Article 39(3) of Regulation 910/2014, and information from Member States on: Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014

[SRC_Alt_Cert] SRC, Certification of the conformity of QSCDs for server-signing with the requirements laid down in Annex II of Regulation (EU) No. 910/2014, Version 1.0, 14.09.2017
https://eidas.ec.europa.eu/efda/browse/notification/alternative-process

[TüViT_Alt_Cert] Certification Process for eIDAS conformant QSCDs of the certification body of TÜV Informationstechnik GmbH, cf.
https://eidas.ec.europa.eu/efda/browse/notification/alternative-process

[AIS 20/31] Application Notes and Interpretation of the Scheme (AIS): AIS 20/AIS 31: A proposal for: Functionality classes for random number generators, Version 2.0 / Wolfgang Killmann (T-Systems GEI GmbH, Bonn), Werner Schindler (Bundesamt für Sicherheit in der Informationstechnik/BSI, Bonn), 18. September 2011

[ANSI-X9.62] ANS X9.62-2005: Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA) ANSI (American National Standards Institute)

[CERT_CP5] TrustCB B.V., Certificate NSCIB-CC-2300142-02, CryptoServer CP5 Se12 5.1.2.0, CryptoServer CP5 Se52 5.1.2.0, CryptoServer CP5 Se500 5.1.2.0, CryptoServer CP5 Se1500 5.1.2.0, Date of issue: 26-05-2025, Certificate expiry: 26-05-2030

[CR_CP5] TrustCB B.V., Certification Report NSCIB-CC-2300142-02-CR, CryptoServer CP5 Se12 5.1.2.0, CryptoServer CP5 Se52 5.1.2.0, CryptoServer CP5 Se500 5.1.2.0, CryptoServer CP5, Se1500 5.1.2.0, Report Version 1, 26 May 2025

[EC DSS APP] European Commission, DSS Demonstration WebApp – Validation, Latest Version

[ETR LuxTrust-SAM] SRC, Evaluation Report, Evaluation Technical Report (ETR), LuxTrust Crypto Box SAM 2.0.0.1, Version 2.2, 23 January 2026

[FIPS 140-2] Federal Information Processing Standards Publication FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001

[FIPS 180-4] Federal Information Processing Standards Publication FIPS PUB 180-4, Specifications for the Secure Hash Standard (SHS), March 2012

[FIPS 186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013

[FIPS 197] Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), U.S. Department of Commerce/National Institute of Standards and Technology, 2001-11-26

[FIPS 198-1] Federal Information Processing Standards Publication, the Keyed-Hash Message Authentication Code (HMAC) July 2008

[FIPS 202] Federal Information Processing Standards Publication FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015

[ISO/IEC 15408-1] ISO/IEC 15408-1:2009: Information technology – Security techniques – Evaluation criteria for IT security – Part 1. ISO, 2009

[ISO/IEC 15408-2] ISO/IEC 15408-2:2008: Information technology – Security techniques – Evaluation criteria for IT security – Part 2. ISO, 2008

[ISO/IEC 15408-3] ISO/IEC 15408-3:2008: Information technology – Security techniques – valuation criteria for IT security – Part 3. ISO, 2008

[CEM] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

[ISO/IEC 19790] ISO/IEC 19790:2012(E): Information Technology – Security Techniques — Security requirements for cryptographic modules. ISO 15th August 2012

[EN 419 221-5] EN 419 221-5:2018 Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020

[ISO/IEC 9569] ISO/IEC 9569:2023(E): Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045

[ANSSI] ANSSI: "Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français" in: Journal Officiel de la République Française (JORF),

n° 0241 du 16 octobre 2011 page 17533 text n° 30 (Announcement about elliptic curve parameters set by the French government). NOR: PRMD1123151V. Available: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024668816

[ITU-T X.509] ITU-T, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, X.509, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Directory, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation ITU-T X.509, 10/2019

[NIST SP 800-38A] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques / National Institute of Standards and Technology (NIST), USA, December 2001

[NIST SP 800-38B] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication / National Institute of Standards and Technology (NIST), USA, May 2005

[ECCBP] ECC Brainpool Standard Curves and Curve Generation, v1.0, 19.10.2005 / ECC Brainpool, http://www.ecc-brainpool.org/ecc-standard.htm

[EN 419 241-1] CEN/EN 419 241-1:2018, Trustworthy Systems Supporting Server Signing, Part 1: General System Security Requirements, July 2018, or newer version

[EN 419 241-2] CEN/EN 419 241-2:2019, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, February 2019, or newer version

[ETSI EN 319 162-1] ETSI EN 319 162-1 – Electronic Signatures and Infrastructures (ESI) – Associated signature containers (ASiC) – Part 1: Building blocks and ASiC baseline containers

[PKCS#1] PKCS #1 v2.2: RSA Cryptography Standard, RSA Laboratories, October 27, 2012

[RFC 5280] IETF, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280, May 2008

[SOG-IS] SOG-IS Crypto Working Group; SOG-IS Crypto Evaluation Scheme; Agreed Cryptographic Mechanisms; Version 1.3 February 2023

[ST LuxTrust-SAM] LuxTrust Crypto Box SAM Security Target, LuxTrust S.A. & achelos GmbH, Version 0.2.7, 2025-07-21

[ST HW] CryptoServer Security Target Lite for CryptoServer Se-Series Gen2 CP5, Utimaco, Version 2.2.0, 4 February 2025

[AGD_PRE] LuxTrust Crypto Box SAM AGD_PRE, LuxTrust S.A, Version 0.4.0

[AGD_OPE] LuxTrust Crypto Box SAM AGD_OPE, LuxTrust S.A, Version 0.3.9

[SAM-Sign-Proc] Utimaco, SAM Module - Signing Procedure, Quick Start Guide, Document Number 2023-0003, Document Version 1.0.1, Date 2023-01-19

[CP5 MAN ADM] Utimaco – CryptoServer Se-Series Gen2 CP5 – Administration Manual, Version 2.3.0, 2024-09-18

End of certification report