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

AMENDMENT

Amendment 1 to the Certification

SRC.00031.QSCD.02.2019 of 28.02.2019

SRC Security Research & Consulting GmbH
Emil-Nolde-Straße 7
D-53113 Bonn
Germany

confirms hereby, pursuant to
Articles 29 (1), 39 (1) and Annex II of the Regulation (EU) No. 910/2014[1]
that for the

Qualified Signature / Seal Creation Device
BV-SAM on CryptoServer CP5
of Bank-Verlag GmbH

the above mentioned Certification has been extended as follows.

Bonn, 29 October 2021

Gerd Cimiotti

SRC Security Research & Consulting GmbH is a Designated Body notified to the EU commission for the certification of qualified electronic signature creation devices to be conformant with the Regulation (EU) No. 910/2014.

[1] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive1999/93/EC.

Description of the Qualified Signature Creation Device (QSCD):

1. Product Name and Scope of Delivery

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

The BV-SAM uses the CryptoServer CP5 for key generation and for creating the digital signature values. The system consists of a local and a 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) are 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 authenticated by verifying a signed authentication evidence.

The logical scope of BV-SAM, which lists the security services that are in the scope of the evaluation, includes:

- Signer management and
- Signature operation.

1.1 Product Name

Qualified Signature Creation Device and Qualified Seal Creation Device with the product name **BV-SAM on CryptoServer CP5** (short "BV-QSCD") 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 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0 and CryptoServer CP5 Se1500 5.1.0.0. This certification at hand covers all these listed CryptoServer CP5 versions.

A basic requirement for such a service is that the (sole) control of the signature or seal keys is ensured. Specifically, the signature key must be under the sole control and the seal key must be under the control of the key owner. A Signature Activation Module (SAM) is provided to ensure (sole) control. The main purpose of BV-SAM is to check the Signature Activation Data (SAD) and to use the correct signature or seal key. The SAD, abstractly described in the corresponding standard [prEN 419 241-1] and protection profile EN 419 241-2 [prEN 419 241-2], are implemented within this project by a signed authentication evidence (cf. [ST BV-SAM]). This evidence binds

the successful authentication of the key owner cryptographically to the data to be signed (DTBS).

1.2 Delivery

The BV-SAM is a firmware module of the CryptoServer CP5. The delivery (cf. [UG_PRE], [UG_OPE]) comprises the delivery of the BV-SAM firmware module and NTP firmware module to the Trust Service Provider (TSP). These firmware modules are built and delivered by Utimaco. The BV-SAM is developed by achelos GmbH in Paderborn. The delivery of the BV-SAM firmware module, NTP firmware module and BV-SAM manuals has to follow strictly the secured delivery procedures.

The firmware module files are delivered encrypted and signed. The project-specific key used for encryption and signing must be exchanged between achelos and the Trust Service Provider. achelos and the Trust Service Provider nominate team members responsible for shipping resp. reception of the file and provide encryption and signing keys to be used. The persons nominated check the integrity of the keys (verbal cross-check of key fingerprints by phone after exchanging the keys by mail). The keys used for encryption and signing are stored safely in the secure environment.

Delivery is enforced by extracting the BV-SAM, NTP firmware modules files and BV-SAM manuals directly from the final product label within the achelos configuration management system. The firmware modules have been built, signed with the project-specific CP5 Module Signature Key and delivered by Utimaco to achelos. As the first step these files are encrypted and signed. PGP is used for this. As the second step the files are send via PGP encrypted mail by the achelos development team member responsible for the shipping to the Trust Service Provider staff member who is responsible for the reception of the file. The Trust Service Provider staff member checks the signature. If the signature is invalid, the shipped files are rejected and the staff member contacts achelos.

1.3 Delivery items

The certified product consists of the Hardware Security Module (HSM) "CryptoServer CP5" and the Signature Activation Module BV-SAM. The BV-SAM is implemented as a firmware module for the HSM "CryptoServer CP5". 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 „BV-QSCD“ consists of the following items:

Table 1: Delivery items and associated delivery methods

No.	Delivery Item	Description / Additional Information	Type	Delivery method
1	BV-SAM v1.0.1.0	Firmware Module	SW	The firmware module files and manuals are delivered encrypted and signed. The project-specific keys used for encryption and signing are exchanged between the team members of achelos and the Trust Service Provider who are responsible for shipping resp. reception of the files. Therefore, the integrity, authenticity and confidentiality can be ensured during the delivery.
2	NTP v1.2.0.10			
3	Associated guidance documentation	Operational Guidance, Guidance Documentation of BV-SAM [UG_OPE]	DOC	The guidance documents of the TOE are delivered always in an encrypted and signed form. Therefore, the integrity and authenticity can be ensured during the delivery.
4		Administrator’s Guidance, Guidance Documentation of BV_SAM [UG_PRE]	DOC	
5	Hardware and Software components of the CryptoServer CP5	cf. [CR_CP5], Chapter 2.1.		

1.4 Manufacturer and Applicant

Manufacturer of CryptoServer CP5 as well as of the firmware module NTP is Utimaco IS GmbH, Germanusstraße 4, D-52080 Aachen, Germany.

Manufacturer of BV-SAM on behalf of Bank-Verlag GmbH is achelos GmbH, Vattmannstraße 1, D-33100 Paderborn, Germany.

Developer, sponsor or applicant of the product is Bank-Verlag GmbH, Wendelinstraße 1, D-50933 Köln, Germany.

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 **BV-SAM on CryptoServer CP5** is used as a Qualified Signature/Seal Creation Device (QSCD). The Signature Activation Module is realised by the firmware module BV-SAM 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 BV-SAM 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 BV-SAM.

The signature operation is performed using a Signature Activation Protocol (SAP), which requires that Signature Activation Data (SAD) are 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 key, the signature or seal operation needs to be authorised. This is carried out by BV-SAM, 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. BV-SAM is a software component integrated into the CryptoServer.

The CryptoServer together with BV-SAM forms the Qualified Signature/Seal Creation Device (QSCD). Within the QSCD, all external interfaces are provided by the BV-SAM. 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 or seals a QSCD provides two eIDAS functions:

- eIDAS Key Generation
- Signature/Sealing

2.1.2 Cryptographic Algorithms

The following cryptographic algorithms are supported for signing and verification of signed evidences (e.g. authentication, certification) as well as for the creation of signatures and seals:

- Hash functions SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512
- Signature scheme RSASSA-PSS for RSA
- ECDSA Signature generation and verification according [ANSI-X9.62]

- Curves brainpoolP224r1, brainpoolP224t1, NIST-P224, brainpoolP256r1, brainpoolP256t1, FRP256v1, NIST-P256, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, NIST-P384, brainpoolP512r1, brainpoolP512t1, NIST-P521 for ECDSA

2.1.3 Function eIDAS Key Generation

With this function an RSA or ECDSA key pair is generated and stored in a so-called "Backup keyblob". In the Backup keyblob the signature verification data (public key) is integrity protected and the signing key (private key) is encrypted. The eIDAS Key Generation function creates an evidence for the certification of the corresponding public key, signs it and returns it to the calling application together with the Backup keyblob.

The private key of the generated key pair is intended to be used to create an eIDAS seal or an eIDAS signature. The intended key usage is coded in a signed data set that is contained in the input of the eIDAS Key Generation function.

With the signed evidence for authentication, also contained in the input of the eIDAS Key Generation function, it can be verified that the person who generates eIDAS key pairs is authenticated by two factor authentication. Thereby, the information to this person is part of a signed data set that is contained in the evidence for authentication.

The function eIDAS Key Generation calls a function of the CryptoServer which generates the key pair in the CryptoServer. Moreover, the CryptoServer builts up the Backup keyblob containing the generated key pair and provides it to the BV-SAM.

2.1.4 Function Signature/Sealing

With this function a remote eIDAS signing or sealing operation is performed depending on the signed configuration information which is part of the function input.

When performing the function Signature/Sealing BV-SAM verifies the SAD. This verification is part of the function Signature/Sealing. SAD verification means that BV-SAM checks the binding between the three SAD elements, i.e. it checks

- that the signer is authenticated,
- that the signing key that shall be used is assigned to the signer and
- that the DTBS are assigned to the signer.

The fact that the signer is authenticated with two factor authentication and the binding of the data to be signed to the signer are verified with the signed authentication evidence. Thereby, the information assigned to the signer and to the DTBS is part of a data set that is contained in the signed authentication evidence.

The signing key to be used is identified by its key ID which is derived from information contained in signed input parameters of the function Signature/Sealing.

2.2 Security functions and security properties of the „BV-QSCD“

User Authentication

The Server Signing Application (SSA) handles all the tasks required for a customer to generate a seal or signature. The SSA receives the signed authentication

evidence and initiates the registration with a signed request for certification of the public key and the creation of the signature. Using the incoming authentication evidence (via the trust services API), correct customers and their signature/seal keys are identified and the corresponding functions of the QSCD are called.

The signed authentication evidence is checked by the QSCD functions. This is performed using a public authentication mechanism and a secure configuration to check whether the key is valid. The time of authentication as provided in the authentication evidence is checked against the CryptoServer time and a comparison value specified in the configuration information. Two factor authentication is necessary.

The authentication module generates the signed authentication evidence. It may be operated by the Trust Service Provider or by a client (delegated authentication). If the Trust Service Provider is the operator of the authentication module, this module has access to a CryptoServer, which generates the authentication evidence in addition to checking authentication data. For this purpose a database with registration data is used.

User authentication is necessary to apply any of the security-relevant services of the CryptoServer. Only if a defined authentication status has been obtained the services can be realised. Here the necessary user authentication status depends on the individual service. Command authentication can only be done by subjects (so-called users) which have to be registered at the CryptoServer before.

At registration, together with the user's name (Identity), his permission (Role), authentication mechanism, the reference authentication data (RAD: public key or password, depending on the authentication mechanism) and further attributes will be stored in the user database of the CryptoServer. Only the RAD may be changed later, all other user attributes cannot be changed. The command for changing a user's RAD has to be authenticated by the user himself. The user's permission decides which of the security-relevant services may be performed by this user (i.e. which user role the user may assume). The step immediately preceding the user authentication is the identification of a user.

The CryptoServer supports the following roles for the different users:

- administrator roles
    - User Administrator (user management tasks like creation of users, deletion of users)
    - Administrator (general administration of the CryptoServer, like system time setting, load, update and deletion of firmware)
    - Key Manager (key management tasks necessary for the usage of the CryptoServer, like unblocking of blocked keys, key generation, key export and import, key backup and key restore, key deletion)
    - Security Officer (creating, modifying or deleting key group specific configuration objects and initiating a key group)
- Key User (who uses the CryptoServer for cryptographic operations like signature creation)
- External Client Application (that uses the CryptoServer for creating a secure channel; hence, each authenticated user can in addition assume the role External Client Application)

- Local Client Application:
    - Non-internal Local Client Application that connects to the CryptoServer via the local PCIe interface and which uses the CryptoServer for creating a secure channel; hence, each authenticated user can in addition assume the role Non-internal Local Client Application.
    - Internal SAM: Internal Local Client Application that invokes the internal CryptoServer interface. It is authenticated by signature verification when initially loaded to the CryptoServer and integrity protected by the physical boundary of the CryptoServer. Therefore, it does not need to establish a cryptographically protected secure channel.

At registration, for every user a dedicated authentication mechanism has to be chosen. The CryptoServer 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 demands a 16 bytes random value (challenge) from the CryptoServer. The challenge is generated by hybrid RNG. 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. This challenge and response mechanism is also used for the RSA Signature authentication mechanism.

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 too many unsuccessful user authentication attempts the corresponding user is blocked. Any additional attempt of this user to authenticate towards the CryptoServer 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 and the (local non-internal or remote external) client application. Such a Secure Messaging session is usable for each command which requires user authentication. A Secure Messaging channel is established after a mutual authentication using RSA and Diffie-Hellman key agreement to generate AES keys. These keys are used for encryption, decryption and MAC-calculation.

Key Usage

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 [prEN 419 221-5]: As mandated

by CryptoServer 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 can implicitly derive prior successful key authorisation of the signature key from each invocation of the SAEK signature interface.

Physical Access Control and Security Audits

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

The BV-SAM 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 (level of audit not specified),
- Privileged User management,
- Privileged User authentication,
- Signer management,
- Signer authentication,
- Signing key generation,
- Signing key destruction,
- Signing key activation and usage including the hash of the data to be signed and the signature and
- change of BV-SAM configuration.

The BV-SAM stores within each audit record at least the following information:

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

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

The CryptoServer 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 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 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,
- Self-test fails,
- External erase and
- General alarm condition.

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 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.

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

The implemented sensory and software parts of the CryptoServer 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 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 supplies effective hardware and software based mechanisms.

Due to the implemented alarm mechanism, the CryptoServer 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 or if extreme temperature is monitored, an alarm is triggered, all data is deleted and the CryptoServer will be reset cleanly. The CryptoServer 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 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 enters the secure Error State.

The CryptoServer 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 supports a secure software update by providing the "Load File" service.

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

The "Load File" service allows the upload 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 upload 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 will be set to a secure Error State.

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

Cryptographic Algorithms

The CryptoServer 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.

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.

During the key generation, the keys are assigned a unique key ID. This key ID consists of a prefix that identifies the use of the key and a unique identifier. In the case of a user key, the unique identifier is identical to the user's registration number.

The BV-SAM uses the CryptoServer for key generation.

The BV-SAM generates cryptographic keys in accordance with the 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 BV-SAM also generates cryptographic keys in accordance with the 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 D,
- brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1 or brainpoolP512t1 as specified in [RFC 5639], chapter 10 and
- curve FRP256v1 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 (32 bytes, 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 BV-SAM. 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. 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 can key management tasks 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 "User Authentication" and "Key Authorisation".

The CryptoServer 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 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 zeroing the encryption key in case of a physical attack. For permanent storage inside the CryptoServer, the CryptoServer enforces all secret and private keys to be stored encrypted with the internal Master Key of the CryptoServer. The commands for key deletion delete the encrypted secret and private keys by deletion of the logical addresses. After that it is no longer possible to address the memory areas of the encrypted keys via the CryptoServer 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 and its hard, opaque tamper-evident enclosure. The Master Key will be actively zeroed 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 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 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 BV-SAM within a signed data set that is part of the signed authentication evidence. The BV-SAM checks the integrity of the received data before signing them.

The BV-SAM uses the CryptoServer to perform cryptographic operations:

- The BV-SAM is able to generate and to verify a digital signature with RSA signature schemes RSASSA-PSS or RSASSA-PKCS-v1_5 and cryptographic key sizes of minimum 2048 bits modulus length according to [PKCS#1], chapters 8.1.1 or 8.2.1.
- The BV-SAM is able to generate and to verify 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 [RFC 5639], chapter 10 and

  - curve FRP256v1 as specified in [ANSSI].

- The BV-SAM performs HMAC calculation according to [FIPS 198-1] with a MAC key that is derived from the Master Backup Key. Both keys are 256-bit AES keys.
- The BV-SAM 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

A dual control principle is enforced for the generation of MACs and signature keys. The functions are implemented in BV-SAM and check the correct registration of the required roles at the CryptoServer before execution.

The BV-SAM relies on the CryptoServer for authorisation and management of Privileged Users. Privileged Users are created and authenticated by the CryptoServer before administrative functions of the BV-SAM can be used. During HMAC calculation, the BV-SAM checks the authentication state, i.e. it checks whether a user authentication with level 4 in group 3 has been done by using an internal interface to the CryptoServer.

The Signer creation and authentication is performed by the Local Environment of the Trust Service Provider, including the creation of a unique ID for the signer. If the Signer is authenticated correctly by the SSA, a signed authentication evidence is created by the TSP's Signature Creation Application in the local environment. This evidence is passed to the BV-SAM by the SSA on behalf of the Signer if an eIDAS function for key generation sealing or signing is called. The signed authentication evidence is the Signer authentication assertion for the BV-SAM. For the BV-SAM, the subject Signer consists of the Server Signing Application (SSA). Signer creation includes that a privileged user creates a secure configuration information (containing restrictions on parameters and keys) and the public key used for verification of the signed authentication evidence. The BV-SAM checks the authentication evidence using the configuration information and the public key.

Security-relevant administration of the CryptoServer cannot be done without user authentication. Only if a defined authentication status has been obtained can administration tasks 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,
- Unblocking of user accounts due to authentication failures,
- Unblocking 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 signed authentication evidence (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) 910/2014 [Reg No. 910/2014].

Table 2: 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.
(2)	**Requirement** The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48 (2).
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.	**Requirement** Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.
4.	**Requirement** Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for backup purposes provided the following requirements are met:
(a)	the security of the duplicated datasets must be at the same level as for the original datasets;
(b)	the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

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 BV-SAM (cf. [ETR BV-SAM], chapter 4.2) shall be considered.

3.3 Cryptographic algorithms and parameters

For the generation of digital signatures and digital seals BV-SAM on CryptoServer CP5 provides the ECDSA algorithm according to the standard [ANSI-X9.62] with key lengths of minimum 224 bits and the RSA algorithm according to the standard [PKCS#1] with key lengths of minimum 2048 bits and maximum 8192 bits. The used RSA signature scheme is RSASSA-PSS. For ECDSA key lengths of 224, 256, 320, 384 and 512 bits are supported.

In addition, the product „BV-QSCD“ supports the use of the curves brainpoolP224r1, brainpoolP224t1, NIST-P224, brainpoolP256r1, brainpoolP256t1, FRP256v1, NIST-P256, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, NIST-P384, brainpoolP512r1, brainpoolP512t1, NIST-P521 for ECDSA.

Signatures and seals are generated with hash values that have been computed by the external world as well as generated internally by the „BV-QSCD“ itself. For the internal generation of hash values the Hash algorithms SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384 and SHA3-512 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.

All cryptographic algorithms are provided by the CryptoServer CP5 (cf. [ST HW], chapter 7.3.1). The cryptographic algorithms used by the product „BV-QSCD“ are classified as “recommended” or “legacy” by the algorithm catalogue SOG-IS [SOG-IS]. Nevertheless the digital signature scheme PKCS#1, version 1.5 should not be used for the generation of qualified electronic signatures or seals.

Among others, [SOG-IS] lists the following recommended cryptographic algorithms or algorithms that are evaluated as legacy. Restrictions are set for legacy algorithms in terms of their time suitability.

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

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

Table 4: Recommended RSA primitive sizes

Recommended (R)
At least 3000 Bits

Table 5: Recommended Digital Signature Schemes

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

Table 6: Recommended Elliptic Curve Parameters

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

FRP256v1

Table 7: Legacy Algorithms

Legacy (L)
SHA-224: suitable until 31.12.2025 PKCS #1, v1.5: suitable until 31.12.2027

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). 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" [prEN 419 221-5], and
- „EN 419 241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing" [prEN 419 241-2].

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 (BV-SAM) and the firmware module NTP.

The BV-SAM was successfully evaluated (cf. [ETR BV-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 TÜV Rheinland Nederland BV under the certificate number **CC-19-222073** (cf. [CR_CP5]). This certificate is valid until 19-12-2023 (cf. [CR_CP5]). For this certification two Assurance Continuity Maintenance Reports issued by TÜV Rheinland Nederland BV are available (cf. [MA_CP5], [3MA1_CP5]). In both cases, the product was not changed. There were no changes in the hardware and software components of the Target of Evaluation (cf. [MA_CP5], [3MA1_CP5], section 2.2 in each case).

The certification at hand of the QSCD “BV-SAM on CryptoServer CP5” is valid until

December, 31st 2027

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

[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

[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)

[CR_CP5] TÜV Rheinland Nederland B.V., Certification Report NSCIB-CC-222073-CR, CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5, Se1500 5.1.0.0, Version 1.1, 14 March 2019

[MA_CP5] TÜV Rheinland Nederland B.V., Assurance Continuity Maintenance Report, Report Number NSCIB-CC-222073-MA, CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5, Se1500 5.1.0.0, Report Version 1, 21.04.2020

[3MA1_CP5] TÜV Rheinland Nederland B.V., Assurance Continuity Maintenance Report, Report Number NSCIB-CC-222073-3MA1, CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5, Se1500 5.1.0.0, Report Version 1, 20.11.2020

[ETR BV-SAM] SRC, Evaluation Report, Evaluation Technical Report (ETR), Bank-Verlag Signature Activation Module, Version 1.0, 25th January 2019

[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

[prEN 419 221-5] CEN/prEN 419 221-5:2016, Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, v0.15, 2016-11-29

[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

[ANSSI CRP] ANSSI, Rapport de certification ANSSI-CC-PP-2016/05 du profil de protection “Protection profiles for TSP Cryptographic modules - Part

5- Cryptographic Module for Trust Services" (prEN 419 221-5, version 0.15), 16.12.2016

[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

[prEN 419 241-1] CEN/prEN 419 241-1:2017, Trustworthy Systems Supporting Server Signing, Part 1: General System Security Requirements, v1.1.1, 24.08.2017, or newer version

[prEN 419 241-2] CEN/prEN 419 241-2:2017, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, 19.10.2017, or newer version

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

[RFC 2104] HMAC: Keyed-Hashing for Message Authentication, February 1997

[RFC 5639] M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03

[RFC 7519] JSON-based open standard, May 2015

[SOG-IS] SOG-IS Crypto Working Group; SOG-IS Crypto Evaluation Scheme; Agreed Cryptographic Mechanisms; Version 1.2, January 2020

[ST BV-SAM] achelos GmbH, BV-SAM Security Target, Version 0.6.0, 21.08.2018

[ST HW] Utimaco IS GmbH, CryptoServer Security Target Lite for CryptoServer Se-Series Gen2 CP5, Document Version 2.0.0, 23th November 2018

[UG_PRE] achelos GmbH, BV-SAM Preparative User Guidance, AGD_PRE, Version 0.0.1, 12.06.2018

[UG_OPE] achelos GmbH, BV-SAM Operational User Guidance, AGD_OPE, Version 0.0.8, 23.11.2018

5. Abbreviations

AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
CBC	Cipher Block Chaining
CC	Common Criteria
CID	Commission Implementing Decision
DH	Diffie-Hellman
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
DTBS	Data to be signed
DTBS/R	Representation of the data to be signed
EAL	Evaluation Assurance Level
EC / ECC	Elliptic Curve
ECB	Electronic Codebook
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	DSA on elliptic curve cryptography
eIDAS	electronic Identification, Authentication and trust Services
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
kid	Key ID
MAC	Message Authentication Code
MBK	Master Backup Key
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OID	Object Identifier
OFB	Output Feedback
OS	Operating System (Betriebssystem)
PCIe	Peripheral Component Interconnect Express
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PP	Protection Profile
PTRNG	Physical True Random Number Generator
QSCD	Qualified Signature Creation Device
	Qualified Seal Creation Device
RAD	Reference Authorisation Data
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Asymmetric Algorithm (Rivest, Shamir and Adleman)
SAD	Signature Activation Data
SAEK	SAM Authorised External Key
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SHA	Secure Hash Algorithm
SSA	Server Signing Application
ST	Security Target
TRNG	True Random Number Generator

TSP	Trust Service Provider
UUID	Universally Unique Identifier

End of certification report