Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 1/21

(Certification No.)

Prodotto: Primus HSM FW 2.8.21 Series E, Series X

(Product)

Sviluppato da: Securosys SA

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(AVA_VAN.5)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 14 aprile 2021

Fino a EAL2 *(Up to EAL2)*

Common Criteria

SOGIS IT SECURITY CERTIFIED

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Primus HSM FW 2.8.21 Series E, Series X

OCSI/CERT/CCL/04/2020/RC

Version 1.0

14 April 2021

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	14/04/2021

2 Table of contents

3 Acronyms

AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard - Galois/Counter Mode
API	Application Programming Interface
CAD	Computer Aided Design
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CNG	Cryptography API: Next Generation
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DPCM	Decreto del Presidente del Consiglio dei Ministri
DSA	Digital Signature Algorithm
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
eIDAS	Electronic IDentification, Authentication and Signature
EMS	Electronic manufacturing service
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
FW	Firmware
HSM	Hardware Security Module
HW	Hardware
ID	Identifier
IT	Information Technology
JCA/JCE	Java Cryptography Architecture / Java Cryptography Extension

KAS	Key Agreement Scheme
KDF	Key Derivation Function
KEK	Key Encryption Key
LCD	Liquid Crystal Display
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
MS CSP	Microsoft Cloud Solution Provider
NIS	Nota Informativa dello Schema
NTP	Network Time Protocol
OCSI	Organismo di Certificazione della Sicurezza Informatica
PCB	Printed Circuit Board
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SAM	Signature Activation Module
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SKA	Smart Key Attributes
SO	Security Officer
SOGIS	Senior Officials Group Information Systems Security
ST	Security Target

SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	Trust Service Provider
USB	Universal Serial Bus

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

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

[eIDAS] 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, Official Journal of the European Union L 257, 28 August 2014

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[ETR] “PRIMUS HSM FW 2.8.21 Series E, Series X” Evaluation Technical Report, v2, CCLab Software Laboratory, 25 March 2021

[PP] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, EN 419221-5:2018, May 2018

[LC] “Primus HSM Life-cycle support”, v1.01, Securosys SA, 16 February 2021

[ST] “PRIMUS HSM Security Target”, v1.02, Securosys SA, 19 March 2021

[UG] “Primus HSM User Guide”, V2.8 Edition 08, Securosys SA, December 2020

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA up to EAL4.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “Primus HSM FW 2.8.21 Series E, Series X”, also referred to in the following as “Primus HSM”, developed by Securosys SA.

The TOE is a physically secure HSM, i.e., a physical computing device that creates, safeguards, and manages digital keys for digital signatures and other cryptographic operations, with cryptographic toolkit functionality provided over multiple APIs (PKCS #11, JCE, CNG). The TOE includes all models of the E and X series of the Primus HSM.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister’s Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with AVA_VAN.5, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Primus HSM FW 2.8.21 Series E, Series X” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Primus HSM FW 2.8.21 Series E, Series X
Security Target	“PRIMUS HSM Security Target”, v1.02 [ST]
Evaluation Assurance Level	EAL4 augmented with AVA_VAN.5
Developer	Securosys SA
Sponsor	Securosys SA
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	EN 419221-5:2018 [PP]
Evaluation starting date	23 June 2020
Evaluation ending date	25 March 2021

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE “Primus HSM FW 2.8.21 Series E, Series X” (Primus HSM) is a physically secure HSM, i.e., a physical computing device that creates, safeguards, and manages digital keys for digital signatures and other cryptographic operations, with cryptographic toolkit functionality provided over multiple APIs (PKCS #11, JCE, CNG).

The TOE includes all models of the E and X series of the Primus HSM (also referenced as E-Modules and X-Modules, respectively).

All TOE Modules run the same firmware and differ only in storage and computing resources. According to the manufacturer, the Primus HSM meets and is already certified according to FIPS 140-2 overall Level 3 requirements.

Besides key management, the TOE performs a variety of authentication and encryption tasks. Primus HSM supports symmetric (AES, Camellia), asymmetric (RSA, DSA, ECC, Diffie-Hellman), and hashing (SHA-2, SHA-3) cryptographic algorithms. Primus HSM also contains a secure vault implemented inside a dedicated security chip, and also offers FIPS 140-2 Level 3 compliant tamper protection.

The TOE can be used as a Cryptographic Module by TSPs for signing, or sealing, operations and authentication services, as specified in Regulation (EU) 910/2014 [eIDAS]. The TOE can also be used as a general-purpose Cryptographic Module, providing network interfaces for external applications for many cryptographic functions, ranging from simple data encryption to identity management, PKI, strong authentication, and digital signature generation and verification.

For a detailed description of the TOE, consult sect. 3.4 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE Architecture

The physical forms of the Modules are depicted in Figure 1, Figure 2, Figure 3, and Figure 4. The boundary of the module includes the chassis and everything within. However, this does not include the removable power supplies on the X-Module; they are outside the TOE boundary and may be removed and replaced. The X-Module also relies on Smart Cards as external input/output devices, for the purposes of operator authentication.

Figure 1 - E-Module front with cryptographic boundary in red

Figure 2 - E-Module back with cryptographic boundary in red

Figure 3 - X-Module front with cryptographic boundary in red

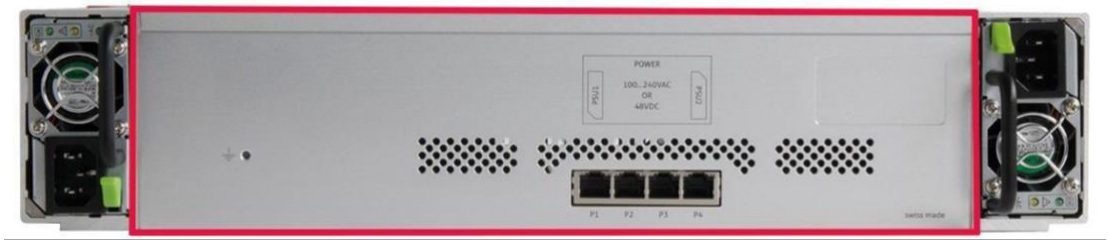

Figure 4 - X-Module back with cryptographic boundary in red

The logical scope of the TOE is depicted in Figure 5.

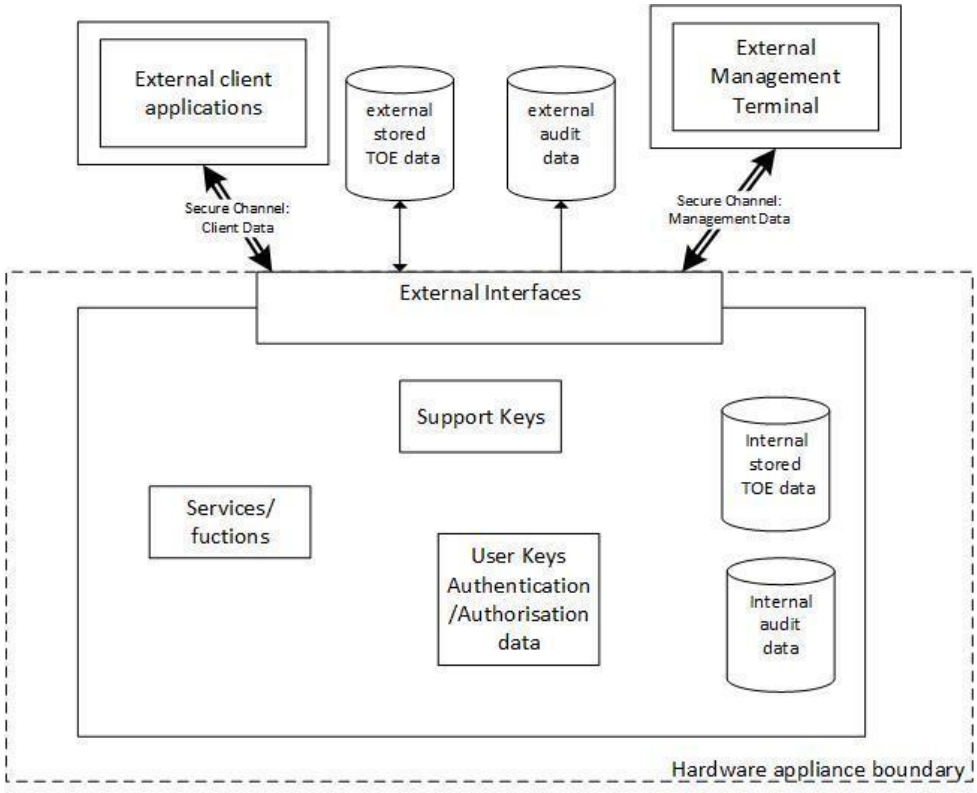

Figure 5 - TOE architecture

The hardware appliance boundary in Figure 5 represents the enclosure of the computing appliance which hosts the TOE.

The TOE implements separate authentication or authorisation of the following distinct types of entity:

- administrators of the TOE;
- application users of TOE cryptographic functions (external client applications, authenticated by their use of secure channels);
- users of secret keys (which in at least some cases need to have their use limited to a certain natural person or legal person).

7.3.1.1 Roles & Available Functions

The detailed Role description of Primus HSM is as follows:

- **Genesis**: Administrative role. Sets up the module. Performs factory reset.
- **Security Officer (SO)**: Administrative role which manages the module.
- **User** (client application): Technical User. This role is accessed through the API and provides general cryptographic functionality for the client application.
- **Partition SO** (Partition security officer): Administrative role which manages only a partition.

According to EN 419221-5 [PP] terminology Genesis, SO and Partition SO roles are the Administrators of the TOE.

The TOE supports external client applications. They use a channel that provides authentication of its end-points and protection of confidentiality and integrity of data sent on the channel.

Authorisation as a user (key owner) of a secret key before a key can be used in a cryptographic function (or exported), regardless of any other authorisation that may have been established for administrators or client applications can be done with Primus HSM's SKA (Smart Key Attributes) keys. If the client application is a certified SAM according to the PP EN 419241-2, the use of the normal keys is also allowed for signatures without the user (key owner) authorisation because in that case the sole control is guaranteed by the SAM.

Multiple users (client applications) can be registered to the TOE. Each user (client application) will have their separate partition of the TOE with their Partition Security Officers defined.

7.3.1.2 Non-TOE functionalities

Primus HSM includes the cloning and high availability clustering functions. Nevertheless, there are no requirements for cloning and high availability clustering use of the TOE in [PP]; these functions are not part of the TOE and out of the scope of the evaluation.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sects. 4 and 5 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 9 of the Security Target [ST]. The most significant aspects are summarized in the following.

7.3.2.1 Authorisation

The TOE requires identification and authentication of users before giving access to any security relevant function. There are four different roles in Primus HSM: Genesis, Security Officer, Partition Security Officer and User (client application). Genesis, Security Officer (SO) and Partition Security Officer (Partition SO) are considered the Administrators of the TOE. Users represent the remote client applications accessing the TOE via its API.

Administrators

The Administrators (Genesis, SO and Partition SO) authenticate themselves using their smart cards and PINs. In some types of the TOE (E-Series) the Administrators are using their “virtual” cards, but the authentication/authorisation process is the same. The operator inserts a Card and provides a PIN. The module retrieves and decrypts the correct PIN from the Card and compares it with the PIN entered by the operator. The PIN is 8-digits in length.

This method of authentication is impossible without possession of a valid Card. As such, false authentication would require a Card to be spoofed. Card integrity is provided by a 32-bit CRC across the internal data; both are stored encrypted with one of the Smart Card Keys. After four wrong tries of entering the PIN, the smart card becomes locked along with its Administrator account and there is no way of unblocking it.

Users

Security Officers can create new users (partitions). At creation, an identity belonging to this role is given the User Setup Password. User Setup Password is a temporary password. It consists of 25 alphanumeric characters, each of which can be any of 36 values (A-Z, 0-9). This password expires after three days by default.

After the first-time use with the User Setup Password, a User Secret is exchanged between the TOE and the User. This is a random 256-bit value for machine-to-machine authentication. This User Secret along with the user name is used to derive the trusted path for the Users in operational use. By default, after 100 failed login attempts to the TOE within 5 minutes the User becomes locked for 5 minutes. These values are configurable by Administrators. Also, the failed attempts are logged.

Key Owner

In case of SKA key, the key owner is identified by its digital signature. The public keys of the people who can authorise the keys are stored within the key attributes. This can be different for block, unblock, use and modify authorisation settings. On each request for the usage of the SKA key, the client application forwards the authorisation (signature). If the authorisation signature cannot be verified successfully for the selected operations the

authoriser will be blocked for 5 minutes. Therefore, the authoriser is not able to authorise any key in the TOE during this time.

Whenever a User tries to use one of its private keys a re-authentication is needed.

7.3.2.2 Key Management

The TOE supports the secure management of cryptographic keys necessary for its implemented cryptographic functions, including:

- key establishment (including key generation);
- protection of keys held within the TOE and held externally (for use by the TOE);
- control of access and use of keys by the cryptographic functions within the TOE;
- deletion of keys within the TOE.

The TOE handles System keys and user keys.

System keys

System keys are supporting the operation of the TOE. Encrypting keystore, backups, supports authentication, etc. Some system keys are generated in setup wizard and cannot be changed (KEK, Keystore Key, Genesis PIN, SO Card Keys, Backup Key). SO PINs are created when creating new SO. API keys are created when a new User (client application) is created. User keys are created by the client applications in operational state. Partition SO keys are generated by Security Officers during creating new users (new partitions). All those keys have their predefined format and size.

Administrators can create backup of the keystore therefore backing up the keys as well. They can restore the backup on the same device or on other devices as well. The keys can be exported for external storage as well but there is no way any key can leave the TOE in plain format. Both backups or wrapped keys leave the TOE only in encrypted format and protected by integrity and confidentiality. The backup and restore operation always need at least two Security Officers to be performed due to dual control.

User Keys

User keys are generated by the Users (client application) and they can be used for different purposes controlled by API commands. User keys can be generated, used and deleted by the Users. The supported algorithms, key sizes and operations can be found in sect. 3.4.2.3 of the Security Target [ST] (Table 7: Cryptographic Algorithms table).

User keys have many attributes and capabilities stored along with the keys. The capabilities and attributes store all information of the keys. For example: whether the key can be exported or not, whether the key is modifiable or deletable. Whether it is a private or public key, etc. Capabilities define what can be done with the keys. For example, the key can be used for encrypt, decrypt, sign, etc.

The different types of keys have their default values for all capabilities and flags but some of the values can be changed on creation (not all of them, for example an assigned key is never extractable).

Keys are destroyed according to FIPS 140-2 Level 3 zeroisation method.

SKA Keys

SKA Keys are special user keys implemented by Securosys. Smart Key Attributes feature allows for a fine-grained authorization of private key usage.

They have additional authorisation properties defining who can authorise the keys for different purposes. It can be defined who can block/unblock the key, who can use it and who can change the authorisation rules. With SKA Keys it is possible to identify the Signer (key owner not the client application).

7.3.3 Cryptographic functions

The TOE provides the following cryptographic functions:

- digital signature generation and verification;
- message digest generation;
- message authentication code generation and verification;
- encryption and decryption (symmetric and asymmetric);
- key generation;
- key agreement and distribution;
- key derivation;
- generation of shared secret values;
- cryptographic support for one-time password and other non-PKI based authentication mechanisms;
- random number generation.

The TOE implements the approved and allowed cryptographic functions listed in sect. 3.4.2.3 (Cryptographic Algorithms) of the Security Target [ST].

7.3.3.1 Crypto API

The Primus HSM provides a wide selection of application programming interfaces (PKCS #11, JCA/JCE, MS CSP) so that it can be used with almost any business application ranging from simple data encryption to identity management, PKI, strong authentication, and digital-signature generation and verification.

Cryptographic operations are available through the above-mentioned APIs for the Users (client application). The User role is accessed over the API (e.g., by business applications or clients) and serves to manage and use the User Keys. The User role may generate, load, and perform cryptographic operations with these keys.

User Keys, private, secret and public can only be accessed if the user (client application or in case of SKA keys the key owner) is authenticated. This includes listing of available keys or any other operation with keys.

Keys are destroyed according to FIPS 140-2 Level 3 zeroisation method.

7.3.3.2 Random number generation

The random number generator used by the TOE is composed of two main blocks:

- PTG.3 compliant entropy source, `block_cipher_df` (based on AES 256), SP800-90Ar1.
- DRG.4 compliant random number generator seeded by the above entropy source. This is HMAC-DRBG SP800-90Ar1 with SHA256.

The RNG provides forward secrecy, backward secrecy, enhanced forward secrecy as defined in DRG.4 class.

7.3.4 Audit/Administration

The TOE maintains the following roles: Administrator (Genesis, SO, Partition SO), User (External client application).

Key Users (key owner) are identified by a certified SAM according to [PP] outside the TOE or can be identified by the TOE if the client application uses SKA keys. SKA keys allow the TOE to identify the key owner itself, not only the client application.

SO can block User (client application) accounts by making them offline and unblock them making them online. Also, a SKA key can be blocked/unblocked if the User (key owner) has the block/unblock rules configured on the specific key but this operation is handled by the client application, the TOE only provides API for it.

The TOE logs each security relevant actions such as startup, shutdown, user authentication, all cryptographic operations and many more. Each error (if there are any) is audited during any security relevant functions. Each audit record contains a proper timestamp (NTP configuration available), the user ID who caused the event and the event type. Audit data is stored securely in a ring buffer. There is no deletion operation, but the oldest records are overwritten when the storage of audit records is full. Audit records can be deleted only by factory reset which is restricted to Administrator role. There is no way to modify any audit records. Administrators can export the audit logs to USB so they can back up the logs any time. Also, they can configure an external audit server (e.g., syslog). The TOE can forward the audit records to the external server. This channel is only for outgoing communication. The external server has no access to the TOE.

7.3.5 Secure Channels/Data Protection

7.3.5.1 Secure Channels

The TOE uses a special protocol for securing the communication with the external client applications and also with Decanus remote terminal. This protocol ensures the authentication and Diffie-Hellmann key agreement between the TOE and external entities.

The encryption algorithm for securing the communication uses different algorithms for securing the channel. KAS for key agreement, KDF to derive the session key and AES-CGM to encrypt the messages.

7.3.5.2 Integrity Protection

The TSF data is integrity protected by a checksum (64 Bit Hash), which is verified before each use of the key. The Keyfiles include the standard attributes (flags and capabilities) and the extended SKA Attributes (Authorizations). In case the hash doesn't match the operation cannot be processed and the user (client application) is notified that its data is corrupted.

Whenever a key is deleted all its attributes are also deleted. Whenever a User (client application with its partition) is deleted all its keys and configuration data are deleted.

7.3.5.3 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly, and that sensitive data have not been damaged (integrity). Power up self–tests are available on demand by power cycling the module. On power up, the Module performs many self-tests. It tests all the supported cryptographic algorithms (encryption/decryption/key generation/signature verification, etc.) Power up test also runs an integrity check on the firmware. All tests must be completed successfully prior to any other use of cryptography by the Module. If one of the tests fails, the Module enters the error state. Only after successful self-test and power up, the Ethernet goes up and the HSM is available to the user (client application).

Additionally, conditional tests are also available on the TOE. These tests run each time a condition occurs.

7.3.5.4 Physical protection

All critical CSPs are encrypted with KEK in the HSM. There are factory mounted tamper-evident seals on Primus HSM and a tamper-response mechanism is implemented which can zeroise KEK and the digital seal in the event of physical breach, therefore none of the keys can be used in the HSM. The TOE also has multiple sensors for detecting different types of tamper attacks. The TOE is protected against removing the cover, light detection or freeze attack with low or high temperature as well. The protection is FIPS 140-2 Level 3 compliant.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims strict conformance to the following Protection Profile:

- EN 419221-5:2018, Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services [PP]

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2]. In particular, considering that the Security Target claims strict conformance to the Protection Profile EN 419221-5:2018 [PP], all the SFRs from such PP are also included.

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory (Debrecen site).

The evaluation was completed on 25 March 2021 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 30 March 2021. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered

after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Primus HSM FW 2.8.21 Series E, Series X" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with AVA_VAN.5, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with AVA_VAN.5.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		Verdict
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Advanced methodical vulnerability analysis	AVA_VAN.5	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product “Primus HSM FW 2.8.21 Series E, Series X” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 5.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational security policies and the assumptions described, respectively, in sect. 4.4 and 4.5 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([UG]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

The delivery steps and the procedures that are necessary to maintain security when distributing the TOE to the customer are described in sect. 7 of the Life-cycle support document [LC].

The TOE Products are designed by Securosys. Hardware products are manufactured by an electronic manufacturing service (EMS) partner. The EMS receives the design documentation CAD files for the mechanics, PCB (Printed Circuit Board) design and bill of material for production. The EMS responsibility is to source the parts, produce and assemble the PCB, assemble the mechanics and ensure quality.

Partially assembled products are transported by the means of a trusted logistics provider from the EMS in a bulk package to the staging facility in the Securosys headquarters where the final assembly, verification and mating with secure software is performed.

In the staging process the initial setup with security critical software is done. The process is performed with background checked, security cleared personnel as it is critical for the security of the device. This is when the final assembly happens.

After purchasing a Primus HSM module from Securosys SA, the customer receives the TOE deliverable items described in Table 2.

Type	Description	Delivery method
HSM module	Both E and X series	Courier
Accessories	E-Series: • 1 power cable • 1 USB memory stick X-Series: • 2 power cable • 1 USB memory stick • 2 Genesis Card (GN) • 3 Security Officer (SO) Card	Courier
Guidance	QuickStart guide (PDF format)	Courier
Guidance	User Guide (PDF format)	Web Download
Firmware	Primus HSM Firmware 2.8.21 (.hsm - encrypted file format)	Courier (pre-installed) or Web Download

Table 2 - TOE Deliverables

To ensure integrity of the device the customer must follow the steps described in sect. 3 of the user guide [UG] (Setup). Identifying the TOE can be done with the following measures:

- The TOE is physically labelled so the type of the TOE (Primus HSM E/X) can be read.
- The TOE is secured by tamper detection during the whole delivery. Tamper detection can be checked upon receiving by visual inspection of the tamper proof sticker seals and validation of the digital seal on the Securosys Support Portal.
- TOE Firmware can be downloaded from Securosys Portal. After installation the FW version can be verified via console (`hsm_diagnostics frw` command) or front panel/Decanus under the menu System/Diagnostic/Firmware.
- The customer can validate the digital seal as described in sect. 3.1.4 of [UG]. This ensures the device has not been tampered with in transport. After the digital seal has been examined on the TOE the user has to rise a ticket on the Securosys Support Portal, containing the serial number and code on individual lines for several devices, to validate the digital seal(s).

9.2 Installation, initialization and secure usage of the TOE

TOE installation, configuration and operation should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the following document contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST]:

- “Primus HSM User Guide”, V2.8 Edition 08, December 2020 [UG]

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Primus HSM FW 2.8.21 Series E, Series X”, developed by Securosys SA. The TOE has been evaluated in the configuration described in sect. 3.4.1 of the Security Target [ST].

The TOE includes the following models of the Primus HSM:

- Series E: E20, E60, E150
- Series X: X200, X400, X700, X1000

All TOE models include the following firmware version:

- FW 2.8.21

The various TOE models differ only in storage and computing resources.

The following HW and SW components are non-TOE components and are excluded from the evaluation:

- Power supply (X-Module): the power supply is not considered security relevant.
- Decanus - Remote access Terminal: Decanus is the remote Administration Terminal for the Primus HSM.

10.1 TOE operation modes

The TOE can operate in 3 different modes:

- Normal mode
- FIPS 140-2 mode
- Restricted mode

Each mode and their characteristics are described in sect. 3.2.1. of the User Guide [UG]. In the evaluated configuration the TOE must be set either to Normal or FIPS mode during the initial setup. The Restricted mode has not been evaluated and shall not be used in a CC compliant configuration.

Furthermore, for CC compliance the user must follow the additional instructions and apply the special settings described in sect. 25.1 of [UG] (Appendix - Common Criteria operating instructions and conditions).

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL4, augmented with AVA_VAN.5, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage and level of detail;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

All testing activities have been carried out at the LVS premises on samples of the TOE provided by the Developer to the Evaluators.

The Evaluators received one instance of the main functional TOE from the E-Series and another one from the X-Series:

- PRIMUS HSM FW 2.8.21 Series E150 with operation mode normal, Firmware version RE-2.8.21, Rollback version V2.8.21, Bootloader version V02.08.0000-rel.
- PRIMUS HSM FW 2.8.21 Series X700 with operation mode normal, Firmware version RX-2.8.21, Rollback version V2.8.21, Bootloader version V02.08.0000-rel.

The main functionalities of the two TOE models are the same, the only difference is in resources and the X-Series has an LCD screen for configuration purposes.

The Evaluators examined the TOE and determined that it was consistent with the configuration under evaluation as specified in the Security Target [ST].

The Evaluators created the test environment according to the description in the Security Target [ST] and the Developer's test documentation. The Evaluators configured only one Master TOE as the high availability and cloning capabilities are out of the TOE boundary and not part of the evaluation.

The Evaluators checked the TOE integrity, then set up and configured the HSM modules applying the preparation procedures described in [UG] which provide detailed information for secure installation of the TOE and all the necessary configuration steps. The Evaluators was able to prepare the TOE securely using only the supplied preparative procedures.

After the installation, the Evaluators checked the status of the TOE and verified that it was installed properly and in a known state.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer performed manual and automated tests to verify the functionality of the TOE. The functional testing approach is to test all TSFI and enforce all SFRs during TOE testing.

The Developer created automatic and manual test cases. The tests are performed by the Developer through execution of test scripts and a testing application. Automated test can also be repeated manually based on the test case descriptions.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements (SFR) and the TSFIs described in the functional specification.

11.2.3 Test results

The Evaluators executed the automated test cases provided by the Developer on the test environment which was also provided by the Developer.

The Evaluators verified the correct behaviour of the TSFIs and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the Evaluators

The Evaluators selected the tests aiming to test the TOE in depth and created own test cases to further increase the tested functionalities of the TOE, resulting in a more rigorous coverage of the tested functionalities. The Evaluators also tried to select those test cases, which could cover most of the related modules.

The Evaluators executed the electronic signature and electronic seal operations provided by the TOE and confirmed that the signatures and seals returned by the TOE correspond to the correct DTBS.

Software and/or firmware updates are supported by the TOE, hence the Evaluators carried out tests to ensure that only updates with valid digital signatures can be installed on the TOE.

The testing results show that the TOE exhibits the expected behaviour. No deviations were found.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the same TOE samples already used for the functional test activities, verifying that the test configuration were consistent with the version of the TOE under evaluation.

The Evaluators designed tests to meet the requirements of AVA_VAN.5. The Evaluators based the analysis on a source code review, and employed a fuzzing strategy to test the functionality of a subset of the TSFIs instead of testing all of the interfaces.

The Evaluators reviewed the Developer documents to find some areas of concern, then conducted searches on public sources, identifying a number of potential vulnerabilities. The Evaluators verified during the site visit that the corresponding patches are applied, hence the TOE is not vulnerable to any publicly known vulnerability.

The Evaluators then performed an advanced methodical vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify potential vulnerabilities in the TOE.

The Evaluators' analysis focused on the following aspects, identifying several potential vulnerabilities:

- buffer overflow;
- code injection;
- format string injection;
- null byte injection.

The Evaluators found a buffer overflow vulnerability during the code review part of the site visit, but the Developer has patched it already and provided a new TOE firmware. The Evaluators also tested other possible buffer overflows, but none of them resulted in successful bypass.

The Evaluators examined the source code, searching for code injections and did not find any cases when user input could reach a dangerous function.

The Evaluators tried several payloads that could result in format string injection vulnerability and also reviewed the source code but did not find any cases that could be exploitable.

At the end of all the penetration testing sessions, the Evaluators could conclude that no attack scenario with potential High or lower can be completed successfully in the operating environment of the TOE as a whole. Therefore, none of the previously identified potential vulnerabilities can be exploited effectively.

The Evaluators also reviewed other parts of the TOE source code and TOE related documentation manually and managed to identify two residual vulnerabilities:

- null byte injection resulting in insufficient logging;
- null byte injection resulting in keys that cannot be deleted.

Both these vulnerabilities can be exploited only by an attacker with attack potential beyond High.