Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) ver .3.1 rel. 5

Certificato n. *(Certificate No.)*	02/2026
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/07/2023/RC, v 1.1
Decorrenza *(Date of 1st Issue)*	23 gennaio 2026
Nome e Versione del Prodotto *(Product Name and Version)*	Primus HSM Firmware 2.8.22 Series E, Series X
Sviluppatore *(Developer)*	Securosys SA
Tipo di Prodotto *(Type of Product)*	Prodotti per firme digitali (Products for Digital Signatures)
Livello di Garanzia *(Assurance Level)*	EAL4+ (AVA_VAN.5) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	EN 419221-5:2018, Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services
Funzionalità di sicurezza *(Conformance of Functionality)*	Funzionalità conformi a PP, CC Parte 2 estesa

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 27 gennaio 2026

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando Metodologia Comune per la Valutazione di Sicurezza della tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Primus HSM Firmware 2.8.22

Series E, Series X

OCSI/CERT/CCL/07/2023/RC

Version 1.1

27 January 2026

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute 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	23/01/2026
1.1	OCSI	Editorial revision	27/01/2026

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

AES	Advanced Encryption Standard
AES-GCM	Advanced Encryption Standard - Galois/Counter Mode
CAD	Computer Aided Design

CNG	Cryptography API: Next Generation
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EMS	Electronic manufacturing service
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
JCA/JCE	Java Cryptography Architecture / Java Cryptography Extension
KAS	Key Agreement Scheme
KDF	Key Derivation Function
KEK	Key Encryption Key
MS CSP	Microsoft Cloud Solution Provider
NTP	Network Time Protocol
PCB	Printed Circuit Board
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SAM	Signature Activation Module
SKA	Smart Key Attributes
SO	Security Officer

4 References

4.1 Normative references and national Scheme documents

[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

[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. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 - Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

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

4.2 Technical documents

[CCGUIDE] Primus HSM User Guide, Version 2.8, Edition 08.6, September 2025.

[CR] Certification Report for Primus HSM FW 2.8.21 series E, series X, April 14th 2021.

[ETRv1] Final Evaluation Technical Report Re-evaluation of PRIMUS HSM FW 2.8.22 Series E, Series X Assurance Level EAL4 augmented with AVA_VAN.5, v1, 21st October 2025.

[ETRv2] Final Evaluation Technical Report Re-evaluation of PRIMUS HSM FW 2.8.22 Series E, Series X Assurance Level EAL4 augmented with AVA_VAN.5, v2, 4th December 2025.

[LC] Primus HSM Life-Cycle support, version 2.0, 8th October 2025.

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

[ST] Securosys SA Primus HSM Security Target version 2.0, 10th October 2025.

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 recognised under the terms of this agreement by signatory nations.

This certificate is recognised under SOGIS-MRA for all claimed assurance components 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] was ratified on 8 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 EAL2, 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 for all claimed assurance components up to EAL2.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**PRIMUS Hardware Security Module with Firmware 2.8.22 Series E, Series X**" (also referred in this document as "Primus HSM FW 2.8.22"), developed by Securosys SA.

The TOE is a hardware security module (HSM) which is a physical computing device that creates, safeguards, and manages digital keys for digital signatures and other cryptographic operations. The TOE performs a variety of authentication and encryption tasks supporting symmetric (AES, Camellia), asymmetric (RSA, DSA, ECC, Diffie-Hellman), and hashing (SHA-2, SHA-3) cryptographic algorithms provided over multiple APIs (PKCS11, JCE, CNG). The TOE includes the "E" series models 20, 60 250 and the "X" series models 200, 400, 700. 1000 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, NIS5]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

This Certification Report was issued at the conclusion of the re-certification of an earlier version of the same TOE (Primus HSM FW 2.8.21 series E and series X), already certified by OCSI (Certificate no. 01/2021 of April 21, 2021 [CR]).

The TOE had minor changes in the root key storage with a zeroization of the communication key required to talk to the IC and of the root key store. There are no changes to the environment of the TOE with respect to the previous certification.

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 version 3.1 Revision 5 for the assurance level EAL4, augmented with AVA_VAN.5, and with the Protection Profile (PP) "*Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, EN 419221-5:2018* [PP 419221-5]*"* 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 named "Primus HSM FW 2.8.22" 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 also review the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Primus HSM FW 2.8.22
Security Target	Securosys SA Primus HSM Security Target, Version: 2.0, v.2.0 October 10th, 2025
Evaluation Assurance Level	EAL4 augmented with AVA_VAN.5
Developer	Securosys SA
Sponsor	Securosys SA
LVS	CCLab Software Laboratory, Debrecen site
CC version	3.1 Rev. 5
PP conformance claim	Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, EN 419221-5:2018
Evaluation starting date	December 11th 2023
Evaluation ending date	October 22nd 2025

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 and, in the configuration, shown in "Annex B – Evaluated configuration" of this Certification Report.

7.3 Evaluated product

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

The Target of Evaluation (TOE) is Primus HSM FW 2.8.22 with the software components as described in Table 2, sect. 9.1.1.

The TOE is a hardware security module (HSM) which is a physical computing device that creates, safeguards, and manages digital keys for digital signatures and other cryptographic operations. the TOE performs a variety of authentication and encryption tasks supporting symmetric (AES, Camellia), asymmetric (RSA, DSA, ECC, Diffie-Hellman), and hashing (SHA-2, SHA-3) cryptographic algorithms provided over multiple APIs (PKCS11, JCE, CNG). The TOE includes the "E" series models 20, 60 250 and the "X" series models 200, 400, 700. 1000 of the Primus HSM.

The TOE generates cryptographic keys, stores these keys, and manages the distribution of these keys. The TOE also contains a secure vault implemented inside a dedicated security chip and also offers FIPS-140-2 Level3 compliant tamper protection.

For a more detailed description of the TOE, please refer to sect. “*TOE description*” of the Security Target [ST].

7.3.1 TOE architecture

The physical forms of the Module 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 boundary and may be removed, or replaced. The X-Module also relies on Smart Cards as external input/output devices, for the purposes of operator authentication.

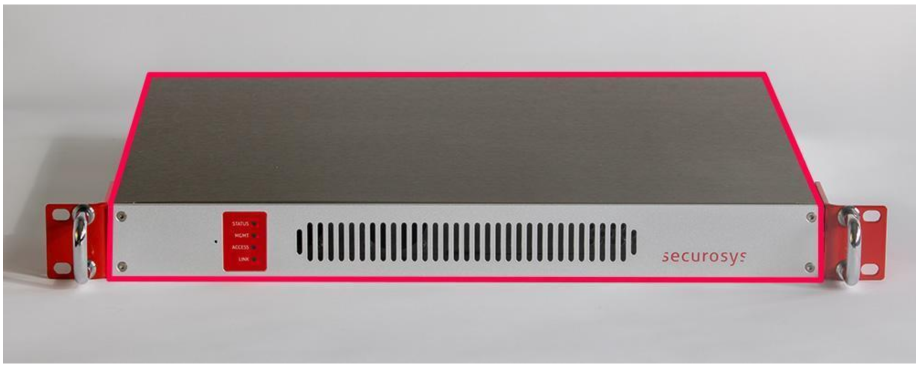

Figure 1 - E-Module front with cryptographic boundary in red.

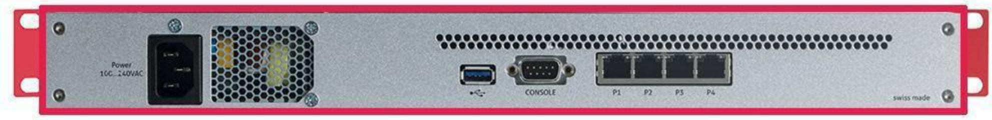

Figure 2 - E-Module back with cryptographic boundary in red.

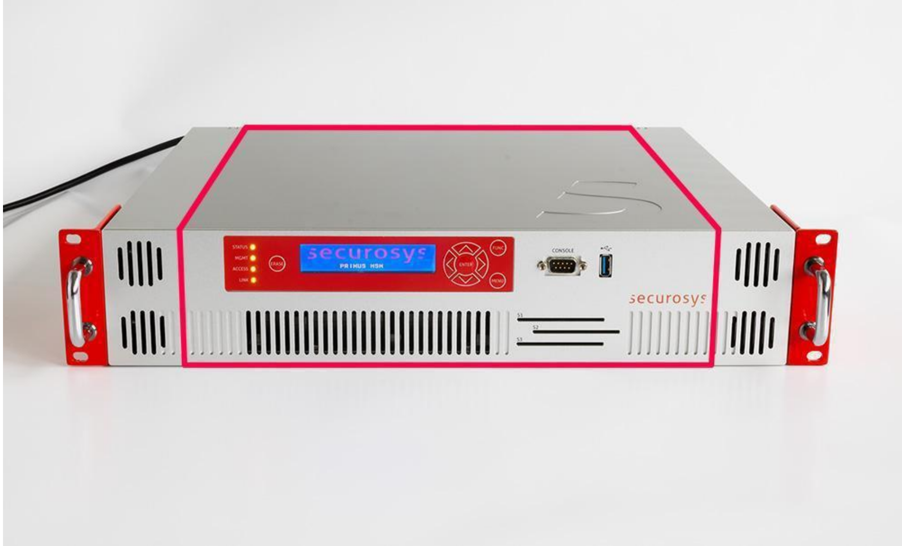

Figure 3 - X-Module Front with cryptographic boundary in red.

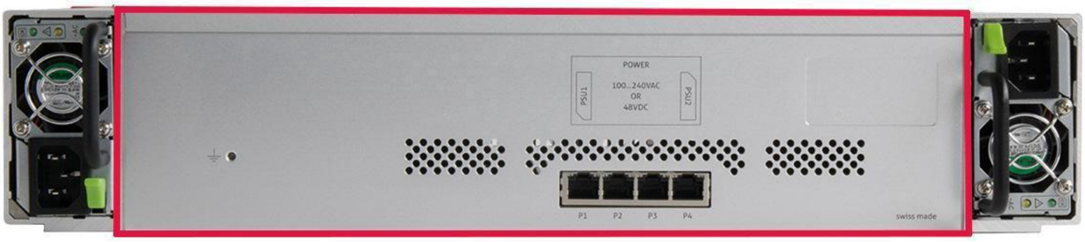

Figure 4 - X-Module back with cryptographic boundary in red.

The logical scope of the TOE is the represented in Figure 5 based on [ST]:

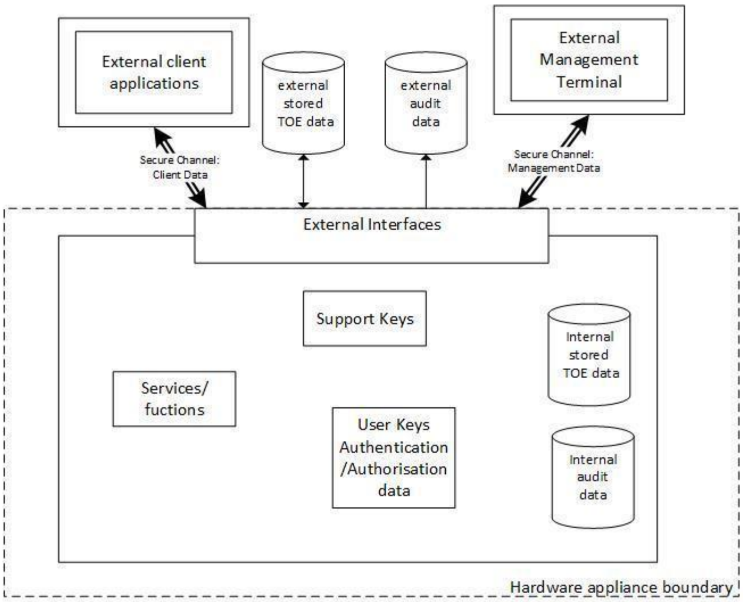
External client applications
external stored TOE data
external audit data
External Management Terminal
Secure Channel: Client Data
Secure Channel: Management Data
External Interfaces
Support Keys
Internal stored TOE data
Services/ fuctions
User Keys Authentication /Authorisation data
Internal audit data
Hardware appliance boundary

Figure 5 - TOE Architecture.

Primus HSM includes the cloning and clustering functions. Nevertheless, there are no requirements for cloning and clustering use of the TOE in [PP 419221-5]; **these functions are not part of the TOE and out of the scope of the evaluation**.

7.3.2 TOE security features

The primary security features of the TOE are:

- Authorisation
- Key Management
- Cryptographic functions
- Audit/administration
- Secure Channels/Data Protection

7.3.2.1 Authorisation

The TOE requires identification and authentication 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 the E-Series) TOE 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 dimension of the PIN is 8-digits.

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. 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 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 as the User wants to use them 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 Table 7: Cryptographic Algorithms table in the [ST].

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, and sign.

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 as there are rules, 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).

7.3.2.3 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].

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

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 AES256), 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

7.3.2.4 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 (Signature Activation Module) according to [PP 419221-5] 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 unblocking 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.

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 (eg. 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.

The timestamps for the audit logs are reliable. The TOE supports connection to multiple NTP servers and verifies the received timestamp.

7.3.2.5 Secure Channels/Data Protection

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.

Integrity Protection

The integrity of TSF data is 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, it is deleted with all its attributes. Whenever a User (client application with its partition) is deleted, it is deleted with all its keys and configuration data.

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 (e.g. encryption/decryption/key generation/signature verification). 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. The system uses simple memory comparison to test the value of a test against its expected value. In cases where the comparison operation could be used for side channel attacks, the memory compare function is expanded in a way to compare all bytes instead of just until the first mismatch. 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 when a condition occurs.

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 because. 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 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 of 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 section 9 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does 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 419221-5].

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected or derived from CC Part 3 [CC3]. This includes ALC_TSU_EXT.1.1 - Timely Security Updates, as defined in [VPP].

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 419221-5], all the SFRs from such PP are also included

It is possible to refer to the Security Target [ST] for the description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFRs) 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 [NIS5] 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 October 22nd, 2025 with the issuance by LVS of the Evaluation Technical Report [ETRv1] that has been approved by the Certification Body on 20 November 2025. On 5 December, the LVS has provided an updated version of the ETR [ETRv2] to apply some minor changes. 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; there is a probability 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 regularly check 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 v.2 [ETRv2] issued by CCLab Software Laboratory (Debrecen Site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named “PRIMUS HSM FW 2.8.22” 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 components reported in the assurance level EAL4 augmented with AVA_VAN.5 (In *Italics* are reported the augmented assurance components).

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 descriptio	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
Identification of security measure	ALC_DVS.1	Pass

Assurance classes and components		**Verdict**
Developer defined life-cycle mode	ALC_LCS.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: modular design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - Conformance	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 section 6 (Statement of Certification).

Potential customers of the product “PRIMUS HSM FW 2.8.22” are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the “*Objectives for the Operational Environment*” specified in section 5.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the organizational security policies and assumptions described, respectively, in section 4.4 and 4.5 of the Security Target [ST] shall be satisfied.

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, installation, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE.

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

9.1.1 Scope of TOE supply

The following table contains the item that comprise the different elements of the TOE.

No	Type	Descritpion	Release/Version	Form of Delivery
1	HSM module	HSM module Both E and X series and accessories (Genesis Card, Security Officer Card)	FW 2.8.22	Courier
2	Guidance	QuickStart guide (PDF format)		Courier
3	Guidance	User Guide (PDF format) [CCGUIDE]]	Version 2.8, Edition 08.6	Web Download
4	Firmware	Primus HSM Firmware 2.8.22 (.hsm - encrypted file format)	2.8.22	Courier (pre-installed) or Web Download

Table 2 - TOE Deliverables

9.1.2 Delivery procedure

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 SA. 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 SA 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.

9.2 Identification of the TOE by the user

To ensure integrity of the device the customer must follow the steps described in sect. 3 of the user guide [CCGUIDE] (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 [CCGUIDE]. 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).

9.3 Installation, configuration and secure usage of the TOE

TOE installation, configuration and secure usage should be done by following the instructions in the appropriate sections of the guidance documentation [CCGUIDE] provided with the product to the customer.

10 Annex B – Evaluated configuration

The Target of Evaluation is “PRIMUS HSM FW 2.8.22 Series E, Series X”, developed by Securosys SA. The TOE is accompanied by guidance documentation. The items listed in Table 2 represent the TOE.

The TOE name and version number uniquely identify the TOE and its components, which constitute the evaluated configuration of the TOE verified by the Evaluator at the time they perform the tests and to which the evaluation results apply.

10.1 TOE operational environment

The assumptions about the technical environment in which the TOE is intended to be used are reported in section 5.2 of [ST].

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

The test systems were running PRIMUS HSM FW 2.8.22 in the evaluated configuration.

All testing activities have been carried out remotely at the LVS premises on samples of the TOE provided by the Developers to the evaluator.

The Evaluators examined the TOE and determined that it was consistent with the configuration under evaluation as specified in the Security Target [ST] and in [CCGUIDE]. The Evaluators created the test environment according to the description in the Security Target [ST] and the Developer's test documentation.

11.2 Functional tests performed by the Developer

The Developer prepared a program that automatically tested the correct operation of the TSFI.

The tests were performed on both devices, which the manufacturer used to distinguish between "X" and "E".

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

The Evaluators performed the all the automated test on the E series E20 while some of them were performed manually to validate the results of the automated tests.

In addition to the Developer's test, the Evaluators devised and performed 4 more independent test cases to test the TSF more in depth.

11.3.2 Test results

All test cases devised by the Evaluators were run successfully and all the test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked on the test environment and TOE already used for the functional test activities, verifying that the TOE and the test environment were properly configured.

The Evaluator analysed the Security Target [ST], design documentation, and test results for potential vulnerabilities. In addition, the Evaluators performed a search on public sources for known or claimed potential vulnerabilities of the TOE or components of the TOE.

Twelve potential vulnerabilities have been investigated: after the exclusion of the ones mitigated by the environment, remaining vulnerabilities the Evaluators devised an attack method and calculated the respective attack potential. These where related to buffer overflows exploitations, command injections, memory exploitations (write/read in arbitrary locations), logging exploitation, user enumerations, keys modifications, unencrypted application data disclosure, privilege escalation, exploitation in weakenesses in Generic Key lifecycle.

No attack resulted in a vulnerability.

The Evaluators could then conclude that the TOE is resistant to an attack potential **High** in its intended operating environment. No exploitable or residual vulnerabilities have been identified.