



Agenzia per la Cybersicurezza Nazionale



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) CC:2022 Release 1

Certificato n. (Certificate No.)	13/2026
Rapporto di Certificazione (Certification Report)	OCSI/CERT/CCL/01/2025/RC, v 1.0
Decorrenza (Date of 1 st Issue)	23 febbraio 2026
Nome e Versione del Prodotto (Product Name and Version)	Primus HSM FW 3.1.0 Series E, Series E2, Series X, Series X2
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, Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services, EN 419241-2, Trustworthy Systems Supporting Server Signing - Part 2
Funzionalità di sicurezza (Conformance of Functionality)	Funzionalità conformi a PP, conforme a CC Parte 2



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, 23 febbraio 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 CEM:2022 Release 1 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione CC:2022 Release 1. 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 CEM:2022 Release 1 for conformance to Common Criteria for Information Technology Security Evaluation version CC:2022 Release 1. 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 FW 3.1.0 Series E, Series E2, Series X, Series X2

OCSI/CERT/CCL/01/2025/RC

Version 1.0

23 February 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	23/02/2026

2 Table of contents

1	Document revisions	3
2	Table of contents	4
3	Acronyms.....	6
3.1	National scheme.....	6
3.2	CC and CEM.....	6
3.3	Other acronyms.....	6
4	References	8
4.1	Normative references and national Scheme documents	8
4.2	Technical documents	8
5	Recognition of the certificate	10
5.1	European recognition of CC certificates (SOGIS-MRA).....	10
5.2	International recognition of CC certificates (CCRA).....	10
6	Statement of certification.....	11
7	Summary of the evaluation.....	12
7.1	Introduction.....	12
7.2	Executive summary	12
7.3	Evaluated product	12
7.3.1	TOE architecture	13
7.3.2	TOE security features	15
7.4	Documentation.....	20
7.5	Protection Profile conformance claims.....	20
7.6	Functional and assurance requirements	20
7.7	Evaluation conduct	20
7.8	General considerations about the certification validity	21
8	Evaluation outcome	22
8.1	Evaluation results.....	22
8.2	Recommendations.....	23
9	Annex A – Guidelines for the secure usage of the product	24
9.1	TOE delivery	24
9.1.1	Delivered items.....	24
9.1.2	Delivery procedure	24
9.2	Identification of the TOE by the user	25
9.3	Installation, configuration and secure usage of the TOE.....	25

10	Annex B – Evaluated configuration	26
10.1	TOE operational environment	26
11	Annex C – Test activity	27
11.1	Test configuration	27
11.2	Functional tests performed by the Developer	27
11.2.1	Testing approach	27
11.2.2	Test coverage.....	27
11.2.3	Test results.....	27
11.3	Functional and independent tests performed by the Evaluators	27
11.3.1	Test approach	27
11.3.2	Test results.....	28
11.4	Vulnerability analysis and penetration tests	28

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-CGM	Advanced Encryption Standard - Galois/Counter Mode
API	Application Programming Interface
CAD	Computer Aided Design
CLI	Command Line Interface
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
FW	FirmWare
GN	Genesis Card
HMAC-DRBG	Hash-based Message Authentication Code Deterministic Random Bit Generator
HSM	Hardware Security Module
ICSF	Integrated Cryptographic Services Facility
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
PDF	Portable Document Format
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
QSCD	Qualified Signature/Seal Creation Device
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SKA	Smart Key Attributes
SO	Security Officer
SSH	Secure Shell
TLS	Transport Layer Security
TSP	Trust Service Provider
USB	Universal Serial Bus

4 References

4.1 Normative references and national Scheme documents

- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, November 2022, CC:2022 Revision 1 CCMB-2022-11-001
- [CC2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, November 2022, CC:2022 Revision 1 CCMB-2022-11-002
- [CC3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, November 2022, CC:2022 Revision 1 CCMB-2022-11-003
- [CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, November 2022, CC:2022 Revision 1 CCMB-2022-11-004
- [CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, November 2022, CC:2022 Revision 1 CCMB-2022-11-005
- [CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, July 2014
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, November 2022, CC:2022 Revision 1 CCMB-2022-11-006
- [EN 419221-5] Protection Profiles for TSP Cryptographic modules – Part 5: Cryptographic Module for Trust Services, EN 419221 - 5:2018, May 2018
- [EN 419241-2] Trustworthy Systems Supporting Server Signing –Part 2: Protection Profile for QSCD for Server Signing, EN 419241-2:2019, February 2019
- [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
- [SOGIS] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3, January 2010

4.2 Technical documents

- [AGD] Primus HSM User Guide Edition 29 (v3.1, v3.2) , October 2025

- [ETR2] Evaluation of Primus HSM FW 3.1.0 Series E, Series E2, Series X, Series X2 according to CC Assurance Level EAL4 augmented with AVA_VAN.5, PRIMUS31-028_ETR_v2, CCLab – The Agile Cybersecurity Laboratory, Version: v2, 13th January 2026

- [ETR3] Evaluation of Primus HSM FW 3.1.0 Series E, Series E2, Series X, Series X2 according to CC Assurance Level EAL4 augmented with AVA_VAN.5, PRIMUS31-028_ETR_v3, CCLab – The Agile Cybersecurity Laboratory, Version: v3, 16th February 2026

- [FIPS-140-3] Security Requirements for Cryptographic Modules, 22nd March 2019

- [LC] Primus HSM Life-cycle support version 2.3, 24th September 2025

- [ST] Securosys SA Primus HSM Security Target, Version: 3.1, 28th 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 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 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 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named “**Primus HSM FW 3.1.0 Series E, Series E2, Series X, Series X2**”, also referred as Primus HSM or Primus HSM 3.1, developed by Securosys SA.

The Target of Evaluation (TOE) is a physically secure HSM with cryptographic toolkit functionality provided over multiple APIs (PKCS11, JCE, CNG). The HSM is a physical computing device that creates safeguards and manages digital keys for digital signatures and other cryptographic operations. The TOE software implements the Signature Activation Protocol (SAP). It uses the Signature Activation Data (SAD) from the signer to activate the corresponding signing key. The TOE (as a SAM and a CM) is a QSCD. It can also be used as a standalone CM and can be connected to another external SAM.

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 and Scheme Information Notes [NIS1, NIS2, NIS3, NIS4]. 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).

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 CC:2022 Release 1 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]”, and Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, EN 419241-2:2019 [PP 419241-2], 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], [CC5]) 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 3.1.0 Series E, Series E2, Series X, Series X2” 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 3.1.0 Series E, Series E2, Series X, Series X2
Security Target	Securosys SA Primus HSM Security Target, Version: 3.1 October 28 th , 2025 [ST]
Evaluation Assurance Level	EAL4, augmented with AVA_VAN.5
Developer	Securosys SA
Sponsor	Securosys SA
LVS	CCLab – The Agile Cybersecurity Laboratory (Debrecen site)
CC version	CC:2022 Release 1
PP conformance claim	Protection profiles for TSP Cryptographic modules - Part 5, EN 419221- 5:2018 [EN 419221-5] Trustworthy Systems Supporting Server Signing – Part 2, EN 419241-2:2019 [EN 419241-2]
Evaluation starting date	January 24, 2025
Evaluation ending date	January 13, 2026

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 it is possible to refer to the Security Target [ST].

The TOE is the Primus HSM which is a physically secure HSM with cryptographic toolkit functionality provided over multiple APIs (PKCS11, JCE, CNG). The HSM is a physical computing

device that creates safeguards and manages digital keys for digital signatures and other cryptographic operations.

The TOE software implements the Signature Activation Protocol (SAP). It uses the Signature Activation Data (SAD) from the signer to activate the corresponding signing key. The TOE (as a SAM and a CM) is a QSCD. It can also be used as a standalone CM and can be connected to another external SAM.

The TOE is not only one product but the whole E, E2, X and X2 series of the Primus HSM. All products of the series run the same firmware and differ only in storage and computing resources. Everything else is the same.

The evaluated types of Primus HSM are the following:

- Series E: E20, E60, E150, ED250, EP700
- Series X: X200, X400, X700, X1000, X2000
- Series E2: E2-C914, E2-LX212
- Series X2: E2Y-C914, E2Y-LX212

For a detailed description of the TOE, refer to section 3.4 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, 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 and X2-Module – they are outside the boundary and may be removed, replaced, etc. The X-Module and X2 also rely on Smart Cards as external input/output devices, for the purposes of operator authentication.

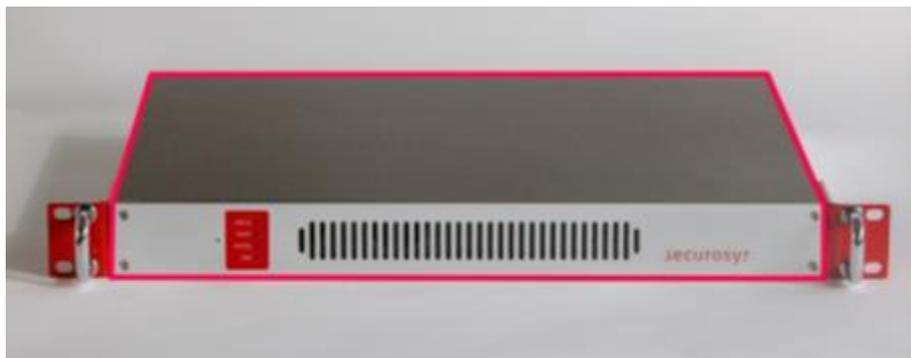


Figure 1 - E-Module front with cryptographic boundary in red.



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 TOE consists of the following subsystems and their modules:

- admin subsystem and its modules,
- crypto subsystem and its modules,
- audit subsystem,
- device protection subsystem,
- time subsystem.

The architecture of the TOE is the represented in Figure 5 based on [ST].

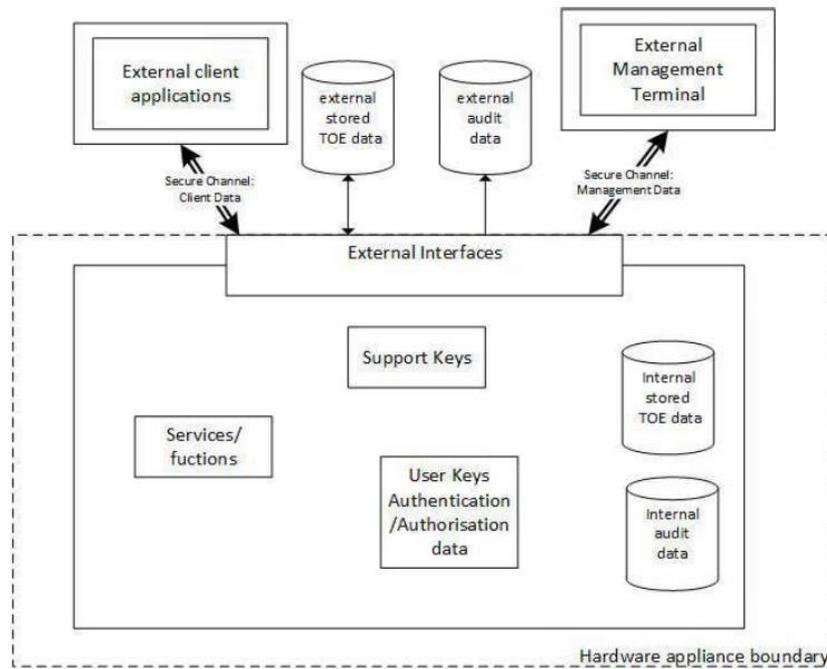


Figure 5 - TOE Architecture

7.3.2 TOE security features

According to the [ST] section 3.3.1.1 “Usage and major security features of the TOE” and section 9 “TOE Summary Specification” the primary security features of the TOE are:

- Authorization
- Key Management
- Cryptographic functions
- Audit/Administration
- Secure Channels/Data Protection

7.3.2.1 Authorization

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 of TOE 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 long.

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

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.

Privileged 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 (Signer)

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 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 to 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.

Destroying keys are according to FIPS-140-3 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;
- Key Zeroisation according to [FIPS-140-3].

The TOE implements the approved and allowed cryptographic functions listed in sect. 3.4.2.4 (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. The units can be installed, configured, and integrated into existing networks.

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.

Destroying keys are according to FIPS-140-3 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 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 (Security Officer) 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 140-3 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 section 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] claims strict conformance with the following Protection Profiles:

- EN 419221-5:2018, Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services [EN 419221-5]
- EN 419241-2:2019, Trustworthy Systems Supporting Server Signing – Part 2: Protection Profile for QSCD for Server Signing [EN 419241-2]

7.6 Functional and assurance requirements

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3] and are from EAL 4 assurance package, augmented with the CC part 3 component AVA_VAN.5.

All the SFRs have been selected from CC Part 2 [CC2].

It is possible to 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 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 – The Agile Cybersecurity Laboratory (Debrecen site).

The evaluation was completed on January 13th, 2026, with the issuance by the LVS of the approved Evaluation Technical Report [ETR2].

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 Body recommends reviewing the assumptions in the [ST], section 4.5, which are necessary conditions to be implemented for the TOE security.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, 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 [ETR2] issued by the LVS CCLab – The Agile Cybersecurity 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 3.1.0 Series E, Series E2, Series X, Series X2” meets the requirements of Part 2 and 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 (augmentation in *italics* in Table 1).

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
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 measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass

Assurance classes and components		Verdict
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
<i>Advanced methodical vulnerability analysis</i>	<i>AVA_VAN.5</i>	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 3.1.0 Series E, Series E2, Series X, Series X2” 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 “Security 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 Assumptions described in section 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 ([AGD]).

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 Delivered items

The following table contains the items included the TOE, including software elements and documentation.

Type	Description	Delivery
HSM Module	All E, X, E2, X2 series	Courier
Accessories	<p>E and E2-Series</p> <ul style="list-style-type: none"> - power cable(s) - 1 USB memory stick <p>X and X2-Series</p> <ul style="list-style-type: none"> - 2 power cables - 1 USB memory stick - 2 Genesis Card (GN) - 3 Security Officer (SO) Card 	Courier
Guidance	QuickStart guide (printed format)	Courier
Guidance	User Guide (.pdf format) [AGD] ¹	Web Download
Firmware	Primus HSM Firmware 3.1.0 (.hsm - encrypted file format)	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 elements 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

¹ Completely contains “QuickStart guide”.

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.

After final assembly the devices are monitoring for tamper with a built-in battery tamper circuitry.

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 as described in the user guide.

In summary these are:

- identification of the customer, independent of the delivery chain logistics;
- use of genesis card (GN) for setup. The GN card is uniquely mated with the device. To set the PIN of the GN card the customer requires an activation secret. In order to get this secret the customer has to be identified and access to the customer portal granted. The process ensures identification of the customer and prevents exchange of devices in the delivery chain;
- validation of physical integrity of the device. The customer is required to validate the integrity of the physical device visually and validate the integrity of the physical security tamper seals;
- the customer can validate the digital seal. This ensures the device has not been tampered with in transport.

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;
- the 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.

9.3 Installation, configuration and secure usage of the TOE

TOE installation, configuration and secure usage must be performed following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

In particular, the document [AGD] contain detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure usage of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Target of Evaluation is “Primus HSM FW 3.1.0 Series E, Series E2, Series X, Series X2”, 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 Evaluators at the time they perform the tests and to which the evaluation results apply.

Refer to “Chapter 3: Setup” of the [AGD] for instructions on installing the TOE.

10.1 TOE operational environment

The assumptions about the operational environment in which the TOE is intended to be used are reported in section 4.5 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

Testing activities have been carried out in LVS premises.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the AGD documentation [AGD] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer performed extensive tests to verify the functionality of the TOE. The tests cover all Subsystems, Modules and TSFIs of the TOE.

The following aspects of the TSF are covered by the tests:

- Authorization
- Key Management
- Cryptographic functions
- Audit/Administration
- Secure Channels/Data Protection

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 (SFRs) and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behaviour and the properties of the TSF.

11.2.3 Test results

All Developer's tests were run successfully, and the Evaluators verified the correct behaviour of the TSFIs and TSFs and the correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

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

PRIMUS31-MAX_USER_1: The purpose of this test is to illustrate that the maximum allowed users' option cannot be lower than the existing users.

PRIMUS2822-MAX_USER_2: The purpose of this test is to illustrate that the maximum allowed users option's valid value is the current users number.

PRIMUS31-CREATE_PRIV_1: The purpose of this test is to examine if the TOE is able to protect the communication path between itself and client applications.

PRIMUS2822-USER_AUTH_1: The purpose of this test is to illustrate that username can be changed. After that trying to login with the previous username and password is not successful.

11.3.2 Test results

All test cases devised by the Evaluators were passed 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 with the TOE already used for the functional test activities and verified that the TOE and the test environment were properly configured.

A search on public vulnerabilities on TOE and TOE components (e.g. OS) has been conducted. The analysis confirmed that there are no public vulnerabilities exploitable with the TOE implementation and configuration.

The Evaluators conducted penetration testing activities on the same instance of the TOE configured for functional and independent testing.

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