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) v.3.1 rel. 5

Certificato n. *(Certificate No.)*	01/2025
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/08/2023/RC, v1.0
Decorrenza *(Date of 1st Issue)*	16 gennaio 2025
ASI-HSM AHX5 kNET Cryptographic Module v1.1.0	ASI-HSM AHX5 kNET Cryptographic Module v1.1.0
KRYPTUS Segurança da Informação S.A.	KRYPTUS Segurança da Informação S.A.
Tipo di Prodotto *(Type of Product)*	Prodotti per le firme digitali
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_FLR.3 e 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, 16 gennaio 2025

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 la 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.*

Organismo di Certificazione della Sicurezza Informatica

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

ASI-HSM AHX5 kNET Cryptographic Module v1.1.0

OCSI/CERT/CCL/08/2023/RC

Version 1.0

16 January 2025

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	16/01/2025

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
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
API	Application Programming Interface
CLI	Command Line Interface

CM	Cryptographic Module
CPU	Central Processing Unit
DB	Database
ECDSA	Ellictic Curve Digital Signature Algorithm
GUI	Graphical User Interface
HSM	Hardware Security Module
KMIP	Key Management Interoperability Protocol
OS	Operating System
PCO	Physical Crypto Officer
PHSM	Physical HSM – Una istanza fisica di HSM
RSA	Rivest Shamir Adleman
SSL	Secure Socket Layer
SQL	Structured Language Query
VCO	Virtual Crypto Officer
VHSM	Virtual HSM – Una istanza logica di HSM, in esecuzione su un HSM fisico.

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

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

4.2 Technical documents

[ADMIN] Kryptus kNET Manager User Manual, version: 1.8.1, 13 May 2024

[OPER] Kryptus kNET HSM Operators Manual, version: 1.1.1, 13 May 2024

[CLI] Kryptus kNET HSM Command Line Interface User Manual, version: 1.12.1, 13 May 2024

[CC_GUIDE] ASI-HSM AHX5 kNET Cryptographic Module, Common Criteria Certification, PP EN 419221-5:2018 - Common Criteria Mode Manual, Version: 1.1.2, Date: 6 September 2024

[ETR] Evaluation Technical Report ASI-HSM AHX5 kNET Cryptographic Module v1.1.0 (HW:v1.0.1 FW:v1.1.0 SW:v1.48.1), KRYPTUSEVHSM-050_ETR_v1, CCLab Software Laboratory, 18 October 2024

[PP] EN 419221-5:2018, Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services.

[ST] Security Target ASI-HSM AHX5 kNET Cryptographic Module, Version: v1.6.1, 13 September 2024

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 declared 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 declared assurance components up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "ASI-HSM AHX5 kNET Cryptographic Module v1.1.0", developed by KRYPTUS Segurança da Informação S.A.

The TOE is a Hardware Security Module (HSM) that provides cryptographic services with native implementation of the Key Management Interoperability Protocol (KMIP). This protocol defines the structure and execution of cryptographic operations, such as generation of asymmetric key pairs, issuing of certificates, generation of random data and others. The communication between the user and the module itself occurs through standard Ethernet interface using TCP protocols.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister 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 3.1 Revision 5 for the assurance level EAL4, augmented with AVA_VAN.5 and ALC_FLR.3 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 "ASI-HSM AHX5 kNET Cryptographic Module v1.1.0" 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	ASI-HSM AHX5 kNET Cryptographic Module v1.1.0 (HW:v1.0.1, FW:v1.1.0, SW:v1.48.1)
Security Target	ASI-HSM AHX5 kNET Cryptographic Module Security Target Evaluation Assurance Level (EAL): 4 augmented with ALC_FLR.3 and AVA_VAN.5, Version: 1.6.1, 13 September 2024
Evaluation Assurance Level	EAL4, augmented with ALC_FLR.3 and AVA_VAN.5
Developer	KRYPTUS Segurança da Informação S.A. Rua Maria Tereza Dias da Silva 270, Campinas, SP, Brazil
Sponsor	KRYPTUS INFORMATION SECURITY SA
LVS	CCLab – The Agile Cybersecurity Laboratory (Budapest site)
CC version	3.1 Rev. 5
PP conformance claim	EN 419221-5: 2018 [PP]
Evaluation starting date	January 23, 2024
Evaluation ending date	October 18, 2024

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 a Hardware Security Module that provides cryptographic services with native implementation of the Key Management Interoperability Protocol. The TOE is a cryptographic module that executes cryptographic operations with appropriate parameters, which includes but are

not restricted to generation and management of AES Symmetric keys and of Asymmetric keys with RSA and ECDSA algorithms. All of these operations use cryptographic objects, which keys are part of, contained within the TOE and only require a safe environment that provides a power supply and User access to the TOE through an Ethernet connection.

All TOE's operators are stored and maintained in isolation, each one with a different scope: PCOs [1] manage the entire product (physical environment); VCOs[2] oversee an independent virtual environment called VHSM (isolated from each other) and the Users create objects and execute cryptographic operations. All these TOE's operators can authenticate by username and password, OTP, certificate, token or session. Additionally, by activating the Quorum Authentication (M of N), it is possible to protect chosen objects by only allowing the execution of Critical Operations on them with the agreement of a defined group of Users.

The TOE protects the keys against logical attacks that would result in disclosure, compromise and unauthorised modification, and for ensuring that the TOE's services are available only if authentication is verified. Also, the TOE provides physical mechanisms to detect and protect data against physical attacks, such as an opaque epoxy resin applied over components and sensors, power input and environment monitoring.

The TOE is capable of storing external keys and using them internally, or momentarily using them without storing.

The TOE provides two types of backup, each one related to the correspondent environment (PHSM or VHSM). When creating a backup, you can specify any number of target HSMs, with a minimum of one, by supplying their device certificates and, after authentication has been confirmed, it can be stored in removable media or downloaded through the network to the operator's device. In case of failure, the same options are supported by the restore operation.

The TOE generates audit records of all processes, such as: startup, shutdown, key generation and destruction, import and export keys and others.

The TOE provides a trusted communication path between external client applications and itself, using TLS over TCP protocol or pure TLS.

The TOE allows the execution of Python scripts internally, extending its inherent security features to the applications executing those scripts and providing further security by encapsulating them into their own independent environments, guaranteeing their execution and safety.

For a detailed description of the TOE, refer to sections 3.3 and 3.4 of the Security Target [ST].

7.3.1 TOE architecture

The TOE is the board containing the entire ASI-HSM AHX5 kNET Cryptographic Module, enclosed by the red rectangle in Figure 1. The ASI-HSM AHX5 kNET Cryptographic Module Figure 2 is a multi-user, multi-chip embedded crypto-module (also "module" for brevity). It is embedded within a stand-alone network appliance, which is a Non-TOE part, that gives easy access to its Ethernet, RS232 and Frontal Board interfaces and includes a dual power supply. That appliance is typically used in large-scale cloud infrastructures, where ease of remote configuration and operation is required.

[1] An administrator category with privileged access to the PHSM, responsible for managing the entire device.
[2] An administrator category responsible for managing a single VHSM and the Key Users within it.

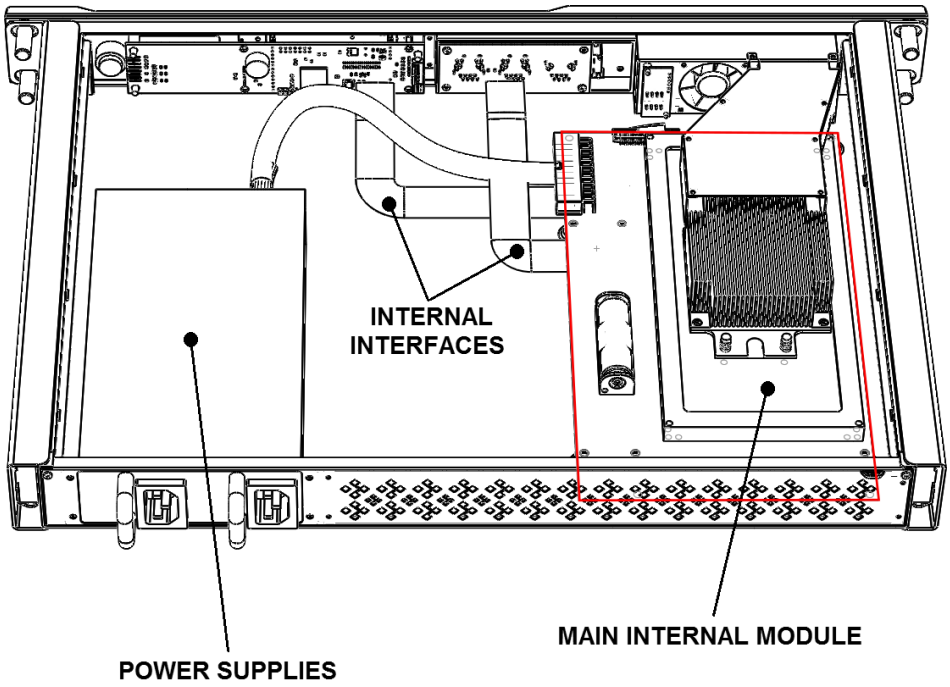

Figure 1 – Schematic description of the TOE

The module exists to provide cryptographic services to applications running on behalf of its Users who communicate with it via a standard Ethernet interface using IP protocols. In order to provide these services, the module also requires a power supply.

Figure 2 – ASI-HSM AHX5 kNET Cryptographic Module (the TOE)

The component that manages the cryptographic services and system's assurances, called Software, and the one which calls the low hardware-level cryptographic capabilities, called Firmware, are both responsible for enforcing all SFRs and SARs. All other parts of the TOE, which are contained within the boundary shown in red in Figure 1, support but do not interfere with enforcement e.g., OS, DB, logging system, ethernet interface driver and CPU.

The module is divided into two logical parts: physical and virtual. The physical part is named Physical HSM (PHSM) with its administrator Physical Crypto Officer (PCO), its virtual counterpart is the Virtual HSM (VHSM) with its administrator Virtual Crypto Officer (VCO). The module provides cryptographic services only from VHSMs logical security modules and they are created and managed by the PHSM.

The administrators do not have access to the TOE's cryptographic services, those are solely reserved to the Key User role and only this role can manage and use cryptographic objects. The Key Users are created and managed by the VCO in their respective VHSM. Multiple VHSMs can be created in the PHSM by the PCO, and each VHSM has its own Key Users and data, which cannot be accessed by other VHSMs, nor by the PHSM.

7.3.2 TOE security features

Assumptions, threats, and security objectives are defined in section 5 of the Security Target [ST]. TOE Security Functions are described in section 10, TSS, of the Security Target [ST].

The major security features are summarised in the following, the TOE:

- Provides Cryptographic Support.
- Implements Trusted path/channels.
- Implements Secure boot, to ensure that the module will only execute trusted firmware.
- Stores sensitive data encrypted/obfuscated at all times.
- Restricts access to objects.
- Restricts usage of objects.
- Provides Quorum authentication.

To ensure and verify that the module is working correctly, the module run self-tests and allows auditing its operations through logs.

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 to the following Protection Profile:

- EN 419221-5:2018, Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services [PP].

7.6 Functional and assurance requirements

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

All the SFRs have been selected or derived by extension from CC Part 2 [CC2] and are taken from [PP]. It is possible to refer to the Protection Profile [PP] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

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

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST] and the Protection Profile [PP] to which it claims strict conformance. 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 (Budapest site).

The evaluation was completed on October 18th, 2024, with the issuance by the LVS of the approved Evaluation Technical Report [ETR].

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, 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 [ETR] issued by the LVS CCLab – The Agile Cybersecurity Laboratory (Budapest site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "ASI-HSM AHX5 kNET Cryptographic Module v1.1.0" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with ALC_FLR.3 and 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 ALC_FLR.3 and 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
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 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
Systematic Flow Remediation	*ALC_FLR.3*	*Pass*
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Advanced methodical vulnerability analysis	*AVA_VAN.5*	*Pass*

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

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

Potential customers of the product "ASI-HSM AHX5 kNET Cryptographic Module v1.1.0" 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 6.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 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 ([ADMIN], [OPER], [CLI], [CC_GUIDE] and all other support documents delivered with the TOE as described in section 3.5.1 of the [ST]).

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

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

9.1 TOE delivery

The TOE and the appliance that contains the TOE are delivered in a cardboard box. Users shall open and check the box. The following material should have been retrieved from the box:

- Assembled kNET
- Rails kit
- 2 AC power cables (EXTCABLE0 and EXTCABLE1)
- RS-232 cable (EXTCABLE2)
- Cradle (2 “H”-shaped foam pieces and 2 main foam pieces - half-height)
- 10 Smart cards and smart card reader
- A printed “leaflet” containing an installation guide

Verify the kNET’s serial number, which can be found on its back, as illustrated in Figure 3.

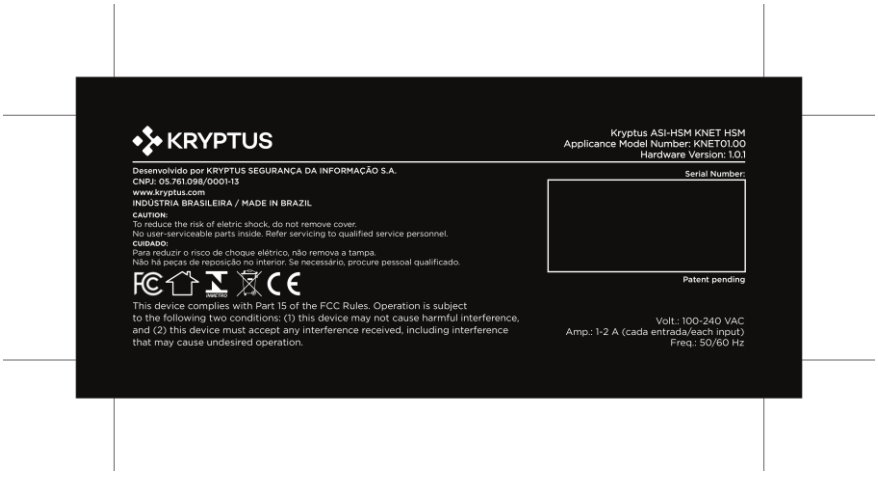

Figure 3 – kNET serial number

The appliance is also provided with tamper evident seals, they must be checked to verify that the package delivered has not been tampered with.

9.2 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 provided with the product to the customer.

Accessing all available user documentation is made seamless through the TOE’s Software Development Kit (SDK), accessible to all customers upon the acquisition of one or more HSMs. This

resource is conveniently provided via a password-protected link to a *NextCloud* repository housing all the essential SDK files for effortless download.

Documents [ADMIN], [OPER], [CLI], and in particular [CC_GUIDE], 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].

Following setup, it is highly advisable to extract logs from the acquired devices prior to initiating any cryptographic operations. In the event of tampering attempts occurring between shipment and receipt, these logs will provide comprehensive details regarding any such incidents and the nature of tampering detected. It is imperative to verify the absence of any such log entries before proceeding with routine operations using the TOE, ensuring the utmost safety and security.

After extracting the log in the previous step, the header of the log file should include information about the device's serial. Please check that the serial number therein informed is equal to the serial number printed on the label affixed to the back of the device.

Software validation occurs automatically upon boot-up by the TOE during the decryption of the system image. If the decryption process fails, the device will reject the boot-up sequence.

To verify the authenticity of the received TOE as the Common Criteria-certified version, reference the firmware version number. Access the Frontal Board interface: Navigate from the Home screen to MENU, then select Settings, and proceed to Info. If the displayed Firmware Version is 1.1.0, it confirms the reception of a fully evaluated instance of the TOE.

10 Annex B – Evaluated configuration

The Evaluators followed the preparation steps defined in the [CC_GUIDE] document for the TOE being in the evaluated configuration.

The TOE is identified in the Security Target [ST] as in the following:

- TOE Hardware Version: 1.0.1
- TOE Firmware Version: 1.1.0
- TOE Software Version: 1.48.1

The evaluation of the TOE was conducted on this configuration. The name, version and configuration number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

The TOE module comes along with libraries for the mainstream application programming languages:

- kkmip-cpp: C++ library;
- kkmip-py: Python library;
- kkmip-java: Java library;
- kkmip-js: JavaScript library.

Also, the module is provided with the most common cryptographic APIs for prompt integration with already implemented systems, which are the following:

- PKCS#11;
- OpenSSL Engine;
- Java JCA Provider.

10.1 TOE operational environment

The TOE only requires a secure environment that provides power supply and User access to the TOE through an Ethernet connection. For details about environment's security please refer to the following assumptions included in [PP], section 6.5, to which the TOE claim conformance:

- *A.ExternalData* - Protection of data outside TOE control
- *A.Env* - Protected operating environment
- *A.DataContext* - Appropriate use of TOE functions
- *A.UAuth* - Authentication of application users
- *A.AuditSupport* - Audit data review
- *A.AppSupport* - Application security support

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 evaluator conducted the tests locally. The test configuration was installed by the evaluator who followed the steps described in the [CC_GUIDE] document and AGD_PRE.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The tests were performed by using a computer connected with a switch to the TOE chassis. A connection with a serial cable was also used between the same two components. During the testing, the evaluator did not use sampling method and ran all the tests in each analysis cycle.

11.2.2 Test coverage

The Evaluators verified the complete coverage between the test cases in the test documentation provided by Developer and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behaviour and properties of the TSF.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

Due to the relatively small sample size, all Developer's tests were repeated by the Evaluators to confirm the validity of expected results. These are:

- Test Case 1 - Create
- Test Case 2 – Create Key Pair
- Test Case 3 - Register
- Test Case 4 - Derive Key
- Test Case 5 - Get
- Test Case 6 - Get Attributes
- Test Case 7 - Get Attributes List
- Test Case 8 - Add Attribute
- Test Case 9 - Modify Attribute
- Test Case 10 - Delete Attribute
- Test Case 11 - Revoke

- Test Case 12 - Destroy
- Test Case 13 - Validate
- Test Case 14 - Encrypt
- Test Case 15 - Decrypt
- Test Case 16 - Sign
- Test Case 17 - Signature Verify
- Test Case 18 - MAC
- Test Case 19 - MAC verify
- Test Case 20 - RNG Retrieve
- Test Case 21 - RNG Seed
- Test Case 22 - Hash
- Test Case 23 - Create Split Key
- Test Case 24 - Join Split Key
- Test Case 25 - Export Virtual HSM
- Test Case 26 - Import Virtual HSM
- Test Case 27 - Export Physical HSM
- Test Case 28 - Import Physical HSM
- Test Case 29 - Get System Log
- Test Case 30 - Sign XML
- Test Case 31 - Generate CSR
- Test Case 32 - USB port
- Test Case 33 - RS-232 Server
- Test Case 34 - Frontal Board

The Evaluator also created ten additional test cases for independent testing to test TOE specific features (one test was about physical protection/anti-tampering and one concerning ACVP - *Automated Cryptographic Validation Protocol*).

11.3.2 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.

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.

The Evaluators designed the following attack scenarios:

- Security bypass via brute force
- Username enumeration
- XXE and XML vulnerabilities
- Command injection and search unauthenticated function in SDK
- SNMP vulnerabilities
- SSL test and vulnerabilities search
- Insecure JSON deserialization
- Directory and Subdomain search and HTTP smuggling
- Request manipulation
- Public vulnerability validation
- SQL injection
- Physical attack on TOE

The Evaluators has concluded that the TOE is resistant to High attack potential in its intended operating environment.