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.)*	03/2025
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/01/2024/RC, v1.0
Decorrenza *(Date of 1st Issue)*	14 febbraio 2025
Nome e Versione del Prodotto *(Product Name and Version)*	Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM
Sviluppatore *(Developer)*	Nextsense Ltd
Tipo di Prodotto *(Type of Product)*	Prodotti per firme digitali
Livello di Garanzia *(Assurance Level)*	EAL4+ (AVA_VAN.5) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	EN 419241-2:2019, Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing
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, 14 febbraio 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

Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM

OCSI/CERT/CCL/01/2024/RC

Version 1.0

14 February 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	14/02/2025

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
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
API	Application Programming Interface

CLI	Command Line Interface
CM	Cryptographic Module
CO	Crypto Officer
DB	Database
DTBS/R	Data To Be Signed / Representation
EC	Elliptic Curve
eIDAS	electronic IDentification, Authentication, and trust Services
FM	Functional Module
GUI	Graphical User Interface
HSM	Hardware Security Module
IDP	Identity Provider
JSON	JavaScript Object Notation
JWT	JSON Web Token
LCO	Limited Crypto Officer
LTS	Long Term Support
MITM	Man-in-the-Middle
QSCSD	Qualified Signature and Seal Creation Device
QTSP	Qualified Trust Service Provide
OS	Operating System
REST	Representational State Transfer
RSA	Rivest-Shamir-Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCA	Signature Creation Application
SHA	Secure Hash Algorithm 256-bit
SIC	Signature Interactive Component

SKS	Scalable Key Storage
SMK	SKS Master key
SSA	Server Signing Application
SSL	Secure Socket Layer
SQL	Structured Language Query
SVD	Signature Verification Data
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing

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

[eIDAS] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[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

[EN419241-1] Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements

[ETR2] Evaluation Technical Report Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM, NSEVNSSAM-043_ETR_v2, CCLab Software Laboratory, 22 November 2024

[ETR3] Evaluation Technical Report Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM, NSEVNSSAM-043_ETR_v3, CCLab Software Laboratory, 13 January 2025

[INST_GUIDE] Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Installation Guide, v1.4, 2024.09-09

[OPE] Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Operations Guide, v1.4, 2024.09.09

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

[PP-SAM] EN 419241-2:2019, Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing, February 2019

[PRE] Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Installation Prerequisites, v1.4, 2024.09-09

[ST] Security Target of Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM, version v1.6, date: 15.11.2024

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 "**Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM**", developed by Nextsense Ltd.

The TOE is the Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM software component that implements the Signature Activation Protocol (SAP) to obtain user Signature Activation Data (SAD). The TOE uses the SAD from the signer to activate the corresponding signing key for use in a Cryptographic Module (CM). The TOE uses a Cryptographic Module certified according to the protection profile [PP-CM], as mandated by the Protection Profile [PP-SAM]. The TOE and the Cryptographic Module are a QSCD as specified in [eIDAS] regulation. The TOE shares the same tamper protected device and operates inside Thales Luna K7 Cryptographic Module (Thales Luna K7) as a functional module (FM). The TOE uses all Thales Luna K7's crypto functions to operate.

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, 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 "Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM" 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	Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM
Security Target	Security Target of Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM, version v1.6, date: 15.11.2024
Evaluation Assurance Level	EAL4 augmented with AVA_VAN.5
Developer	Nextsense Ltd.
Sponsor	Nextsense Ltd.
LVS	CCLab Software Laboratory (Budapest site)
CC version	3.1 Rev. 5
PP conformance claim	EN 419241-2:2019 [PP-SAM]
Evaluation starting date	19 March 2024
Evaluation ending date	20 December 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 the Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna software component that implements the Signature Activation Protocol (SAP) to obtain user Signature Activation Data (SAD). The TOE uses the SAD (Signature Activation Data) from the signer to activate the corresponding signing key for its usage in a Cryptographic Module (CM). The TOE uses a Cryptographic Module certified according to the protection profile [PP-CM], as mandated by

the Protection Profile [PP-SAM].

The TOE shares the same tamper protected device and operates inside Thales Luna K7 Cryptographic Module (Thales Luna K7 shown in Figure 1) as a functional module (FM). The TOE uses all Thales Luna K7's crypto functions to operate.

However, this hardware device is the environment of the TOE and not the TOE itself.

Figure 1 – Thales Luna K7 hosting the TOE

NSSAM module is designed to operate as a part of the Trustworthy System Supporting Server Signing TW4S architecture according to [EN 419241-1] and to [PP-SAM]. It integrates with Server Signing Application (SSA) products to provide remote signing functionality to business applications. The TOE in the TW4S architecture is further detailed in the picture and description below in section 7.3.1.

There are two additional non-TOE components outside the TOE that are worth mentioning. These are the NSSAM Driver and NSSAM Admin components.

NSSAM Driver is the component that is responsible for the operational requests. It works with translating the requests from external entities, Signature Creation Applications (SCA) and forwarding them to the TOE, while every operational request goes through the NSSAM Driver, there is no direct connection between the TOE and external entities.

On the other hand, NSSAM Admin is a component that is responsible for the configuration and management of the TOE, by calling the appropriate functions of the TOE. It has a Command Line Interface (CLI), the NSSAM Admin Console. Only the Admins can have access to the NSSAM Admin Console to set up and manage the TOE.

In summary NSSAM Admin is only a tool so the admins can use the TOE easier, while the Driver is responsible for the operational requests. These components communicate with the NSSAM FM Module using Message Dispatch API which is the main communication channel to the NSSAM as shown in the following Figure 2.

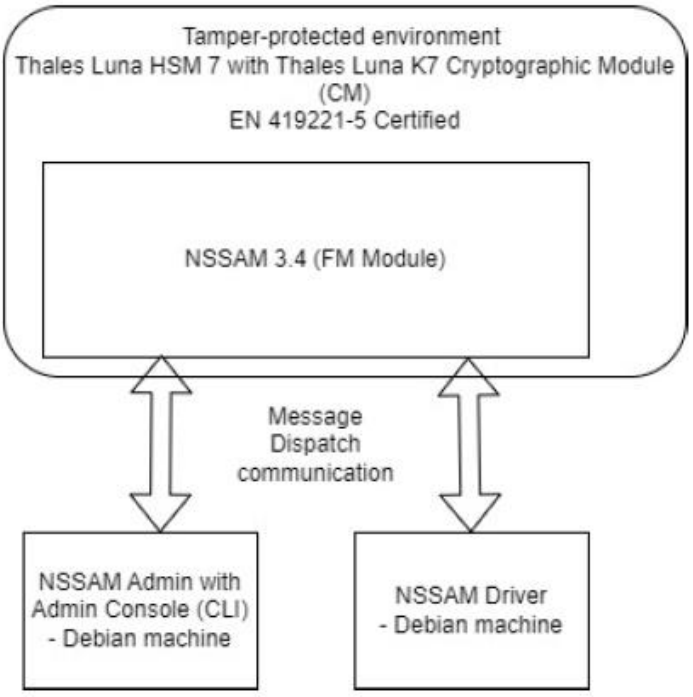

Figure 2 – Main components

For a detailed description of the TOE, refer to sections 1.3 and 1.4 of the Security Target [ST].

7.3.1 TOE architecture

The TOE is the Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 which is a functional module (FM module) made for Thales Luna K7 Cryptographic Module with Luna HSM Firmware 7.7.0 with two critical non-TOE components that can access the TOE: NSSAM Driver and NSSAM Admin.

NSSAM follows the standard architecture of Thales regarding FM modules. The Luna HSM provides utility libraries to be able to communicate with FM modules, while external entities like the NSSAM Driver communicate with NSSAM FM module using Thales Message Dispatch API. The encrypted keys are stored in an external storage, in an external database.

System architecture is shown in the following Figure 3 that highlights the TOE boundaries.

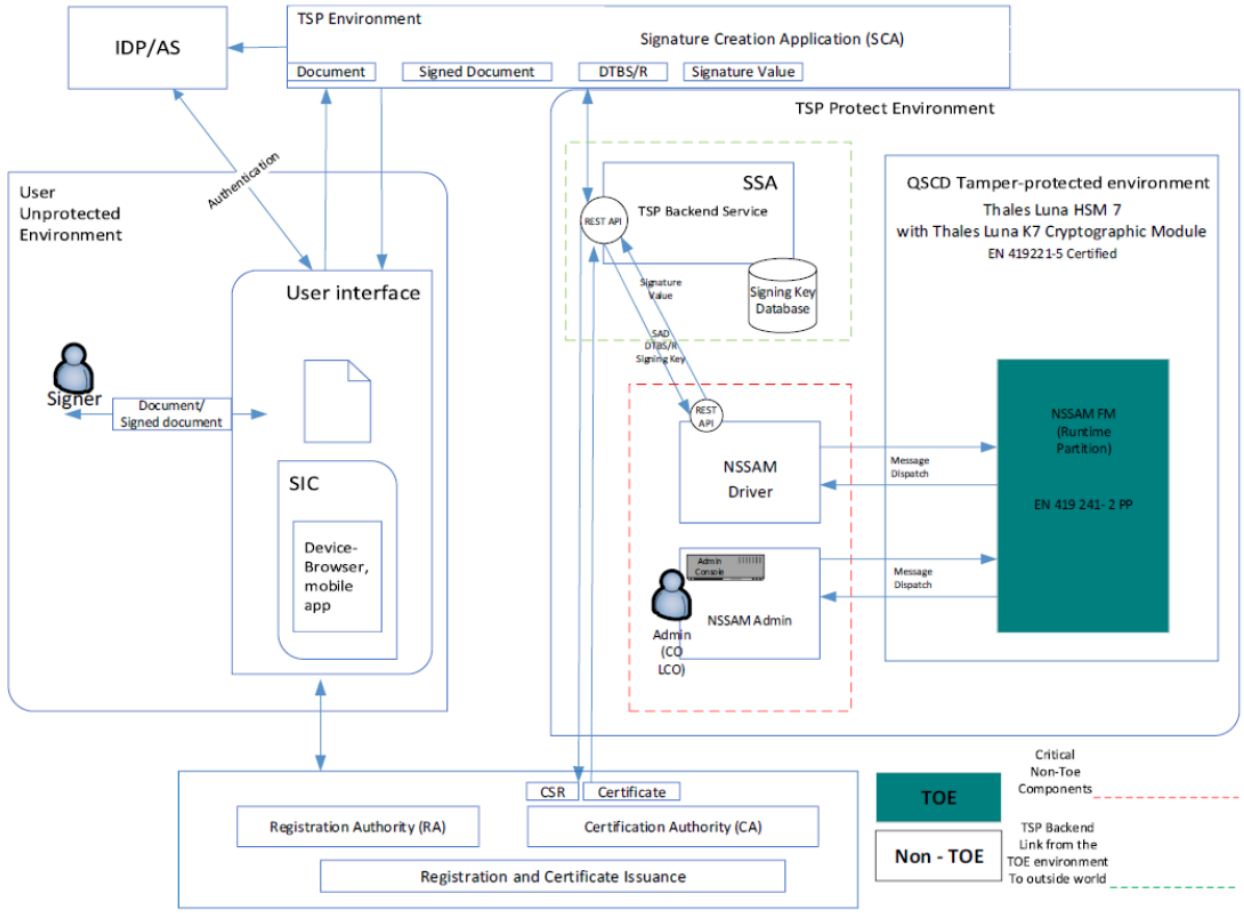

Figure 3 – System architecture with TOE boundaries

The TOE is highlighted with a green filled rectangle.

There are two critical non-TOE components that can access the TOE. NSSAM Driver and NSSAM Admin, they are drawn in a red dashed box. The critical non-TOE components use the Thales HSM client, especially the Luna Functionality Module Tools which are installed as part of the Thales HSM client. NSSAM communicates with NSSAM Driver, which is a critical non-TOE component. The NSSAM Driver acts as a secure channel between NSSAM and the Server Signing Application (SSA – which is the TSP Backend Service). SSA needs an externally connected storage to store the encrypted signing keys, which is recommended to be a database kept in the QTSP secure protected environment, but it can be any other storage under the control of the TSP. It stores encrypted data for every signer, that has the signer's private key with all its attributes in an encrypted form.

NSSAM Driver consists of a REST API and the NSSAM Utility Functions and acts as a bridge between the TOE and the components used by the TSP. It also handles the requests coming from external applications and from the Signers. The NSSAM Driver has a REST API that translates the request to NSSAM compatible format and forwards it to the NSSAM via Thales Message Dispatch API.

NSSAM Admin is a component that sends management commands to the NSSAM module. The NSSAM Admin Console is a CLI that has only configuration and management commands available, like setting up the TOE or creating backup, delete locked keys but it doesn't have commands to access the Signer data and keys. The NSSAM Admin Console is used only for privileged actions, for TOE configuration and management.

Both of these components are installed on a Linux Debian distribution (Ubuntu 22.04 LTS).

7.3.2 TOE security features

Assumptions, threats and security objectives are defined in section 3 and 4 of the Security Target [ST].

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

- Ensure the signers has sole control of their signing keys, which is carried out to authorize the signature operation.
- The SAM activates the signing key within a CM, handling a Signature Activation Protocol (SAP) which requires Signature Activation Data (SAD) to be provided at the local environment.
- The SAM component uses the SAD in order to guarantee with a high level of confidence. The SAD binds together the signer authentication with the signing key and the data to be signed DTBS/R.
- NSSAM is software component loaded at tamper protected environment.

The TOE relies on the identification and authentication of an external identity provider (IDP) of each user before granting access to their signing keys. The TOE makes additional authentication by implementing key authorization mechanism for each user.

The TOE also generates keypairs that can be used to create for example digital signatures and allows to perform HSM certified signing operations.

Every operation performed by the TOE is reliably logged and could be reviewed in case it is needed. The TOE also provides secure channels to protect data integrity and confidentiality in transition.

In summary the Signers can use the product and perform authorized signing operations and generate keypairs in a tamper protected environment where the signing keys are under the sole control of that signing user..

The TOE has the following security features:

- **Security Audit**

  The TOE provides reliable audit logs for all important features. Each audit record contains the event type, the date and time of the event, who performed the operation and whether it was successful or not. The audited operations amongst others are:

  - start and stop of the system
  - managing users
  - login of any users
  - signing key generation and deletion
  - signing key usage
  - update of any configuration of the TOE

  The TOE generates the logs and forwards them to the HSM, which means that logs are transferred outside the TOE logical boundaries, but within the HSM physical boundaries. The HSM keeps the logs in the local filesystem, and it can be set to further transfer the logs using a remote syslog server. As the storage of the logs is outside the TOE logical boundaries, the

review of the logs is also performed outside of the logical boundaries of the TOE. The audit records of the TOE are forwarded to the HSM, then are further forwarded to the SSA, the audit records generated by the TOE are stored in the SSA in a transitive way.

- **Cryptographic support**

  The TOE uses Thales Luna K7 Crypto functionality for cryptographic operations such as key generation, data encryption and decryption, securing communication channels and creating digital signatures. The TOE always generates the keys in the certified crypto module (the Thales Luna K7 crypto module). The operations performed with the keys, such as creating electronic signatures, encryption and decryption of data or securing the communication, are always done within the crypto module.

- **User Data Protection**

  There is no Signer data stored in the TOE only the Signer identifier and the key that belongs to the user. The keys are stored outside the TOE in an external database encrypted with the HSM partition SKS Master key and the 2 SKS Passwords entered during the TOE initialization. The Signer is authenticated by an external IdP that issues a signed JWT token. The IdP must be registered in the TOE with the public key that corresponds to the private key used to sign the JWT. The JWT token, as a Signer authentication data, is checked by the TOE (the signature, the IdP name, the validity: not before, issued at, and expires values).

  The keys are also protected with the Signer PIN that is never stored in the TOE, and a particular key can be used only if it is authorized for use within the HSM by the key authorization data (combination of email, issuer name and PIN). Nobody can have access to the keys for signing purposes but the owner that is the only one that knows the PIN. Because the PIN is known ONLY by the signer that is the owner of the keypair, by entering the PIN, the TOE ensures that the user signing with the key is the same user that has initiate the keypair creation (when the keypair was created). With this, the PIN is becoming the Signer's authentication factor that is known only by the Signer, but also it is part of the key authorization data used to authorize the key usage. The keys are stored in the Signing Key database of the SSA (see Figure 3).

  For the purpose of this document the term "key authorization data" refers to the combination of the email, issuer name (which are data from the IdP signed JWT token) and the Signer PIN.

  Privileged User data (Admin passwords and IDP public keys) are stored in the TOE secure filesystem.

- **Identification and authentication**

  The TOE supports Privileged Users and Signers. Privileged Users are administrators of the TOE or Identity Providers that authenticate the Signer.

  The different Admins of the TOE are:

  - Thales Crypto Officer (CO) is identified by its Crypto Officer PIN. This role is used to install and configure the TOE on the Thales Luna K7
  - Thales Limited Crypto Officer (LCO) is identified by Limited Crypto Officer PIN. This role is used to access the Thales Luna K7 functionality including crypto and audit.

  CO and LCO are provided by the Thales Luna K7 but as the TOE runs inside Thales Luna K7 it needs the same CO and LCO passwords as Thales Luna K7.

During the initialization of the TOE, five different passwords need to be entered, maintained separately by 5 different password owners. These passwords cannot be changed after the initialization of the TOE:

- 2 SKS Passwords: There should be 2 SKS password owners, each entering a unique password. These two passwords together are used for encryption of the signer's private keys, in combination with the HSM SMK key.
- 3 Session Passwords: there should be three session password owners, each entering a unique password. These passwords are used for the generation of the Master RSA Key and as Authorisation data for the AES session key. This Master RSA key is created in the HSM. The sessions are signed using this Master RSA key.

The password owners are not treated as Privileged Users, as their only function is to maintain the passwords in a secure way. These passwords are only entered during the setup of the TOE or during a recovery from a backup.

The Signer is always authenticated by an external Identity Provider that fulfils the requirements of delegated authentication defined in [EN 419241-1]. The identity provider (IDP) identifies the Signer and then issues a JWT token which must be signed by the IDP, which is then passed to the TOE, so that the TOE can accept and process it. The JWT token, as a part of itself, contains the Signer's e-mail and the identity provider name. The IDP must be registered in the TOE with its public key (the private is used to sign the JWT). Only JWT tokens signed by registered IDPs are accepted. Still, to get access to the Signer keypair, the Signer also needs to provide their PIN, so the Signer is authenticated based on the content and the signature of the IDP signed JWT token and the PIN, while the key usage is authorized with a key authorization data (a combination of the email, JWT issuer name and the PIN). The PIN is uniquely connected to a Signer, and only the Signer knows the PIN which must be provided in order to use the keypair of that Signer, which means that the knowledge of the PIN verifies that the Signer is the owner of that particular keypair and is part of the key authorization data to authorize the use of the Signer keypair.

- **Security Management**

  The management of the TOE is restricted to privileged users (Admins). The admins set up, configure, and manage the TOE via the NSSAM Admin Console.

- **Protection of TSF**

  The TOE relies on the physical protection of Thales Luna K7 as it runs within the same HW boundary. Thales Luna K7 erases all its keys in case of tamper is detected including the SAM architectural keys used for data encryption meaning nobody can decrypt the data stored outside the TOE.

  The TOE uses reliable timestamps for the logs it creates. It protects the data when it's exchanged between the TOE and other IT systems.

- **Trusted Path/Channels**

  The TOE uses encrypted channels for communicating with the SCAs. Also, the requests are signed by an IDP. The TOE is loaded and operates as a functional module within the logical and physical security of a Luna HSM 7 as part of the HSM firmware where all internal communication resides.

For a detailed description of the TOE Security Functions refer to sections 1.4.2 and 7 of the Security Target [ST].

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 419241-2:2019, Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing [PP-SAM].

7.6 Functional and assurance requirements

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

All the SFRs have been selected or derived by extension from CC Part 2 [CC2]. Considering that the Security Target claims strict conformance to the Protection Profile EN 419241-2:2019 [PP-SAM], all the SFRs from such PP are also included.

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 Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

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

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

The evaluation was completed on 22 November 2024 with the issuance by the LVS of the Evaluation Technical Report [ETR2], which was approved by the Certification Body on 20 December 2024.

A final version of the ETR was delivered by the LVS on 14 January 2025 [ETR3] including minor changes. Then, the Certification Body issued this Certification Report.

In compliance with application notes 68, 69 and 70 of [PP-SAM], FTP_PHP.1 and FTP_PHP.3 requirements have not been addressed because of the characteristics of the TOE. Namely, the TOE is a software-only product which is deployed inside a tamper protected environment provided by the certified CM. Therefore, FTP_PHP.1 and FTP_PHP.3 requirements do not apply to this TOE and for this reason physical protection tests have not been performed.

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 [ETR2] issued by the LVS CCLab Software Laboratory (Budapest site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with AVA_VAN.5, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4 augmented with AVA_VAN.5 (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
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 vulneraability 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 "Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM" 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 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.6 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 ([INST_GUIDE], [OPE] and [PRE]).

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 is an FM Module that is specifically made only for HSM devices with Thales Luna K7 Cryptographic Module compliant with Common Criteria certified against [PP-CM].

The procurement and delivery of the HSM device is not related with the TOE, but the TOE does not work on any other device type.

The TOE can only be activated on such a device (HSM devices with Thales Luna K7 Cryptographic Module compliant with Common Criteria certified against [PP-CM]) with a license activation file that is bound to a certified CM model (Thales Luna K7), firmware version (7.7.0) and a serial number.

The serial number for the HSM needs to be provided by the owner of the HSM in order to receive a license activation file for the NSSAM. The Thales Luna K7 HSM with firmware version 7.7.0 can be purchased from Thales official points of sale. The license activation file for the NSSAM is provided, at a request from the user of the TOE.

The TOE consists of the software components and guidance documents of the TOE. They can be delivered to the customers on the following ways:

1. Downloaded from the Nextsense customer support portal.
2. Sent by e-mail, in an encrypted format.

The final user will receive the TOE ZIP file package from the Developer via e-mail, PGP encrypted.

To check the authenticity and the integrity of the software, it is possible to create the checksum of the file “NSSAM34.zip” on the customer workstation by issuing the following command:

```
certutil -hashfile .\NSSAM34.zip SHA256
```

Then it is necessary to verify that the created SHA256 checksum and the SHA256 checksum in “zipcheksum.txt“, and on the published location given, are identical. It proves that there is no malicious actor replacing the file or packets being lost in the transport.

Also, the checksum is published on the Nextsense public website:

https://nextsense.com/content/compliance_docs/EU_EIDAS/nssam_validation_hash_v3_4.pdf

According to this the SHA256 hash of the NSSAM34.zip:

5a1c35e54b28f591609e084996e6380c8dae59c1d51efc1404bdccd32d6a0f6e

The content of the zip file is made of the following three files:

- A certification file (fmcert.cer)
- The actual FM Module that should be loaded in Thales HSM (NSSAM34.fm)
- and the checksum value (binchecksum.txt).

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.

In particular, the documents [INST_GUIDE], [PRE] and [OPE] 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 Evaluators followed the preparation steps defined in the [INST_GUIDE] and [PRE] for the TOE being in the evaluated configuration.

The TOE is identified in the Security Target [ST] with the version number 3.4. The name and version 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 evaluated configuration uses the Common Criteria certified-mode security settings and a certified CM. The steps for securely installing the TOE according to the CC evaluated configuration are described the Preparation Procedure document [PRE] and Installation Guide document [INST_GUIDE].

The items described in section 10.1 “TOE operational environment” must be available before performing the installation.

10.1 TOE operational environment

The TOE needs, at least, the following hardware/software/firmware to operate:

- TW4S compliant with [EN 419241-1] and [PP-SAM] component supporting the NSSAM 3.4.
- SSA component that handles communications between SAM in the QSCD and SCA.
- An Identity Provider providing signed JSON Web tokens (JWT) to state the authentication and authorization of the users.
- Hardware Security Module: HSM with Thales Luna K7 Cryptographic Module compliant with Common Criteria certified against [PP-CM].
- SIC – Signer Interaction Component used locally by the signer to communicate with the remote systems. Typically, it consists of a web browser, a mobile app with an embedded browser or a desktop application with an embedded browser.
- NSSAM Driver and NSSAM Admin.
- Externally database attached to SSA for HSM encrypted signing keys.

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 in the laboratory premises. The test configuration was installed by the evaluator who followed the steps described in [PRE] and [INST_GUIDE] documents.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The tests are highly automated using Azure DevOps Services pipelines and are performed by using the critical non-TOE components. Testing is performed using an automated process that has predefined scenarios. The 8 test groups, each contain a number of tests, are grouped as a scenario. To run the pipelines required for automated testing, an Azure Agent is also installed on the on-prem build server, that communicates with Azure Devops Services. The agent is connected to the project site where the pipelines that run the tests are and must be running to start the pipelines and the tests. An agent pool containing this agent has to be set in Azure Devops Services project site where the tests are. The build server and the cloud pipeline for performing tests was set up following the guidelines provided by the Developer during the evaluation. This document contains the necessary steps and information needed to perform the tests on the Azure cloud pipeline.

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

As introduced in section 11.2.1 there are 8 defined groups of tests. The groups are the following:

1. General Tests – Test the NSSAM configuration, the license needed for NSSAM, the IdP registration, start session with unknown IdP provider, the time settings and validation of the JWT tokens.
2. Signature Tests – Test the signing process using RSA and/or EC keys.
3. Change pin tests – Test the pin settings and change pin functionality.
4. User session tests – Test the session start process.
5. Enroll user key tests – Test the key enrolment scenarios.
6. Configuration tests – Test the functions used to set and read the NSSAM configurations.

7. Locked key Tests – test the lock of a key when 3 consecutive wrong pins are entered.
8. Manual Tests – tests that are performed manually.

The evaluator conducted each test case from each category to cover each SFR. It provided maximum rigor for testing and a deep test coverage.

Although, the Developer tests cover all TSFIs and SFRs the evaluator created 4 additional test cases to test the TOE's behaviour with additional inputs. The following tests were run:

- NSSAM_Enroll_RSA_Key.
- NSSAM_Admin_Manual_IDP_Test.
- Failed Backup and Restore of NSSAM.
- NSSAM_User_sessions.

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 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:

1. *Authentication attempt limit bypass*: Bypass the authentication attempt limits for the Signer.
2. *REST API Injection attacks*: Inject command malicious input into the REST API request parameters, allowing the attacker to conduct harmful operations.
3. *Man-in-the-Middle (MITM) and unencrypted traffic flow*: Intercept and check for unencrypted traffic. Try to perform impersonation of the user whose data is obtained.
4. *Unauthorized access*: Test to see if it is possible to interact with the resources of other users. The known user's token used to create a session as another user.
5. *Buffer overflow attacks*: try to exploit the TOE with the hypothesised buffer overflow.
6. *Integer overflow*: Examine and test the integer overflow vulnerability.
7. *Admin Console prompt input manipulation*. Try different attack vectors to escape from the CLI.
8. *API endpoint search*: Try different API endpoints that are generated based on possible keywords or phrases in the dictionary
9. *Excessive Data Exposure*: Send various requests in order to check that the API sends back full data objects or sensitive data.

At the end of the evaluation, the Evaluators have concluded that the TOE is resistant to High attack potential in its intended operating environment.