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.)*	04/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/14/2022/RC, v1.0
Decorrenza *(Date of 1st Issue)*	16 aprile 2024
Nome e Versione del Prodotto *(Product Name and Version)*	Trident, the distributed remote Qualified Signature Creation Device version 3.1.3
Sviluppatore *(Developer)*	I4P-informatikai Kft- (i4p informatics ltd)
Tipo di Prodotto *(Type of Product)*	Prodotti per firme digitali
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_FLR.3 e AVA_VAN.5) conforme a CC
Conformità a PP *(PP Conformance)*	Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, EN 419221-5:2018, May 2018 Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, EN 419241-2:2019, February 2019
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 aprile 2024

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

Trident, the distributed remote Qualified Signature Creation Device version 3.1.3

OCSI/CERT/CCL/14/2022/RC

Version 1.0

16 April 2024

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	16/04/2024

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 9
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 18
7.5 Protection Profile conformance claims 18
7.6 Functional and assurance requirements 19
7.7 Evaluation conduct 19
7.8 General considerations about the certification validity 19
8 Evaluation outcome 20
8.1 Evaluation results 20
8.2 Recommendations 22
9 Annex A – Guidelines for the secure usage of the product 23
9.1 TOE delivery 23
9.2 Installation, configuration, and secure usage of the TOE 24
10 Annex B – Evaluated configuration 25

10.1 TOE operational environment 25
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
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 Program Interface
CM	Cryptographic Module

DRNG	Deterministic Random Number Generator
DTBS/R	Data to Be Signed/Representation
ECA	External Client Application
eIDAS	Electronic Identification, Authentication and Signature
LCA	Local Client Application
MPCA	Multi-Party Cryptographic Appliance
MPCM	Multi-Party Cryptographic Module
OS	Operating System
QSCD	Qualified Signature Creation Device
RHEL	Red Hat Enterprise Linux
SAD	Signature Activation Data
SAM	Signature Activation Protocol
SAP	Signature Activation Module
SIC	Signer's Interaction Component
SSA	Server Signing Application
TLS	Transport layer Security
TOTP	Time-based-One-Time Password
TSP	Trusted Service Provider

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

[AIS34] Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1) version 3, Bundesamt für Sicherheit in der Informationstechnik (BSI), September 3rd 2009

[CCECG-ADM] Trident Administrators' Guide CM and SAM, Version 2.4, I4P-Informatikai Kft. October 2nd, 2023

[CCECG-DEV] Trident Developers' Guide CMAPI and SAP Version 2.4, I4P-Informatikai Kft. June 12th, 2023

[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

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

[EN 419241-1] Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements, EN 419241-1:2018, July 2018

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

[ETR] "Trident version 3.1.3" Evaluation Technical Report, Version 2, CCLab Software laboratory, January 22nd, 2024

[RC] Rapporto di Certificazione Trident version 2.1.3, OCSI/CERT/CCL/02/2020/RC, versione 1.0, 2 settembre 2020.

[ST] Security Target, Trident, the distributed remote Qualified Signature Creation Device, ST reference: Trident-ST, version: 3.5, January 16th, 2024, I4P-Informatikai Kft,

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 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 up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product "Trident, the distributed remote Qualified Signature Creation Device version 3.1.3", developed by I4P-Informatikai Kft. (i4p informatics ltd).

The TOE is a multi-user, multi-key devices, designed to be used as Qualified Signature Creation Device (QSCD) and composed by a Cryptographic Module and a Signature Activation Module, suitable for both Local and Remote use cases.

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).

This Certification Report was issued at the conclusion of the re-certification of an earlier version of the same TOE (Trident version 2.1.3), already certified by OCSI (Certificate no. 5/20 of September 2nd, 2020 [CR]).

Following some changes made to the product by I4P-informatikai KfT., it was necessary to proceed with a re-certification of the TOE. The modified components fall within the physical/logical scope of the TOE and have had an impact on the following evidence produced by the Developer: security target, functional specifications, TOE design and security architecture description.

The Evaluators were able to reuse part of the documentation and evidence already provided in the previous evaluation.

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 also review 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 ALC_FLR.3 and 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 "Trident, the distributed remote Qualified Signature Creation Device version 3.1.3" 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	Trident, the distributed remote Qualified Signature Creation Device version 3.1.3
Security Target	Trident, the distributed remote Qualified Signature Creation Device Security Target, I4P-Informatikai Kft, version 3.5, January 16th 2024 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.3 and AVA_VAN.5
Developer	I4P-informatikai Kft. (i4p informatics ltd).
Sponsor	I4P-informatikai Kft. (i4p informatics ltd).
LVS	CCLab Software Laboratory (Debrecen site).
CC version	3.1 Rev. 5
PP conformance claim	Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, EN 419221-5:2018, May 2018 Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, EN 419241-2:2019, February 2019
Evaluation starting date	19 September 2022
Evaluation ending date	22 January 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.

The TOE "Trident, the distributed remote Qualified Signature Creation Device version 3.1.3"is a multi-user, multi-key device designed to be used as a QSCD suitable for both local and remote use cases of [EN 419221-5] Protection Profile.

The certification is applicable to eight supporting hardware models for the TOE: A11, A21, A31, A33, B11, B31, B33, C16.

It is possible to consult sections 1.3, 1.4 of the Security Target [ST] for a more detailed description of the TOE.

7.3.1 TOE architecture

Depending on its configuration, the TOE consists of one or more MPCAs (Multi-Party Cryptographic Appliances). An MPCA comes in the form of a metal, rack mountable box.

In case of Distributed Configuration, the TOE consists of n (with n = 2, 3 or 4) identical TOE parts (MPCAs) to operate as a logical whole in order to fulfil the requirements of the Security Target [ST]. It is an *active-active configuration*, i.e. if some of the MPCAs becomes dysfunctional (as result of a fatal error or a network unavailability) the other MPCAs (if there are any) can ensure a limited functionality.

In case of **High-availability Configuration**, the TOE consists of one or more fully redundant instances of an active (online) MPCA node, one of which is only brought online when the active node fails. This is an active-passive (or online-standby) configuration.

The TOE is composed of two main components which can work together to fulfil different sets of requirements:

- The **Cryptographic Module (CM)** component is a general-purpose cryptographic module suitable for cryptographic support needed by its legitimate users (e.g., service providers supporting local or remote electronic signature and electronic sealing operations, certificate issuance and revocation, time stamp operations and authentication services). The TOE can also be configured to generate, store, and activate signer's keys in one or more external CMs for speed enhancement or legacy reasons;
- The **Signature Activation Module (SAM)** component is a local application deployed within the tamper protected boundary of the TOE and implements the Signature Activation Protocol (SAP). It uses the Signature Activation Data (SAD) from a remote signer to activate the corresponding signing key for use in a cryptographic module.

The "Local" use case (see Figure 1) is aimed at local key owners applying their own electronic signatures or seals. In this use case only the CM functionality of the TOE is used, which performs local cryptographic operations, and associated key management.

The TOE can also make use of other external CMs.

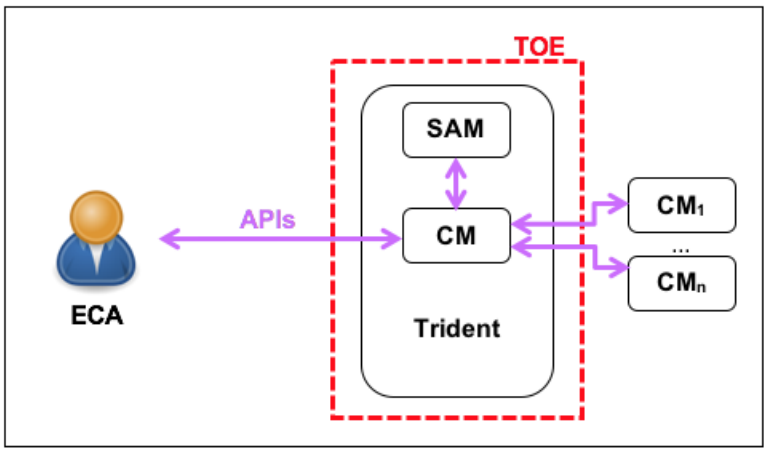

Figure 1 – TOE architecture in the "Local" use case

These operations can be used by external or local client applications (ECA, LCA) to create qualified and non-qualified electronic signatures and electronic seals for the local key owner natural or legal person. Examples include TSPs issuing certificates and timestamps, as well as supporting application services such as e-invoicing and registered e-mail where the service provider applies its own seal or signature.

The "Remote" use case (see Figure 2) is aimed at TSPs supporting requirements for remote signing, or sealing, as specified in [eIDAS] regulation. In this case the inbuilt CM, as well as other external CMs configured to be used (if there are any) and the SAM functionality of the Trident together meets the requirements for QSCDs in the context of remote signing set out in Annex II of [eIDAS].

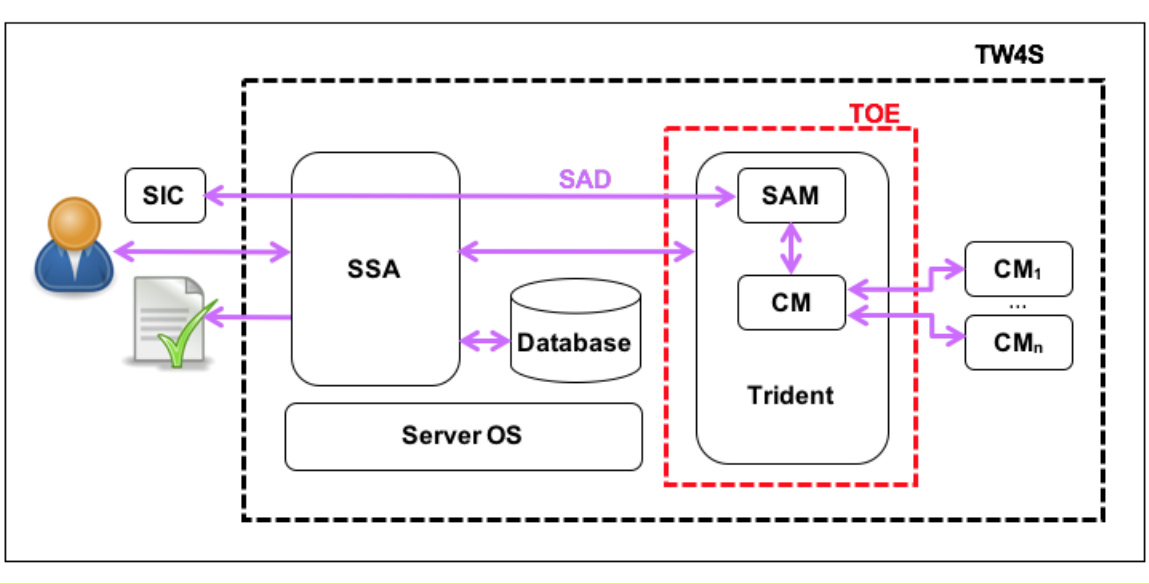

Figure 2 - TOE architecture in the "Remote" use case

The Signer's Interaction Component (SIC) is a piece of software and/or hardware, operated on the signer's environment under its sole control.

The Server Signing Application (SSA) uses the TOE to generate, maintain and use the signing key.

The Signature Activation Protocol (SAP) allows secure use of the signing key for the creation of a digital signature to be performed by a Cryptographic Module on behalf of a signer. The use of the

Signature Activation Data (SAD), which is the essential part of the SAP, ensures control over the signer's key.

The SAM Module is a software part of TOE, which uses the SAD to guarantee with a high level of confidence that the signing keys are used under sole control of the signer.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in section 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult section 7.1 of the Security Target [ST]. The major security features are summarized in the following sections.

7.3.2.1 User Roles and Authentication

The CM maintains the Administrator, Key User, LCA and ECA roles, associating users with roles. The CM uses a common method for identification and authentication in case of each role: a unique identifier and a static password and/or TOTP (Time-based-One-Time Password) and/or a JWT (Json Web Token). Before using a secret key an authorisation or a reauthorisation is required. The CM blocks the account/key after a predefined number of consecutive failed authentication /authorisation attempts.

The SAM maintains the Privileged Users and Signer roles. The SAM ensures that all users have only one role, consequently a signer can't be a privileged user. For the Signer, the SAM requires two different authentication factors, a password and a TOTP or a JWT. The identification and authentication method is: a unique user identifier + static password + TOTP or JWT. The SAM blocks the account after a predefined number of consecutive failed authentication attempts. When a signer account has been locked the SAM also suspends the usage of all signing keys of the Signer. The SAM maintains accounts (with different security attributes) belonging to individual users.

7.3.2.2 Security Management (CM)

The Administrator is able to:

- Unblock a blocked user account or a blocked key.
- Specify alternative initial value for the "Key Usage" security attribute, setting its value to "General" or to "Signing".
- Export and delete the local audit and error log file.
- Backup and restore of the CM's TSF state.

The Key User is able to modify the following attributes of his/her key:

- Authorisation Data.
- Unprotected Flag (which indicates whether his/her stored key is protected only with an infrastructural key, or additionally with his/her Authorisation Data.).
- Operational Flag (which indicates whether the key is in operational state.).

7.3.2.3 Security Management (SAM)

The SAM implements the following management functions:

- Signer management.
- Privileged User management.

- Configuration management.
- Backup and restore functions.

7.3.2.4 Key Security

The CM implements the following security functions related to the whole lifecycle of the keys:

- Key import.
- Key generation.
- Key restore from backup.
- Binding of a set of attributes to the key.
- Storage of the key.
- Key export.
- Key usage.
- Key backup.
- Key destruction.

For the SAM Crypto - The SAM does not perform cryptographic operations with Key User's key and does not delete Key User's key. The SAM invokes the CM with appropriate parameters whenever a cryptographic operation, a key generation or a key deletion is required. At the same time SAM performs non-distributed cryptographic operations with infrastructural keys.

7.3.2.5 Access and information flow control

The CM enforces the following Security Function Policies:

- Key Basics: import of secret keys is not allowed. Export of secret key is allowed only for non-Assigned keys with "Export Flag=”yes". Public keys will always be exported with integrity protection of their key value and attributes. Unblocking access to a key will not allow any subject other than those authorised to access the key at the time when it was blocked. No subject will be allowed to access the plaintext value of any secret key directly or to access intermediate values in any operation that uses a secret key.
- Key Usage: Key User can only change the „Unprotected Flag" and „Operational Flag" key attributes. The Key User can only change the Authorisation Data. Only subjects with current authorization for a specific secret key are allowed to conduct operations using the plaintext value of that key. Only cryptographic functions permitted by the secret key's Key Usage attribute shall be carried out using the secret key.
- Backup: only Administrator can perform the backup or restore function (restore function is under dual control). All backups are signed and encrypted. Consequently, any backup preserves their integrity and confidentiality.

The SAM enforces the following additional security functions:

- Privileged User Creation: only a Privileged User can create a new Privileged User's account.
- Signer Creation: only a Privileged User can create new Signers.
- Signer Maintenance: only a Privileged User or the owner Signer can delete a key identifier and a public key from a Signer's account.

- Supply DTBS/R: Only an authorised Privileged User is able to supply the DTBS/R on behalf of the Signer.
- Signer Key Pair Generation: only a Signer can conduct the KeyReq SAP command, requesting a new asymmetric key pair generation. Only a Privileged User can conduct the keygen CMAPI command generating a new asymmetric key pair and assigning it to a Signer's account.
- Signer Key Pair Deletion: only a Signer can conduct the NewKeyDel SAP command, requesting a key pair deletion.
- Signing: only a Signer can conduct the ChKeyPWD SAP command (which establishes or modifies the key Authorisation Data) and the "SAD" SAP command.
- SAM Maintenance: only a Privileged User can carry out the SAM Maintenance related commands, transmitting information to the SAM to manage roles and configuration.
- Signer: the order of "Signer" related commands is regulated and controlled.
- Privileged User: The order of "Privileged User" related commands is regulated and controlled.

7.3.2.6 TSF data protection

The CM ensures the security of its TSF data with:

- Self-tests: which demonstrate the correct operation of the TSF.
- Secure failure: the capability to preserve a secure state when the different types of failures occur.
- Tamper protection: tamper detecting and tamper response capabilities.

The SAM is implemented as a local application within the same physical boundary as the CM. Consequently, the CM provides its security services also for protecting the SAM.

7.3.2.7 Audit

The CM and the SAM audit all security related events. Every audit record includes a reliable time stamp, subject identity (if applicable), identifier of the related CM or SAM and a human readable descriptive string about the related event. For audit events resulting from actions of identified users, the CM and SAM associate each auditable event with the identity of the user that caused the event.

The SAM invokes the CM to protect its audit records (from unauthorized modification, deletion and audit storage exhaustion).

The CM and SAM receives a reliable time source from TOE environment.

7.3.2.8 Communication Protection

The CM enforces:

- A secure channel based on TLS protocol, for communication with ECAs;
- A secure channel based on TLS protocol, for communication with Administrator, through the SSA.
- Secure channel based on TLS protocol for internal communication among MPCAs.
- A secure channel based on SSH protocol, for communication with Administrators, using the console command interface in the provided limited shell.
- A direct channel for communication with Administrators, using the console command interface with a physical keyboard.

The SAM enforces:

- A secure channel based on TLS protocol, for communication with Privileged Users, through the SSA.
- A secure channel based on SSH protocol, for communication with Privileged Users, using the console command interface in the provided limited shell.
- A secure channel based on the proprietary SAP protocol.
- A direct channel for communication with Privileged Users, using the console command interface with a physical keyboard.

7.3.2.9 Distributed and High availability structure

In case of distributed configuration, this security function based on the distributed structure of the TOE ensures the following:

- Distributed cryptography.
- Secret sharing.
- Consistency protection.
- Fault tolerance.

In case of high availability configuration, each primary (active) MPCA has a fully redundant secondary (passive) MPCA couple. The secondary MPCA is only brought online when its associated primary node fails.

7.3.2.10 Trusted Update

The TOE provides an SSH communication path between itself and remote supplier (Developer/Manufacturer) for trusted software/firmware update. It ensures the trusted update, trusted path, and management of security functions behavior.

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 Profiles (PPs).

- EN 419221-5:2018, Protection profiles for Trust Service Provider 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].

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

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

7.7 Evaluation conduct

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

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

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

The evaluation was completed on 22 January 2024 with the issuance by LVS of the Evaluation Technical Report v2 [ETR], which was approved by the Certification Body on 15 February 2024. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

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

The certification is not a guarantee that no vulnerabilities exist; there is a probability, 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 v2 [ETR] issued by the LVS CCLab Software Laboratory (Debrecen site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Trident, the distributed remote Qualified Signature Creation Device version 3.1.3" 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".

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
Well-defined development tools	ALC_TAT.1	Pass

Assurance classes and components		Verdict
Systematic Flaw 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 2 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 (augmentations are represented 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

Assurance classes and components		**Verdict**
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Systematic Flaw 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 2 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 "Trident, the distributed remote Qualified Signature Creation Device version 3.1.3" 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 3.2 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, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([CCECG-ADM], and [CCECG-DEV]).

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

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

9.1 TOE delivery

The delivery steps and the procedures that are necessary to maintain security when distributing the TOE to the customer are described in sect. 4 of [DEL].

When the TOE is shipped by the distribution service, the customer also receives an e-mail with the following information:

- shipment information - including the serial numbers of the tamper evident seals,
- the serial number of the TOE, initial admin credentials,
- steps to be taken when the shipment arrives.

In case of TOE model B31 and B33, customer is further provided with the passwords for “bisk” and “wisk” infrastructural keys set up for the additional challenge-response check as well as the challenge and response strings - via the same email as above.

Customer is required to perform the following:

- checks the tamper evident seals on the shipment box
    - if shipment box was not physically tampered with then customer unpacks and checks the tamper evident seals and cables on the TOE;
    - if the TOE was not physically tampered with then customer starts the TOE, boots the device with the supplied disk encryption password, then checks the version and model information and the serial number shown on the screen;
- checks the TOE version and model information and the serial number with the information he/she received earlier;
- logs in to the Trident with the supplied credentials and gains access to the Limited Shell;
- (In case of TOE model B31 and B33) checks the hardware integrity by a challenge-response mechanism of the TDM device in the MPCA. The challenge-response mechanism may be declared to be optional by I4P.
- checks the validity of the received PTRNG PIN with the trng-test Limited Shell command;
- fills the acceptance checklist, signs it, and sends it back to I4P in scanned or paper form upon which the customer gets registered for guarantee and flaw remediation;

If any of the tamper seals, version information, serial number control or credential verification shows a tamper event, the customer should contact I4P and discuss further steps which may include sending back the TOE to I4P for inspection.

In case of TOE model B31 and B33, if the additional challenge-response mechanism fails it is considered a tamper event and the steps above should be followed.

9.2 Installation, configuration, and secure usage of the TOE

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

In particular, the Common Criteria Evaluated Configuration Guide [CCECG-ADM] [CCECG-DEV] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure operation of the TOE in accordance with the security objectives specified in the Security Target [ST].

10 Annex B – Evaluated configuration

The Evaluators has followed the preparation steps for the TOE defined in [CCECG-ADM] and [CCECG-DEV] for the evaluated configuration.

The evaluated configuration of the TOE includes the following items:

- one, two, three or four MPCAs;
- one CD containing the guidance documentation in PDF format which provides guidance on the evaluated configuration and refers the reader to the relevant product guides to enable him to install and operate the Trident correctly [CCECG-ADM] [CCECG-DEV].

All MPCAs include the following items:

- a metal, rack mountable box with external power supply unit;
- physical interfaces of the MPCA and internal hardware;
- the internal software:
    - the hardened OS (Red Hat Enterprise Linux, Version 7.9 (based on RHEL v7.1, which has a Common Criteria EAL 4 augmented by ALC_FLR.3, certification: BSI-DSZ-CC-0999-2016) with security fixes)
    - limited shell;
    - Multi-Party Cryptographic Module (in case of distributed configuration, then MPCAs jointly provide the CM functionality);
    - Signature Activation Module local client application (in case of distributed configuration, the n SAM LCAs jointly provide the SAM functionality);
    - OpenSSL v3.0.3 in its FIPS container with security fixes, which performs the TLS protocol and all non-distributed cryptographic functions, supports distributed cryptographic functions, and provides base functions for DRNG;
    - others LCAs (non-TOE parts).

For more details, please consult sect. 1.4 of the Security Target [ST] and to [CCECG-DEV].

10.1 TOE operational environment

The LVS reproduced the test environment consistent with [ST], [CCECG-ADM] and [CCECG-DEV]

The Evaluator’s test environment is represented in Figure 3:

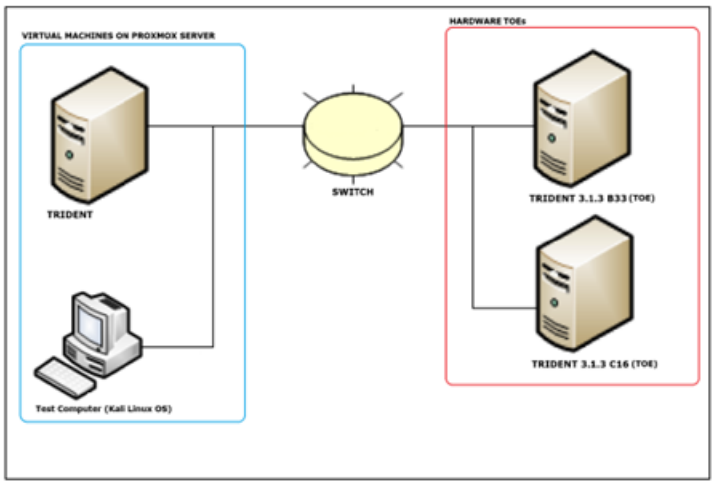

Figure 3 - TOE Environment

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 from the LVS premises.

The Evaluators verified the configuration of the test environment, including the TOE, and found it to be consistent with the Common Criteria Evaluated Configuration Guides [CCECG-ADM] and [CCECG-DEV] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The [CCECG-DEV] contains a description about how to use the CMAPI and SAP APIs. Testing the TOE can be divided into three parts:

- manual tests,
- automated tests,
- tests prepared by the laboratory.

The Developer has provided manual tests with step-by-step description and automated tests. In the site visit the Evaluators examined the Developer's testing environment where the automated tests run.

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

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

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly.

Evaluators applied sampling approach for testing the Limited Shell and fully conducted MPCM, TDM and tamper protection related tests.

Independent tests prepared by the laboratory focus, among the others, on Tampering, user management and access control functionalities, TOE status information update.

11.3.2 Test results

All Developer's tests were run successfully; 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 the actual test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

The Evaluators conducted vulnerability analysis and penetration testing activities using [AIS34] as a basis for the applied methodology of Vulnerability Assessment.

A search on public vulnerabilities on TOE and TOE components (e.g. OS) have 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 an attack potential of level High in its intended operating environment. No exploitable or residual vulnerabilities have been identified.