Agenzia per la Cybersicurezza Nazionale

OCSI

Organismo di Certificazione della Sicurezza Informatica

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

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

Certificato n. *(Certificate No.)*	05/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/01/2023/RC, v1.0
Decorrenza *(Date of 1st Issue)*	16 aprile 2024
Nome e Versione del Prodotto *(Product Name and Version)*	eTugra SAM V1.4
Sviluppatore *(Developer)*	E-Tugra EBG Information Technologies and Services Joint Stock Company
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, 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.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

eTugra SAM v1.4

OCSI/CERT/CCL/01/2023/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 16
7.5 Protection Profile conformance claims 16
7.6 Functional and assurance requirements 16
7.7 Evaluation conduct 17
7.8 General considerations about the certification validity 17
8 Evaluation outcome 18
8.1 Evaluation results 18
8.2 Recommendations 19
9 Annex A – Guidelines for the secure usage of the product 20
9.1 TOE delivery 20
9.2 Installation, configuration and secure usage of the TOE 20
10 Annex B – Evaluated configuration 21

10.1 TOE operational environment 21
11 Annex C – Test activity 22
11.1 Test configuration 22
11.2 Functional tests performed by the Developer 22
11.2.1 Testing approach 22
11.2.2 Test coverage 22
11.2.3 Test results 22
11.3 Functional and independent tests performed by the Evaluators 22
11.3.1 Test approach 22
11.3.2 Test results 23
11.4 Vulnerability analysis and penetration tests 23

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

API	Application Programming Interface
BFLA	Broken Function Level Authorization

BOLA	Broken Object Level Authorization
CM	Cryptographic Module
DB	Database
DTBS/R	Data To Be Signed / Representation
GUI	Graphical User Interface
HSM	Hardware Security Module
IdP	Identity Provider
OS	Operating System
QSCSD	Qualified Signature and Seal Creation Device
REST	Representational State Transfer
RSA	Rivest-Shamir-Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCA	Signature Creation Application
SIC	Signature Interactive Component
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

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

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

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

[NIS5] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 5/23 – Condizioni per lo svolgimento di test da remoto in valutazioni Common Criteria, versione 1.1, 21 agosto 2023

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

4.2 Technical documents

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

[ETR1] Evaluation Technical Report eTugra SAM v1.4, ETUGRA-030_ETR_v3, CCLab Software Laboratory, 15 January 2024

[ETR2] Evaluation Technical Report eTugra SAM v1.4, ETUGRA-030_ETR_v4, CCLab Software Laboratory, 10 April 2024

[INST_GUIDE] eTugra SAM v1.4 Installation Guide, Document Version: 5, Date: 2023-07-26

[OPE] eTugra SAM V1.4 AGD_OPE: Operational User Guidance Common Criteria version 3.1 revision 5 Assurance Level EAL 4+, Version: V9, Date: 2024-01-09

[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] eTugra SAM V1.4 AGD_PRE: Preparation Procedure Common Criteria version 3.1 revision 5 Assurance Level EAL 4+, Version: V8, Date: 2024-01-09.

[ST] eTugra SAM Security Target Common Criteria version 3.1 revision 5 Assurance Level EAL 4+, Document Version: v10, Date: 2024-01-09

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 named "**eTugra SAM v1.4**", developed by E-Tugra EBG Information Technologies and Services Joint Stock Company.

The TOE is eTugra Signature Activation Module (SAM) solution. eTugra SAM is deployed by Trust Service Providers (TSPs) as Trustworthy System Supporting Server Signing (TW4S) which supports both remote signatures & sealing (as defined in [EN419241-1]). The main goal of eTugra SAM is to ensure that the Signer's signing key or keys are only used under the sole control of the Signer and only used for the intended purpose by both users for remote signatures and sealing.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3, NIS5]. The Scheme is operated by the Italian Certification Body "Organismo di Certificazione della Sicurezza Informatica (OCSI)", established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

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 "eTugra SAM v1.4" 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	eTugra SAM V1.4
Security Target	eTugra SAM Security Target Common Criteria version 3.1 revision 5 Assurance Level EAL 4+, Document Version: v10, Date: 2024-01-09
Evaluation Assurance Level	EAL4 augmented with AVA_VAN.5
Developer	E-Tugra EBG Information Technologies and Services Joint Stock Company
Sponsor	E-Tugra EBG Information Technologies and Services Joint Stock Company
LVS	CCLab Software Laboratory (Budapest site)
CC version	3.1 Rev. 5
PP conformance claim	EN 419241-2:2019 [PP-SAM]
Evaluation starting date	9 February 2023
Evaluation ending date	15 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. For a detailed description it is possible to refer to the Security Target [ST].

The Target of Evaluation (TOE) is eTugra Signature Activation Module (SAM) solution. eTugra SAM is deployed by Trust Service Providers (TSPs) as Trustworthy System Supporting Server Signing (TW4S) which supports both remote signatures & sealing (as defined in [EN419241-1]). The primary objective of eTugra SAM is to guarantee that the Signer's signing key or keys are utilized exclusively under the sole control of the Signer and are employed solely for their intended purpose

for remote signatures and sealing.

The system utilizes an EN 419 221-5 Cryptographic module (CM) ([PP-CM]) to generate signing/sealing keys and produce signature values using these keys. The CM functioning as an HSM provides the necessary cryptographic functionalities. TOE is able to authenticate signer users indirectly and establish relationship between users and keys. These keys are protected keys and no other signer users can get access over other signer users key to apply signature operations.

TOE defines two types of privileged users (User Managers and Authenticated Applications i.e., Server Signing Applications). TOE authenticates both User Managers and Authenticated Applications before executing any operations. Privileged users are divided by their role to indicate which tasks they can perform:

- User Managers: Manages the TOE, create new roles / operators and performs TOE configurations.
- Authenticated Applications: Management of signer user keys, sealing keys and invoke cryptographic functions.

TOE is software component deployed in secure tamper protected environment which interacts with cryptographic module (CM) i.e., HSM to perform key generation and signature operations. Once the TOE is set up, signer user in local environment interacts with authenticated application i.e. Server Signing Application (SSA) which is registered in TOE as privileged user. SSA holds the complete signer user information (signer keys, passphrase and key handles). To perform the signature operation the SAP is used, the SAD is provided using the SAP along with other information. SAD binds the signer user authentication factor, signing key identifier, validity and DTBS/R.

Signature Creation Application (SCA) acting as business application interacts with SSA to sign document / transaction and provides the hash to be signed. Signer user authentication is performed indirectly by TOE either through IdP or a mobile application via SSA. Signer user authentication assertion, DTBS/R along with signer key identifier is attached in the Signature Activation Data (SAD). SAD is shared with TOE over Signature Activation Protocol (SAP). TOE verifies the SAD and assertion before signer user key is activated to produced qualified signature. Therefore, it follows that the signer user accesses the TOE indirectly.

Before signature operation is performed, TOE ensures that signer user has sole control of his signing / sealing keys. TOE validates the SAD integrity, verify SAD, verifies the bindings of SAD elements and then finally activate the signing key in CM to perform signature operation. During the SAD elements binding validation, TOE ensures that signer user is authenticated well before signature operation is triggered in the CM. TOE and CM are located in secure tamper protected environment.

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 primary objective of the TOE is to guarantee that the Signer's signing key or keys are utilized exclusively under the sole control of the Signer and are employed solely for their intended purpose for remote signatures and sealing.

TOE architecture is shown in Figure 1.

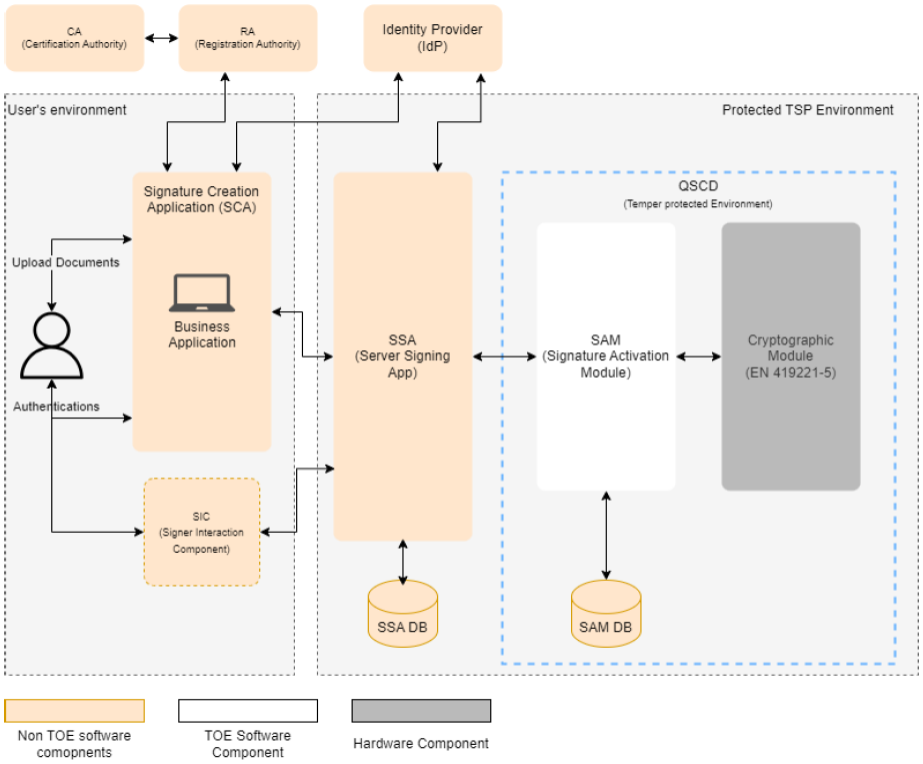

Figure 1 – TOE architecture

There are two environments which works together to perform signing; the connection between the two environments is SSA (Server Signing Application). SSA receives all the requests from the SCA or any third-party application and ensures that request format is correct and interacts with TOE for respective operation. SCA acts as a business application for SSA.

The business application initiates the signing transaction on behalf of the signer. The business application communicates with the SSA for key generation or signing requests on behalf of the signers. The signing request is kept in the queue by SSA until the signer securely authorises the signing transaction using SIC and SAP protocol.

The signer is authenticated either using IdP or a mobile application and secure channel is established from SIC to SSA. Authorisation is performed over SAP protocol. Finally, the signed hash value is sent back to the business application.

All the functions of the TOE for external components are available through SSA and SAM APIs.

SSA is available only for Business Applications and SIC to interact with. SSA has its own Administration GUI and accessible through authenticated operators using secure channel. SSA provides the required web-service interface for Applications to register signers, send signing requests etc.

eTugra SAM consists of four modules:

1. Administration APIs

   eTugra SAM provides RESTful services to apply TOE configurations e.g., Crypto Profile, Crypto Configuration keys, register authenticated applications (SSAs) and manage user managers etc.

2. Services APIs

   eTugra SAM provides RESTful services to generate signer's keys, sealing's keys and to perform signing operations etc.

3. Scheduler

   This module performs the house keeping tasks.

4. Common

   This module facilitates the other modules for the completion of their tasks. It provides supporting features for DB interaction, access management and crypto management.

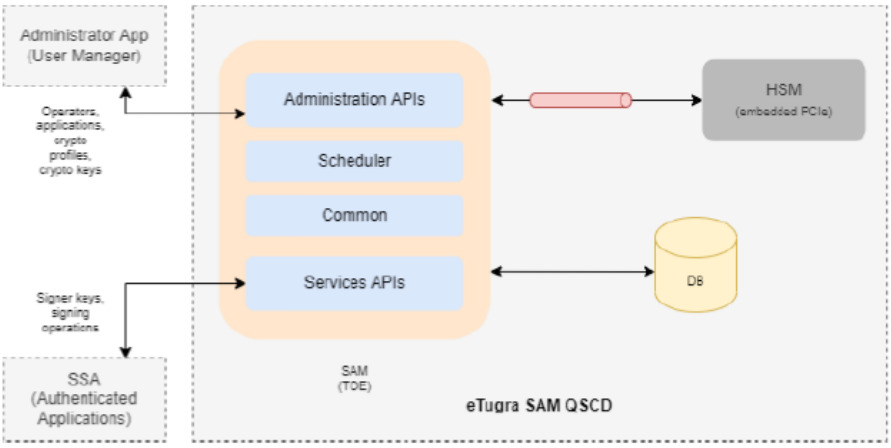

Figure 2 – eTugra SAM QSCD

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:

1) Operator management

a) User Managers create more roles and User Managers which can define other operators / security officers which can approve configurations etc.

b) User Managers create authenticated applications.

2) Signer User management

a) Authenticated applications generate signing / sealing keys and Signature Verification Data (SVD) using a CM and bind signing key ID and SVD to a signer user.

b) Authenticated applications can disable a signing key identifier to be used by a signer.

3) Signature operation

a) Signer users interacts with business application (SCA) to sign a document.

b) Business application interacts with authenticated applications (SSA) and provides hash to be signed.

c) Signer authentication along with DTBS/R, signing key identifier etc. is bound together within the Signature Activation Data (SAD). SAD is securely exchanged with the TOE over the

Signature Activation Protocol (SAP). TOE performs the following operations on the SAD before the signature operation is performed on the DTBS/R.

i) TOE verifies the SAD integrity.

ii) Signer user identify is authenticated via provided SAD.

iii) DTBS/R is taken from the provided SAD before signature operation is performed.

iv) Signing Key identifier is taken from the SAD and linked with the signer user.

v) TOE receives the authorisation data to activate the signing key referred to by the Signing Key Identifier from the SSA, and then interacts with Cryptographic module (CM) to perform signature operations.

4) Audit logs

TOE generates complete audit logs for each operation performed in the TOE either by User Managers, authenticated applications or interaction with CM. System administrators can access the audit logs and its outside the scope of TOE. Audit logs are accessible via system operations and are stored in a file which is being rotated based on the configurations defined. To protect the integrity of the contents in the log file, digital signature is applied on the log file. The path for the storage of log file is also configurable and defined by System administrator and access to that storage area is restricted to authorised representatives only. System administrators can apply the log file configuration, and this is outside of TOE scope.

5) TOE Setup

The TOE provides interfaces for the TOE setup and creation of privileged users.

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 [NIS5] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

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

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

The evaluation was completed on 15 January 2024 with the issuance by the LVS of the Evaluation Technical Report [ETR1], which was approved by the Certification Body on 12 February 2024. Then, the Certification Body issued this Certification Report. A final version of the ETR was delivered by the LVS on 10 April 2024 [ETR2] including minor changes. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in “Annex B – Evaluated configuration”.

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; there is a probability, however small, that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to regularly check the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the Developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab 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 "eTugra SAM v1.4" 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 vulnerability analysis	*AVA_VAN.5*	*Pass*

Table 1 Final verdicts for assurance requirements

8.2 Recommendations

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

Potential customers of the product "eTugra SAM v1.4" 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 overall delivery process for the e-Tugra SAM QSCD runs as follows:

1. e-Tugra initiates the process upon successful identification of the customer details and the completion of the necessary purchase order documentation between e-Tugra and the customer..
2. e-Tugra provides the eTugra SAM application binaries to the distributor on a secured channel which mandates the robust authentication measures.
3. e-Tugra notifies to the SAM distributor about the customer order through official email communication.
4. The content of the email is:
   a. Checksum of the eTugra SAM application package.
   b. Customer details where the QSCD is to be delivered.
   c. Location of the eTugra SAM application package e.g., /home/SAM-Home/SAM-Package.
   d. Location of the HSM drivers and documentation e.g., /home/SAM-Home/SAM-Drivers.
5. The SAM distributor will ensure that the SAM QSCD is properly sealed/protected through SECURITY VOID red security seal and placed in SAFEBLOCK Deposit bag. SAM distributor delivers the SAM QSCD to the customer through courier. SAM distributor informs e-Tugra and the customer about the status of the delivery. SAM Distributor will also share the details of the login credentials of the machine to the customer.
6. The customer who receives the QSCD will ensure the eTugra SAM QSCD seals have not been tampered and can also verify the checksum for the eTugra SAM application package.
7. The eTugra SAM application can be configured and setup by the end customer as provided in the documentation.

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 1.4. 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

TOE requires the following components to perform its operations:

- Cryptographic module (CM) certified against EN 419 221-5 [PP-CM] which generates signer user signing / sealing keys and activate key to perform signature operations.
- RDBMS Server (SAM DB) which holds the configuration information and a file-based storage system to hold the generated audit logs.
- Business application or signature creation application (SCA) that holds the document to be signed and sends the hash to SSA.
- Server Signing Application (SSA) which holds the signer user information and provides interfaces for signer user on-boarding, SIC interface and then interacts with SAM located inside QSCD.
- Signature Interactive Component (SIC) held by signer user in its local environment which interacts with SSA using standard secure protocols to perform SIC operations.
- An external Identity Provider (IdP) which meets the [EN419241-1] requirements and holds the authentication factors for the signer user. The IdP authenticates the user and provides an authentication assertion or token to the TOE for verification.
- eTugra SAM QSCD is authenticated from Active Directory and receives an encrypted Kerberos ticket. This Kerberos ticket is being exchanged through a secure channel with a time server which provides reliable time source.

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 both remote and local environments. The test configuration was installed by the evaluator who followed the steps described in [PRE] augmented with the [INST_GUIDE] documents.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The tests were performed via the Postman API Platform as currently there is no available GUI for the TOE. The developer provided their specific environment and collection files to repeat the tests. The collection file contains all the tests that were performed by the developer under unique identifiers.

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

The Evaluator has imported the files prepared by the Developer and ran a group of requests to correctly set up the environment for testing and to satisfy the prerequisites. The Evaluator executed the selected subset of tests on both the remote and the local instances of the TOE. Overall, there were 12 test cases conducted by the Evaluator, and these were the following (new tests):

- TCL 1: Login API - valid credentials (As an operator).
- TCL 6: Login API – Invalid or empty Password (As an operator).
- TCL 7: Login API – Valid Credentials (As an operator with Two-Factor Authentication).
- TCR 9: Create Role API – without modules.
- TCR 20: Update Role API – without modules.
- TCO 1: Create Operator – Valid data.
- TCO 4: Create Operator – Empty or Invalid Mobile.
- TCCP 12: Create Crypto Profile – Unauthorized user.
- TCCK 3: Create LOG_SIGNING_KEY (With RSA).

- TCAS 1: Add Signer API with valid data.
- TCUS 1: Update Signer API with valid data.
- TCDS 2: Delete Signer API with Invalid token.
- Reliable timestamps.

The Evaluator also created additional test cases to cover a broader range of the functionalities provided by the TOE.

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:

- Force unencrypted HTTP connection.
- Broken Object Level Authorization (BOLA) and Broken Function Level Authorization (BFLA).
- Injection attacks (SQL and OS).
- Improper Assets Management.
- Excessive Data Exposure.
- SSL Vulnerability.
- Password Brute-Force Authentication Attack.

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