Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 8/22

(Certification No.)

Prodotto: Ascertia ADSS Server Signature Activation Module v7.0.2

(Product)

Sviluppato da: Ascertia Ltd.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(AVA_VAN.5)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 29 aprile 2022

Fino a EAL2 *(Up to EAL2)*

Common Criteria

SOGIS IT SECURITY CERTIFIED

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2

OCSI/CERT/CCL/11/2021/RC

Version 1.0

29 April 2022

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for 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	29/04/2022

2 Table of contents

3 Acronyms

API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CM	Cryptographic Module
CPU	Central Processing Unit
DB	Database
DMZ	Demilitarized Zone
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
eIDAS	Electronic IDentification, Authentication and Signature
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HMAC	Keyed-hash Message Authentication Code
HSM	Hardware Security Module
HW	Hardware
ID	Identifier
IdP	Identity Provider
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
OTP	One-time Password
OS	Operating System
PIN	Personal Identification Number

PP	Protection Profile
QES	Qualified Electronic Signatures and Seals
QSCD	Qualified Signature Creation Device
RAS	Remote Application Server
SAD	Signature Activation Data
SAM	Signature Activation Module
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCAL2	Sole Control Assurance Level 2
SFR	Security Functional Requirement
SIC	Signer's Interaction Component
SSA	Server Signing Application
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Arrangement
ST	Security Target
SW	Software
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TW4S	Trustworthy System Supporting Server Signing
XML	eXtensible Markup Language

4 References

4.1 Criteria and regulations

[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, Official Journal of the European Union L 257, 28 August 2014

[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. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

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

4.2 Technical documents

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

[DEL] “ALC_DEL: Delivery Procedures - ADSS Server Signature Activation Module (SAM) v7.0”, v4, Ascertia Ltd., 28 March 2022

[ETR] “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2” Evaluation Technical Report, v2, CCLab Software Laboratory, 20 April 2022

[PRE] “AGD_PRE: Preparation Procedure - Ascertia ADSS Server Signature Activation Module (SAM) v7.0”, v5, Ascertia Ltd., 6 April 2022

[RC] “Certification Report Ascertia ADSS Server Signature Activation Module v6.0”, OCSI/CERT/SYS/08/2017/RC, version 1.0, 13 March 2019

[ST] “Security Target of Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2”, v8, Ascertia Ltd., 19 April 2022

[USR] “AGD_OPE: Operational User Guidance - Ascertia ADSS Server Signature Activation Module (SAM) v7.0”, v3, Ascertia Ltd., 28 March 2022

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 recognized under the terms of this agreement by signatory nations.

This certificate is recognized 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] has been 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 EAL 2, 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.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2”, also referred to in the following as “ADSS Server SAM”, developed by Ascertia Ltd.

The TOE is a Trustworthy System Supporting Server Signing (TW4S) that offers remote digital signature & sealing services. It ensures 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. The TOE provides remote Qualified Electronic Signatures and Seals (QES) according to eIDAS Regulation [eIDAS].

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’s 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 (Ascertia ADSS Server Signature Activation Module (SAM) v6.0), already certified by OCSI (Certificate no. 2/19 of March 13, 2019 [RC]).

Due to some changes made to the product by the Developer Ascertia Ltd., it was deemed necessary to undertake a re-certification of the TOE. The LVS CCLab Software Laboratory was able to reuse part of the documentation and evidences already provided in the previous evaluation.

Note that the changes have also led to the revision of the Security Target [ST]. Customers of the previous version of the TOE are therefore advised to take also into account the new ST.

While the considerations and recommendations already expressed for the previous TOE remain largely valid, for ease of reading this Certification Report has been rewritten in its entirety so as to constitute an autonomous document associated with the new TOE “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2”.

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 v 3.1 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 “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2” 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 review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2
Security Target	“Security Target of Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2”, v8 [ST]
Evaluation Assurance Level	EAL4 augmented with AVA_VAN.5
Developer	Ascertia Ltd.
Sponsor	Ascertia Ltd.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	EN 419241-2:2019 [PP-SAM]
Evaluation starting date	13 September 2021
Evaluation ending date	20 April 2022

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.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2” is a Trustworthy System Supporting Server Signing (TW4S) that offers remote digital signature & sealing services. It ensures 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.

The TOE provides a remote Qualified Electronic Signatures and Seals (referred to collectively as QES) service according to eIDAS Regulation [eIDAS] at Sole Control Assurance Level 2 (SCAL2) according to EN 419241-1.

The ADSS Server SAM remote signing solution consists of a local and a remote environment as illustrated in Figure 1. The Signer can initiate a signing transaction by interacting with the TOE through a Business Application.

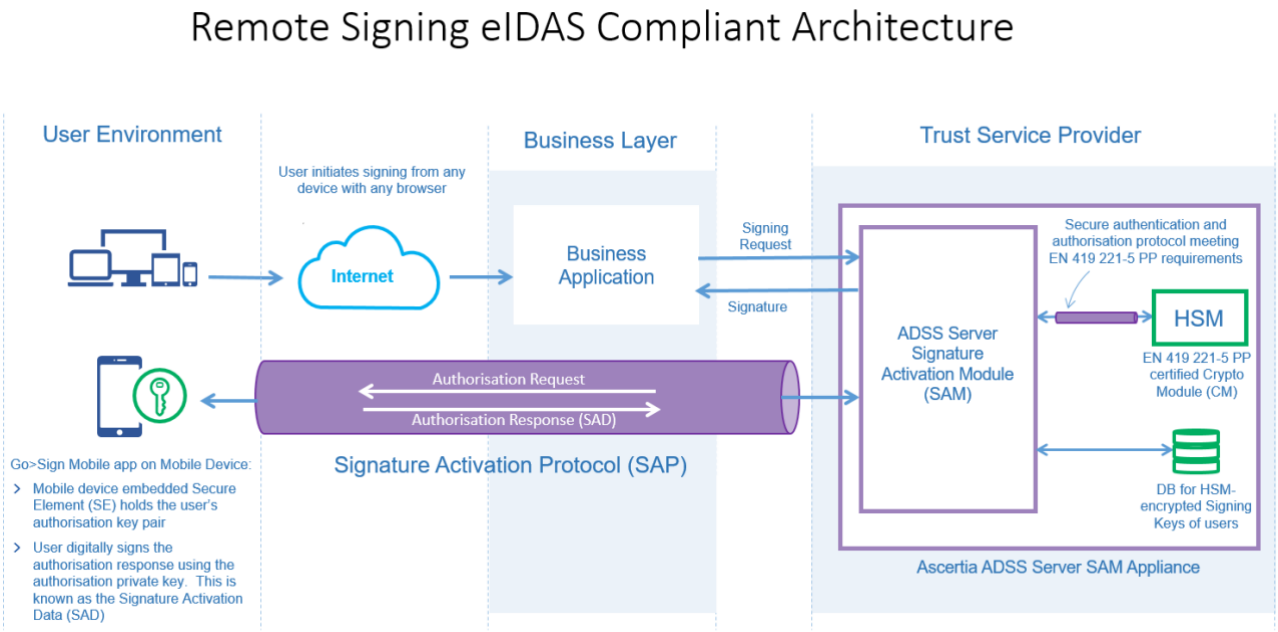

Figure 1 - Remote solution for QES according to eIDAS Regulation

For a detailed description of the TOE, consult sects. 1.4 and 1.5 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE Architecture

The TOE consists of the following main software components:

- **ADSS Server SAM Service**: provides different web services to perform various operations, e.g. User Account Registration, user key enrollment, user mobile device registration, transaction/hash signing, etc.

- **ADSS Server SAM Admin Console**: allows administrators to configure the product, e.g. define access control, signer/user management, signer device management, configuring crypto source (HSM), etc.

- **ADSS Server SAM Core**: performs various background tasks, e.g. Logs archiving, DB monitoring, HSM monitoring, etc.

The TOE is delivered within a tamper-protected hardware device to ensure a secure execution environment. The tamper protected hardware is also part of the TOE but not everything inside is part of the TOE. The operating system, application server, HSM, database, etc. do not belong to the TOE. The TOE consists of the tamper protected

hardware and the software components inside ADSS Server SAM logical boundary depicted in Figure 2.

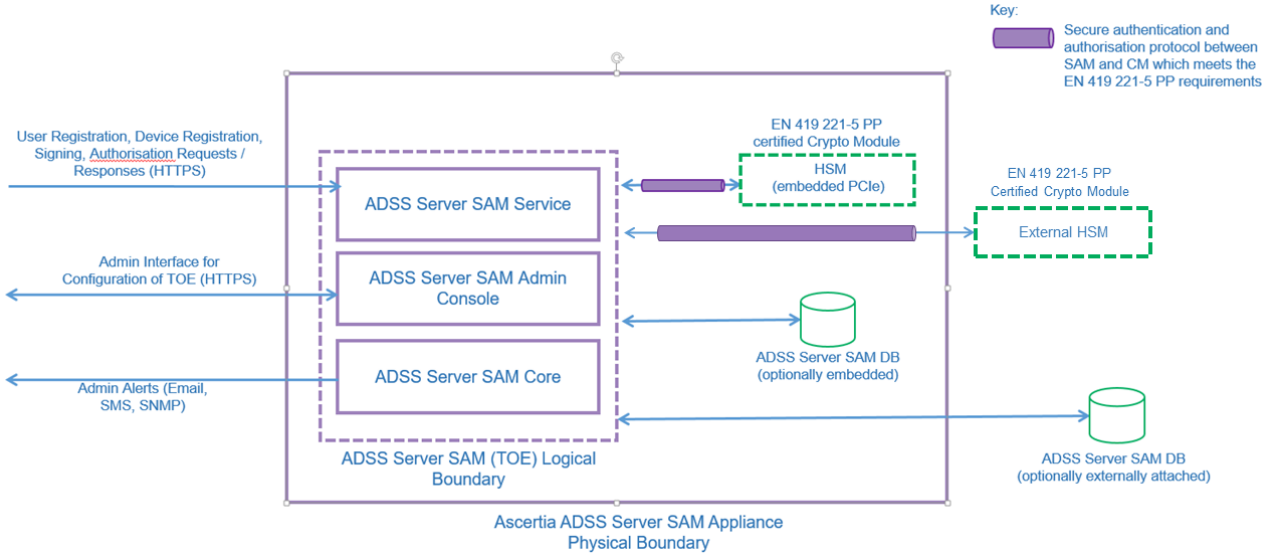

Figure 2 - TOE logical boundary

7.3.1.1 Roles & Available Functions

The TOE maintains the following roles:

- *Privileged Users*. There are two types of Privileged Users who can perform TOE specific operation through either the ADSS Server SAM Admin Console or the externally available ADSS Server SAM API:
    - *Ascertia ADSS Server SAM Operators (Operators)*: they access the Ascertia ADSS Server SAM Admin Console to perform different TOE specific operations, e.g. configuring communication with the HSM, etc. These trusted Operators are created in ADSS Server SAM Admin Console and each operator is identified by an “Operator ID”.
    - *Business Applications*: these access the TOE via APIs provided by RAS service to perform different TOE specific operations. On one hand they manage Signers (User Module) and the other, they act as Signature Creation Application (SCA). Business applications are identified by their “Client ID”.
- *Unprivileged Users*.
    - *Signers*: these are able to request remote signing operations by interacting with above business applications and then authorise these operations using the Ascertia Go>Sign Mobile app to supply the required authorisation data.

7.3.1.2 Authentication & Authorisation

The following authentication and authorisation processes occur:

- *Operators*: they must logon to the TOE using TLS client certificates before being allowed to perform any activity on the ADSS Server SAM Admin Console. Operator TLS client certificates and associated private keys should be stored on a secure smart card/USB token thereby providing an extra layer of security for the private key plus two-factor authentication of the operator. The Ascertia ADSS Server SAM Admin Console ensures that access to system objects is strictly controlled according to the user's role. Each role has a definition of which system objects it can access, and the type of access, e.g. read only, or edit/create/delete.

- *Business Applications*: they must be authenticated before accessing the TOE APIs. The business applications must also authenticate using their respective TLS client certificate because all the communication is via mutually authenticated TLS channel. The term business application refers to the ADSS RAS Service through which all business app interactions are conducted with the TOE.

- *Signers*: they are identified by the user ID and authenticated during device registration by two OTPs sent to the user's registered mobile number and email address. During the signing operation, Signers are identified via their user ID and authenticated by the signed authorisation response XML (SAD).

7.3.1.3 Cryptographic Support

The TOE does not perform cryptographic operations for its users (Signers): it does not generate/store/destroy, export/import, backup/restore, or use user key. The TOE invokes the CM with appropriate parameters whenever a cryptographic operation for the Signer is required, i.e. to authorise usage of the Assigned Key.

The TOE uses different infrastructure keys to protect its stored files and database records, and data transmitted or received via communication channels.

7.3.2 TOE security features

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

For a detailed description of the TOE Security Functions, consult sect. 7.1 of the Security Target [ST]. The most significant aspects are summarized below:

- **User Roles and Authentication**: the TOE maintains Privileged User (Operator or Business Application) and Unprivileged User (Signer) roles and associates users with roles. The TOE identifies users by means of a unique user identifier. The TOE ensures that each user has only one role, consequently a Signer can't be a Privileged User. These users are stored and maintained in different subsystems and identified with different IDs (Operator ID, Client ID, User ID).
  Privileged Users authenticate via TLS channel to the TOE. Business Application authenticates with its Client ID and certificate. Operator authenticates himself with his certificate stored on a PIN protected card.
  Signers use fingerprint authentication inside the Go>Sign Mobile app (if the Signer is already logged in) to authorize a signing request, i.e. create the SAD. This applies for direct authentication. In case of delegated authentication, supported IdP

will provide the assertion after successful authentication of the user and that assertion is added in the generated SAD at the time of authorisation.

- **Key Security**: the TOE calls with appropriate parameters a CM certified in conformance with EN 419221-5 [PP-CM] for any key management or cryptographic operations, random number generation.

- **Access and information flow control**: when ADSS Server SAM is installed, a default ADSS Server SAM Operator account is automatically created with a default Operator's certificate. The default Operator logs in to the ADSS Server SAM Admin Console and creates Privileged Users, i.e. ADSS Server SAM Operators and Client Applications.
  The TOE guarantees that only a Business Application as a Privileged User can create new Signer and initiate key pair generation on behalf of the Signer. A typical Signer registration process involves registering Signer details and generating remote signing key pair and digital certificate. Once the Signer details are registered, the Business Application requests the ADSS RAS Service to generate the signing key pair for the Signer. ADSS Server SAM uses the CM to generate and securely store the signing key pair for the Signer.

- **Data protection**: the TOE implements security functionality against physical tamper. The TOE detects when the enclosure of the TOE is opened and zeroises sensitive data, and terminates main power. This ensures that the integrity and confidentiality of the assets are preserved. During tamper state, all functionality of the TOE is stopped and no service is provided (both signatory ones and administrative ones) even if the TOE is hardware restarted. When the TOE is hardware restarted it will maintain the tamper state such that the previous tamper condition can be reported.

- **Audit**: the TOE uses an audit Database outside the TOE boundaries. The TOE logs every security related events into the Database. Each audit record contains date and time of the event (using reliable timestamp), type of event, subject identity (the identity of the user that caused the event if applicable, i.e., an identified user initiated the event), and the outcome (success or failure) of the event. The audit trail does not include any data which allows the retrieval of sensitive data.
  The integrity of the data stored in any of the tables of the Database is protected by sequenced HMAC approach. The HMAC symmetric key is securely held in the CM.

- **Communication protection**: the TOE provides protection of user data while in transit. It ensures both confidentiality and integrity. The SIC securely communicates with the RAS Service module, the SCA with the SSA and the SSA with the TOE over TLS v1.2/1.3 channel. Communication with the CM is through a secure channel using vendor specific APIs commands. TOE Operators (as Privileged Users) access the Ascertia ADSS Server SAM Admin Console GUI over a mutually authenticated TLS v1.2/1.3 channel.

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 sect. 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]. In particular, 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.

Please 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.

The evaluation was completed on 20 April 2022 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 22 April 2022. 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; it remains a probability (the smaller, the higher the assurance level) 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 check regularly 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 and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2” 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.

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

Assurance classes and components		Verdict
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
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 sect. 6 (Statement of Certification).

Potential customers of the product “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2” are suggested to properly understand the specific purpose of certification 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 sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational security policies and the assumptions described, respectively, in sects. 4.2.2.2 and 4.2.2.3 of the Security Target [ST] are respected.

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 ([DEL], [PRE], [USR]).

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 the Delivery Procedures document [DEL].

Ascertia will provide the ADSS Server SAM software to its authorised SAM distributor as a download from a secure site. Ascertia will grant access to the distributor to the dedicated ADSS SAM Appliance area of the product download site. Confirmation that the download is ready is sent to the SAM distributor via email. The email contains the cryptographic checksum of the uploaded software, and details of the customer to whom the ADSS Server SAM Appliance is to be shipped.

The SAM distributor will download the ADSS Server SAM software from the secure Ascertia site using the provided credentials and verify the checksum of the ADSS Server SAM software. The SAM distributor will construct the ADSS Server SAM Appliance by installing the required components, i.e.:

- operating system;
- database;
- the approved EN 419221-5 certified HSM (by contacting the HSM vendor and ensuring its securely delivery according to its defined procedures).

Then checksum-verified ADSS Server SAM software will be placed inside the appliance by the SAM distributor.

The SAM distributor will ensure that the SAM Appliance is properly sealed/protected and once done securely deliver the SAM appliance to the customer and inform Ascertia and the customer about the status.

The end-customer who receives the appliance will ensure the ADSS Server SAM appliance seals have not been tampered with.

9.2 Installation, initialization 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 following document 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]:

- “AGD_PRE: Preparation Procedure - Ascertia ADSS Server Signature Activation Module (SAM) v7.0”, v5, 6 April 2022 [PRE]

- “AGD_OPE: Operational User Guidance - Ascertia ADSS Server Signature Activation Module (SAM) v7.0”, v3, 28 March 2022 [USR]

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2”, developed by Ascertia Ltd.

The TOE is identified in the Security Target [ST] with the version number 7.0.2. 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 in sect. 5 of the Preparation Procedure document [PRE].

10.1 TOE operational environment

In Table 2 are summarized the hardware and software requirements of the TOE operational environment components.

For more details on the preparation of the TOE operational environment, please refer to sect. 4 of the Preparation Procedure document [PRE].

Components	Requirements
ADSS Server SAM (a Java EE 8 application supported on the listed platforms)	**Operating System** The following 64-bit operating systems are supported: • Red Hat Enterprise Linux 8.4
	Hardware AIC-TB116AN with FIPS 140-2 Level 3 Protection Intel Xeon CPU 32GB ECC DIMM RAM and 960GB SSD
	Database ADSS Server SAM saves its configuration and transactional log data in a database. The following databases are supported: • Percona-XtraDB-Cluster v8.x (A variant of MySQL)
Operator browsers	The following browsers are supported for ADSS Server SAM Operators: • Google Chrome 70.x or above • Firefox 60.x or above • Edge 35.x or above • Internet Explorer (IE) 11.X+
HSMs	The following EN 419221-5 CC certified Hardware Security Modules are supported: • Utimaco HSMs (CP5 Se500 or Se1500) • Thales Luna K7 HSMs • Entrust nShield Solo XC HSMs

Components	Requirements
Optional DMZ Proxy machine	If required, a DMZ proxy server can be configured. The following DMZ proxy machines are supported: • Windows Server + IIS or Apache or IBM HTTP Server • Linux + Apache or IBM HTTP Server Use a reasonable CPU, 8GB RAM,40 GB disk space
Mobile Devices OS	For authorised remote signing, the native apps (iOS and Android) of Go>Sign Mobile will require the following OS versions: • iOS 11 or above • Android 6 (Marshmallow) or above

Table 2 - TOE operational environment components and system requirements

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL4, augmented with AVA_VAN.5, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage and level of detail;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

For the execution of these activities a test environment has been arranged at the LVS site with the support of the Developer, which provided the necessary resources.

Before the tests, the TOE has been initialized and configured in accordance with the guidance documentation ([PRE], [USR]). After configuration of the TOE the Evaluators checked its status and found that the TOE was installed properly, and the needed services were running.

The test environment is the same as the Developer used for testing the TSFI. In particular, for testing API interfaces, the Postman tool was used, together with a short explanatory document on its usage provided by the Developer.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer used a testing approach that resulted in covering all of the TSFIs with at least one test case. The Developer created several test cases that are well-described, with all the information required to be properly repeated, including test prerequisites, step-by-step test procedures, expected and actual test results.

The Evaluators checked that the actual test results in the Developer's test documentation were consistent with the expected test results.

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 SFR and the TSFIs described in the functional specification.

11.2.3 Test results

The Evaluators executed a series of tests, a sample chosen from those described in the test plan presented by the Developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the Evaluators

Therefore, the Evaluators have designed independent testing to verify the correctness of the TSFI.

The Evaluators re-executed the independent test cases selected during the evaluation of the previous CC certified version of the TOE, with some corrections due to modifications in the Developer's test cases. To achieve a better coverage, the Evaluators selected additional test cases to further increase the number of test cases repeated.

The additional test cases executed by the Evaluators covered the following aspects of the TSF:

- Restart All Services
- Register New Client
- Import / Export Settings
- ADSS Server SAM Login
- ADSS Server SAM Logout
- Register User
- Change Password

The basis of these test cases were the test cases created during the previous evaluation; the Evaluators modified them to be applicable to the current TOE version based on the received Postman package.

Although there were issues during the execution of some test cases, the Developer corrected them and the Evaluators were finally be able to repeat all the test cases without any problem.

All independent tests performed by Evaluators passed, i.e., all the actual 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 on the same test environment already used for the functional test activities, verifying that the test configuration was consistent with the version of the TOE under evaluation.

The Evaluators first performed a search of public domain sources to identify potential vulnerabilities in the TOE, focusing on vulnerabilities discovered after the previous evaluation. The Evaluators used the Google search engine and various vulnerability databases, including Snyk Open Source Vulnerability Database, CVE Details, and NIST National Vulnerability Database (NVD), to search for vulnerabilities in the packages used by the TOE. This activity revealed two potential vulnerabilities.

In a second step, The Evaluators conducted a methodical analysis of the Security Target, guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE. The Evaluators found one additional potential vulnerability to further investigate into, but the subsequent analysis showed that it was not applicable to the TOE. No additional potentially exploitable vulnerabilities were identified.

The Evaluators then devised attack scenarios and penetration tests to verify the exploitability of the identified potential vulnerabilities in the TOE's operational environment, considering a High attack potential.

The two found vulnerabilities resulted actually exploitable during the first test session. The Developer released a minor update of the TOE containing the fixes related to these issues. The Evaluators repeated the penetration tests and determined that the two vulnerabilities had indeed been corrected.

On the basis of the results of the second session of penetration tests, the Evaluators could then conclude that no attack scenario with potential High can be completed successfully in the operational environment of the TOE as a whole. Therefore, none of the previously identified potential vulnerabilities can be exploited effectively. They have not identified residual vulnerabilities, i.e. vulnerabilities that could be exploited only by an attacker with attack potential beyond High.