Ministero dello Sviluppo Economico

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. 2/19

(Certification No.)

Prodotto: Ascertia ADSS Server Signature Activation Module v6.0
(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 Rita Forsi)
Rita Forsi

Roma, 13 marzo 2019

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Ascertia ADSS Server Signature Activation Module v6.0

OCSI/CERT/SYS/08/2017/RC

Version 1.0

13 March 2019

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	13/03/2019

2 Table of contents

3 Acronyms

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CM Cryptographic Module

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

eIDAS Electronic IDentification, Authentication and Signature

HSM Hardware Security Module

HW Hardware

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

OCSI Organismo di Certificazione della Sicurezza Informatica

PP Protection Profile

QSCD Qualified Signature Creation Device

RFV Rapporto Finale di Valutazione (Evaluation Technical Report)

SAD Signature Activation Data

SAR Security Assurance Requirement

SCA Signature Creation Application

SFR Security Functional Requirement

SIC Signer's Interaction Component

SSA Server Signing Application

SW Software

TDS Traguardo di Sicurezza (Security Target)

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

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

[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, prEN 419 221-5, v015, 29 November 2016

[PP-SAM] Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, prEN 419 241-2, v0.16, 11 May 2018

[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

[DEL] “Ascertia ADSS Server Signature Activation Module (SAM)” Delivery Procedures, v2, 24 October 2018

[PRE] “Ascertia ADSS Server Signature Activation Module (SAM)” Preparation Procedure, v4, 30 January 2019

[RFV] “Ascertia ADSS Server Signature Activation Module (SAM) v6.0” Evaluation Technical Report, v1, 7 February 2019

[TDS] “Ascertia ADSS Server Signature Activation Module (SAM) v6.0” Security Target, v18, 1 October 2018

[USR] “Ascertia ADSS Server Signature Activation Module (SAM)” Operational User Guidance, v4, 10 December 2018

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 http://www.sogisportal.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 http://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) v6.0”, short name “ADSS Server SAM v6.0”, developed by Ascertia Ltd.

The TOE is a Trustworthy System Supporting Server Signing (TW4S) that offers remote digital signature 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 No 910/2014 [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 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 [TDS]; 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 [TDS] 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 “ADSS Server SAM v6.0” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [TDS], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Ascertia ADSS Server Signature Activation Module (SAM) v6.0
Security Target	“Ascertia ADSS Server Signature Activation Module (SAM) v6.0” Security Target, v18, 1 October 2018
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	prEN 419 241-2, v0.16 [PP-SAM]
Evaluation starting date	27 September 2017
Evaluation ending date	7 February 2019

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 [TDS] are fulfilled.

7.3 Evaluated product

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

The TOE is a Trustworthy System Supporting Server Signing (TW4S) that offers remote digital signature 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 No 910/2014 [eIDAS]. This remote solution consists of a local and a remote environment as illustrated in Figure 1.

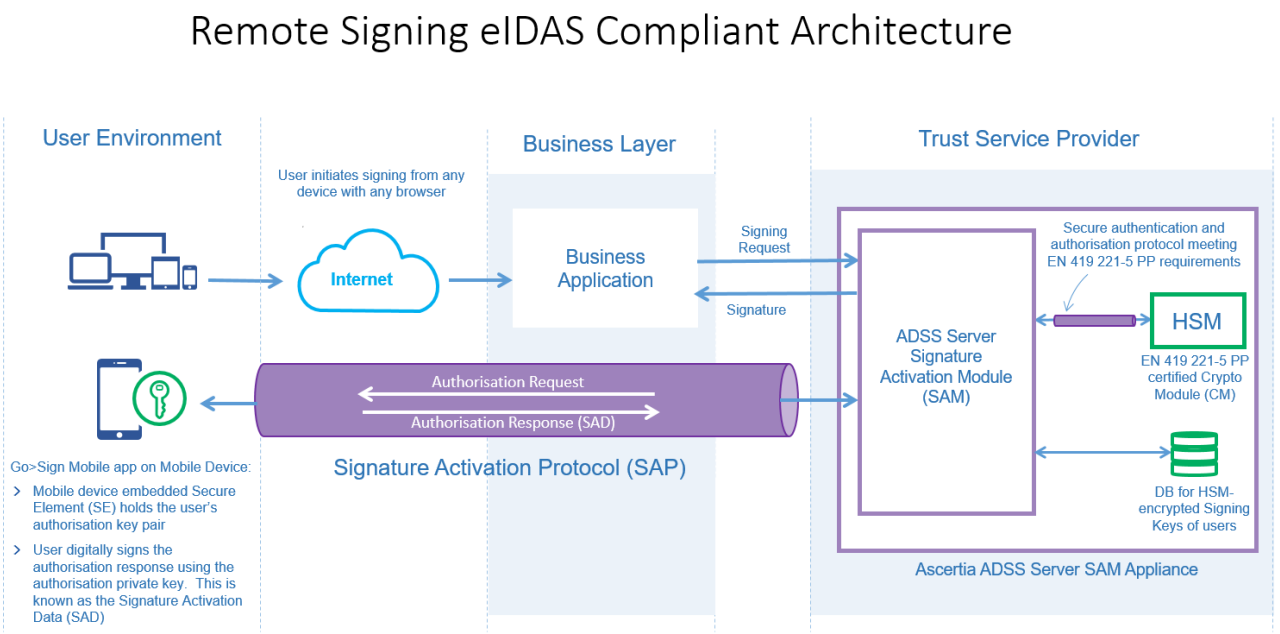

Figure 1 – Remote solution for Qualified Electronic Signatures according to eIDAS Regulation

For a detailed description of the TOE, consult sect. 1.5 of the Security Target [TDS]. The most significant aspects are summarized below.

7.3.1 TOE Architecture

The TOE "ADSS Server SAM" consists of the three components named:

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

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

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

The physical boundary of the TOE is a tamper protected hardware, which also includes some components not belonging to the TOE: the operating system, application server, HSM, database etc. The TOE consists of the tamper protected hardware and the software components inside the TOE logical boundary shown in Figure 2.

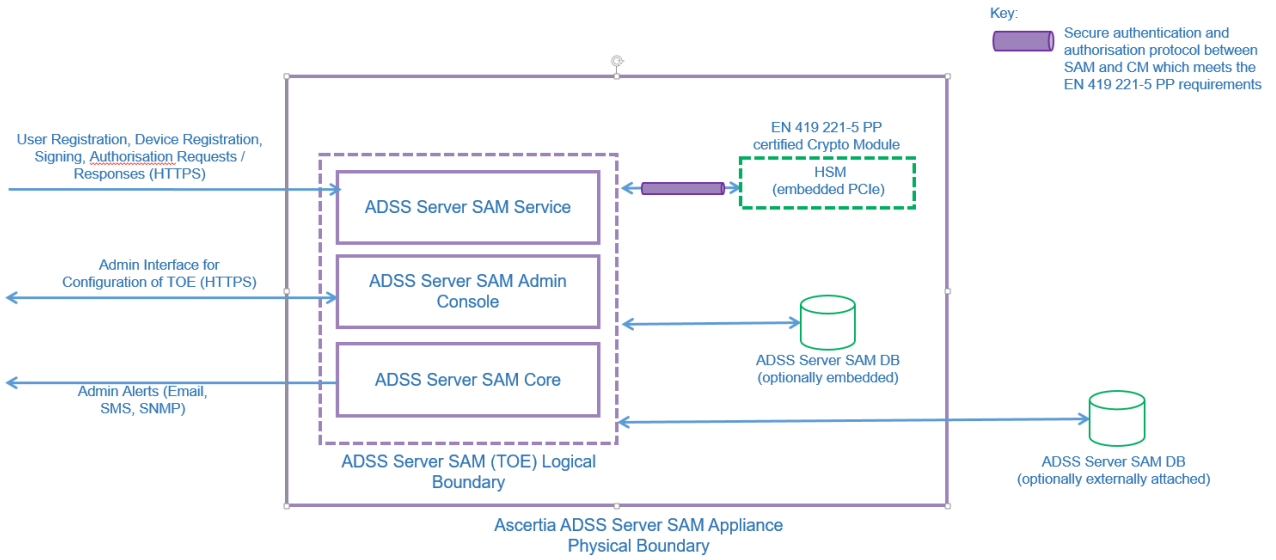

Figure 2 – TOE logical boundary

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:
  - *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 application 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 Ascertia ADSS Server SAM using TLS client certificates before being allowed to perform any activity on the Ascertia 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 revocation status of Ascertia ADSS operator TLS certificates can also be checked at the time of logon by configuring this in Ascertia ADSS Server SAM Admin Console. However, it is recommended that operators' accounts are also immediately updated on Ascertia ADSS Server SAM at the time a certificate is revoked. The Ascertia ADSS Server SAM Admin Console ensures that access to system objects is strictly controlled. Users are first identified and authenticated as explained above, and once this process is complete and the user has successfully logged in, then access to system objects is 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 Ascertia ADSS Server SAM APIs. The business applications must also authenticate using their respective TLS client certificate because all the communication is via mutually authenticated TLS channel. Note here the term Business Application refers to the ADSS RAS Service through which all business app interactions are conducted with the TOE.

- *Signer*s: 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): explicitly it does not generate/store/destroy, export/import, backup/restore, or use user key. The TOE invokes the Cryptographic Module (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 [TDS].

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

- **User Roles and Authentication (TSF_AUTH)**: 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).

- **Key Security (TSF_CRYPTO)**: The TOE calls with appropriate parameters a CM certified in conformance with prEN 419 221-5 [PP-CM] for any key management or cryptographic operations, random number generation.

- **Access and information flow control (TSF_CTRL)**: When Ascertia ADSS Server SAM is installed, a default Ascertia ADSS Server SAM Operator account is automatically created with a default Operator's certificate. The default operator logs in to the Ascertia ADSS Server SAM Admin Console and creates Privileged Users, i.e. Ascertia ADSS Server SAM Operators and Client Applications. When Operator logs in to Ascertia ADSS Server SAM Admin Console using the default operator's certificate, then a warning dialog is shown to the Operator to instruct how to change the default certificate with new Operator certificate. If Operator doesn't setup new Operator certificate within 7 (seven) days, then operator access to Ascertia ADSS Server SAM Admin Console is blocked and complete reinstallation of Ascertia ADSS Server SAM would be required. Only Operators can manage Privileged Users after successful authentication.

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

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 [TDS] claims strict conformance to the following Protection Profile:

- Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, prEN 419 241-2, v0.16, 11 May 2018 [PP-SAM]

7.6 Functional and assurance requirements

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

Please refer to the Security Target [TDS] 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.

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 prEN 419 241-2, v0.16 [PP-SAM], all the SFRs from such a PP are also included.

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 [TDS]. 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 7 February 2019 with the issuance by LVS of the Evaluation Technical Report [RFV], which was approved by the Certification Body on 26 February 2019. 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 [TDS], with reference to the operating 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 [RFV] 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 “ADSS Server SAM v6.0" 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 [TDS] 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 "ADSS Server SAM v6.0" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [TDS].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [TDS]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the [TDS] are respected.

This Certification Report is valid for the TOE in the 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

Ascertia will provide the Ascertia ADSS Server SAM software to its authorised SAM distributor. The software is encrypted using zip password-protection and uploaded to a secure FTP area hosted by Ascertia. Credentials for accessing the FTP area will be provided to the authorised SAM distributor securely using encrypted email. The email will also contain the cryptographic checksum of the uploaded software. The same email will also contain details of the customer to whom the ADSS Server SAM Appliance is to be shipped. Ascertia will provide details of how to verify the cryptographic checksum to its SAM distributor.

The SAM distributor verify the checksum on the ADSS Server SAM software after downloading it from the Ascertia FTP site. The SAM distributor will construct the ADSS Server SAM Appliance by installing the required components, i.e.:

- operating system;
- database,
- the 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 deliver the SAM appliance to the customer and inform Ascertia and the customer about the status (ETA).

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

More detail on such a procedure are contained in “Ascertia ADSS Server Signature Activation Module (SAM)” Delivery Procedures [DEL].

9.2 Installation, initialization and secure usage of the TOE

The ADSS Server SAM software will then installed by the end-customer following the defined deployment documentation.

- “Ascertia ADSS Server Signature Activation Module (SAM)” Preparation Procedures [PRE]. Preparation requires that the delivered copy of the TOE is accepted, configured and activated by the user to exhibit the protection properties as needed during operation of the TOE. The preparative procedures provide

confidence that the user will be aware of the TOE configuration parameters and how they can affect the TSF.

- “Ascertia ADSS Server Signature Activation Module (SAM)” Operational user guidance [USR]. This document helps to ensure that all types of users are able to operate the TOE in a secure manner. Operational user guidance is the primary vehicle available to the developer for providing the TOE users with the necessary background and specific information on how to correctly use the TOE's protection functions.

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “Ascertia ADSS Server Signature Activation Module (SAM) v6.0”, short name “ADSS Server SAM v6.0”, developed by Ascertia Ltd.

The TOE is identified in the Security Target [TDS] with the version number 6.0. 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.

For more details, please refer to sect. 1.5 of the Security Target [TDS].

10.1 TOE operational environment

In Table 2 are summarized the components of the operational environment of the TOE to allow its correct working.

For more details, please refer to sect. 1.4.3 of the Security Target [TDS].

Component	Requirement
ADSS Server SAM (a Java EE 8 application supported on the listed platforms)	Operating System: • Red Hat Enterprise Linux 7.4
	Hardware: • AIC-TB116-AN A modern multi-core CPU such as the Xeon E3-xxxx or E5-xxxx series is recommended, with 8GB RAM (minimum 4GB RAM) and 2GB disk space. Consider 12 GB RAM if the database is deployed on the same host as ADSS Server SAM or for high performance or throughput systems.
	Database: • Percona-XtraDB-Cluster 5.7.21 (A variant of MySQL)
Client systems (system sending service request to ADSS Server)	Any reasonable system: • ADSS Client SDK for Java API requires JRE v1.6 or above • ADSS Client SDK for .NET requires Microsoft .NET Framework 4.0 or above
Operator browsers	The following browsers are supported for ADSS Server SAM Operators: • Google Chrome 30+ • Firefox 25+ • Edge 38+ • Internet Explorer (IE) 9+

HSM	The following Hardware Security Modules are supported: • Utimaco HSMs (CP5 Se500 or Se1500)
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, 2GB RAM,100 MB 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 9.0 or above • Android 6 (Marshmallow) or above

Table 2 – TOE operational environment components

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 software application has been initialized and configured in accordance with the guidance documentation ([DEL], [PRE], [USR]), as indicated in sect. 9.2. After configuration of the TOE the evaluators checked the 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 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.

11.2.2 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.

Apart from the above mentioned Postman for API interfaces, they did not used other testing tools in addition to the specific components of the TOE that allowed to check all TSFI selected for independent testing.

In the design of independent tests, the evaluators have considered aspects that in the developer test plan were not present, or ambiguous, or inserted in more complex tests, which covered a mix of interfaces but with a level of detail not adequate.

The evaluators also designed and executed some tests independently from similar tests of the developer, based only on the evaluation documentation.

All independent tests performed by evaluators generated positive results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see sect. 11.1)

The evaluators have first verified that the test configurations were consistent with the version of the TOE under evaluation, that is indicated in the [TDS], sect. 1.3.

In a first phase, the evaluators have conducted researches using various sources in the public domain, such as Internet, books, publications, conference proceedings, including the various editions of ICCC, JIL and CCDB documents, etc., in order to identify known vulnerabilities applicable to types of products similar to the TOE. In this research the Linux operating system has been also considered, part of the operational environment, but needed for the correct operation of the TOE. They identified some potential vulnerabilities.

In a second step, the evaluators examined the evaluation documentation (Security Target, functional specification, TOE design, security architecture and operational documentation) to identify any additional potential vulnerabilities of the TOE. From this analysis, together with the source code examination, the evaluators have actually determined the presence of other potential vulnerabilities.

The evaluators have analyzed in detail the potential vulnerabilities identified in the two previous steps, to ensure their effective exploitability in the TOE operating environment. This analysis led to identify some actual potential vulnerabilities.

Therefore, the evaluators have designed some possible attack scenarios, with High attack potential, and penetration tests to verify the exploitability of the potential candidate vulnerabilities. The penetration tests have been described with sufficient detail for their repeatability using for this purpose test sheets, also used, appropriately compiled with the results, as the report of the tests themselves. The evaluator used several tools (Kali Linux, Burp Suite Pro, boofuzz, TLS Attacker 1.2 and tlsfuzzer) for executing the tests.

On the basis of the penetration tests, the evaluators have actually found that no attack scenario with potential High can be completed successfully in the operating 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.