Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

OCSI

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. 6/23

(Certificate No.)

Prodotto: ADSS PKI Server v8

(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

p. il Direttore Generale
dell'ACN

Il Capo Servizio
Certificazione e Vigilanza
(Andrea Billet)

Roma, 17 aprile 2023

[ORIGINAL SIGNED]

Common Criteria

SOGIS
IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Fino a EAL2 *(Up to EAL2)*

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Ascertia ADSS PKI Server v8

(ADSS PKI Server)

OCSI/CERT/CCL/07/2022/RC

Version 1.0

17 April 2023

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	17/04/2023

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
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

ADSS	Ascertia Digital Signing Solutions
AES	Advanced Encryption Standard

API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CM	Cryptographic Module
CMC	Certificate Management over CMS
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CVC	Card Verifiable Certificates
DB	Data Base
DEK	Data Encryption Key
ECC	Elliptic Curve Cryptography
EE	Enterprise Edition
HMAC	Hash-based Message Authentication Code (or Keyed-Hash Message Authentication)
HSM	Hardware Security Module
HTTPS	Hyper Text Transfer Protocol Secure
HW	Hardware
IT	Information Technology
KEK	Key Encryption Key
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OE	Operational Environment
OS	Operating System
PKI	Public Key Infrastructure
RA	Registration Authority
RBAC	Role Based Access Control
RSA	Rivest, Shamir, Adleman
SW	Software

TLS	Transport Layer Security
TSA	Time Stamping Authority

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. 1/13 – 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

[DEL] ADSS PKI Delivery Procedures, Version: 5, 2023-01-09.

[ETR] “Evaluation Technical Report Evaluation Assurance Level EAL 4 based on ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security Ascertia ADSS PKI Server v8 (ADSS PKI Server), v1, CCLab Software Laboratory, 13 January 2023

[ETR_v2] “Evaluation Technical Report Evaluation Assurance Level EAL 4 based on ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security Ascertia ADSS PKI Server v8 (ADSS PKI Server), v2, CCLab Software Laboratory, 15 February 2023

[PP] National Information Assurance Partnership (NIAP) - Protection Profile for Certification Authorities, Version: 2.1, 2017-12-01

[PRE] ADSS PKI Preparative procedures, Version: 4, 2022-12-14

[OPE] ADSS PKI Operational user guidance, Version: 5, 2022-12-21

[ST] ADSS PKI Server Security Target, Version: 9, 2023-01-09

[TR-03110] BSI TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1: eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015

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.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “Ascertia ADSS PKI Server v8”, short name “ADSS PKI Server”, developed by Ascertia Limited.

The TOE provides a modular trust service framework that comprises all the components required to issue, validate, and manage X.509 and ISO 7816 Card Verifiable Digital Certificates. Ascertia’s ADSS Server also provides a high performance OCSP solution for the validation of digital certificates. It provides real-time revocation and certificate whitelisting, which can be leveraged as a certificate validation hub for multiple CA’s.

The TOE delivers scalable PKI services to enterprises, governments, and trust service providers. ADSS Server exposes a web interface for system operators and a collection of API’s and standards based interfaces for the issuance, lifecycle management and validation of certificates and digital signatures.

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

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4 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 [ST] does not claim exact conformance to the Protection Profile for Certification Authorities, version 2.1 [PP] although this PP has been used as a reference.

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 PKI Server v8” 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	ADSS PKI Server v8
Security Target	ADSS PKI Server Security Target, Version: 9, 2023-01-09 [ST]
Evaluation Assurance Level	EAL4
Developer	Ascertia Ltd.
Sponsor	Ascertia Ltd.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	None
Evaluation starting date	16 May 2022
Evaluation ending date	13 Jan 2023

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 “ADSS PKI Server” is a PKI solution that manages the complete life cycle of public key certificates based on X.509 v3 and CVC BSI [TR-03110] and Certificate Revocation List based on X.509 v2 standards. It is suitable for enterprise and Internet-based Public PKIs as well as national CAs and Qualified Trust Service Providers (QTSPs) enabling the issuance, validation and lifecycle management of digital certificates for a variety of use cases, including:

- Digitally signing documents
- Code Signing
- Email Security
- Strong authentication of web servers and client via TLS
- Secure logical access to desktops and servers via smartcard logon
- Secure access to VPN Networks
- Secure physical access to buildings
- Issuing identity cards to employees, ID cards or electronic passports to citizens
- Creating and managing Country Verifying, Document Verifying CA’s and inspection system certificates for the inspection of EAC enabled machine readable travel documents.

7.3.1 TOE architecture

The TOE consists of three components:

1. **ADSS PKI Server Service**

   ADSS PKI Server Service provides different web services to perform various operations (certificate generation/revocation requests etc.) it is further divided into two sub-components:

   - **ADSS CA Service**: provides APIs to generate/renew/revoke certificates.
   - **ADSS OCSP Service**: provides APIs to get the revocation status of a certificate.

   Both ADSS CA Service and ADSS OCSP Service can be deployed on the same machine running the same application server and they can also be deployed on separate machines with their own application server.

2. **ADSS PKI Server Admin Console**

   ADSS PKI Server Admin Console allows administrators configuring the product, e.g.: define access control, certification profile management, certificate template management, configuring crypto source (i.e. HSM) etc.

3. **ADSS PKI Server Core**

   ADSS PKI Server Core performs various background tasks, e.g. Logs archiving, DB monitoring, HSM monitoring etc.

In a typical PKI infrastructure, one TOE can be deployed as a Root CA and another TOE as a subordinate CA. The ADSS OCSP Service can also be deployed separately.

TOE exists as Java EE 11 supported on a range of 64-bit operating systems as illustrated in Figure 1. The ADSS PKI Server Services are typically deployed on separate machines in an n-tier architecture. The lower-level security services are available to the higher-level trust services where applicable.

The TOE interacts with other components to implement its security functions. In the below Figure 1, the TOE is represented with blue color, all other components are outside the scope of TOE.

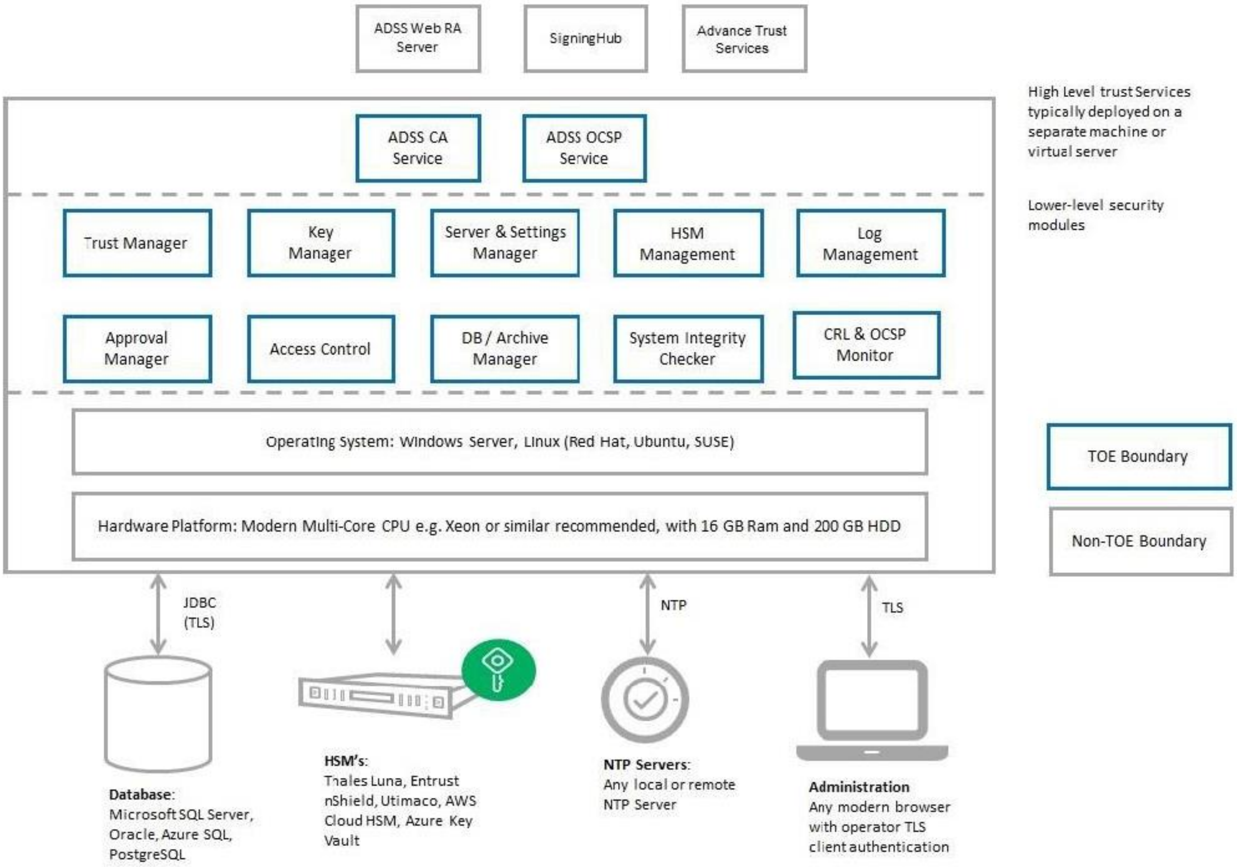
ADSS Web RA Server
SigningHub
Advance Trust Services
High level trust Services typically deployed on a separate machine or virtual server
ADSS CA Service
ADSS OCSP Service
Lower-level security modules
Trust Manager
Key Manager
Server & Settings Manager
HSM Management
Log Management
Approval Manager
Access Control
DB / Archive Manager
System Integrity Checker
CRL & OCSP Monitor
Operating System: Windows Server, Linux (Red Hat, Ubuntu, SUSE)
TOE Boundary
Hardware Platform: Modern Multi-Core CPU e.g. Xeon or similar recommended, with 16 GB Ram and 200 GB HDD
Non-TOE Boundary
JDBC (TLS)
NTP
TLS
Database: Microsoft SQL Server, Oracle, Azure SQL, PostgreSQL
HSM's: Thales Luna, Entrust nShield, Utimaco, AWS Cloud HSM, Azure Key Vault
NTP Servers: Any local or remote NTP Server
Administration Any modern browser with operator TLS client authentication

Figure 1 – TOE logical architecture and TOE boundaries

For a detailed description of the TOE, consult the Security Target [ST], section 1.4, where additional information can be found about:

- the physical and logical parts of the TOE;
- TOE delivery;

- TOE security features (TOE logical boundaries).

7.3.2 TOE security features

7.3.2.1 Security Audit

Each part of the TOE provides detailed and HMAC-protected transaction logging. The TOE audits all security related events. All the audit records produced as a result of the TOE operator actions or the API requests from any clients, are stored in Ascertia ADSS PKI Server database. The audit records do not include any data which allows the retrieval/decryption of confidential data. Each Audit record are associated with the relevant user (who performed the action), and with the relevant object (what did the user do).

TOE provides ability to view, search the audit events for specified roles (Auditors). Audit logs are stored in HMAC integrity protected database and can be backed up in digitally signed format on the file system.

In case of the audit trail cannot be written (for example he audit service is down or run out of space) there will be a rollback, meaning no operation can be committed, so there will be no change to any data that are not audited.

7.3.2.2 Communication, Trusted Path

The TOE implements and enforces the following trusted communication methods and protocols:

- Operators: operators (Administrator, Auditor, Security Officer, CA Operations Staff) access the ADSS PKI Server Admin Console GUI over a mutually authenticated TLS v1.2 channel.
- TOE Services: TOE communicates with all its services (e.g. OCSP Service) through a mutually authenticated TLS v1.2 channel.
- External Services: TOE communicates with all external client services (e.g. RA and Web RA, Remote Signing Service, Signature Validation Service, TSA Service) using TLS v1.2 channels.
- CM: the TOE communicates with CM using vendor specific APIs. User passwords do not travel on this channel. This communication with the CM is enforced by the CM to be secure, authenticated and protected from replay attacks.

The TOE provides certificate-based proof of origin and proof of receipt for issued certificates through CRLs and OCSP responses. The TOE also verifies certificate related messages using signed CMC requests and responses.

7.3.2.3 Cryptographic support

The TOE is highly dependent on a certified HSM. Most crypto operations are performed by the HSM.

Due to performance issues the TOE itself generates TLS Client and TLS Server keys and stores it in database encrypted by DEK. HTTPS using TLS is used to connect to database external services and also to connect to internal TOE components.

DEK is generated by the TOE but encrypted with KEK that is generated by and stored in HSM.

Whenever a key is generated by the TSF, the random is also generated by the TSF. If the key is generated in the HSM, the random is also generated by the HSM.

RSA and ECC schemes are supported. Key establishment is also supported.

All keys are destructed when they are not more needed. For example, when a client or a user is removed from the system, all their keys and passwords are deleted from database, device and memory and are not used anymore for any purpose.

Public keys are protected and the keyed hash of them are verified each time they are used.

Crypto functions used:

- AES encryption
  - KEK: it uses AES to encrypt/decrypt DEK.
  - DEK: it uses AES encryption to encrypt/decrypt passwords/keys in ADSS database.
  - TLS/HTTPS session keys: during TLS communication an AES key is generated to encrypt/decrypt the traffic.
- Signing
  - Certificates signed by CA keys.
  - TLS Session keys.
  - Log signing key.
  - If the key is generated by the TSF, signature is performed by the TSF. If the keys are generated in the HSM, signature is also performed by HSM.
- Hashing
  - Hashing is performed before each signing operation (certificate sign, CRL sign, TLS, log sign etc…).
  - If the key is generated by TSF, hashing is also done by the TSF. If the key is generated by the HSM, hashing is also performed by HSM.

- Keyed-Hash Message Authentication
  - If HMAC key is generated in the TOE, TOE performs the HMAC operation, if HMAC key is generated in the HSM, HSM performs the HMAC.

7.3.2.4 User Data Protection

All the user data is stored in an external database. The sensitive data is always encrypted, and the database records are HMAC integrity protected.

The user certificates are always created based on certificate templates that are pre-configured by Administrators. The certificate requests are always linked to the issued certificates. The certificate requests approvals can be done by CA Operations Staff. The TOE supports both CRL and OCSP standards for providing certificate status information. In case of any user deallocation, all its passwords and keys are made unavailable and are not re-used anymore.

All communication between any of the TOE components and its environment are TLS protected.

All the keys that are used for authentication or channel encryption are protected by integrity mechanisms just like all records in the database.

7.3.2.5 Identification and Authentication

Upon accessing the TOE, the user has to logon to the ADSS PKI Server using TLS client certificates before being allowed to perform any activity. 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. The revocation status of the TLS certificates can also be checked at the time of logon by configuring this in ADSS PKI Server. However, it is recommended that the accounts are also immediately updated on ADSS PKI Server at the time a certificate is revoked. The Ascertia ADSS PKI Server 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.

7.3.2.6 Security Management

The following subjects/entities have access to the TOE:

- **Operator:** the operator has access to ADSS PKI Server Admin Console where operator’s permissions are controlled using Role Based Access Control (RBAC) mechanism. In RBAC different roles with different permissions are created on ADSS PKI Server Admin Console and then these roles are assigned to operators. One operator is mapped to only one role at a time. These operator roles are Administrator, Auditor, Security Officer and CA Operations Staff. The first three roles come pre-installed whereas the CA Operations Staff role is created after installation to perform CA specific operations only.

- **Business Application:** it has access to web APIs of the ADSS PKI Server Service to perform different operations. A business application is first registered in ADSS PKI Server using ADSS PKI Server Admin Console where TLS client certificate of the business application is also configured. During interaction of the business application with ADSS PKI Server Service it is authenticated using its registered TLS client certificate.

7.3.2.7 Protection of the TSF

The TSF is protected via multiple security mechanisms. All sensitive data are stored encrypted via DEK (data encryption key) in the database. All the data that are stored in database are HMAC integrity protected. KEK (Key Encryption Key – that the DEK is encrypted with) is generated and stored in a certified HSM module and can never leave the HSM in plain text. Neither any other keys from the database.

The TOE monitors its services and, at any time, if any of its or its environment services become unavailable it stops working. The TOE keeps polling the relevant services and whenever they are up and running it can resume working without any user interaction. The TOE uses external database, HSM and NTP server and whenever any of these are down, it will stop working. In case of failures in the operational environment (e.g. if database or HSM is down), ADSS PKI Server detects it, stops the services and sends alerts to the operators.

TOE also supports a trusted update in case of any bugfix is needed.

7.3.2.8 TOE Access

The TOE is accessible via Admin Console and its service interfaces.

The service interfaces are protected, and each client must authenticate with their own TLS certificate before invoking any functions. The Admin Console is available after TLS certificate authentication. The Operators can logout and terminate their sessions.

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 8.3 of this report.

7.5 Protection Profile conformance claims

No Protection Profile claims are present.

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].

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].

Evaluation assurance activities that are defined in the [PP] was performed during the product evaluation. These assurance activities have augmented the CEM and are not considered to be alterations to CC Part 3 [CC3].

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 13 January 2023 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 17 February 2023 in the revised version [ETR_v2]. 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 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 and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "ADSS PKI Server v8" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, 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.

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

Assurance classes and components		**Verdict**
Sufficiency 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: security enforcing modules	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.3	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Additional assurance activities

The evaluation also included evaluation assurance activities that are defined in the [PP]. These activities augmented the CEM and are not considered to be alterations to CC Part 3.

8.3 Recommendations

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

Potential customers of the product “Ascertia ADSS PKI Server v8” 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 the Organizational Security Policies and the Assumptions described, respectively, in section 3.3 and 3.2 of the Security Target [ST] are complied.

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 ([AGD], [OPE]).

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 procedures between Ascertia and the end-customer (user) are the following:

1. Ascertia will initiate the process once the end-customer details are identified and the required purchase order between Ascertia and the end-customer paperwork is in place.
2. “Ascertia PKI Server v8” product and guidance documentation are available in “.ZIP” format in the Ascertia Community Portal for download under the Products area (https://ascertia.force.com/partners/s/product-downloads). This site requires user authentication.
3. Ascertia will grant access to the clients to grant them access to the ADSS PKI Server Software area of the product download site, ensuring at least one user account has already been created and operational.
4. Clients will authenticate to the Ascertia Community Portal and access the ADSS PKI Server Software area, when selecting the ADSS PKI Server download the site will display:
   a) Cryptographic checksum of the uploaded software.
   b) How to verify the cryptographic checksum.
5. The Client will download the ADSS PKI Server software from the secure Ascertia Community site using the provided credentials and verify the checksum on the ADSS PKI Server software.
6. Ascertia will record each download for audit purposes, this data includes the date and time of the request, Username, the Users email, the originating IP, Browser and country.
7. The ADSS PKI Server software can then be installed by the end-customer following the defined deployment documentation. The “.ZIP” package contains all the necessary documents such as the guidance documents.

End users of the certified product will be provided with instructions by e-mail about how to find and download the ADSS PKI Server by accessing the Ascertia Community Portal.

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. The guidance documents are part of the installer ".ZIP" package under <TOE-Release/docs> directory.

In particular, the following documents contain 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]:

- ADSS PKI Preparative procedures [PRE].
- ADSS PKI Operational user guidance [OPE].

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the ADSS PKI Server version 8, and it is a web application software implementing a PKI CA infrastructure running on an application server.

Ascertia's ADSS PKI Server provides a modular trust services framework that delivers all the components required to issue, validate, and manage X.509 and ISO 7816 Card Verifiable Digital Certificates. Ascertia's ADSS Server also provides a high performance OCSP solution for the validation of digital certificates and can provide real-time revocation and certificate whitelisting and can be leveraged as a certificate validation hub for multiple CA's.

ADSS PKI Server exposes a web interface for system operators and a collection of API's and standards based interfaces for the issuance, lifecycle management and validation of certificates and digital signatures. The TOE consists of three components:

1. **ADSS PKI Server Service**

   ADSS PKI Server Service provides different web services to perform various operations (e.g. certificate generation/revocation requests). it is further divided into two sub-components:

   - ADSS CA Service: Provides APIs to generate/renew/revoke certificates

   - ADSS OCSP Service: Provides APIs to get the revocation status of a certificate

   Both ADSS CA Service and ADSS OCSP Service can be deployed on same machine running on same application server and they can also be deployed on separate machines with their own application server.

2. **ADSS PKI Server Admin Console**

   ADSS PKI Server Admin Console allows administrators to configure the product, e.g. define access control, certification profile management, certificate template management, configuring crypto source i.e. HSM etc.

3. **ADSS PKI Server Core**

   ADSS PKI Server Core performs various background tasks e.g. Logs archiving, DB monitoring, HSM monitoring etc.

Other information about the TOE Environment:

- Operating System: Windows Server, Linux.

- Database: e.g. Microsoft SQL Server, Azure SQL Database, Oracle, PostgreSQL, MySQL.

- HSMs: e.g. Thales Luna, Entrust nShield, Utimaco.

- NTP Servers: Any local or remote NTP Server
- Administrator Clients: Any modern internet browser with operator TLS client authentication (smartcard/token based).

For more details, please refer to sections 1.3 and 1.4 of the Security Target [ST].

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, 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 was set up at the LVS site and it was consistent with the [ST]. The test configuration has been carried out in conformance with relevant guidance ([PRE] and [OPE]).

External tool Postman was used for testing web services.

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer used a testing approach that resulted in covering all the TSFIs with at least one test case. For each test case, the Developer's test documentation describes its purpose, the relevant TSFI(s) and SFR(s), test prerequisites, step-by-step test procedures, and 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 (SFRs) and the TSFIs described in the functional specification.

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 Testing approach

The Evaluator's sampling approach was selecting a sample of test cases created by the Developer to cover several functionalities of the TSF.

The following test cases were conducted by the Evaluator on the ADSS PKI Server Admin Console:

- TC6 – Create Certification Profile

- TC11 – Search Identity Certificate
- TC16 – Export Certification Service Logs
- TC41 – Update High Availability (HA) Configuration
- TC128 – CRL Generator Thread
- TC133 – Auto CRL Archiving Thread

11.3.2 Test results

By conducting these test cases, the Evaluator was able to properly determine the behaviour of the TOE's ADSS PKI Server Admin Console and ADSS PKI Core, and to ascertain that it is consistent with the documented TSFIs.

For the Business Application the Developer provided 4 test cases which also covers the client-sided functionalities. These test cases were also conducted to verify that the TOE behaves as described, namely – TC201, TC202, TC203, TC204.

For conducting the client-sided test cases the Developer provided the Postman package where the necessary headers and configurations were also provided.

Three tests (ADSS1, ADSS2, and ADSS3) for the ADSS PKI Server Admin Console were generated for testing the OCSP service and unused prerequisites because it was not tested using the Developer tests.

All test results conformed to what expected.

11.4 Vulnerability analysis and penetration tests

For the execution of vulnerability analysis and penetration test activities, the Evaluators worked on the same TOE sample already used for the functional test activities, verifying that the test configuration was consistent with the version of the TOE under evaluation.

The Evaluators examined sources of information publicly available and identified potential vulnerabilities regarding to:

- TLS v1.2
- Java EE 11

After further examination of these vulnerabilities the Evaluator determined that due to the specific implementation these are not exploitable.

The Evaluators performed a focused search of the Developer documentation, and three vulnerabilities were identified:

- Hidden TSFIs – undocumented open ports.
- Session termination is not working properly – the TOE can be reached even after terminating the user session.

- The TOE can be reached through unsecured network protocol (HTTP).

All the determined vulnerabilities were pertinent because the assumptions did not countermeasures them.

On the first analysis step the vulnerabilities were exploitable, but the Developer provided new TOE instance where these vulnerabilities have been fixed.

During the second analysis step the Evaluators extended the analysis to the Business Application's structure and behaviour and determined that it does not contain any vulnerability.

During site visit the Evaluator performed source code analysis and did not find any potential vulnerability regarding the implementation representation.

Based on the available information, the Evaluator did not identify residual vulnerabilities, i.e., vulnerabilities that could be exploited only by an attacker with attack potential beyond Enhanced-Basic.