Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Maintenance Report

ADSS PKI Server v8

Certificate 06/23

OCSI/MNT/ASC/01/2024/RM

Version 1.0

17 October 2024

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	17/10/2024

2 Table of contents

3 Acronyms

3.1 National scheme

LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica
IAR	Impact Analysis Report

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
SOG-IS	Senior Officials Group Information Systems
ST	Security Target
TOE	Target of Evaluation

3.3 Other acronyms

ADSS	Ascertia Digital Signing Solutions
PKI	Public Key Infrastructure

4 References

4.1 Normative references and national scheme documents

[AC] Assurance Continuity: CCRA Requirements, version 3.1 February 2024

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April Version 3.1, Revision 5, April 2017

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, luglio 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[NIS4] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 4/23 – Gestione nel tempo delle garanzie di prodotti certificati, versione 1.0, Luglio 2023

4.2 Technical documents

[CMS_v10] ADSS PKI Server v8 ALC_CMS: PROBLEM TRACKING, CM COVERAGE, version 10, 22 July 2024 (confidential document)

[CR] Certification Report of Certificate n. 6/23 ADSS PKI Server v8, version 1.0, 17 April 2023

[DELv6] ALC_DEL: Delivery Procedures, version 6, 5 March 2024 (confidential document)

[ETRv2] Evaluation Technical Report Veritas ADSS PKI Server v8 based on CC Assurance Level EAL4 augmented with ALC_FLR.3, CCLab Software Laboratory, version 2, 27 July 2024 (confidential document)

[FLRv2] ADSS PKI Server ALC_FLR: FLAW REMEDIATION PROCEDURES, version 2, 5 June 2024 (confidential document)

[IARv2] Impact Analysis Report ADSS PKI Server V8.0, version 2, 16 May 2024 (confidential document)

[SSG] Ascertia Support Services Guide, version 8.0, June 2022

[ST] ADSS PKI Server Security Target, version 11, 22 July 2024

[ST_v9] ADSS PKI Server Security Target, version 9, 9 January 2023

5 Statement of maintenance

This report is an addendum to the Certification Report [CR] of Certificate 06/2023.

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

The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The maintenance activity of the certificate identified in this report has been performed according to the Assurance Continuity requirements adopted under the international ad European mutual recognition agreements (CCRA and SOG-IS) [AC], the related Scheme Information Note (Nota Informativa dello Schema, NIS) NIS04/23, the developer’s Impact Analysis Report [IARv2].

The objective of the maintenance is to confirm the assurance that the product still complies with the security requirements specified in the associated Security Target [ST] with changes classified as *minor* as defined in [NIS4] and in [AC]. The resistance to attacks has not been re-assessed in the course of this maintenance process, therefore, the assurance as outlined in the Certificate of the product is preserved for the maintained version of the product.

The present Maintenance Report must be consulted in conjunction with [ST], specifying the functional and assurance requirements and the intended operational environment.

6 Information on maintenance

TOE name	Ascertia ADSS PKI Server v8
Security Target	ADSS PKI Server Security Target, Version 11, 22 July 2024
Evaluation Assurance Level	EAL4, augmented with ALC_FLR.3
Developer	Ascertia Ltd.
Sponsor	Ascertia Ltd.
LVS	CCLab - The Agile Cybersecurity Laboratory (Debrecen site)
Evaluation starting date	April 30, 2024
Evaluation ending date	July 25, 2024

7 Description of the changes

This section summarizes the changes applied to TOE and to other evaluation evidence.

The developer requested to include ALC_FLR.3 component. **After this update the assurance level is EAL4 augmented with ALC_FLR.3**. This added component required some additional evaluation tasks to be performed as detailed in following sections.

The TOE software is not changed. Changes to the certified product as described in [IARv2] are minor and are related to the following evidence:

- Security Target;
- Flaw Remediation Procedures;
- Content Management System;
- Delivery Procedures.

OCSI confirmed the classification *minor* of the changes. Details of changes are provided in the following sections.

7.1 Security Target

The modification in the Security Target [ST], replacing the previous one [ST_v9], is related to evaluation assurance level, in particular the sections "Conformance claims" and "Security Assurance Requirements" are updated to include ALC_FLR.3. In addition, reference to the Ascertia Support Service Guide [SSG] is added.

7.2 Flaw remediation procedures

This is new evidence with respect to the previous evaluation; it contains the description of how the Developer handles the flaws of the TOE. ALC_FLR procedures consist of two documents:

- Flaw Remediation Procedures [FLRv2]: internal procedures and handling of the flaws;
- Ascertia Support Services Guide [SSG]: instruction for the customers on how to report flaws and how they are going to be notified about the resolution of the flaws, the availability of a patch and how to apply the corrective actions.

7.3 Delivery procedures

New version of Delivery Procedures document [DELv6] is updated to include how the Ascertia Support Services Guide document is delivered to the customer together with the TOE.

7.4 Content management system

Modification reflected in [ST], [FLRv2], [DELv6] documents are listed in the [CMSv10]. There is no other change in the configuration items of the TOE.

8 Conclusion

The analysis confirmed that none of the changes affect the baseline security assurance provided by the Security Functions of the TOE except for ALC_FLR.3.

Namely, the assurance as outlined in the Certification Report [CR] is preserved for this version of maintained TOE.

All changes are confirmed as *minor*. With reference to the addition of ALC_FLR, this is explicitly classified as *minor* in the latest interpretation provided in [AC].

This report is an addendum to the Certification Report [CR] of Certificate **06/2023**.