National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Axway Validation Authority Suite 5.0

Report Number: CCEVS-VR-10959-2019
Dated: 08/02/2019
Version: 0.2

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell (Senior Validator)
Linda Morrison (Lead Validator)
Michelle Carlson
Randy Heimann
Lisa Mitchell
Clare Olin
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Tammy Compton
Raymond Smoley
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Axway Validation Authority Suite solution provided by Axway, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in August 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the Protection Profile for Application Software, Version 1.2, 22 April 2016.

The Target of Evaluation (TOE) is the Axway Validation Authority Suite Version 5.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Axway Validation Authority Suite (ASPP12) Security Target, Version 1.0, 08/01/2019 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Axway Validation Authority Suite Version 5.0 (Specific models identified in Section 8)
Protection Profile	Protection Profile for Application Software, Version 1.2, 22 April 2016
ST	Axway Validation Authority Suite Security Target, Version 1.0, 08/01/2019
Evaluation Technical Report	Evaluation Technical Report for Axway Validation Authority Suite, Version 0.4, 08/02/2019
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Axway, Inc.
Developer	Axway, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Axway Validation Authority (VA) Suite provides a comprehensive, scalable, and reliable framework for real-time validation of digital certifications for the Public Key Infrastructure (PKI). The Axway VA Suite provides a variety of PKI and certificate management functionality to prevent revoked credentials from being used for secure email, smart card login, network access (including wireless), or other sensitive electronic transactions. The Axway VA Suite provides the following functionality:

- Maintains and processes a store of digital certificate revocation data by obtaining the digital Certificate Revocation List (CRL) from multiple CA or VA sources and performing end-to-end certificate validation if one or more intermediate CAs are used and the validation policy requires a complete certificate chain validation.
- Generates and signs OCSP/SCVP responses.[1] Maintains a cache loaded with OCSP responses that are pre-computed or dynamically built up by proxy client requests to a responder.
- Allows caching of CRLs and delta CRLs to support non-OCSP clients or clients that want to maintain their own revocation data caches for backup and in low-bandwidth and non real-time environments.
- Supports SSL-based communications with clients, digitally signed client requests/responses, and digitally signed XML logs and CRL archives, as well as SSL-based server administration.
- Supports software PKCS #11 or CAPI token based hardware signing and encryption products, including hardware security modules from leading vendors that comply with FIPS 140-2 Level 2 or above.[2]

For purposes of this evaluation, the Axway VA Suite is a software application that offers CAVP certified cryptographic functions (key generation, hashing, signing, random bit generation), secure remote administration, secure storage of credentials, X.509 certificate validation and authentication, trusted update, anti-exploitation capabilities and restricted network communications.

3.1 TOE Evaluated Configuration

Details regarding the evaluated configuration are provided in Section 8.

[1] The generation and signing of OCSP/SCVP has not been tested in the evaluated configuration.
[2] The use of a Hardware Security Module (HSM) is not included in the evaluated configuration.

3.2 TOE Architecture

The Axway Validation Authority Suite consists of three software components, the Validation Authority Server, the Desktop Validator (Standard and Enterprise Editions) and the Server Validator, which run on one of the following platforms:

- Microsoft Windows 2012 (64 bit) on a 64 bit Intel Xeon processor
- RHEL 7 (64 bit) on a 64 bit Intel Xeon processor

The Windows and RHEL platforms are part of the operating environment of the TOE. The Axway VA Suite applications and the particular platforms they each run on are described below:

1. Validation Authority Server (VA Server) – the VA Server is comprised of the VA validation server acting as either a Repeater or Responder operating on a Windows or Linux platform, and the Web based administration (Admin UI). The VA Server maintains a store of digital certificate revocation data and ensures the integrity and validity of online transactions by delivering realtime validation of digital certificates.

2. Desktop Validator (DV) - (Standard and Enterprise Editions) - the Desktop Validator is a Microsoft CAPI compliant revocation trust provider that communicates with the Validation Authority Server (VA server) in responder mode to check status of digital certs in real time. DV runs as a service on a 64bit Microsoft Windows platforms and can be invoked to validate standard X.509v3 digital certificates issued by any Certificate Authority (CA). The DV Standard edition provides certificate validation support for client applications, while the DV Enterprise edition provides certificate validation support for both client and server applications.
3. Server Validator (SV) – the Server Validator provides revocation status checking of client certificates for web servers. SV serves as an interface between a secure web server and a VA Server. The SV runs on Windows and Linux. Web servers requiring SSL and client authentication can use the Server Validator to add revocation checking for certificates to authenticate to web servers or web-enabled applications.

The cryptographic capabilities of Axway VA Suite are provided by the Axway Security Kernel and are maintained across all three TOE software applications. The Axway Security Kernel (version 3.0.2) is a software cryptographic module that is implemented as two dynamic link libraries (DLLs) on Windows or two Shared Objects (SOs) on Linux. It is a user space shared library built upon a custom version of OpenSSL 1.0.2k. The implementation of TLS/HTTPS to secure communication channels is supported using Apache.

The TOE components of the Axway VA Suite all share the same underlying cryptographic library and can be deployed together to provide a robust and flexible certificate validation solution that covers both desktop and web enabled applications.

3.3 Physical Boundaries

The TOE is composed of three software-only applications which execute on a Microsoft Windows or RHEL operating system platform. The underlying platform is considered part of the operating environment but provides some of the security functionality required by the ASPP12.

Specifically, the evaluated configuration includes the following:

- Axway Validation Authority Server v5.0 - a software server application running on the following two platforms:
  - Microsoft Windows 2012 (64 bit) on a 64 bit Intel Xeon processor
  - RHEL 7 (64 bit) on a 64 bit Intel Xeon processor
- Axway Desktop Validator (Standard & Enterprise Editions)[3] v5.0 – a software client application running on the following platform:
  - Microsoft Windows 2012 (64 bit) on a 64 bit Intel Xeon processor
- Axway Server Validator v5.0 – a software client application running on the following two platforms:
  - Microsoft Windows 2012 (64 bit) on a 64 bit Intel Xeon processor
  - RHEL 7 (64 bit) on a 64 bit Intel Xeon processor

Server Validator provides revocation checking for the following web servers in the operational environment: Apache 2.4.39 or higher and Oracle HTTP Server (OHS) 12c.

[3] The Enterprise Edition of the Desktop Validator was tested in the evaluated configuration.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted path/channels

4.1 Cryptographic support

The TOE uses CAVP-validated cryptographic algorithm implementations, provided by the Axway Security Kernel, a cryptographic module built upon a custom version of OpenSSL 1.0.2k, to support asymmetric key generation, encryption/decryption, signature generation and verification and establishment of trusted channels to protect data in transit. The TOE provides a web server for TLS/HTTPS to facilitate trusted remote communications and implements functionality to securely store key data related to secure communications. The TOE also relies on the underlying platform to generate entropy that is used as input data for the TOE's deterministic random bit generator (DRBG).

4.2 User data protection

The TOE does not access any hardware resources or sensitive information repositories and no sensitive data is stored in non-volatile memory. Inbound and outbound network communications are restricted to those that are user-initiated.

4.3 Identification and authentication

The TOE implements X509 certificate validation to validate the revocation status of certificates using CRL. The TOE uses X509 certificates to support HTTPS/TLS authentication.

4.4 Security management

The TOE provides a Web-based Graphical User Interface (Web GUI) to access and manage the TOE security functions. When configured with default credentials or no credentials, the TOE restricts its functionality and only allows the ability to set new credentials. By default, the TOE is configured with file permissions to protect itself and its data from unauthorized access.

4.5 Privacy

The TOE does not transmit personally identifiable information (PII) over any network interfaces.

4.6 Protection of the TSF

The TOE protects itself against exploitation by implementing address space layout randomization (ASLR) and by not allocating any memory region for both write and execute permission. The TOE is compiled for both Windows and Linux with stack-based buffer overflow protection and does not allow user-modifiable files to be written to directories that contain executable files. The TOE uses standard platform APIs and includes a number of third party libraries used to perform its functions.

The TOE includes mechanisms to check for updates and to query the current version of the application software. TOE software is digitally signed and distributed using the platform-supported package manager (Windows or Linux). The TOE does not update its own binary code in any way and when removed, all traces of the TOE application software are deleted.

4.7 Trusted path/channels

The TOE protects communications between itself and remote administrators using HTTPS/TLS.

5 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Application Software, Version 1.2, 22 April 2016

That information has not been reproduced here and the ASPP12 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP12 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the ASPP12 and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP12 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Axway Validation Authority Version 5.0 Common Criteria Guide, 31 July 2019

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report (ASPP12) for Axway Validation Authority Suite, Version 0.4, 08/02/2019 (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the ASPP12 including the tests associated with optional requirements.

8 Evaluated Configuration

The TOE is composed of three software-only applications which execute on a Microsoft Windows or RHEL operating system platform. The underlying platform is considered part of the operating environment but provides some of the security functionality required by the ASPP12.

- Axway Validation Authority Server v5.0 - a software server application running on the following two platforms:
  - Microsoft Windows 2012 (64 bit) on a 64 bit Intel Xeon processor
  - RHEL 7 (64 bit) on a 64 bit Intel Xeon processor
- Axway Desktop Validator (Standard & Enterprise Editions)[4] v5.0 – a software client application running on the following platform:
  - Microsoft Windows 2012 (64 bit) on a 64 bit Intel Xeon processor
- Axway Server Validator v5.0 – a software client application running on the following two platforms:
  - Microsoft Windows 2012 (64 bit) on a 64 bit Intel Xeon processor
  - RHEL 7 (64 bit) on a 64 bit Intel Xeon processor

Server Validator provides revocation checking for the following web servers in the operational environment: Apache 2.4.39 or higher and Oracle HTTP Server (OHS) 12c.

[4] The Enterprise Edition of the Desktop Validator was tested in the evaluated configuration.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Validation Authority Suite TOE to be Part 2 extended, and to meet the SARs contained in the ASPP12.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Axway Validation Authority Suite 5.0 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the ASPP12 related to the examination of the information contained in the TSS.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the ASPP12 and recorded the results in a Test Report, summarized in the AAR.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)

The search was performed on 08/02/2019 with the following search terms:

- Axway Validation Authority Suite
- Axway
- Validation Authority
- Server Validator
- Desktop Validator
- Curl
- Openldap
- Apache
- Zlib
- Xerces
- sqlite 3
- Sqlite
- net snmp
- openssl

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 **Validator Comments/Recommendations**

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Axway Validator Authority Common Criteria Guide version 5.0, dated July 31, 2019*.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target.

11 **Annexes**

Not applicable

12 **Security Target**

The Security Target is identified as: *Axway Validation Authority Suite (ASPP12) Security Target, Version 1.0, 08/01/2019*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Protection Profile for Application Software, Version 1.2, 22 April 2016.

[5] Axway Validation Authority Suite (ASPP12) Security Target, Version 1.0, 08/01/2019 (ST).

[6] Assurance Activity Report (ASPP12) for Axway Validation Authority Suite, Version 0.4, 08/02/2019 (AAR).

[7] Detailed Test Report (ASPP12) for Axway Validation Authority Suite, Version 0.3, 08/02/2019 (DTR).

[8] Evaluation Technical Report for Axway Validation Authority Suite, Version 0.4, 08/02/2019 (ETR)