National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Axway Desktop Validator, version 5.2

Report Number: CCEVS-VR-VID11451-2024
Dated: July 15, 2024
Version: 1.0

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Lisa Mitchell
Linda Morrison
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Julia Miller
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Axway Desktop Validator 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. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in July 2024. 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 Extended, and meets the assurance requirements of the *Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14).

The Target of Evaluation (TOE) is the Axway Desktop Validator, version 5.2.

The TOE identified in this VR 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 VR 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 Desktop Validator, version 5.2 Security Target*, version 0.5, July 2, 2024 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 Desktop Validator, version 5.2 (Specific models identified in Section 8)
Protection Profile	*Protection Profile for Application Software*, Version 1.4, 7 October 2021 (ASPP14)
ST	*Axway Desktop Validator, version 5.2 Security Target*, version 0.5, July 2, 2024
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor & Developer	Axway, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Lisa Mitchell, Linda Morrison, Lori Sarem

3 Architectural Information

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

The Target of Evaluation (TOE) is the Validation Authority Desktop Validator, version 5.2.

3.1 TOE Description

The Axway Desktop Validator (DV) is part of Axway's Validation Authority Suite, which 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 DV 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.
- 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.

3.2 TOE Evaluated Platforms

The Axway Desktop Validator allows installation on Microsoft Windows on one of the following platforms:

- Microsoft Windows 10/11 (64 bit) on a 64 bit Intel Xeon processor
- Microsoft Windows Server 2022 (64 bit) on a 64 bit Intel Xeon processor

The Windows platform is part of the operating environment of the TOE. The TOE can execute on any Intel Xeon processor, however the lab tested the TOE on an Intel Xeon E5-2670. The lab also tested the TOE on Windows 11 (64 bit) and Windows Server 2022 (64 bit) in the evaluated configuration.

3.3 TOE Architecture

The Axway VA Suite is composed of the following applications:

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 real-time 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.

As the focus of this evaluation is on the DV, the lab tested the DV Enterprise edition as the Enterprise edition is a superset that includes the Standard edition's functionality. The diagram below shows the TOE's interaction with components in its environment.

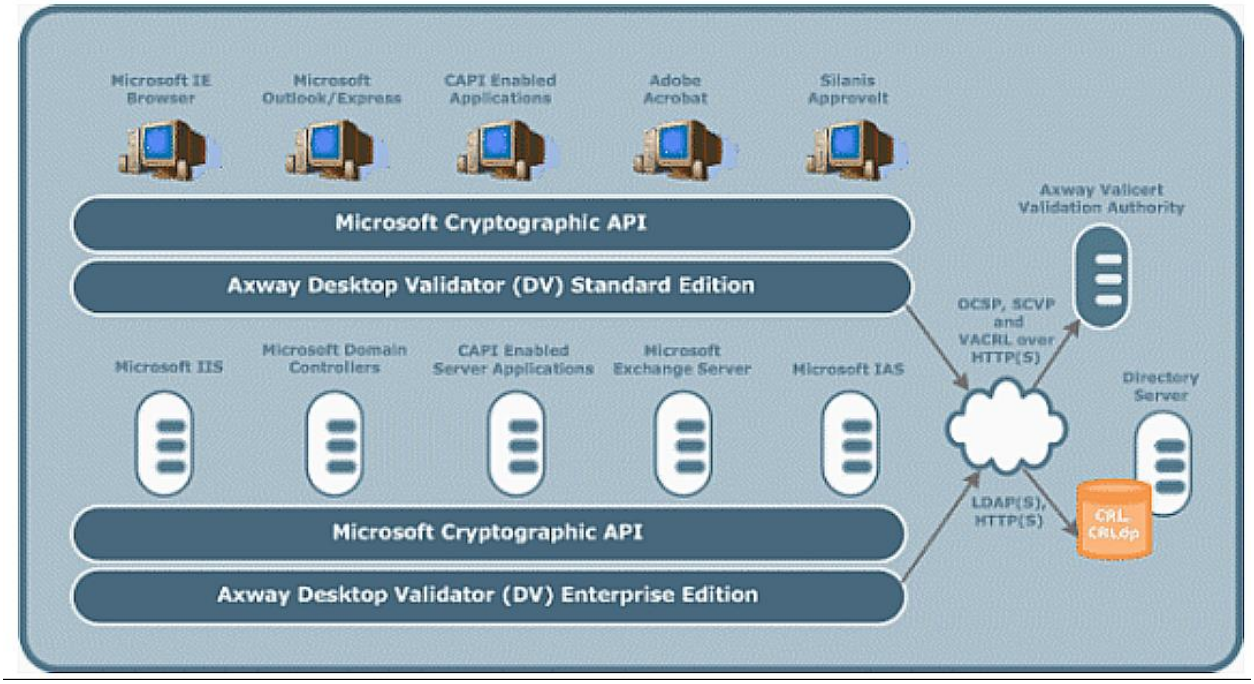

Figure - Axway Desktop Validator (DV) Diagram

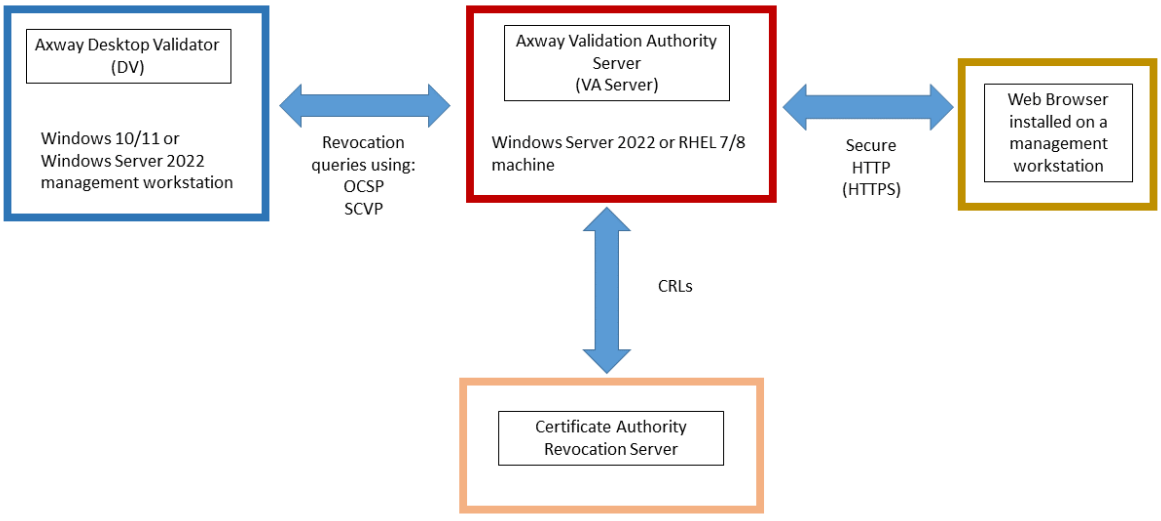

Figure - Axway Desktop Validator (DV) interaction with additional components

The cryptographic capabilities of Axway DV are provided by the Axway OpenSSL version 3.0.13 (with 3.0.8 FIPS), which is a software cryptographic module that is implemented as two dynamic link libraries (DLLs) on Windows. It is a user space shared library built upon a custom version of OpenSSL 3.0.

3.4 Physical Boundaries

The TOE is a software-only application which executes on a Microsoft Windows operating system platform. The underlying platform is considered part of the operating environment but provides some of the security functionality required by the ASPP14.

Axway Desktop Validator (Standard & Enterprise Editions)[1] v5.2 – a software client application running on Windows 10, Windows 11, or Microsoft Windows Server 2022 (64 bit) on a 64 bit Intel Xeon processor.

The TOE also requires a Certificate Authority (CA) Revocation Server in the operational environment to provide the revocation status of valid digital certificates.

4 Security Policy

This section summaries the security functionality of the TOE:

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

4.1 Cryptographic support

The TOE does not generate any asymmetric keys.

4.2 User data protection

The TOE does not access any hardware resources (other than network connectivity) or sensitive information repositories. The TOE does not store any sensitive data in non-volatile memory. Inbound and outbound network communications are restricted to those that are application initiated.

4.3 Security management

The TOE provides the ability to configure enhanced revocation checking. The TOE also provides the ability to check for TOE updates.

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

4.4 Privacy

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

4.5 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 Windows 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). The TOE does not update its own binary code in any way and when removed, all traces of the TOE application software are deleted.

4.6 Trusted path/channels

The TOE does not transmit any sensitive data across the network.

5 Assumptions & Clarification of Scope

Assumptions
The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

Clarification of scope
The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14 as described for this TOE in the ST. 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.

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 Protection Profile for Application Software 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.
- Apart from the Admin Guide, additional customer documentation for the specific Software Application models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- 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 ASPP14 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The vendor offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- *Validation Authority Common Criteria Guide*, Version 5.2, July 1, 2024

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

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 proprietary *Detailed Test Report for Axway Desktop Validator*, version 5.2, Version 0.2, July 2, 2024 (DTR), as summarized in the *Assurance Activity Report for Axway Desktop Validator*, version 5.2, Version 0.2, July 2, 2024 (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 to a Common Criteria Certification document and ran the tests specified in the ASPP14 including the tests associated with optional and selection-based requirements. The evaluation team executed the tests specified in the test plan and documented the results in the test report listed above.

Testing took place from October 2023 through July 2024 within the Gossamer Security Solutions laboratory in Columbia, MD following the procedures identified in the Gossamer Quality Manual with no deviations. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 Evaluated Configuration

The TOE runs on the evaluated platforms identified in Section 3.2.

The environmental components described in the following table are required to operate the TOE in the evaluated configuration.

Component	Description
Axway VA server (Mandatory)	The Axway Validation Authority server is another application in the Axway Validation Authority Suite. The TOE interfaces with the VA Server to use the VA server's certificates for outgoing revocation queries.
Management Workstation (Mandatory)	A workstation used by an administrator to locally manage the TOE. The workstation must have an operating system that is one of the claimed versions. The TOE is also installed on the workstation.
Certificate Authority Revocation Server (Mandatory)	The Axway DV requires a Certificate Authority (CA) Revocation Server to obtain certificate revocation data. The Axway DV obtains a digital Certificate Revocation List (CRL) from the CA revocation server.

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 Axway Desktop Validator TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14.

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 Desktop Validator, version 5.2 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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 ASPP14 related to the examination of the information contained in the TSS.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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 ASPP14 and recorded the results in a Test Report, summarized in the AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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 evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “Axway”, “Axway Desktop Validator”, “Axway Security Kernel”, “curl”, “openldap”, and “openssl”.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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 suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the SFRs specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Axway Desktop Validator, version 5.2 Security Target, Version 0.5, July 2, 2024.*

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 1.4, 7 October 2021 (ASPP14).

[5] *Axway Desktop Validator, version 5.2 Security Target*, Version 0.5, July 2, 2024 (ST).

[6] *Assurance Activity Report for Axway Desktop Validator*, version 5.2, Version 0.2, July 2, 2024 (AAR).

[7] *Detailed Test Report for Axway Desktop Validator, version 5.2*, Version 0.2, July 2, 2024 (DTR).

[8] *Evaluation Technical Report for Axway Desktop Validator, version 5.2*, Version 0.2, July 2, 2024 (ETR).

[9] *Validation Authority Common Criteria Guide*, Version 5.2, July 1, 2024 (AGD).