Axway Desktop Validator, version 5.2 Security Target

Version 0.5
07/02/2024

Prepared for:

Axway, Inc.

16220 N Scottsdale Road, Ste 500
Scottsdale, AZ 85254

Prepared By:

Gossamer Laboratories

www.gossamersec.com

1. SECURITY TARGET INTRODUCTION 3
1.1 SECURITY TARGET REFERENCE 3
1.2 TOE REFERENCE 3
1.3 TOE OVERVIEW 4
1.4 TOE DESCRIPTION 4
1.4.1 TOE Architecture 4
1.4.2 TOE Documentation 7
2. CONFORMANCE CLAIMS 8
2.1 CONFORMANCE RATIONALE 8
3. SECURITY OBJECTIVES 9
3.1 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 9
4. EXTENDED COMPONENTS DEFINITION 10
5. SECURITY REQUIREMENTS 11
5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 11
5.1.1 Cryptographic support (FCS) 11
5.1.2 User data protection (FDP) 12
5.1.3 Security management (FMT) 12
5.1.4 Privacy (FPR) 13
5.1.5 Protection of the TSF (FPT) 13
5.1.6 Trusted path/channels (FTP) 14
5.2 TOE SECURITY ASSURANCE REQUIREMENTS 14
5.2.1 Development (ADV) 14
5.2.2 Guidance documents (AGD) 15
5.2.3 Life-cycle support (ALC) 16
5.2.4 Tests (ATE) 17
5.2.5 Vulnerability assessment (AVA) 17
6. TOE SUMMARY SPECIFICATION 18
6.1 CRYPTOGRAPHIC SUPPORT 18
6.2 USER DATA PROTECTION 18
6.3 SECURITY MANAGEMENT 18
6.4 PRIVACY 19
6.5 PROTECTION OF THE TSF 19
6.6 TRUSTED PATH/CHANNELS 21

LIST OF TABLES

Table 1 IT Environment Components 6
Table 2 TOE Security Functional Components 11
Table 3 Assurance Components 14

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Validation Authority Desktop Validator provided by Axway, Inc.. The TOE is being evaluated as a software applications.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – Axway Desktop Validator, version 5.2 Security Target

ST Version – Version 0.5

ST Date – 07/02/2024

1.2 TOE Reference

TOE Identification – Axway Desktop Validator, version 5.2

TOE Developer – Axway, Inc.

Evaluation Sponsor – Axway, Inc.

1.3 TOE Overview

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

1.4 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.

The focus of this evaluation is the Axway Desktop Validator (DV). The Axway DV is a software application that offers configuration of advanced revocation status reporting, anti-exploitation capabilities and restricted network communications. This evaluation is limited to the security functions claimed in Section 5 and further described in Section 6 of this Security Target (ST).

1.4.1 TOE Architecture

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.

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.

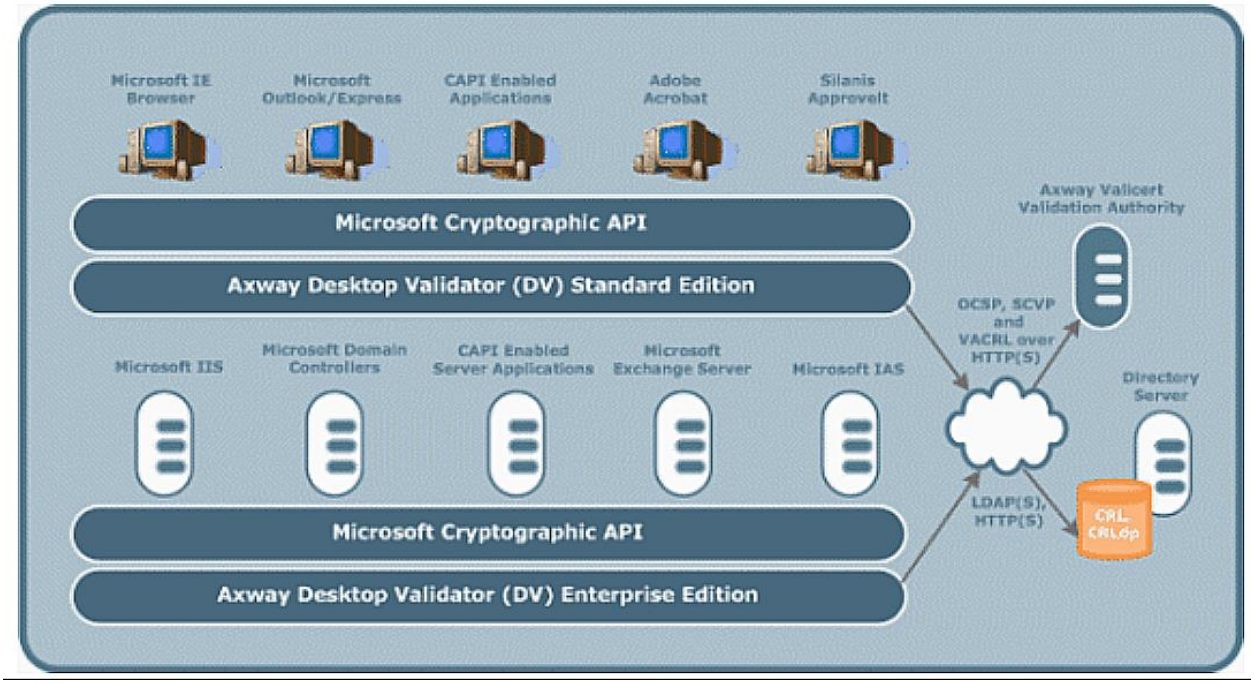

Figure 1 - Axway Desktop Validator (DV) Diagram

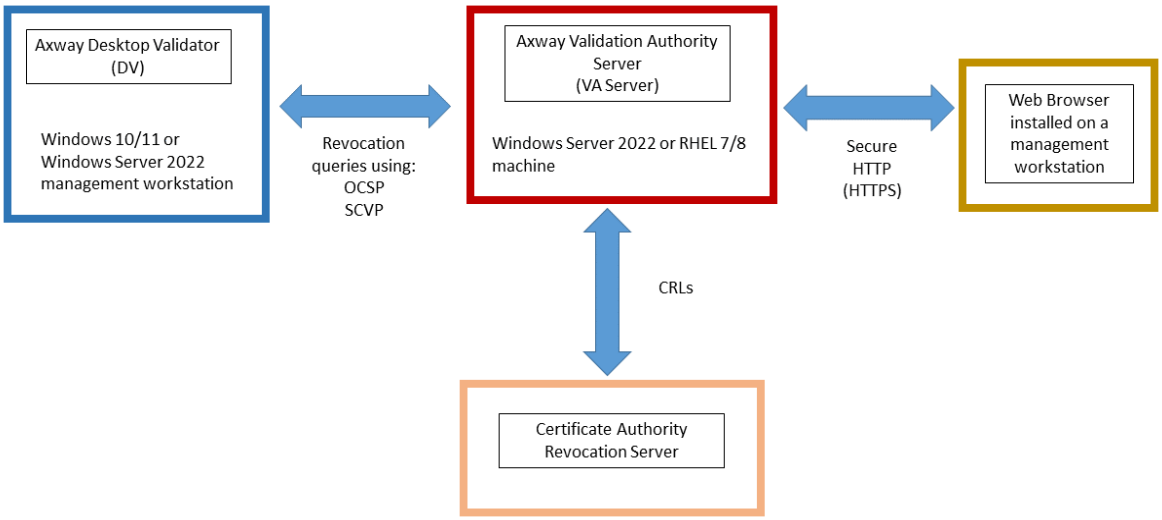

Figure 2 - Axway Desktop Validator (DV) interaction with additional components

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.

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.

Table 1 IT Environment Components

1.4.1.1 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.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by Axway Desktop Validator (Standard & Enterprise Editions):

- Cryptographic support
- User data protection
- Security management
- Privacy
- Protection of the TSF
- Trusted path/channels

1.4.1.2.1 Cryptographic support

The TOE does not generate any asymmetric keys.

1.4.1.2.2 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.

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

1.4.1.2.3 Security management

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

1.4.1.2.4 Privacy

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

1.4.1.2.5 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.

1.4.1.2.6 Trusted path/channels

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

1.4.2 TOE Documentation

The following user and administrative guidance is available:

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

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
  - Part 3 Extended
- Package Claims:
  - 'Protection Profile for Application Software', Version 1.4, 07 October 2021 (ASPP14)

Package	Technical Decision	Applied	Notes
PP_APP_V1.4	TD0823	Yes	Updated link in FPT_AEX_EXT.1.3 test description
PP_APP_V1.4	TD0822	Yes	Updated Windows manifest file name in tests FDP_DEC_EXT.1.1 and FDP_DEC_EXT.1.2
PP_APP_V1.4	TD0815	Yes	Added a TSS activity and modified the test for FPT_AEX_EXT.1.5
PP_APP_V1.4	TD0798	Yes	Applies to evaluation activities only
PP_ASPP_V1.4	TD0780	No	FIA_X509_EXT.1 not claimed
PP_ASPP_V1.4	TD0756	Yes	Applies to test evaluation activity only
PP_ASPP_V1.4	TD0747	Yes	Applies to test description for Android platform only
PP_ASPP_V1.4	TD0743	Yes	Changes to FTP_DIT_EXT.1 selections and Application Note
PP_ASPP_V1.4	TD0736	No	FCS_HTTPS_EXT.1/Server is not claimed
PP_ASPP_V1.4	TD0719	No	PP document updated to include Extended Component Definitions appendix
PP_ASPP_V1.4	TD0717	Yes	Formatting changes to FCS_CKM.1 and FCS_COP SFRs
PP_ASPP_V1.4	TD0664	Yes	Applies to tests only
PP_ASPP_V1.4	TD0650	Yes	New module claims
PP_ASPP_V1.4	TD0628	Yes	Applies to tests and includes a selection in FPT_TUD_EXT.2

2.1 Conformance Rationale

The ST conforms to the ASPP14. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the ASPP14 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The ASPP14 offers additional information about the identified security objectives, but that has not been reproduced here and the ASPP14 should be consulted if there is interest in that material.

In general, the ASPP14 has defined Security Objectives appropriate for software applications and as such are applicable to the Validation Authority Desktop Validator TOE.

3.1 Security Objectives for the Operational Environment

OE.PLATFORM The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

OE.PROPER_ADMIN The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

OE.PROPER_USER The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the ASPP14. The ASPP14 defines the following extended requirements and since they are not redefined in this ST the ASPP14 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- ASPP14:FCS_CKM_EXT.1: Cryptographic Key Generation Services
- ASPP14:FCS_RBG_EXT.1: Random Bit Generation Services
- ASPP14:FCS_STO_EXT.1: Storage of Credentials
- ASPP14:FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
- ASPP14:FDP_DEC_EXT.1: Access to Platform Resources
- ASPP14:FDP_NET_EXT.1: Network Communications
- ASPP14:FMT_CFG_EXT.1: Secure by Default Configuration
- ASPP14:FMT_MEC_EXT.1: Supported Configuration Mechanism - per TD0747
- ASPP14:FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable
- ASPP14:FPT_AEX_EXT.1: Anti-Exploitation Capabilities
- ASPP14:FPT_API_EXT.1: Use of Supported Services and APIs
- ASPP14:FPT_IDV_EXT.1: Software Identification and Versions
- ASPP14:FPT_LIB_EXT.1: Use of Third Party Libraries
- ASPP14:FPT_TUD_EXT.1: Integrity for Installation and Update
- ASPP14:FPT_TUD_EXT.2: Integrity for Installation and Update - per TD0664
- ASPP14:FTP_DIT_EXT.1: Protection of Data in Transit - per TD0743

Extended SARs:

- ALC_TSU_EXT.1: Timely Security Updates

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the ASPP14. The refinements and operations already performed in the ASPP14 are not identified (e.g., highlighted) here, rather the requirements have been copied from the ASPP14 and any residual operations have been completed herein. Of particular note, the ASPP14 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the ASPP14. The ASPP14 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Validation Authority Desktop Validator TOE.

Requirement Class	Requirement Component
FCS: Cryptographic support	ASPP14:FCS_CKM_EXT.1: Cryptographic Key Generation Services
	ASPP14:FCS_RBG_EXT.1: Random Bit Generation Services
	ASPP14:FCS_STO_EXT.1: Storage of Credentials
FDP: User data protection	ASPP14:FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
	ASPP14:FDP_DEC_EXT.1: Access to Platform Resources
	ASPP14:FDP_NET_EXT.1: Network Communications
FMT: Security management	ASPP14:FMT_CFG_EXT.1: Secure by Default Configuration
	ASPP14:FMT_MEC_EXT.1: Supported Configuration Mechanism - per TD0747
	ASPP14:FMT_SMF.1: Specification of Management Functions
FPR: Privacy	ASPP14:FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable
FPT: Protection of the TSF	ASPP14:FPT_AEX_EXT.1: Anti-Exploitation Capabilities
	ASPP14:FPT_API_EXT.1: Use of Supported Services and APIs
	ASPP14:FPT_IDV_EXT.1: Software Identification and Versions
	ASPP14:FPT_LIB_EXT.1: Use of Third Party Libraries
	ASPP14:FPT_TUD_EXT.1: Integrity for Installation and Update
	ASPP14:FPT_TUD_EXT.2: Integrity for Installation and Update - per TD0664
FTP: Trusted path/channels	ASPP14:FTP_DIT_EXT.1: Protection of Data in Transit - per TD0743

Table 2 TOE Security Functional Components

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic Key Generation Services (ASPP14:FCS_CKM_EXT.1)

ASPP14:FCS_CKM_EXT.1.1

The application shall [***generate no asymmetric cryptographic keys***].

5.1.1.2 Random Bit Generation Services (ASPP14:FCS_RBG_EXT.1)

ASPP14:FCS_RBG_EXT.1.1
The application shall [***use no DRBG functionality***] for its cryptographic operations.

5.1.1.3 Storage of Credentials (ASPP14:FCS_STO_EXT.1)

ASPP14:FCS_STO_EXT.1.1
The application shall [***not store any credentials***] to non-volatile memory.

5.1.2 User data protection (FDP)

5.1.2.1 Encryption Of Sensitive Application Data (ASPP14:FDP_DAR_EXT.1)

ASPP14:FDP_DAR_EXT.1.1
The application shall [***not store any sensitive data***] in non-volatile memory.

5.1.2.2 Access to Platform Resources (ASPP14:FDP_DEC_EXT.1)

ASPP14:FDP_DEC_EXT.1.1
The application shall restrict its access to [***network connectivity***].
ASPP14:FDP_DEC_EXT.1.2
The application shall restrict its access to [***no sensitive information repositories***].

5.1.2.3 Network Communications (ASPP14:FDP_NET_EXT.1)

ASPP14:FDP_NET_EXT.1.1
The application shall restrict network communication to [***/application requests to retrieve and verify revocation status via network communications (by downloading CRLs and sending outgoing OCSP revocation queries), and check for updates/***].

5.1.3 Security management (FMT)

5.1.3.1 Secure by Default Configuration (ASPP14:FMT_CFG_EXT.1)

ASPP14:FMT_CFG_EXT.1.1
The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.
ASPP14:FMT_CFG_EXT.1.2
The application shall be configured by default with file permissions which protect the application's binaries and data files from modification by normal unprivileged user.

5.1.3.2 Supported Configuration Mechanism - per TD0747 (ASPP14:FMT_MEC_EXT.1)

ASPP14:FMT_MEC_EXT.1.1
The application shall [***invoke the mechanisms recommended by the platform vendor for storing and setting configuration options***].

5.1.3.3 Specification of Management Functions (ASPP14:FMT_SMF.1)

ASPP14:FMT_SMF.1.1
The TSF shall be capable of performing the following management functions [***configuration of enhanced revocation options and to check for TOE updates***].

5.1.4 Privacy (FPR)

5.1.4.1 User Consent for Transmission of Personally Identifiable (ASPP14:FPR_ANO_EXT.1)

ASPP14:FPR_ANO_EXT.1.1
The application shall [***not transmit PII over a network***].

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Anti-Exploitation Capabilities (ASPP14:FPT_AEX_EXT.1)

ASPP14:FPT_AEX_EXT.1.1
The application shall not request to map memory at an explicit address except for [**no exceptions**].
ASPP14:FPT_AEX_EXT.1.2
The application shall [***not allocate any memory region with both write and execute permissions***].
ASPP14:FPT_AEX_EXT.1.3
The application shall be compatible with security features provided by the platform vendor.
ASPP14:FPT_AEX_EXT.1.4
The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.
ASPP14:FPT_AEX_EXT.1.5
The application shall be built with stack-based buffer overflow protection enabled.

5.1.5.2 Use of Supported Services and APIs (ASPP14:FPT_API_EXT.1)

ASPP14:FPT_API_EXT.1.1
The application shall use only documented platform APIs.

5.1.5.3 Software Identification and Versions (ASPP14:FPT_IDV_EXT.1)

ASPP14:FPT_IDV_EXT.1.1
The application shall be versioned with [***[a vendor assigned version number]***]

5.1.5.4 Use of Third Party Libraries (ASPP14:FPT_LIB_EXT.1)

ASPP14:FPT_LIB_EXT.1.1
The application shall be packaged with only [**curl, openldap, openssl**].

5.1.5.5 Integrity for Installation and Update (ASPP14:FPT_TUD_EXT.1)

ASPP14:FPT_TUD_EXT.1.1
The application shall [***provide the ability***] to check for updates and patches to the application software.
ASPP14:FPT_TUD_EXT.1.2
The application shall [***provide the ability***] to query the current version of the application software.
ASPP14:FPT_TUD_EXT.1.3
The application shall not download, modify, replace or update its own binary code.
ASPP14:FPT_TUD_EXT.1.4
Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.
ASPP14:FPT_TUD_EXT.1.5
The application is distributed [***as an additional software package to the platform OS***].

5.1.5.6 Integrity for Installation and Update - per TD0664 (ASPP14:FPT_TUD_EXT.2)

ASPP14:FPT_TUD_EXT.2.1
The application shall be distributed using **[*the format of the platform-supported package manager*]**.

ASPP14:FPT_TUD_EXT.2.2
The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events

ASPP14:FPT_TUD_EXT.2.3
The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

5.1.6 Trusted path/channels (FTP)

5.1.6.1 Protection of Data in Transit - per TD0743 (ASPP14:FTP_DIT_EXT.1)

ASPP14:FTP_DIT_EXT.1.1
The application shall [***not transmit any [sensitive data]***] between itself and another trusted IT product.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
	ALC_TSU_EXT.1: Timely Security Updates
ATE: Tests	ATE_IND.1: Independent Testing - Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 3 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d
The developer shall provide a functional specification.

ADV_FSP.1.2d
The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c
The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c
The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The application shall be labelled with a unique reference.

ALC_CMC.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d

The developer shall provide a description in the TSS of how timely security updates are made to the TOE. Application developers must support updates to their products for purposes of fixing security vulnerabilities.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Timely Security Updates (ALC_TSU_EXT.1)

ALC_TSU_EXT.1.1d

The developer shall provide a description in the TSS of how timely security updates are made to the TOE. Note: Application developers must support updates to their products for purposes of fixing security vulnerabilities.

ALC_TSU_EXT.1.2d

The developer shall provide a description in the TSS of how users are notified when updates change security properties or the configuration of the product.

ALC_TSU_EXT.1.1c

The description shall include the process for creating and deploying security updates for the TOE software.

ALC_TSU_EXT.1.2c

The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.

ALC_TSU_EXT.1.3c

The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.

Note: The reporting mechanism could include web sites, email addresses, as well as a means to protect the sensitive nature of the report (e.g., public keys that could be used to encrypt the details of a proof-of-concept exploit).

ALC_TSU_EXT.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d

The developer shall provide the TOE for testing.

ATE_IND.1.1c

The TOE shall be suitable for testing.

ATE_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Cryptographic support
- User data protection
- Security management
- Privacy
- Protection of the TSF
- Trusted path/channels

6.1 Cryptographic support

ASPP14:FCS_CKM_EXT.1:

The TOE does not generate any asymmetric keys.

ASPP14:FCS_RBG_EXT.1

The TOE does not use any DRBG functionality.

ASPP14:FCS_STO_EXT.1:

The TOE does not store any credentials.

6.2 User data protection

ASPP14:FDP_DAR_EXT.1:
The TOE does not store any sensitive data as the TOE does not store any data. It provides enhanced revocation services to other applications executing on the Windows OS, returns the revocation status to the calling application, and stores no data (sensitive or otherwise).

ASPP14:FDP_DEC_EXT.1:
The TOE accesses only network connectivity (and no other hardware resources) and does not utilize any sensitive information repositories.

ASPP14:FDP_NET_EXT.1:
The TOE requires network access for downloading CRLs, checking for software updates, and sending outgoing OCSP revocation queries.

6.3 Security management

ASPP14:FMT_CFG_EXT.1:

The TOE requires no credential (beyond needing installation by a Windows administrator) during installation or thereafter.

ASPP14:FMT_MEC_EXT.1:

The TOE (DV) installation on the Windows machine by a user with administrative privileges. During installation, the administrator enters user information and company name. The DV software installation makes the application available for all users on the system. However, users without Administrator privileges will have a read-only view of

configuration options, and will not be able to make any modifications to the configuration options set by the Administrator. The DV provides a configuration application which can be accessed via a desktop shortcut or by using the Start Menu. The Desktop Validator Configuration application allows the administrator to view and configure the TOE security management functions.

ASPP14:FMT_SMF.1:

The TOE allows users with administrator privileges to configure the TOE's enhanced revocation options.

The Desktop Validator (DV) Standard edition provides certificate validation support for client applications on Microsoft Windows platforms. The Enterprise edition provides certificate validation support for both client and server applications on Microsoft Windows platforms. Desktop Validator Enterprise is required for use of server applications such as Domain Controllers, IIS, and so on.

- From the *General tab,* select the *Use Axway DV as CAPI revocation provider* option to enable digital certificate validation using Desktop Validator.
- From the *General tab,* select the *OCSP* validation protocol to configure communication with the VA Server in order to validate a certificate
- From the *General menu,* click *Check Now* to display the latest available version / build of Desktop Validator.

6.4 Privacy

ASPP14:FPR_ANO_EXT.1:

The TOE does not collect personally identifiable information (PII) for administrators or users and, therefore, does not transmit any PII over a network.

6.5 Protection of the TSF

ASPP14:FPT_AEX_EXT.1:

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 as follows: the /GS flag was used during compilation to enable ASLR and stack-based buffer overflow protection.

Additionally, by default, the TOE does not allow user-modifiable files to be written to directories that contain executable files.

ASPP14:FPT_API_EXT.1:

The TOE only uses documented platform APIs from Microsoft Windows C/C++ SDK, and utilizes the following Windows APIs:

- WinSock
- PSAPI
- BCrypt
- WNetAPI
- C Library API
- WinHTTP
- CryptoAPI
- WinINet
- Native Windows API

- COM
- IPHelper
- Active Directory Services
- ODBC API
- RPC
- Ntsecapi
- Windows API which consists of:
    - Kernel32.dll – for basic services
    - advapi32.dll – for advanced services
    - gdi32.dll – for Graphics Device Interface
    - user32.dll - for User Interface
    - comdlg32.dll – For Common Dialog Box
    - shell32.dll & shlwapi.dll – For Windows Shell
    - ole32.dll & oleaut32.dll – for Object Linking and Embedding

ASPP14:FPT_IDV_EXT.1:

The TOE utilizes a software version with a major version with a minor update and build number.

ASPP14:FPT_LIB_EXT.1:

The TOE includes a number of third party libraries used to perform its functions as identified in the table below:

Third Party Library	Version	Function
curl	8.7.1	Retrieving CRLs
openssl	3.0.13	OCSP / SCVP requests, responses, encryption, decryption, signing, verification.
openldap	2.6.4	LDAP client to alternatively collect CRL information

ASPP14:FPT_TUD_EXT.1/ASPP14:FPT_TUD_EXT.2:

The TOE includes mechanisms to check for updates and to query the current version of the application software. The TOE displays the current version via its DV Configuration Application. The TOE also provide a 'check for update' button via their respective UIs for the administrator to check for updates.

The vendor digitally signs and distributes the TOE software using the platform-supported package manager (Windows). The vendor uses a signing certificate issued by Digicert to sign the installation package for Windows platforms. The TOE does not update its own binary code in any way and when removed, all traces of the TOE application software are deleted.

Axway addresses all vulnerabilities found in the product within 30 days from public disclosure. Users can report any security issues pertaining to the TOE by contacting Axway's technical support via phone or email. The phone number and email address are published on the Axway support website and provided directly to clients. TOE updates are not posted publicly and are only provided to customers who have contracts with Axway. When any changes are made to the product, whether security related or not, users will receive a message from Axway informing them that there is an update available. The updates are deployed to Axway's software repository from which users can download the updates.

6.6 Trusted path/channels

ASPP14:FTP_DIT_EXT.1:

The TOE transmits data (revocation requests) but does not transmit any sensitive data.