# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme

# Validation Report

# for

# Fidelis XPS™ v8.0

**Report Number:** **CCEVS-VR-10610-2015**
**Dated:** **15 May 2015**
**Version:** **1.0**

**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**
***The MITRE Corporation***

**Jean Petty**
***The MITRE Corporation***

**Jay Vora**
***The MITRE Corporation***

## Common Criteria Testing Laboratory

***Leidos Inc. (formerly SAIC, Inc.)***
***Columbia, MD***

# Table of Contents

# List of Tables

# 1 Executive Summary

This report 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 Validation Report (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 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Fidelis XPS™ v8.0 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE 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 of Fidelis XPS™ v8.0 was performed by Leidos (formerly Science Applications International Corporation (SAIC)) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in May 2015. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, and assurance activities specified in *Protection Profile for Network Devices*, v1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

Fidelis XPS™ v8.0 is a network security appliance solution for advanced threat detection. It detects inappropriate and malicious network data based on attributes of the network traffic, including content, source, destination, application, and aspects of the communication channel. Fidelis XPS™ v8.0 is used to prevent the intrusion of attacks and to prevent the transmission of sensitive data. The focus of this evaluation is on the TOE functionality supporting the claims in *Protection Profile for Network Devices*, Version 1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014. The security functionality specified in the Protection Profile includes protection of communications between TOE components and with external IT entities, identification and authentication of administrators, auditing of security-relevant events, and ability to verify the source and integrity of updates to the TOE.

The Leidos evaluation team determined that the TOE is conformant to *Protection Profile for Network Devices*, v1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014. The TOE, when configured as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in Fidelis XPS™ Security Target, Version 1.0, 3 April 2015. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test reports produced by the Leidos evaluation team.

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test reports. The validation team found that the evaluation showed that the TOE satisfies all of the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to *Protection Profile for Network Devices*, v1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014, and that the assurance activities specified in the Protection Profile had been performed appropriately. 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.

## 1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

- TD0004: FCS_TLS_EXT Man-in-the-Middle Tests

This Technical Decision removes the FCS_TLS_EXT man-in-the-middle tests for the NDPP (FCS_TLS_EXT.1.1, Test 2), pending development of new TLS requirements and assurance activities and identification of suitable test tools.

- TD0005: FPT_ITT Test 3 Resolution

This Technical Decision removes the need to perform Test 3 associated with FPT_ITT.1 in NDPP, consistent with the test requirements for FTP_ITC.1 and FTP_TRP.1.

- TD0017: NDPP Audit Shutdown

This Technical Decision allows for the use of a startup audit record to indicate audit shutdown in the event of an uncontrolled shutdown.

- TD0026: Update to FPT_TUD_EXT.1

This Technical Decision allows for the administrator following TOE guidance to reject an illegitimate update detected by the TOE, in addition to the TOE rejecting the update automatically.

## 1.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- User data may be inadvertently sent to a destination not intended by the original sender.

# 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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product and its evaluation.

**Table 1: Evaluation Details**

| | |
|---|---|
| **Evaluated Product:** | Fidelis XPS™ v8.0 |
| **Sponsor:** | Fidelis Cybersecurity<br>4416 East West Highway, Suite 310<br>Bethesda, Maryland 20814 |
| **Developer:** | Fidelis Cybersecurity<br>4416 East West Highway, Suite 310<br>Bethesda, Maryland 20814 |
| **CCTL:** | Leidos (formerly Science Applications International Corporation)<br>6841 Benjamin Franklin Drive<br>Columbia, MD 21046 |
| **Kickoff Date:** | 8 December 2014 |
| **Completion Date:** | May 2015 |
| **CC:** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. |
| **Interpretations:** | None |
| **CEM:** | Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 4, September 2012. |
| **Evaluation Class:** | None |
| **PP:** | Protection Profile for Network Devices, Version 1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014 |
| **Evaluation Personnel:** | Leidos (formerly Science Applications International Corporation):<br>Anthony J. Apted, Greg Beaver, Cody Cummins |
| **Validation Body:** | National Information Assurance Partnership CCEVS |

# 3 Security Policy

The TOE enforces the following security policies as described in the ST.

**Note:** Much of the description of the security policy has been derived from the Fidelis XPS™ Security Target and Final Evaluation Technical Report (ETR).

## 3.1 Security Audit

The TOE is able to generate logs of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and can also be configured to send the logs to a designated external log server.

## 3.2 Cryptographic Support

The TOE is operated in FIPS mode and includes a NIST-validated cryptographic module (OpenSSL). The module provides key management, random bit generation, encryption/decryption, digital signature and cryptographic hashing and keyed-hash message authentication features in support of higher level cryptographic protocols (TLS and HTTPS).

## 3.3 User Data Protection

The TOE ensures resources used in processing network traffic are suitably cleared prior to allocation of the resource.

## 3.4 Identification and Authentication

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions provided by the TOE. The TOE offers a network accessible GUI (HTTP over TLS) for interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. Additionally, the TOE can be configured to use the services of trusted LDAP/Active Directory servers in the operational environment.

## 3.5 Security Management

The TOE provides a GUI to access the security management functions. Security management commands are limited to administrators and are available only after the administrator has provided acceptable user identification and authentication data to the TOE.

The TOE also provides a local management capability. All administrative functionality available from the GUI is also available via direct serial console connection using the special debug account. However, the TOE is intended to be managed from a remote HTTPS/TLS client via the GUI provided by the TOE's CommandPost component. Following the initial configuration, all changes should be performed by an authorized user from CommandPost. The TOE implements a System Administrator role that corresponds to the NDPP Security Administrator.

## 3.6 Protection of the TSF

The TOE implements a number of self-protection features intended to ensure the reliability and integrity of its security features.

It protects sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE uses TLS and HTTPS to protect communications between distributed TOE components.

The TOE implements a self-test integrity mechanism that verifies the integrity of each TOE process before it is started. It also includes mechanisms to verify the authenticity and integrity of software updates to ensure the updates do not introduce malicious or other unexpected changes in the TOE.

## 3.7 TOE Access

The TOE can be configured to display an informative banner that will appear prior to an administrator being permitted to establish an interactive session. Prior to a user logging in, the user must indicate whether or not to continue with the authentication process. The TOE subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated.

## 3.8 Trusted Path/Channels

The TOE protects interactive communications with remote administrators using HTTP over TLS. TLS ensures both integrity and disclosure protection.

The TOE protects communications with network peers, such as log server, Fidelis Insight Server and authentication servers, using TLS connections to prevent unintended disclosure or modification of the transferred data.

# 4 Assumptions and Clarification of Scope

## 4.1 Assumptions

The ST identifies the following assumptions about the use of the product:

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

## 4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 *Protection Profile for Network Devices* and performed by the evaluation team).
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in *Fidelis XPS™ Security Target*, Version 1.0, 3 April 2015. Any additional security related functional capabilities of the product were not covered by this evaluation.
- 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 TOE appliances consist of software and hardware and do not rely on the operational environment for any supporting security functionality.
- Fidelis XPS appliances include the Integrated Management Module (IMM), which consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities in a single chip on the server system board. However, the IMM interface is not secured by Fidelis software and its use is not covered by the evaluation. The TOE guidance documentation advises that the IMM interface should be physically limited to only those users that require access.
- Multiple CommandPosts can operate in concert through a capability called Hierarchical Management. CommandPosts can be set up to be Masters or Subordinates in the hierarchical management architecture. However, the evaluation did not cover this capability and the TOE was not tested with this configuration.
- The TOE must be installed, configured and managed as described in the following guidance documents included in the evaluated configuration:
    a. Fidelis XPS Enterprise Setup and Configuration Guide, Version 8.0, Revised 2015

b. Fidelis XPS User Guide, Version 8.0,  Revised 2015

c. Fidelis XPS Guide to Creating Policies, Version 8.0, Revised 2015

d. Fidelis XPS Collector Quick Start Card, 2013

e. Fidelis XPS Quick Start Card, 2013

f. Fidelis XPS Addendum Versions 8.0 and 8.0.1, April 2015.

# 5 Architectural Information

A TOE deployment comprises:

- One or more Fidelis CommandPost™ v8.0 management console appliances, zero or more Fidelis XPS Collector v8.0 appliances and at least one of the following sensor appliances: Fidelis XPS Direct v8.0, Fidelis XPS Internal v8.0, Fidelis XPS Web v8.0, and Fidelis XPS Mail v8.0.

OR

- Fidelis XPS Scout+ v8.0 (includes a CommandPost, a Direct Sensor, and a Collector in one box)

**Note:** Much of the description of the TOE architecture has been derived from the Fidelis XPS™ Security Target.

The specific appliance models (including virtual appliances) included in the scope of the evaluation are as follows:

- Fidelis CommandPost+ and Fidelis CommandPost PlusVM
- Fidelis XPS Direct 50, Fidelis XPS Direct 100, Fidelis XPS Direct 250, Fidelis XPS Direct 500, Fidelis XPS Direct 1000, Fidelis XPS Direct 2500, and Fidelis XPS Direct VM
- Fidelis XPS Internal 50, Fidelis XPS Internal 100, Fidelis XPS Internal 250, Fidelis XPS Internal 500, Fidelis XPS Internal 1000, Fidelis XPS Internal 2500, and Fidelis XPS Internal VM
- Fidelis XPS Web and Fidelis XPS Web VM
- Fidelis XPS Mail and Fidelis XPS Mail VM
- Fidelis XPS Collector SA and Fidelis XPS Collector SA VM
- Fidelis XPS Collector Cluster, which includes one Fidelis XPS Collector Controller, and multiple Fidelis XPS Collector XA nodes. A redundant Fidelis XPS Collector is optional
- Fidelis XPS Blade Array, which may include blades to implement either a Fidelis XPS Direct 2500 sensor or a Fidelis XPS Internal 2500 sensor on each blade. The blade array provides the same function as Direct or Internal sensors at up to 20Gbps throughput capability when fully loaded with blades.

With the exception of the Fidelis XPS Collector Controller and Fidelis XPS Collector XA appliances (available only in hardware), each appliance is available either as a hardware appliance or as a virtual machine (VM) appliance. The hardware appliances are stand-alone devices ready to be plugged into the target network. The VM appliances are VMWare vSphere or Microsoft Hyper-V images ready to run (i.e., already installed and ready to start) in an environment providing VMWare vSphere or Microsoft Hyper-V with suitable connections to the target network. A Fidelis XPS system can be deployed entirely as hardware appliances, VM appliances, or a mixture, so long as there is a CommandPost and at least one sensor.

Each Fidelis XPS appliance includes a hardened CentOS 6.5 with kernel 2.6.32-431.20.3.el6.x86_6, and custom Fidelis XPS applications.

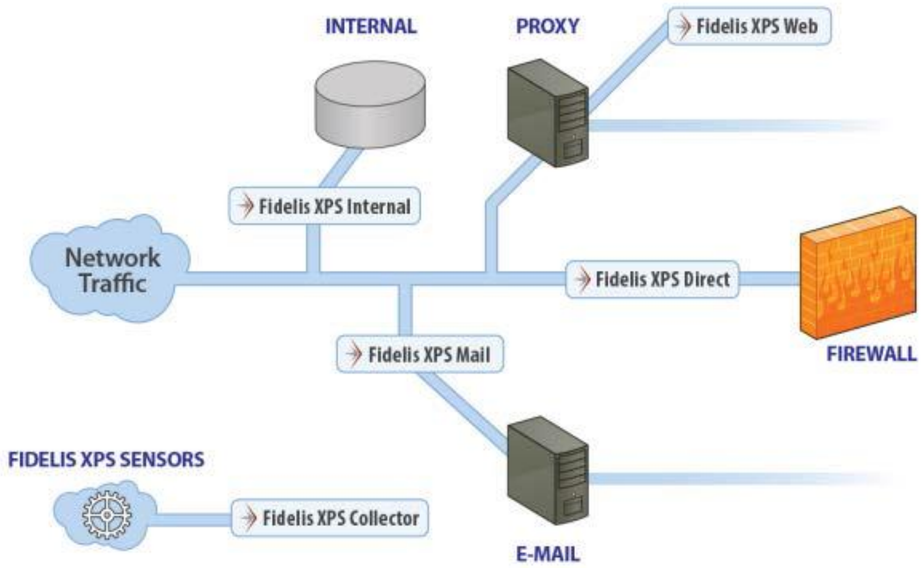
A CommandPost is required when using any of the TOE sensors or Collector. The CommandPost provides the CommandPost Management Console. The Management Console comprises a web-based administrative interface for configuration and management of the TOE. Additional CommandPosts can be set up to be Masters or Subordinates. All CommandPosts are capable of collecting, aggregating, and storing data from multiple sensors.

The Fidelis XPS Collector serves as the storage and access point for metadata information. The Collector listens for incoming connections from CommandPost and any sensors configured to use the Fidelis XPS Collector. The Fidelis XPS Collector SA is recommended for connection to a single sensor. The extensible Fidelis XPS Collector Controller plus Fidelis XPS Collector XA is recommended for connecting to multiple sensors.

The Fidelis XPS sensors are used to monitor, capture, and examine network traffic, sending pertinent findings and other data to the CommandPost, which is used to manage its associated Fidelis XPS sensors and to further analyze the information received from those sensors. Several models exist for the Fidelis XPS sensors to address a variety of network architectures. Each appliance type is designed to monitor specific types of network traffic. The differences in the models for a given appliance type involve data rate capacities and form of deployment (hardware or VM), but each of the models for a given appliance type has the same security features.

- The Fidelis XPS Direct sensor monitors and enforces extrusion/intrusion policies across all 65,535 Internet Protocol (IP) ports on the network. This sensor is normally placed at the border of a protected network and is optimized to process numerous, relatively short-lived connections.
- The Fidelis XPS Internal sensor is similar to Direct, but supports protocols typically seen only inside the network, including Oracle and DB2 database access, SMB/CIFS/SAMBA file transfers, and directory queries. This sensor is normally placed within a protected network and is optimized to process a relatively small number of longer duration sessions (e.g., SMB) and is also capable of decoding the content of some protocols such as LDAP and SMB.
- The Fidelis XPS Web sensor monitors and enforces policy for traffic flowing through ICAP-enabled proxy servers.
- The Fidelis XPS Mail sensor monitors and enforces policy for Simple Mail Transfer Protocol (SMTP) e-mail traffic.

A sample deployment scenario for the sensors is depicted as follows.



CommandPosts communicate with one or more sensors and one or more Collectors. Collectors communicate with CommandPost and any sensors configured to use the Fidelis XPS Collector. All communication channels between TOE components and with trusted external IT entities are protected via TLS and/or TLS/HTTPS.

In order for a CommandPost Client to connect via web-based, remote access, the following software is required on the client machine(s):

- Browser: Microsoft Internet Explorer; Firefox; Google Chrome; or Apple Safari
- Adobe Flash Player.

The virtual (VM) appliances are delivered as an installation disk (or ISO image). The VM appliances are supported on the following virtual environments:

- VMware, which requires:
    - VMware ESX or ESXi 5.1 and newer
    - VMware vSphere 5.1 (and newer) client or VMware VCenter 5.1 and newer
    - The host hardware must be an Intel Core or Xeon processor based on the Ivy Bridge or Haswell microarchitecture that provides Intel Secure Key capability, which is required to meet entropy requirements. The VM must be based on Virtual Hardware version 9 or greater to utilize the Secure Key.

The various VM appliances have the following resource requirements:

| VM Appliance | vCPUs | Memory (GB) | Disk (GB) | Monitoring Virtual Switch |
|---|---|---|---|---|
| CommandPost+ VM | 8 | 24 | 100 | N/A |
| Direct 1000 VM | 8 | 24 | 30 | 1 |
| Internal 1000 VM | 8 | 24 | 30 | 1 |
| Web VM | 4 | 8 | 100 | N/A |
| Mail VM | 4 | 8 | 100 | N/A |
| Collector SA VM | 8 | 32 | 200 | N/A |

Use of the optional syslog and external authentication methods require LDAP and syslog servers.

There are additional hardware requirements depending on the deployment:

- **Network Taps—**required for lossless network monitoring by Fidelis XPS Direct and internal sensors in an out-of-band deployment. A network tap will replicate all network traffic with no data loss or performance degradation. Network taps guarantee complete traffic replication.
- **SPAN Ports—**connecting the Fidelis XPS Direct or internal sensors to the SPAN ports on the router or switch can be done, but unlike Network Taps do not guarantee complete traffic replication and/or processing of all data due to traffic volumes. While they can be used, they are not recommended since the applicable network router or other device supporting SPAN ports generally treat SPAN ports with low priority and may not send all packets when under load.
- **Proxy appliance—**required for connecting the Fidelis XPS Web sensor to analyze proxied traffic.
- **Mail Transfer Agent (MTA)—**required for connecting the Fidelis XPS Mail sensor to analyze e-mail in the operating environment in an out-of-band deployment. The MTA is only required if the Fidelis XPS Mail sensor is connected out-of-band where the Fidelis XPS Mail sensor serves as a content inspection agent to a third party MTA. When the Fidelis XPS Mail sensor is connected in-line, it acts as an MTA and thus an external MTA is not required.

The TOE supports e-mail, syslog, and SNMP (versions 1, 2c, and 3) alerting when an e-mail server, SNMP server, and/or other applicable third party products (e.g., ArcSight, IBM SiteProtector, Verdasys Digital Guardian) are available.

# 6 Documentation

Fidelis provides a set of documentation for the end users of the TOE, providing guidance on the installation, configuration and use of the TOE. The following documents were specifically examined in the context of the evaluation:

- Fidelis XPS Enterprise Setup and Configuration Guide, Version 8.0, Revised 2015
- Fidelis XPS User Guide, Version 8.0, Revised 2015
- Fidelis XPS Guide to Creating Policies, Version 8.0, Revised 2015
- Fidelis XPS Collector Quick Start Card, 2013
- Fidelis XPS Quick Start Card, 2013
- Fidelis XPS Addendum Versions 8.0 and 8.0.1, Revised April 2015.

# 7 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Evaluation Team Test Report for Fidelis XPS*™, Version 1.0, 9 April 2015.

## 7.1 Developer Testing

The assurance activities in *Protection Profile for Network Devices* do not specify any requirement for developer testing of the TOE.

## 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 NDPP including the optional HTTPS and TLS tests.

# 8 Evaluated Configuration

The TOE is Fidelis XPS™ v8.0, which is installed and configured according to the product installation guidance identified in Section 6. The TOE appliances are configured to operate in FIPS mode.

# 9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for Network Devices*, v1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014, in conjunction with Version 3.1, Revision 4 of the CC and CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the PP, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Final ETR, which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

**Table 2: Evaluated Assurance Requirements**

| Assurance Component ID | Assurance Component Name |
|---|---|
| ADV_FSP.1 | Basic functional specification |
| AGD_OPE.1 | Operational user guidance |
| AGD_PRE.1 | Preparative procedures |
| ALC_CMC.1 | Labeling of the TOE |
| ALC_CMS.1 | TOE CM coverage |
| ATE_IND.1 | Independent testing - conformance |
| AVA_VAN.1 | Vulnerability survey |

# 10 Validator Comments/Recommendations

The validators did not have any specific additional comments or recommendations.

# 11 Annexes

Not applicable.

# 12 Security Target

The ST for this product's evaluation is Fidelis XPS™ Security Target, Version 1.0, 3 April 2015.

# 13 Abbreviations and Acronyms

| | |
|---|---|
| AAR | Assurance Activities Report |
| CC | Common Criteria for Information Technology Security Evaluation |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCTL | Common Criteria Testing Laboratory |
| CEM | Common Evaluation Methodology for Information Technology Security |
| CM | Configuration Management |
| ETR | Evaluation Technical Report |
| FIPS | Federal Information Processing Standard |
| GUI | Graphical User Interface |
| IT | Information Technology |
| LDAP | Lightweight Directory Access Protocol |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NTP | Network Time Protocol—a means of synchronizing clocks over a computer network |
| NVLAP | National Voluntary Laboratory Assessment Program |
| PCL | Product Compliant List |
| PP | Protection Profile |
| ST | Security Target |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| VR | Validation Report |

# 14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Part 1: Introduction and general model. CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Part 2: Security functional components. CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012. Part 3: Security assurance components. CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012. Evaluation methodology. CCMB-2012-09-004.

[5] Protection Profile for Network Devices, v1.1, 8 June 2012, as amended by Errata #3, dated 3 November 2014.

[6] Fidelis XPS™ Security Target, Version 1.0, 3 April 2015.

[7] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[8] Evaluation Technical Report for Fidelis XPS™, Parts 1 and 2 Version 1.0, 9 April 2015.

[9] Assurance Activities Report for Fidelis XPS™, Version 3.2, 8 May 2015

[10] Evaluation Team Test Report for Fidelis XPS™, Version 1.0, 8 May 2015