National Information Assurance Partnership

Common Criteria Evaluation and Validation

TM

Scheme Validation Report

For

Fidelis XPS

Report Number: CCEVS-VR-VID10449-2012
Dated: 08/07/2012
Version: 0.1

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

Jandria Alexander
Kenneth Stutterheim

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, Maryland

Table of Contents

List of Tables

1 Executive Summary

The evaluation of **Fidelis XPS** was performed by SAIC, in the United States and was completed in May 2012. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Fidelis XPS TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation versions 3.1, revision 3.

Science Applications International Corporation (SAIC) determined that the product satisfies evaluation assurance level (EAL) 2 as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Fidelis XPS Security Target, version 0.6, April, 2012.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is comprised of Fidelis XPS Scout v7.0 or one or two Fidelis CommandPost v7.0 management console appliances and at least one of the following sensor appliances: Fidelis XPS Direct v7.0, Fidelis XPS Internal v7.0, Fidelis XPS Web v7.0, Fidelis XPS Connect v7.0, Fidelis XPS Mail v7.0, and Fidelis XPS Edge v7.0.

Some of the appliances include multiple models as listed below:

- Fidelis CommandPost, Fidelis CommandPost+, and Fidelis CommandPost Virtual Machine (VM)
- Fidelis XPS Scout
- Fidelis XPS Direct 1000, Fidelis XPS Direct 2500, and Fidelis XPS Direct VM
- Fidelis XPS Internal 1000, Fidelis XPS Internal 2500, and Fidelis XPS Internal VM
- Fidelis XPS Web and Fidelis XPS Web VM
- Fidelis XPS Connect and Fidelis XPS Connect VM
- Fidelis XPS Mail and Fidelis XPS Mail VM
- Fidelis XPS Edge 25 and Fidelis XPS Edge 200

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of Fidelis XPS by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some discrete points during the evaluation, validators formed a Validation Oversight Review panel in order to review the Security Target and other evaluation evidence materials along with the corresponding

evaluation findings in detail. The validation team found that the evaluation showed that the product satisfies all of the security functional 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 Final Evaluation Technical Report for Fidelis XPS ETR parts 1 and 2 and the associated test report produced by SAIC.

1.1 Evaluation Details

Evaluated Product:	Fidelis XPS
Sponsor & Developer:	Fidelis Security Systems, Inc 4416 East West Highway, Suite 310 Bethesda, Maryland 20814
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	May 2012
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, September 2009
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 3, September 2009
PP:	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environment, Version 1.7, July 25, 2007
Evaluation Class:	Evaluation Assurance Level (EAL) 2 Augmented with ALC_FLR.3
Description	The TOE is a combination of Fidelis XPS v7.0 appliances. It is designed to monitor network traffic for malicious content coming into the network (intrusion) and for sensitive and secure data leaving the network (extrusion). The TOE is designed to operate continuously, observing network traffic as it is perceived on the attached networks.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Fidelis XPS by any agency of the U.S. Government and no warranty of Fidelis XPS is either expressed or implied.

Evaluation Personnel: M. Evencie Pierre
Quang Trinh
Christopher Keenen

Validation Team: Jandria Alexander
Kenneth Stutterheim

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) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation. Note that assurance requirements outside the scope of EAL 1 through EAL 4 are addressed at the discretion of the CCEVS.

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.

The following table serves to identify the evaluated Security Target and TOE.

Table 1 ST and TOE identification

ST Title:	Fidelis XPS Security Target, Version 0.6, April, 2012
TOE Identification:	• Fidelis XPS Scout v7.0 OR • One or two Fidelis CommandPost™ v7.0 management console appliances and at least one of the following sensor appliances: Fidelis XPS Direct v7.0, Fidelis XPS Internal v7.0, Fidelis XPS Web v7.0, Fidelis XPS Connect v7.0, Fidelis XPS Mail v7.0, and Fidelis XPS Edge v7.0.
Operating Platform:	Some of the appliances include multiple models as listed below: • Fidelis CommandPost, Fidelis CommandPost+, and Fidelis CommandPost Virtual Machine (VM) • Fidelis XPS Scout • Fidelis XPS Direct 1000, Fidelis XPS Direct 2500, and Fidelis XPS Direct VM • Fidelis XPS Internal 1000, Fidelis XPS Internal 2500, and Fidelis XPS Internal VM • Fidelis XPS Web and Fidelis XPS Web VM • Fidelis XPS Connect and Fidelis XPS Connect VM • Fidelis XPS Mail and Fidelis XPS Mail VM • Fidelis XPS Edge 25 and Fidelis XPS Edge 200

3 Threats to Security

The following are the threats that the evaluated product addresses:

3.1 TOE Threats

The following threats are identified in [IDSSPP]

T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

4 Assumptions

The following assumptions are identified in the Security Target:

4.1 Physical Assumptions

The following conditions are assumed to exist in the operational environment. Each of these assumptions is consistent with the explicit or implicit assumptions made in each of the PPs for which conformance is claimed: [IDSSPP].

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

5 Organizational Security Policies

The following OSPs are identified in the Security Target:

5.1 IDS System PP OSPs

The following OSPs are defined in [IDSSPP]. [IDSSPP] does not identify which organization and which organizational security policy any of these OSPs are drawn from.

P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate

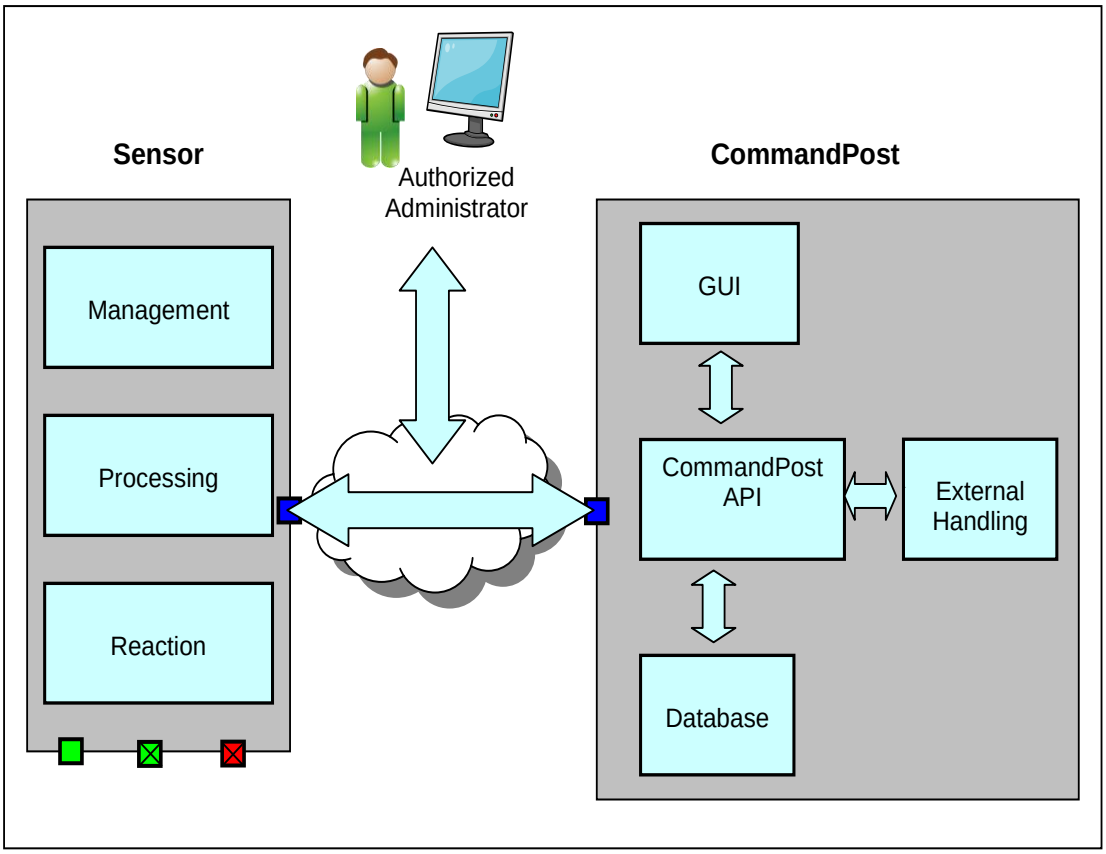
	activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

6 Architectural Information

The TOE is designed to monitor network traffic for malicious content coming into the network (intrusion) and for sensitive and secure data leaving the network (extrusion). It is designed to operate continuously, observing network traffic as it is perceived on the attached networks. Traffic observed by a Fidelis XPS sensor is reassembled into sessions; protocols are identified; applications are identified; and, contents are analyzed in order to determine whether they contain anything inappropriate based on the applicable (intrusion/extrusion) policy rules. When inappropriate content is identified, the sensor takes action, as defined by the rule which was violated. Actions include alert, prevent, throttle, information flow map (i.e., update an information flow map with the occurrence), quarantine, reroute, notify sender, append message, and X-header modification. Additionally, packets can be captured in a .pcap file. A rule may invoke several actions for a single violation.

A given Fidelis XPS configuration includes either a single Fidelis XPS Scout appliance or one or two CommandPost appliances combined with one or more Fidelis XPS sensor appliances. Each Fidelis XPS appliance is a self-contained hardware appliance device or VM image designed to interact with its environment via network connections (real or virtual).

Fidelis XPS TOE Subsystem Decomposition



- Sensor Management

  The sensor management subsystem provides the configuration channel between CommandPost and the sensors. It provides the interface to transfer all configuration information including all policy downloads, between the CommandPost and the sensors. The sensor management subsystem includes an audit daemon that uses HTTPS to communicate auditable events such as configuration changes to the sensors to CommandPost. In addition, the subsystem includes a System Monitor process that routinely monitors the operation of the sensor, and records any detected problem to a local log file.

- Sensor Processing

  The sensor processing subsystem provides the sniffer, decoding and analysis modules which together work to ensure that data received from the monitored network is adequately processed. This subsystem processes TCP, ICAP, Milter, and SCIP from the monitored network; extracts the data to be analyzed based on the fingerprint rules defined in the configured policies.

- Sensor Reaction

  The sensor reaction subsystem provides the system facility to react to a policy violation. Based on the result of analysis performed by the Sensor Processing subsystem, the reaction subsystem may generate an alert, prevent a session, throttle a session, quarantine an email, reroute an email, or perform other type of configured response such sending a notification to the sender, append a message to an email, or modify the X-header of an email message.

- CommandPost GUI

  The GUI subsystem provides a graphical web-based interfaced over HTTPS. It provides all graphical rendering and web hosting functions. It relies on the CommandPost API Subsystem for all CommandPost logic.

- CommandPost API

  The CommandPost Application Programmer's Interface (API) is the main subsystem for all CommandPost operations. The API serves as a middle layer between the CommandPost storage module, sensors, and CommandPost administrators. The API contains the interface to the sensor and is responsible for pushing sensor configuration information, including policies, and receiving and storing information to sensors.

- CommandPost Database

  The database subsystem provides the CommandPost storage facility and includes embedded database software. It stores most data in the database, some in memory-mapped files and some in other variables such as arrays and vectors. The database is only accessible through the CommandPost API subsystem.

- CommandPost External Handling

  CommandPost is designed as an open system which can be integrated with other security products at a customer site. The external handling subsystem provides the functions: Scheduled Events, Feed Manager, and CommandPost System Monitor

6.1 Physical Boundaries

The Target of Evaluation (TOE) is Fidelis XPS version 7.0. A given Fidelis XPS configuration includes either a single Fidelis XPS Scout appliance or one or two CommandPost appliances combined with one or more Fidelis sensor appliances. Each Fidelis XPS appliance is a self-contained hardware appliance device or VM image designed to interact with its environment via network connections (real or virtual).

The Target of Evaluation includes the following components:

- Fidelis XPS Scout appliance (combined both the CommandPost and Sensor)
- Fidelis XPS CommandPost Appliance

- Fidelis XPS Sensor Appliance (Fidelis XPS Web, Fidelis XPS Direct, Fidelis XPS Internal, Fidelis XPS Mail, Fidelis XPS Connect, Fidelis XPS Edge)
- TOE Guidance

7 Documentation

Fidelis offers a number of guidance documents, including CC-specific installation and configuration instructions describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The documentation for the TOE is:

- Fidelis XPS Enterprise Setup and Configuration Guide, Version 7.0
- Fidelis XPS User Guide, version 7.0
- Fidelis XPS Guide to Creating Policies, version 7.0
- Fidelis XPS Guide to Prebuilt Policies, version 7.0
- Fidelis XPS Acceptance Procedures, version 7.0
- Fidelis XPS Application Programmer Interface Guide, version 7.0

The security target used is:

- Fidelis XPS Security Target, Version 0.6, April, 2012

8 IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL2 evaluation.

8.1 Developer Testing

The developer created test procedures specifically to fulfill the test requirements for an EAL2 evaluation. The tests were developed to provide good coverage of the security functions related to each of the security requirements in the Security Target. The developer has documented their tests in a test plan where the results of the tests are presented as prose conclusions, notes, screen shots, and summaries for each of the applicable test platforms.

8.2 Independent Testing

Independent testing took place at the developer's location in Bethesda, Maryland from April 16 through April 17, 2012.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE (in six distinct but representative configurations) in accordance with the provided guidance, and exercised a representative subset of the developers test plan on equipment configured in the testing laboratory.

This effort involved configuring the Fidelis XPS components using the CC specific instructions described in the Setup guides, the TOE was pre-installed. Subsequently, the evaluators exercised a subset of the available developer's test procedures for the Fidelis XPS TOE. The subset of tests was selected in order to ensure that each of the claimed security functions was meaningfully sampled.

Also, the evaluators devised independent tests to ensure that start-up and shutdown operations were audited, to verify that changes of the audit configuration while the audit function is enabled is properly audited, that all user accesses to the audit records are audited, to verify the TOE's ability to use external authentication via LDAP, to verify that the TOE will enforce password constraints, to verify that communication between TOE components is protected using FIPS-compliant encryption, to verify restrictions on custom roles, to verify that the TSF will restrict management of user attributes to the authorized administrator role, to verify the difference between the XPS Direct and XPS Internal sensors, , to verify that sensor logs cannot be accessed from the sensor, and that sensors cannot be impersonated.

In addition to the use of developer provided and independently devised security functional tests, the evaluators also explored the possibility to penetrate or bypass the security mechanisms. Much of this work was based on analysis of the design, source code, and actual configuration information derived from the installed and configured products. However, the evaluators also devised some tests including scans of the installed products (for open ports) attempts at account harvesting, and also examination of actual network traffic between the client and server products

Given the complete set of test results from test procedures exercised by the developer and the sample of tests directly exercised by the evaluators, the testing requirements for EAL2 are fulfilled.

9 Evaluated Configuration

The TOE is Fidelis XPS version 7.0 installed and configured according to the Fidelis XPS Enterprise Setup and Configuration Guide, version 7.0.

10 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, and the CCEVS.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing notes, comments, or vendor actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part I, states:

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary part of the ETR (see Chapter 15).

> 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 [1], [2], [3] and CEM version 3.1 [4]. The evaluation determined the TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) requirements. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report For Fidelis XPS Part 2" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> *Section 6.1, ST Evaluation:* "Each verdict for each CEM work unit in the ASE ETR is a 'PASS'. Therefore, the ST is a CC compliant ST."

Section 6.2, TOE Evaluation: "The verdicts for each CEM work unit in the ETR sections included in the proprietary part of the ETR (see Chapter 15) are each 'PASS'. Therefore, the TOE (see below product identification) satisfies the Security Target, when configured according to the following guidance documentation:

Fidelis XPS Enterprise Setup and Configuration Guide version 7.0

The following documents are available for additional guidance:

- Fidelis XPS User Guide, version 7.0
- Fidelis XPS Guide to Creating Policies, version 7.0
- Fidelis XPS Guide to Prebuilt Policies, version 7.0
- Fidelis XPS Acceptance Procedures, version 7.0
- Fidelis XPS Application Programmer Interface Guide, version 7.0

Additionally, the evaluation team's performance of developer tests, independent tests, and penetration tests further demonstrates the accuracy of the claims in the ST.

11 Validator Comments/Recommendations

The validation team considers the evaluated subset of product functions to be consistent with the product's intended purpose and mode of operation.

The validators recommend that:

- It is critical that the administrators follow the Common Criteria Evaluated Configuration documentation when configuring the devices for use to ensure the evaluated security features are applied. (Fidelis XPS Enterprise Setup and Configuration Guide, Version 7.0 Appendix B.)
- The use of the built in Fidelis account to manipulate the TOE functions and data when the TOE is operational is outside the scope of this evaluation and removes the TOE from the evaluated configuration. The built in account should be evaluated separately if used.
- IPv6 compliance and security implications were not addressed as part of this evaluation. They should be evaluated separately.
- OpenLDAP was the only version of LDAP tested, the use of other versions should be evaluated separately.

12 Annexes

Not applicable.

13 Security Target

Fidelis XPS Security Target, Version 0.6, April, 2012

14 Acronym List

CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CM	Configuration Management
CMP	Configuration Management Plan
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versioning System
DoD	Department of Defense
EAL	Evaluation Assurance Level
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High-level Design
ID	Identity/Identification
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
SAIC	Science Applications International Corporation
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

15 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

[5] Fidelis XPS Security Target, Version 0.6, April, 2012.

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

[7] Evaluation Technical Report For Fidelis XPS parts 1 and 2 (and associated test report), version 0.1, May, 2012.