National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Samsung Electronics Co., Ltd.

416 Maetan-3dong, Yeongtong-gu, Suwon-si, Gyeonggi-do, 443-742 Korea

Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client

Report Number: CCEVS-VR-VID10557-2014
Dated: May 31, 2014
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

Ken Elliott
Luke Florer
Meredith Hennan
Jerry Myers
Ken Stutterheim
Mario Tinto
The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Samsung Galaxy Devices VPN Client solution provided by Samsung Electronics Co., Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in April 2014. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of EAL 1.

The Target of Evaluation (TOE) are the Samsung Galaxy Devices VPN Client including the Galaxy S4, Galaxy Note 3, Galaxy Note 10.1 2014 Edition, Galaxy NotePRO Tablet, and Galaxy S5 products.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

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

The Gossamer Security Solutions evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 1 were satisfied.

The technical information included in this report was obtained from the Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client (IVPNCPP14) Security Target and analysis performed by the EvaluationTeam.

2 Identification

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

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client including the Galaxy S4, Galaxy Note 3, Galaxy Note 10.1 2014 Edition, Galaxy NotePRO Tablet, and Galaxy S5
Protection Profile	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
ST:	Samsung Galaxy Devices VPN Client (IVPNCPP14) Security Target, Version 1.0, May 23, 2014
Evaluation Technical Report	Samsung Galaxy Devices VPN Client (IVPNCPP14) , Version 1.1, May 23, 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Samsung Electronics Co., Ltd.

Item	Identifier
Developer	Samsung Electronics Co., Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Ken Elliott, The Aerospace Corporation
	Luke Florer, The Aerospace Corporation
	Meredith Hennan, The Aerospace Corporation
	Jerry Myers, The Aerospace Corporation
	Ken Stutterheim, The Aerospace Corporation
	Mario Tinto, The Aerospace Corporation

3 Architectural Information

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

The TOE combines with a Mobile Device Management solution that enables the enterprise to watch, control and administer all deployed mobile devices, across multiple mobile service providers as well as facilitate secure communications through a VPN. This partnership provides a secure mobile environment that can be managed and controlled by the environment and reduce the risks that can be introduced through a Bring-Your-Own-Device (BYOD) model.

Data on the TOE is protected through the implementation of Samsung On-Device Encryption (ODE) which utilizes a FIPS 140-2 certified cryptographic modules to encrypt device and SD card storage. This functionality is combined with a number of on-device policies including local wipe, remote wipe, password complexity, automatic lock and privileged access to security configurations to prevent unauthorized access to the device and stored data.

The Samsung Enterprise Software Development Kit (SDK) builds on top of the existing Android security model by expanding the current set of security configuration of options to more than 390 configurable policies and including additional security functionality such as application whitelisting and blacklisting.

3.1 TOE Evaluated Configuration

The evaluated configuration consists of five different models of the TOE, the Galaxy S4, Galaxy Note 3, Galaxy Note 10.1 2014 Edition, Galaxy NotePRO Tablet, and Galaxy S5. The evaluated versions of the mobile devices are as follows.

- Android version: 4.4.2
- Kernel version: 3.4.0
- Build number: KOT49H
- Security software version: MDF v1.0 Release 3, VPN v1.4 Release 2

The model numbers of the mobile devices are as follows.

Carrier	Galaxy Note 3	Galaxy S4	Galaxy NotePRO	Galaxy Note 10.1 2014 Ed	Galaxy S5
Verizon	SM-N900V	SCH-I545	SM-P905V	SM-P605	SM-G900V
AT&T	SM-N900A	SGH-I337	SM-P905A	N/A	SM-G900A
Sprint	SM-N900P	SPH-L720	SM-P905P	N/A	SM-G900P
T-Mobile	SM-N900T	SGH-M919	SM-P905T	N/A	SM-G900T
US Cellular	SM-N900R	SCH-R970	N/A	N/A	SM-G900R4
International	SM-N900	GT-I9505	SM-P905	N/A	SM-G900 F/H/I/M/K/L/S

.

3.2 Physical Boundaries

The TOE is a multi-user operating system based on Android (4.4) that incorporates the Samsung Enterprise SDK. The TOE does not include the user applications that run on top of the operating system, but does include controls that limit application behavior. The method of use for the TOE is as a mobile messaging and VPN device for use within an enterprise environment where the configuration of the device is managed through a compliant device management solution.

The TOE communicates and interacts with 802.11-2012 Access Points to establish network connectivity, and the through that connectivity interacts with MDM servers that allow administrative control of the TOE.

4 Security Policy

This section summarizes the security functionality of the TOE:

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

4.1 Cryptographic support

The IPsec implementation is the primary function of the TOE. IPSec is used by the TOE to protect communication between itself and a VPN Gateway over an unprotected network. With the exception of the IPsec implementation, the TOE relies upon its underlying evaluated platform for the cryptographic services specified in this Security Target.

4.2 User data protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

4.3 Identification and authentication

The TOE provides the ability to use, store, and protect X.509 certificates and pre-shared keys that are used for IPsec Virtual Private Network (VPN) connections.

4.4 Security management

The TOE provides all the interfaces necessary to manage the security functions required by the VPN client to meet the requirements. In particular, the IPsec VPN is fully configurable by a combination of functions provided directly by the TOE and those available to the associated VPN gateway.

4.5 Protection of the TSF

The TOE relies upon its underlying platform to perform self-tests that cover the TOE as well as the functions necessary to securely update the TOE.

4.6 Trusted path/channels

The TOE acts as a VPN client using IPsec to establish secure channels to corresponding VPN gateways.

5 Assumptions and Clarification of Scope

The Security Problem Definition, including the assumptions, may be found in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 (IVPNCPP14). That information has not been reproduced here and the IVPNCPP14should be consulted if there is interest in that material.

6 Documentation

The following documentation was used as evidence for the evaluation of the Samsung Galaxy Devices VPN Client:

- Samsung VPN Client on Galaxy Devices Guidance documentation, Version 0.6, May 13, 2014
- Samsung VPN Client on Galaxy Devices VPN User Guidance Documentation, Version 0.5, May 13, 2014

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report for Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client (IVPNCPP14), Version 1.2, May 22, 2014.

The following diagrams depict the test environments used by the evaluators.

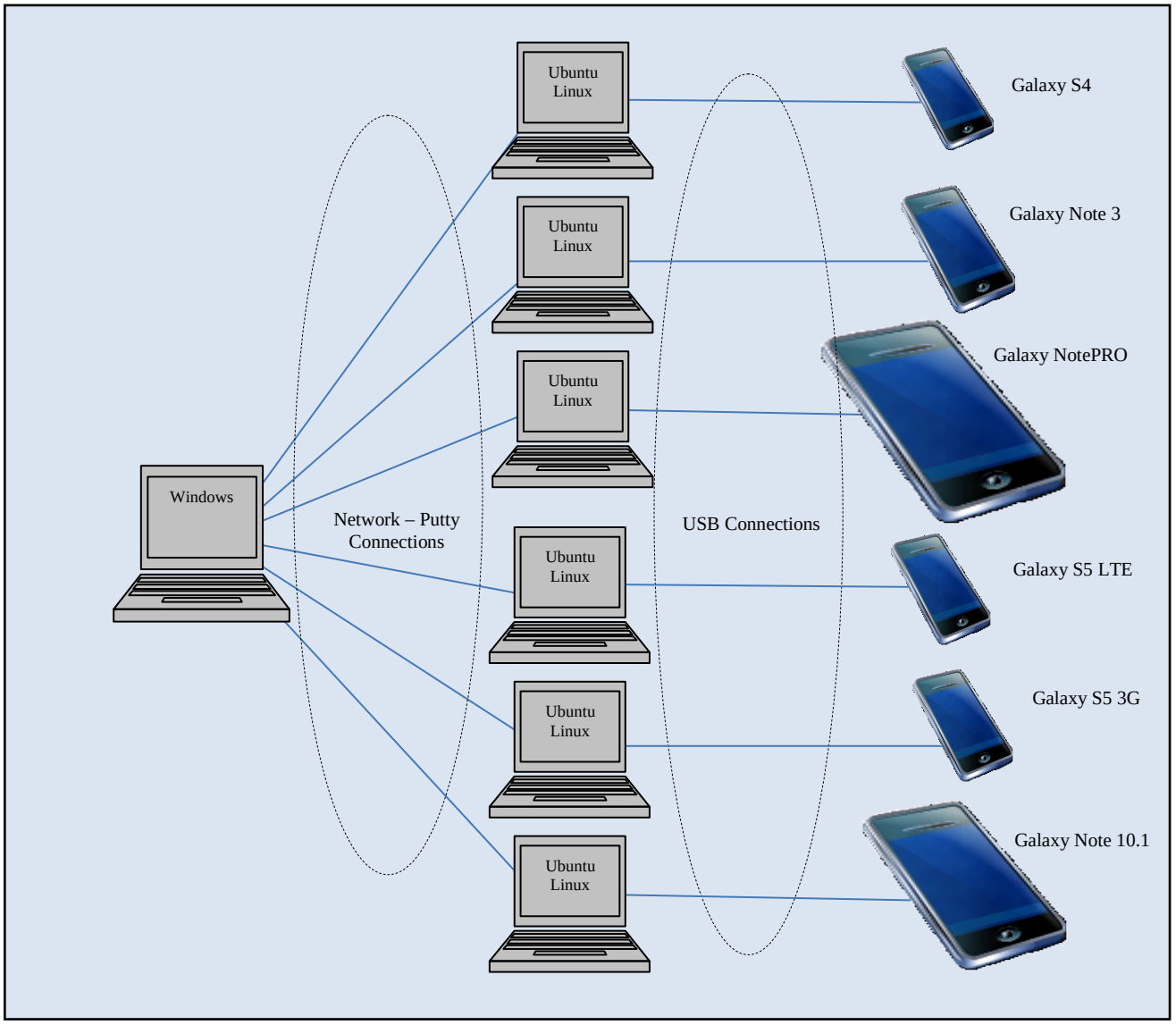

Figure 1 Evaluator Test Setup 1

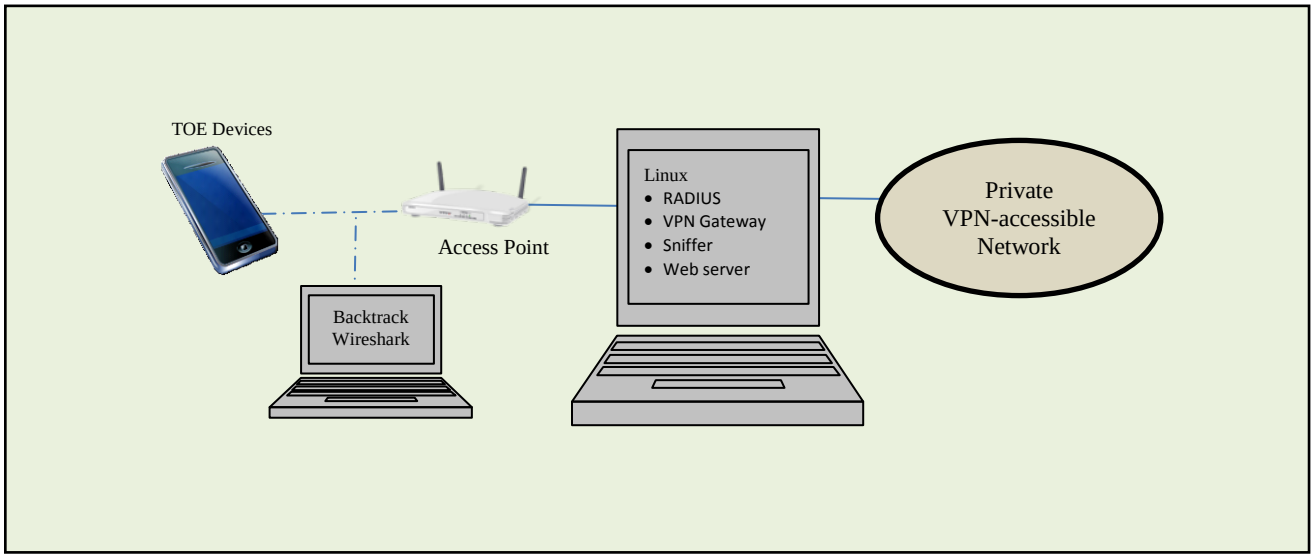

Figure 2 Evaluator Test Setup 2

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Samsung VPN Client on Galaxy Devices Guidance documentation, Version 0.6, May 13, 2014 document and ran the tests specified in the IVPNCPP14.

8 Evaluated Configuration

The evaluated configuration consists of the Samsung Galaxy Devices VPN Client devices.

To use the product in the evaluated configuration, the product must be configured as specified in Samsung VPN Client on Galaxy Devices Guidance documentation, Version 0.6, May 13, 2014.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL1 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon

CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Samsung Galaxy S5 & Galaxy Note 10.1 2014 Edition products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the IVPNCPP related to the examination of the information contained in the TSS.

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

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the IVPNCPP and recorded the results in a Test Report, summarized in the Assurance Activities Report.

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

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities and did not discover any public issues with the TOE.

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

9.7 Summary of Evaluation Results

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

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

10 Validator Comments/Recommendations

During this evaluation the CCTL requested clarification on a couple of aspects of the VPN Protection Profile. The results of this evaluation were delayed while the NIAP Technical Rapid Response Team (TRRT) and the CCTL iteratively refined the discussion and the TRRT formulated its position. The areas of concern were with the implementation of a default SPD at the VPN Client and the extent to which it could be locally administered. At the time of publication of this report, a formal TRRT position regarding the required aspects of the implementation of an SPD by the VPN Client has not been released. A general statement of the finalized interpretations will be posted on the NIAP web site and incorporated into a future revision of IVPNCPP14. It has been determined that the TOE meets the requirements and assurance activities as currently specified.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as *Samsung Electronics Co., Ltd. Samsung Galaxy Devices VPN Client (IVPNCPP14) Security Target, Version 1.0, May 23, 2014*.

13 Glossary

The following definitions are used throughout this document:

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

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

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

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013.