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 Galaxy VPN Client on Android 6 (IVPNCPP14)

Report Number: CCEVS-VR-10727-2016
Dated: June 13, 2016
Version: 0.4

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

Meredith Hennan
Jerome Myers
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
James Arnold
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 VPN Client on Android 6 (IVPNCPP14) 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 June 2016. 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 the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013.

The Target of Evaluation (TOE) is the Samsung Galaxy VPN Client on Android 6.

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 technical information included in this report was obtained from the Samsung Electronics Co., Ltd. Samsung Galaxy VPN Client on Android 6 (IVPNCPP14) Security Target, version 0.2, April 21, 2016 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common

Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Samsung Galaxy VPN Client on Android 6
Protection Profile	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
ST:	Samsung Galaxy VPN Client on Android 6 (IVPNCPP14) Security Target, version 0.2, April 21, 2016
Evaluation Technical Report	Evaluation Technical Report for Samsung Galaxy VPN Client on Android 6 (IVPNCPP14), version 0.4, June 1, 2016
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.
Developer	Samsung Electronics Co., Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Meredith Hennan
	Jerome Myers
	Aerospace Corporation

3 Architectural Information

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

The TOE is a VPN client that runs on a mobile operating system based on Android 6.0.1 with modifications made to increase the level of security provided to end users and enterprises. The TOE is intended to be used as part of an enterprise messaging solution providing mobile staff with enterprise connectivity.

The TOE platform includes a Common Criteria mode (or "CC mode") that an administrator can invoke through the use of an MDM or through the installation and use of the administrative application, CCMode.apk (see the Guidance for instructions to obtain the application). The TOE platform must be configured as follows in order for an administrator to transition the TOE platform to CC mode.

- Require a screen lock password (swipe, PIN, pattern, or facial recognition screen locks are not allowed).
- The maximum password failure retry policy should be less than or equal to ten.
- Device encryption must be enabled.
- SDCard encryption must be enabled (if the device supports SD cards).
- Revocation checking must be enabled.

When CC mode has been enabled on the TOE platform, the TOE behavior is affected. The TOE behaves as follows.

- The TOE restricts the available VPN configurations to those evaluated as part of this evaluation.
- The TOE restricts the use of IKEv1 and IKEv2 IPsec cipher suites to only those conformant with the requirements of the IVPNCPP14.
- The TOE verifies the VPN Gateway's Subject Alternative Name (either IP or DNS) matches the expected.

3.1 TOE Evaluated Configuration

The evaluated configuration consists of the following models:

There are different models of the TOE, the **Error! Reference source not found.**. These models differ physically, differ in their internal components (as described in the table below) in addition to the following functional differences.

1. The Galaxy S6 does not support external SD cards.

The model numbers of the mobile device used during the evaluation are as follows:

Device Name	Model Number	Chipset/CPU	Build Arch/ISA	Android Version	Kernel Version	Build Number
Galaxy Note 4	SM-N910F	Qualcomm APQ8084	ARMv7	6.0.1	3.10.40	MMB29M
Galaxy Note 4	SM-N910C	Exynos 5433	ARMv7	6.0.1	3.10.9	MMB29K

Galaxy S6 Edge	SM-G925V	Exynos 7420	A64	6.0.1	3.10.61	MMB29K
Galaxy S7 Edge	SM-G935F	Exynos 8890	A64	6.0.1	3.18.14	MMB29K
Galaxy S7 Edge	SM-G935A	Qualcomm MSM8996	A64	6.0.1	3.18.20	MMB29M

Based on the evaluated devices, a number of other devices are being claimed through equivalence. These claimed devices have all previously been evaluated or claimed in prior evaluations with Android 5 (Lollipop) installed and are utilizing the same hardware as one of the models that have been tested directly. The following table lists these claimed models. The differences between the evaluated devices and the equivalent ones do not relate to security claims in the evaluated configuration. The Wi-Fi chipsets are the same for each series of common devices.

Evaluated Device	Processor	Equivalent Devices	Differences
Galaxy S7 Edge (Qualcomm)	Qualcomm MSM8996	Galaxy S7 (Qualcomm)	Curved screen vs. Flat screen
Galaxy S7 Edge (Qualcomm)	Qualcomm MSM8996	Galaxy S7 Active (Qualcomm)	Curved screen vs. Flat screen S7 Active has a IP68 & MIL-STD-810G certified body No fingerprint sensor
Galaxy S7 Edge (System LSI)	Exynos 8890	Galaxy S7 (System LSI)	Curved screen vs. Flat screen
Galaxy S6	Exynos 7420	Galaxy S6 Edge	Flat screen vs. Curved screen
Galaxy S6	Exynos 7420	Galaxy S6 Edge+	Flat screen vs. Curved screen Edge+ is larger
Galaxy S6	Exynos 7420	Galaxy Note 5	Note 5 is larger Note 5 includes stylus & functionality to take advantage of it for input (not security related)
Galaxy S6	Exynos 7420	Galaxy S6 Active	S6 Active has a IP68 & MIL-STD-810G certified body No fingerprint sensor
Galaxy Note 4 (Qualcomm)	Qualcomm APQ8084	Galaxy Note Edge (Qualcomm)	Flat screen vs. Curved screen
Galaxy Note 4 (System LSI)	Exynos 5433	Galaxy Note Edge (System LSI)	Flat screen vs. Curved screen
Galaxy Note 4 (System LSI)	Exynos 5433	Galaxy Tab S2	Tab S2 is a tablet without phone capabilities

The devices include a final letter or number at the end of the name that denotes that the device is for a specific carrier (for example, V = Verizon Wireless and A = AT&T, which were used during the evaluation). The following list of letters/numbers denotes the specific models which are validated:

V – Verizon Wireless,
P - Sprint,

R4 – US Cellular,
S – SK Telecom,
L – LG Uplus,
K - Olleh,
A – AT&T,
T – T-Mobile,
C/F/I - International

Only models with one of these suffixes can be placed into the validated configuration.

The following table shows the Security software versions for all the devices.

Device Name	MDF Version	MDF Release	VPN v1.4 Release	KNOX Release
All Devices	2.0	6	6.0	2.6

3.2 Physical Boundaries

The TOE is a multi-user operating system based on Android 6.0.1 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 and cellular networks to establish network connectivity.

This evaluation does not include the underlying hardware and firmware or the device management application that is implemented on the device.

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 platform (evaluated against the Protection Profile For Mobile Device Fundamentals) for the

cryptographic services specified in the Samsung Galaxy VPN Client on Android 6 (IVPNCPP14) 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 identified throughout the Samsung Galaxy VPN Client on Android 6 (IVPNCPP14) Security Target. 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 established secure channels to corresponding VPN gateways.

5 Assumptions

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 IVPNCPP14 should be consulted if there is interest in that material.

6 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:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients and performed by the evaluation team).

2. This evaluation covers only the specific product version identified in this document, and not any earlier or later versions released or in process.
3. 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.
4. The functionality evaluated is scoped exclusively to the security functional requirements specified in the IVPNCPP14 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documentation was used as evidence for the evaluation of the Samsung Galaxy S7, S6, & Note 4:

- Samsung VPN Client on Galaxy Devices Guidance documentation, Version 2.3, April 19, 2016
- Samsung VPN Client on Galaxy Devices VPN User Guidance documentation, Version 2.3, March 23, 2016

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.

8 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 Galaxy Devices VPN Client (IVPNCPP14), Version 0.2, March 30, 2016, which is not publically available. The *Assurance Activities Report for Samsung Galaxy Devices VPN Client (IVPNCPP14), Version 0.4, June 1, 2016* (AAR), provides a non-proprietary overview of testing and the prescribed assurance activities.

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

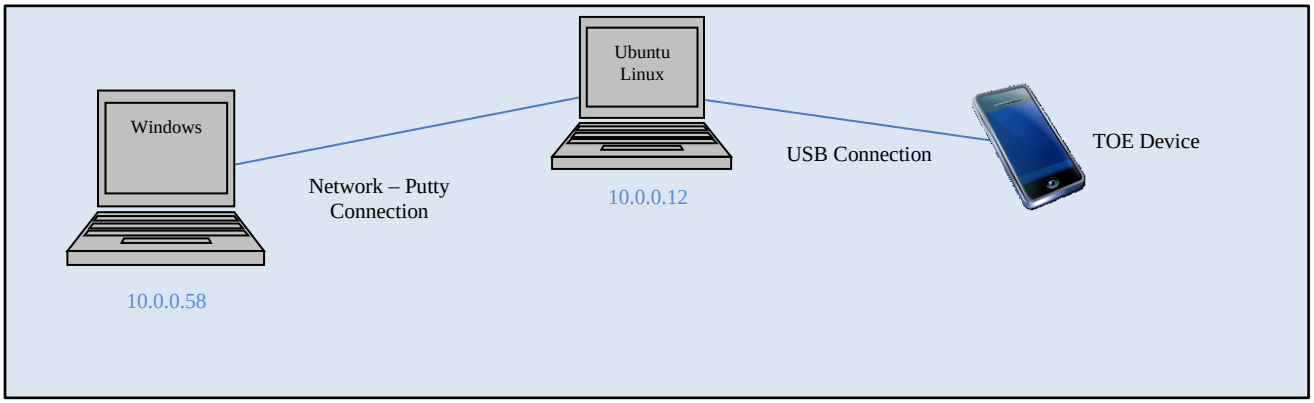

Figure 1 Evaluator Test Setup 1

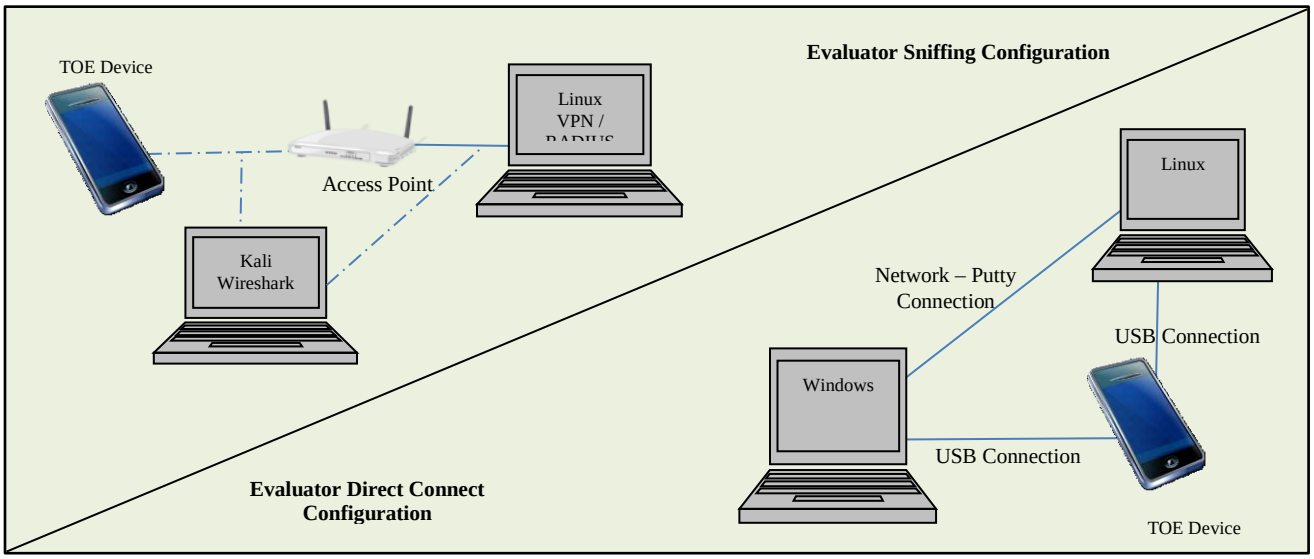

Figure 2 Evaluator Test Setup 2

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Samsung VPN Client on Galaxy Devices Guidance documentation, Version 2.3, April 19, 2016 and Samsung VPN Client on Galaxy Devices VPN User Guidance documentation, Version 2.3, March 23, 2016 documents and ran the tests specified in the IVPNCPP14.

9 Evaluated Configuration

The evaluated configuration consists of the Samsung Galaxy Devices VPN Client devices configured as specified in Samsung VPN Client on Galaxy Devices Guidance documentation, Version 2.3, April 19, 2016.

10 Results of the Evaluation

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

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Samsung Galaxy Devices VPN Client devices TOE to be Part 2 extended, and to meet the SARs contained in the IVPNCPP14.

10.1 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 VPN Client on Android 6 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.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the IVPNCPP14 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.

10.3 Evaluation of the Guidance Documents (AGD)

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

The 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.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

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

The 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.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the IVPNCPP14 and recorded the results in a Test Report, summarized in the AAR.

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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: "Samsung Note 4", "Galaxy Note 4", "Note 4", "Galaxy S6", "Samsung S6", "S6", "Galaxy S7", "Samsung S7", "S7", "Knox", "Samsung", "Android", "strongswan", "charon", "libcharon", "libstrongswan", "libhydra".

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.

10.7 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.

11 Validator Comments/Recommendations

One of the ST's claims deviates from the requirement FCS_IPSEC_EXT.1.14 defined in the VPN Protection Profile. This deviation was approved by the NIAP Technical Rapid Response Team (TRRT), and makes the assurance that the relative key strength negotiated by the product to protect the key strength of the tunnel reliant on the correct functioning and correct configuration of the remote VPN Gateway, which is beyond the scope of this evaluation.

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Samsung Electronics Co., Ltd. Samsung Galaxy VPN Client on Android 6 (IVPNCPP14) Security Target, Version 0.2, April 21, 2016.*

14 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.

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 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

[5] Samsung Electronics Co., Ltd. Samsung Galaxy VPN Client on Android 6 (IVPNCPP14) Security Target, version 0.2, April 21, 2016 (ST)

[6] Assurance Activity Report (IVPNCPP14) for Samsung Galaxy VPN Client on Android 6 (IVPNCPP14), version 0.4, June 1, 2016 (AAR)

[7] Detailed Test Report (IVPNCPP14) for Samsung Galaxy VPN Client on Android 6 (IVPNCPP14), version 0.2, March 30, 2016 (DTR)