National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Samsung Electronics Co., Ltd.

416 Maetan-3dong, Yeongtong-gu, Suwon-si,

Gyeonggi-do, 443-742 Korea

Samsung Galaxy VPN Client on Android 7.1

Report Number:	**CCEVS-VR-10850-2017**
Dated:	**November 15, 2017**
Version:	**0.3**

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

John Butterworth
The MITRE Corporation

Joanne Fitzpatrick
The MITRE Corporation

Stelios Melachrinoudis
The MITRE Corporation

Jerome Myers
The Aerospace Corporation

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
Raymond Smoley
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 7.1 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 November 2017. 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 7.1.

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 7.1 (IVPNCPP14) Security Target, Version 0.4, November 15, 2017 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 Electronics Co., Ltd. Samsung Galaxy VPN Client on Android 7.1 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
ST	Samsung Electronics Co., Ltd. Samsung Galaxy VPN Client on Android 7.1 Security Target, Version 0.4, November 15, 2017
Evaluation Technical Report	Evaluation Technical Report for Samsung Galaxy VPN Client on Android 7.1, version 0.3, November 15, 2017
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	John Butterworth The MITRE Corporation Joanne Fitzpatrick The MITRE Corporation Stelios Melachrinoudis The MITRE Corporation

Item	Identifier
	Jerome Myers Aerospace Corporation

3 Architectural Information

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

The Target of Evaluation (TOE) is **Error! Reference source not found.** with focus on the IPSEC VPN capabilities of the TOE. The IPsec VPN allows users the ability to have confidentiality, integrity, and protection of data in transit, even though it traverses a public network.

The TOE is a VPN client that runs on a mobile operating system (the TOE platform) based on Android 7.1 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 a dedicated administrative application (see the Guidance for instructions to obtain the application). The TOE platform must meet the following prerequisites 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 or a screen lock password required to decrypt data on boot.
- Revocation checking must be enabled.
- External storage must be encrypted.
- Password recovery policy must not be enabled.
- Password history length must not be set.

When CC mode has been enabled, the TOE platform behaves as follows:

- The TOE platform sets the system wide Android CC mode property to "Enabled" if all the prerequisites have been met.
- The TOE platform performs power-on self-tests.
- The TOE platform performs secure boot integrity checking of the kernel and key system executables.
- The TOE platform prevents loading of custom firmware/kernels and requires all updates occur through FOTA (Samsung's Firmware Over The Air firmware update method).
- The TOE platform uses CAVP approved cryptographic ciphers when joining and communicating with wireless networks.

- The TOE platform utilizes CAVP approved cryptographic ciphers for TLS.
- The TOE platform ensures FOTA updates utilize 2048-bit PKCS #1 RSA-PSS formatted signatures (with SHA-512 hashing).

There are different models of the mobile phone into which Samsung embeds the TOE (the **Error! Reference source not found.**). These models differ physically and differ in their internal components (as described in the table below).

3.1 TOE Evaluated Platforms

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

Device Name	Model Number	Chipset Vendor	CPU	Build Arch/ISA	Android Version	Kernel Version	Build Number
Galaxy Note 8	SM-N950F	Samsung	Exynos 8895	A64	7.1.1	4.4.13	NMF26X
Galaxy Note 8	SM-N95oU	Qualcomm	MSM8998	A64	7.1.1	4.4.21	NMF26X
Galaxy Tab Active2	SM-T395N	Samsung	Exynos 7870	A32	7.1.1	3.18.14	NMF26X

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 may be validated:

A – AT&T
C/F/I – International
D – NTT Docom
J – KDD
K - KT, Korea Telecom
L – LG Uplus

P - Sprint
R4 – US Cellular
S – SK Telecom
T – T-Mobile
U – All US Carriers (unified US model)
V – Verizon Wireless

For each device there are specific models which are validated. This table lists the specific carrier models which have the validated configuration.

Device Name	Base Model Number	Android Version	Kernel Version	Build Number	Carrier Models
Galaxy Note 8 (Qualcomm)	SM-N950	7.1	4.4.21	NMF26X	U, J, D
Galaxy Note 8 (Samsung)	SM-N950	7.1	4.4.13	NMF26X	N, F
Galaxy Tab Active2	SM-T390	7.1	3.18.14	NMF26X	None
	SM-T395	7.1	3.18.14	NMF26X	N, None
	SM-T397	7.1	3.18.14	NMF26X	None

The absence of a final carrier letter indicates a device without a carrier model designation suffix can also be placed into the validated configuration.

3.2 TOE Architecture

The TOE platform 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 established by the TOE. 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 platform is protected through the implementation of Samsung On-Device Encryption (ODE) which utilizes CAVP certified cryptographic algorithms to encrypt device 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.

3.3 Physical Boundaries

The TOE is a VPN Client executing on a multi-user mobile device based on Android 7.0 that incorporates the Samsung Enterprise SDK. The method of use for the TOE is as a VPN client for use within an enterprise environment where the configuration of the mobile device on which the TOE executes is managed through a compliant device management solution.

The TOE platform 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 summaries 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 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 platform 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 this 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 is a VPN client that uses IPsec to established secure channels to corresponding VPN gateways.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013

That information has not been reproduced here and the IVPNCPP14 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the IVPNCPP14 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 the Protection Profile for IPsec Virtual Private Network (VPN) Clients and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- 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 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 documents were available with the TOE for evaluation:

- Samsung Electronics Co., Ltd. Samsung VPN Client on Galaxy Devices Guidance documentation, Version 3.1, November 13, 2017
- Samsung Electronics Co., Ltd. Samsung VPN Client on Galaxy Devices VPN User Guidance Documentation, Version 3.1, November 13, 2017

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team as summarized in the public *Assurance Activities Report for Samsung VPN Client on Galaxy Devices (IVPNCPP14), Version 0.3, November 15, 2017* (AAR).

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

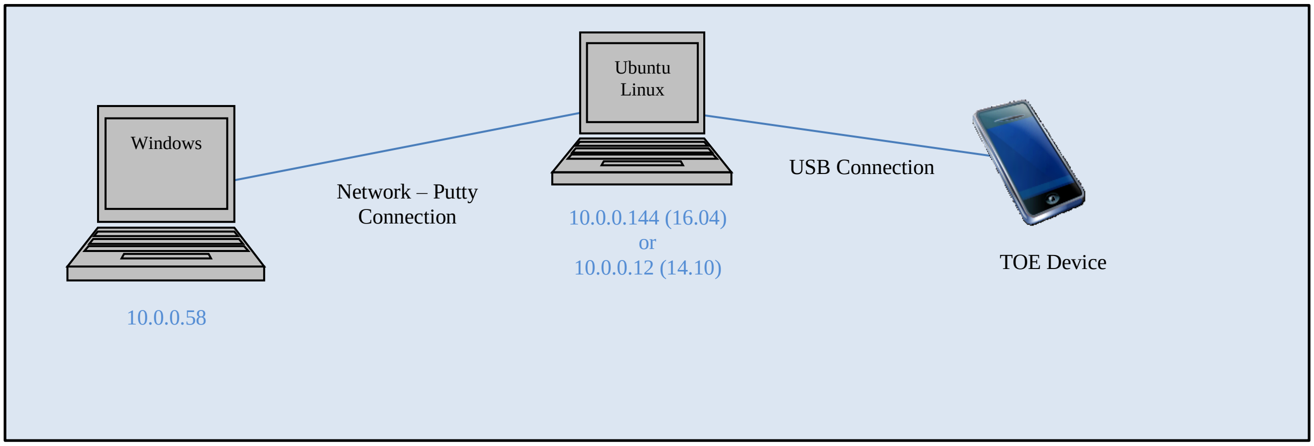
Ubuntu Linux
Windows
Network – Putty Connection
USB Connection
10.0.0.144 (16.04) or 10.0.0.12 (14.10)
TOE Device
10.0.0.58

Figure 1 Evaluator Test Setup 1

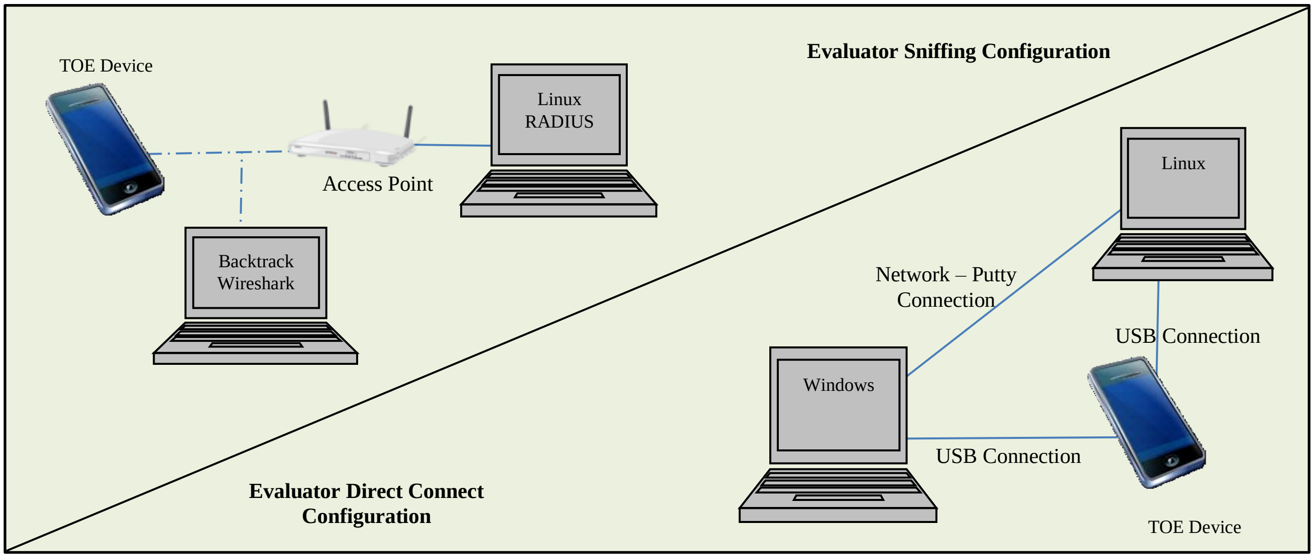

Figure 2 Evaluator Test Setup 2

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 a Common Criteria Certification document and ran the tests specified in the IVPNCPP14 including the tests associated with optional requirements. A description of the evaluation test configurations and the tools used for that testing may be found in the AAR in Sec. 3.4.1 under ATE_IND.1.

9 Evaluated Configuration

The evaluated configuration consists of the Samsung Galaxy Devices VPN Client configured as specified in Samsung VPN Client on Galaxy Devices Guidance documentation, Version 3.1, November 13, 2017.

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 VPN Client on Android 7.1 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 7.1 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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 validators 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 validators 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 validators 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 validators 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 8”, “Galaxy Note 8”, “Note 8”, “Knox”, “Samsung”, “Android”, “strongswan”, “Charon”, “libcharon”, “libstrongswan”, and “libhydra”.

The validators 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

This section is used to impart additional information about the evaluation results. These comments/ recommendations can take the form of shortcomings of the IT product discovered during the evaluation or mention of features which are particularly useful.

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). Those employing the Samsung Galaxy VPN Client on Android 7.1 must follow the configuration instructions provided in the Operational Guidance documentation listed above to ensure the evaluated configuration is established and maintained. As such, operation in FIPS-validated mode is required. 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.

The validators encourage the consumers of these products to understand the relationship between the products and any functionality that may be provided via Mobile Device Management solutions. This evaluation neither covers, nor endorses, the use of any particular MDM solution and only the MDM interfaces of the products were exercised as part of the evaluation.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Samsung Electronics Co., Ltd. Samsung Galaxy VPN Client on Android 7.1 (IVPNCPP14) Security Target, Version 0.4, November 15, 2017.*

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 2012.

[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 7.1 (IVPNCPP14) Security Target, Version 0.4, November 15, 2017 (ST)

[6] Assurance Activity Report (IVPNCPP14) for Samsung Galaxy VPN Client on Android 7.1, Version 0.3, November 15, 2017 (AAR)

[7] Detailed Test Report (IVPNCPP14) for Samsung Galaxy VPN Client on Android 7.1, Version 0.1, September 13, 2017 (DTR)

[8] Evaluation Technical Report for Samsung Galaxy VPN Client on Android 7.1, Version 0.3, November 15, 2017 (ETR)