National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Samsung Z VPN on Tizen v2.3

Report Number: CCEVS-VR-VID10613-2015
Version 1.0
August 21, 2015

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

Jerome Myers, Senior Validator
The Aerospace Corporation

Luke Florer, Lead Validator
The Aerospace Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
Justin Fisher
Chris Rakaczky

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

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 Z VPN on Tizen v2.3, provided by Samsung Electronics Corporation. 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 Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Linthicum Heights, Maryland, United States of America, and was completed in August 2015. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Protection Profile IPsec Virtual Private Network (VPN) Client, version 1.4 (IPsec VPN Client PP).

The Target of Evaluation (TOE) is the Samsung Z VPN on Tizen v2.3. The Samsung VPN TOE allows users the ability to have confidentiality, integrity, and protection of data in transit over a public or private network.

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), as interpreted by the Assurance Activities contained in the IPsec VPN Client PP. 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the IPsec VPN Client PP Assurance Activities. 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 Z VPN on Tizen v2.3 with Qualcomm Processors Security Target Version 1.0 August 21, 2015 and analysis performed by the Validation Team.

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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliance 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 Z VPN on Tizen v2.3 *Refer to Table 2 for Specifications
Protection Profile	Protection Profile IPsec Virtual Private Network (VPN) Client, version 1.4
Security Target	Samsung Z VPN on Tizen v2.3 with Qualcomm Processors Security Target Version 1.0 August 21, 2015
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Samsung VPN on Tizen v2.3 with Qualcomm Processors" Evaluation Technical Report V1.0 dated August 21, 2015
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Samsung Electronics Corporation
Developer	Samsung Electronics Corporation
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Linthicum, Maryland
CCEVS Validators	Jerome Myers, The Aerospace Corporation Luke Florer, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- Information cannot flow onto the network to which the VPN Client's host is connected without passing through the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

3.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- **T.TSF_CONFIGURATION** — Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
- **T.TSF_FAILURE** — Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- **T.UNAUTHORIZED_ACCESS** — A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- **T.UNAUTHORIZED_UPDATE** — A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- **T.USER_DATA_REUSE** — User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is done being used.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- **O.VPN_TUNNEL** — The TOE will provide a network communication channel protected by encryption that ensures that the VPN Client communicates with an authenticated VPN Gateway.
- **O.RESIDUAL_INFORMATION_CLEARING** — The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
- **O.TOE_ADMINISTRATION** — The TOE will provide mechanisms to allow administrators to be able to configure the TOE.
- **O.TSF_SELF_TEST** — The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

- **O.VERIFIABLE_UPDATES** — The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.

3.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile IPsec Virtual Private Network (VPN) Client, version 1.4 to which this evaluation claimed exact compliance.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluated configuration of the TOE includes the Samsung Z VPN on Tizen v2.3 product. The TOE includes all the code that enforces the policies identified (see Section 5).

The Non-FIPS 140-2 mode of operation is excluded from the evaluation. This mode will be disabled by configuration. The exclusion of this functionality does not affect compliance to the Protection Profile IPsec Virtual Private Network (VPN) Client, version 1.4.

4 Architectural Information

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

4.1 TOE Introduction

The Target of Evaluation (TOE) is the Samsung Z VPN on Tizen v2.3. The Samsung Z VPN on Tizen TOE allows users the ability to have confidentiality, integrity, and protection of data in transit over a public or private network. The TOE is a mobile operating system based on Linux 3.4 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 data solution providing mobile staff with enterprise connectivity. The TOE is within a configuration as specified in Section 4.2 below.

4.2 Physical Boundaries

The physical boundary of the TOE includes the TOE platform on which the TOE is installed. This platform includes the MSM8974 model processor of the Snapdragon 800 chipset that has the following specifications:

Table 2 – Operational Environment System Requirements

Component	Details
CPU	Quad-core Krait 400 CPU at up to 2.3 GHz per core
GPU	Qualcomm® Adreno™ 330 GPU
Modem	• Integrated 4G LTE Advanced World Mode, supporting LTE FDD, LTE TDD, WCDMA (DC-HSPA+, DC-HSUPA), CDMA1x, EV-DO Rev. B, TD-SCDMA and GSM/EDGE • 3rd generation integrated LTE modem, with support for LTE-Broadcast
RF	4th generation LTE multimode transceiver with Qualcomm RF360™ Front End solution for world mode bands, lower power and PCB reduction
USB	USB 2.0
Bluetooth	BT4.0 integrated digital core
WiFi	1-stream 802.11n/ac Integrated digital core
Memory/Storage	LPDDR3 800MHz Dual-channel 32-bit (12.8GBps)/eMMC 5.0 SATA3 SD 3.0 (UHS-I)

The TOE resides on a network and supports the following hardware, software, and firmware in its environment:

Table 3 – IT Environment Components

Component	Definition
Certificate Authority	A server in the operational environment that issues digital certificates.
VPN Gateway	A server in the operational environment that performs encryption and decryption of IP packets as they cross the boundary between a private network and a public network.
TOE platform	The Samsung Z device and the Tizen version 2.3 software on which the TOE is installed.
MDM Server	A server in the Operational Environment that is responsible for the administration of Mobile Devices.

5 Security Policy

5.1 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 the underlying TOE platform (evaluated against the Protection Profile For Mobile Device Fundamentals, Version 1.1 12 February 2014) for the cryptographic services specified in this Security Target.

5.2 User Data Protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets by overwriting residual information in the buffer and padding packet payloads.

5.3 Identification and Authentication

The TOE provides the ability to use, store, and protect X.509v3 certificates as defined by RFC 5280 and pre-shared keys that are used for IPsec Virtual Private Network (VPN) connections. The TOE also supports certificate revocation handling.

5.4 Security Management

The TOE, TOE platform, and VPN Gateway provide all functionality 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.

5.5 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. It performs known answer power on self-tests (POST) on its cryptographic algorithms to ensure that they are functioning correctly. Samsung security manager service invokes self-test of the OpenSSL module at start to ensure that those cryptographic algorithms are working correctly. If the TOE platform fails its power-up tests, the TOE platform will lock itself, which will prevent user login. Additionally, the Tizen OS on the TOE platform requires that all applications bear a valid signature before Tizen will install the application.

5.6 Trusted Path/Channels

The TOE acts as a VPN Client using IPsec to established secure channels to corresponding VPN Gateways.

6 Documentation

The following documentation located on NIAP's website was used as evidence for the evaluation of the Samsung Z VPN on Tizen:

- *Samsung VPN Client on Samsung Tizen Devices VPN User Guidance Documentation Version 2.0T August 13, 2015*

There are many documents available on Samsung's support website, but the above mentioned document is the only one that is to be trusted as having been part of the evaluation.

This guidance document contains the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance document is applicable for all configurations of the Samsung Z VPN on Tizen product claimed by this evaluation.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Samsung Z VPN on Tizen v2.3.

To use the product in the evaluated configuration, the product must be configured as specified in the *Samsung VPN Client on Samsung Tizen Devices VPN User Guidance Documentation Version 2.0T August 13, 2015* document. Refer to Section 6 for information on where to retrieve the document from NIAP's website and how to use this document to configure the TOE into the evaluated configuration.

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 *Evaluation Technical Report for a Target of Evaluation "Samsung VPN on Tizen v2.3 with Qualcomm Processors" Evaluation Technical Report V1.0 dated August 21, 2015*, which is not publically available.

8.1 Test Configuration

The evaluation team configured one environment for testing the TOE which was configured according the *Samsung VPN Client on Samsung Tizen Devices VPN User Guidance Documentation Version 2.0T August 13, 2015* document.

The following test tools* were utilized during the testing:

- Wireless access point: Linksys E1200
- NAT Router: Cisco ISR2921
- Wireshark: version 1.12.5
- Ettercap: version 0.8.0
- tcpdump: version 4.3.0
- Certification Authority: OpenSSL 1.0.1
- strongSwan VPN server
- Debugging tools, proprietary to the vendor

*Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the Samsung Z VPN on Tizen by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the IPsec VPN Client PP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.
- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

Note that the underlying OS platform of the mobile device was evaluated concurrently in order to ensure that threats to the VPN client that originate from the mobile device itself are appropriately mitigated.

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 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 Z VPN on Tizen TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the IPsec VPN Client PP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

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 Z VPN on Tizen product that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Protection Profile IPsec Virtual Private Network (VPN) Client, version 1.4 (IPsec VPN Client PP).

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 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's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the IPsec VPN Client PP related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the IPsec VPN Client PP related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, 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 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 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the IPsec VPN Client PP and recorded the results in a Test Report, summarized in the Evaluation Technical Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the IPsec VPN Client PP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any 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 addressed the vulnerability analysis Assurance Activities in the IPsec VPN Client PP, 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 test activities 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 performed the Assurance Activities in the IPsec VPN Client PP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the Samsung Z VPN on Tizen TOE being configured for FIPS operation.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified 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.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Samsung Z VPN on Tizen v2.3 with Qualcomm Processors Security Target Version 1.0 August 21, 2015*.

13 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AF	Authorization factor
AS	Authorization subsystem
CA	Certificate Authority
CLI	Command Line Interface
CMS	Central Management System
COTS	Commercial Off-The-Shelf
CMVP	Cryptographic Module Validation Program
DH	Diffie-Hellman
DN	Distinguished Name
DoD	Department of Defense
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
ES	Encryption Subsystem
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
ID	Identification
IKE	Internet Key Exchange
ISSE	Information System Security Engineers
IT	Information Technology
MDM	Mobile Device Manager
OSP	Organization Security Policy
PP	Protection Profile
PSK	Pre-shared Key
RGB	Random Bit Generator
SA	Security Association
SAR	Security Assurance Requirements
SCP	Secure Copy
SFR	Security Functional Requirement
SPD	Security Policy Database
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
TOE	Target of Evaluation

14 Terminology

Terminology	Definition
Administrator	A user that has administrative privilege to configure the TOE in privileged mode.
Authentication Server (AS)	An entity designed to facilitate the authentication of an entity (user or client) that attempts to access a protected network.
Critical Security Parameter (CSP)	Security related information, e.g. secret and private cryptographic keys, and authentication data such as passwords and PINs, whose disclosure or modification can compromise the security of a cryptographic module.
Entropy Source	This cryptographic function provides a seed for a random number generator by accumulating the outputs from one or more noise sources. The functionality includes a measure of the minimum work required to guess a given output and tests to ensure that the noise sources are operating properly.
FIPS-approved cryptographic function	A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either: 1) specified in a Federal Information Processing Standard (FIPS), or 2) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.
Private Network	A network that is protected from access by unauthorized users or entities.
Privileged Mode	A TOE operational mode that allows a user to perform functions that require IT Environment administrator privileges.
Public Network	A network that is visible to all users and entities and does not protect against unauthorized access (e.g. internet).
Security Administrator	Synonymous with Authorized Administrator.
Security Assurance Requirement (SAR)	Description of how assurance is to be gained that the TOE meets the SFR.
Security Functional Requirement (SFR)	Translation of the security objectives for the TOE into a standardized language.
Security Target (ST)	Implementation-dependent statement of security needs for a specific identified TOE.
Target of Evaluation (TOE)	Set of software, firmware and/or hardware possibly accompanied by guidance. For this PP the TOE is the VPN Client.
Threat Agent	An entity that tries to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
TOE Security Functionality (TSF)	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.
TOE Summary Specification (TSS)	A description of how the TOE satisfies all of the SFRs.
Trusted Channel	An encrypted connection between the TOE and a trusted remote server.
Unauthorized User	An entity (device or user) who has not been authorized by an authorized administrator to access the TOE or private network.
Unprivileged Mode	A TOE operational mode that only provides VPN Client functions for the VPN Client user.
VPN Client	The TOE allows remote users to use client computers to establish an encrypted IPsec tunnel across an unprotected public network to a private network
VPN Client User	A user operating the TOE in unprivileged mode.
VPN Gateway	A component that performs encryption and decryption of IP packets as they cross the boundary between a private network and a public network

Table 4: CC Specific Terminology

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Samsung Z VPN on Tizen v2.3 with Qualcomm Processors Security Target Version 1.0 August 21, 2015.
6. Evaluation Technical Report for a Target of Evaluation "Samsung VPN on Tizen v2.3 with Qualcomm Processors" Evaluation Technical Report V1.0 dated August 21, 2015.
7. Samsung VPN Client on Samsung Tizen Devices VPN User Guidance Documentation Version 2.0T August 13, 2015.
8. Assurance Activity Report, Samsung Z VPN on Tizen v2.3 with Qualcomm Processors V1.0 dated August 21, 2015.