National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Samsung Z with Tizen Version 2.3

Report Number: CCEVS-VR-VID10612-2015
Version 1.0
October 13, 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 with Tizen Version 2.3, 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 Extended, and meets the assurance requirements set forth in the Protection Profile for Mobile Device Fundamentals, version 1.1 (MDF PP).

The Target of Evaluation (TOE) is the Samsung Z with Tizen Version 2.3. The Samsung Z is a mobile device with a mobile operating system based on Linux 3.4 and a hardware platform containing the MSM8974 model processor of the Snapdragon 800 chipset.

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 MDF 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 MDF 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 with Tizen Version 2.3 Security Target V1.0 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 with Tizen Version 2.3 *Refer to Table 2 for Specifications
Protection Profile	Protection Profile for Mobile Device Fundamentals, version 1.1
Security Target	Samsung Z with Tizen Version 2.3 Security Target V1.0 August 21, 2015
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Samsung Tizen Version 2.3" 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 extended
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.

- It is assumed that the TOE‘s security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.
- It is assumed that the mobile user will immediately notify the administrator if the Mobile Device is lost or stolen.
- It is assumed that the mobile user exercises precautions to reduce the risk of loss or theft of the Mobile Device.

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.EAVESDROP** — If positioned on a wireless communications channel or elsewhere on the network, attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints.
- **T.NETWORK** — An attacker may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints.
- **T.PHYSICAL** — Loss of confidentiality of user data and credentials may be a result of an attacker gaining physical access to a Mobile Device.
- **T.FLAWAPP** — Malicious or exploitable code could be used knowingly or unknowingly by a developer, possibly resulting in the capability of attacks against the platform‘s system software.
- **T.PERSISTENT** — An attacker gains and continues to have access the device, resulting it loss of integrity and possible control by both an adversary and legitimate owner.

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.COMMS** — The TOE will provide the capability to communicate using one (or more) standard protocols as a means to maintain the confidentiality of data that are transmitted outside of the TOE.
- **O.STORAGE** — The TOE will provide the capability to encrypt all user and enterprise data and authentication keys to ensure the confidentiality of data that it stores.
- **O.CONFIG** — The TOE will provide the capability to configure and apply security policies. This ensures the Mobile Device can protect user and enterprise data that it may store or process.

- **O.AUTH** — The TOE will provide the capability to authenticate the user and endpoints of a trusted path to ensure they are communicating with an authorized entity with appropriate privileges.
- **O.INTEGRITY** — The TOE will provide the capability to perform self-tests to ensure the integrity of critical functionality, software/firmware and data has been maintained. The TOE will also provide a means to verify the integrity of downloaded updates.

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 for Mobile Device Fundamentals, version 1.1 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 with Tizen Version 2.3 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 for Mobile Device Fundamentals, version 1.1.

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 with Tizen Version 2.3. The Samsung Z is a mobile device with a mobile operating system based on Linux 3.4 and a hardware platform containing the MSM8974 model processor of the Snapdragon 800 chipset. The TOE is within a configuration as specified in Section 4.2 below.

4.2 Physical Boundaries

The physical boundary of the TOE is the Samsung Z, which 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 is responsible for issuing and managing digital certificates.
MDM Server	A server in the Operational Environment that is responsible for the administration of Mobile Devices.
Cellular Carrier Time	A centralized server provided by the carrier that can be used to provide authoritative system time data to the TOE.
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.

5 Security Policy

5.1 Cryptographic Support

The TOE includes a cryptographic module with FIPS 140-2 certified algorithms for a wide range of cryptographic functions including: asymmetric key generation and establishment, symmetric key generation, encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key and protected data destruction. These primitive cryptographic functions are used to implement security protocols such as TLS and IPsec, and HTTPS and also to encrypt the media (including the generation and protection of data, right, and key encryption keys) used by the TOE. Many if these cryptographic functions are also accessible as services to applications running on the TOE.

5.2 User Data Protection

The TOE is designed to control access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE is design to protect user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected.

5.3 Identification and Authentication

The TOE supports a number of features related to identification and authentication. From a user perspective, except for making phone calls to an emergency number, a password (i.e., Password Authentication Factor) must be correctly entered to unlock the TOE. Also, even when the TOE is unlocked the password must be re-entered to change the password. Passwords are obscured when entered so they cannot be read from the TOE's display. The frequency of entering passwords is limited and when a configured number of failures occur, the TOE will be wiped to protect its contents. Passwords can be constructed using upper and lower cases characters, numbers, and special characters and passwords up to 16 characters are supported.

The TOE can also serve as an 802.1X supplicant and can use X.509v3 and validate certificates for EAP-TLS, TLS and IPsec exchanges.

5.4 Security Management

The TOE provides all the interfaces necessary to manage the security functions identified throughout this Security Target as well as other functions commonly found in mobile devices. Several of these functions are accessible by the TOE’s users while others are only accessible through the MDM Server and require administrative permissions. Once an enrolled TOE has been un-enrolled, all MDM policies are removed and CC mode is disabled.

5.5 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features. It protects sensitive data such as cryptographic keys so that they are not accessible or exportable. The TOE provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). It enforces read, write, and execute memory page protections, uses address space layout randomization, and stack-based buffer overflow protections to minimize the potential to exploit application flaws. It is also designed to protect itself from modification by applications as well as to isolate the address spaces of applications from one another via sandboxing.

The TOE includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any of the self-tests fail, the TOE will not go into an operational mode. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious software or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation.

5.6 TOE Access

Locking the TOE will obscure its display, which can be manually done by the user or automatically by the TOE after a configured interval of inactivity. The TOE also has the capability to display an advisory message (banner) when a user unlocks the TOE.
The TOE allows an administrator to specify (via the MDM Server) wireless networks to which the user can have the TOE connect.

5.7 Trusted Path/Channels

The TOE supports the use of 802.11-2012, 802.1X, EAP-TLS, TLS and IPsec to secure communications channels between itself and other trusted network devices.

6 Documentation

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

- *Samsung Tizen 2.3 on Samsung Devices Guidance documentation Version 2.0T August 13, 2015*
- *Samsung Tizen 2.3 on Samsung Devices User Guidance Documentation Version 2.0T August 13, 2015*

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

This guidance documents contain 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 claimed by this evaluation.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Samsung Z with Tizen Version 2.3.

To use the product in the evaluated configuration, the product must be configured as specified in the *Samsung Tizen 2.3 on Samsung Devices Guidance documentation Version 2.0T August 13, 2015* and *Samsung Tizen 2.3 on Samsung Devices User Guidance Documentation Version 2.0T August 13, 2015* documents. Refer to Section 6 for information on where to retrieve these documents from NIAP's website and how to use these documents 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 Tizen Version 2.3" 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 Tizen 2.3 on Samsung Devices Guidance documentation Version 2.0T August 13, 2015* and *Samsung Tizen 2.3 on Samsung Devices User Guidance Documentation Version 2.0T August 13, 2015* documents.

The following test tools* were utilized during the testing:

- WireShark: version 1.12.5
- Cisco ISR2921
- strongSwan VPN Server
- Tektronix RSA306 RF Spectrum Analyzer
- Tek SignalVu-PC version 3.6.0239
- Aruba APIN0225 Wireless Access Point
- Aruba 7010 Controller
- Windows Server 2012 R2 Datacenter (Certificate Authority)
- tcpdump: version 4.3.0

*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 Samsung Z with Tizen 2.3 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 MDF 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.

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 TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the MDF 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 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 for Mobile Device Fundamentals, version 1.1 (MDF 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 MDF 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 MDF 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 MDF 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 MDF 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 MDF 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 MDF 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 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 with Tizen Version 2.3 Security Target V1.0 August 21, 2015*.

13 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Application Processor
CA	Certificate Authority
CC	Common Criteria
CLI	Command Line Interface
CMS	Central Management System
CVL	Component Validation List
DEK	Device Encryption Key
DH	Diffie-Hellman
DKEK	Device Key Encryption Key
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FEK	File Encryption Key
FIPS	Federal Information Processing Standards
FOTA	Firmware Over-the-Air
GUI	Graphical User Interface
HEK	Hardware Encryption Key
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
ISPK	Image Signing Public Key
KCK	Key Confirmation Key
KEK	Key Encryption Key
MD	Mobile Device
MMU	Memory Management Unit
NIST	National Institute of Standards and Technology
ODE	On-Device Encryption
OS	Operating System
PKCS	Public Key Cryptographic Standards
PP	Protection Profile
REK	Root Encryption Key
RGB	Random Bit Generator
RNG	Random Number Generator
SBPK	Secure Boot Public Key
SCP	Secure Copy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TSF	TOE Security Functionality
TSS	TOE Summary Specification
TOE	Target of Evaluation
UI	User Interface
VPN	Virtual Public Network

14 Terminology

Terminology	Definition
Address Space Layout Randomization (ASLR)	An anti-exploitation feature which loads memory mappings into unpredictable locations. ASLR makes it more difficult for an attacker to redirect control to code that they have introduced into the address space of a process or the kernel.
Administrator	The Administrator is responsible for management activities, including setting the policy that is applied by the enterprise on the Mobile Device. This administrator is likely to be acting remotely and could be the Mobile Device Management (MDM) Server Administrator acting through an MDM Agent. If the device is unenrolled, the user is the administrator.
Assurance	The Administrator is responsible for management activities, including setting the policy that is applied by the enterprise on the Mobile Device. This administrator is likely to be acting remotely and could be the Mobile Device Management (MDM) Server Administrator acting through an MDM Agent. If the device is unenrolled, the user is the administrator.
Data	Program/application or data files that are stored or transmitted by a server or mobile device (MD).
Data Encryption Key (DEK)	A key used to encrypt data-at-rest.
Developer Modes	Developer modes are states in which additional services are available to a user in order to provide enhanced system access for debugging of software. Developer modes are states in which additional services are available to a user in order to provide enhanced system access for debugging of software. For the purpose of this profile, these modes also include boot modes which are not verified according to FPT_TUD_EXT.2.
Enterprise Applications	Applications that are provided and managed by the enterprise.
Enterprise Data	Enterprise data is any data residing in the enterprise servers, or temporarily stored on mobile devices to which the mobile device user is allowed access according to security policy defined by the enterprise and implemented by the administrator.
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.
Enrolled state	The state in which the Mobile Device is managed with active policy settings from the administrator.
File Encryption Key (FEK)	A DEK used to encrypt a file when File Encryption is used. FEKs are unique to each encrypted file.
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.
Key Chaining	The method of using multiple layers of encryption keys to protect data. A top layer key encrypts a lower layer key which encrypts the data. This method can have any number of layers.
Key Encryption Key (KEK)	A key used to encrypt other keys, such as DEKs or storage that contains keys.
Locked State	Powered on but most functionality is unavailable for use. User authentication is required to access functionality (when so configured).
MDM Agent	The MDM Agent is installed on a mobile device as an application or is part of the mobile device‘s OS. The MDM Agent establishes a secure connection

	back to the MDM Server controlled by the administrator.
Mobile Device User (User)	This is the person who uses and is held responsible for the mobile device‘s physical control and operation.
Operating System (OS)	Software which runs at the highest privilege level and can directly control hardware resources. Modern mobile devices typically have at least two primary operating systems: one which runs on the cellular baseband processor and one which runs on the application processor. The OS of the application processor handles most user interaction and provides the execution environment for apps. The OS of the cellular baseband processor handles communications with the cellular network and may control other peripherals. The term OS, without context, may be assumed to refer to the OS of the application processor.
Password Authentication Factor	A type of authentication factor requiring the user to provide a secret set of characters to gain access.
Powered-Off State	The device has been shutdown.
PP	Protection Profile
Protected Data	Protected data is all non-TSF data, including all user or enterprise data. Protected data is encrypted while the TSF is powered off. Protected data includes all keys in software-based secure key storage. Some or all of this data may be considered sensitive data as well.
Root Encryption Key (REK)	A key tied to the device used to encrypt other keys.
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 Samsung Z with Tizen 2.3.
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.
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 with Tizen Version 2.3 Security Target V1.0 August 21, 2015.
6. Evaluation Technical Report for a Target of Evaluation "Samsung Tizen Version 2.3" Evaluation Technical Report V1.0 dated August 21, 2015.
7. Samsung Tizen 2.3 on Samsung Devices Guidance documentation Version 2.0T August 13, 2015
8. Samsung Tizen 2.3 on Samsung Devices User Guidance Documentation Version 2.0T August 13, 2015
9. Assurance Activites Report for a Target of Evaluation "Samsung Z with Tizen Version 2.3" Assurance Activities Report V1.0 dated August 21, 2015.