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 Electronics Co., Ltd. Samsung Galaxy S6 and S6 Edge

Report Number:	**CCEVS-VR-VID10633-2015**
Dated:	**April 8, 2015**
Version:	**1.1**

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

Version 1.1
April 8, 2015

ACKNOWLEDGEMENTS

Validation Team

Meredith Hennan
Jerry Myers
Ken Stutterheim
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

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

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Samsung Galaxy S6 and S6 Edge solution provided by Samsung Electronics Co., Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in April 2015. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of EAL 1 and the Protection Profile for Mobile Device Fundamentals, Version 2, 17 September 2014.

The Target of Evaluation (TOE) is the Samsung Galaxy S6 and S6 Edge devices.

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

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

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

The technical information included in this report was obtained from the Samsung Electronics Co., Ltd. Samsung Galaxy S6 and S6 Edge (MDFPP20) Security Target and analysis performed by the evaluation 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 S6 and S6 Edge
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 2, 17 September 2014
ST:	Samsung Electronics Co., Ltd. Samsung Galaxy S6 and S6 Edge (MDFPP20) Security Target, Version 0.5, April 8, 2015
Evaluation Technical Report	Evaluation Technical Report for Samsung Galaxy S6 and S6 Edge (MDFPP20) , Version 1.2, April 8, 2015
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Samsung Electronics Co., Ltd.
Developer	Samsung Electronics Co., Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Meredith Hennan, The Aerospace Corporation Jerry Myers, The Aerospace Corporation

Item	Identifier
	Ken Stutterheim, The Aerospace Corporation

3 Architectural Information

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

The TOE is a mobile operating system based on Android 5.0.2 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 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 must be configured as follows in order for an administrator to transition the TOE 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.
- Revocation checking must be enabled.

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

- The TOE sets the system wide Android CC mode property to “Enabled”.
- The TOE performs FIPS 140-2 power-on self-tests.
- The TOE performs self-tests for the key management.
- The TOE performs secure boot integrity checking of the kernel and key system executables.
- The TOE prevents loading of custom firmware/kernels and requires all updates occur through FOTA (Samsung’s Firmware Over The Air firmware update method)
- The TOE uses CAVP approved cryptographic ciphers when joining and communicating with wireless networks.
- The TOE utilizes CAVP approved cryptographic ciphers for TLS.
- The TOE ensures FOTA updates utilize 2048-bit PKCS #1 RSA-PSS formatted signatures (with SHA-512 hashing).

The TOE includes a containerization capability, KNOX. This container provides a way to segment applications and data into two separate areas on the device, such as a personal area and a work area, each with its own separate apps, data and security policies. For this effort the TOE was evaluated both without and with a KNOX container created (and to create and enable a KNOX container, one must purchase an additional license). Thus, the evaluation includes several KNOX-specific claims that apply to a KNOX container when created.

There are different models of the TOE, the Samsung S6 and S6 Edge. These models differ in physical form factor. In addition, Samsung offers each model in differing hardware models that are specific to a cellular carrier.

- Samsung manufactures the Galaxy S6 hardware with an LTE cellular radio with 3GB of RAM and with 32GB, 64GB, or 128GB of internal Flash.
- Samsung manufactures the Galaxy S6 Edge hardware with an LTE cellular radio, with 3GB of RAM, and with 32GB, 64GB, or 128GB of internal Flash

3.1 TOE Evaluated Configuration

The evaluated configuration consists of the following devices, all with the Exynos 7420 processor:

Device Name	Base Model Number	Android Version	Kernel Version	Build Number
Galaxy S6	SM-G920T	5.0.2	3.10.61	LRX22G
Galaxy S6 Edge	SM-G925T	5.0.2	3.10.61	LRX22G
Galaxy S6	SM-G920V	5.0.2	3.10.61	LRX22G
Galaxy S6 Edge	SM-G925V	5.0.2	3.10.61	LRX22G

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). The following list of letters/numbers denotes the specific models which are validated:
V, P, R4, S, L, K, A, T, I

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

The security software version is MDF v2 Release 2.

3.2 TOE Architecture

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

Data on the TOE is protected through the implementation of Samsung On-Device Encryption (ODE) which utilizes a CAVP certified cryptographic algorithms to encrypt device. 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.

KNOX provides the ability to enhance the BYOD model by creating a separate container for the Enterprise. Within this container, the Enterprise can provision separate applications and ensure they are kept separate from anything the user may do outside the KNOX container. The Enterprise can use policy controls to manage the device as a whole or the KNOX container specifically, as needed by the organization.

3.3 Physical Boundaries

The TOE is a multi-user operating system based on Android (5.0.2) that incorporates the Samsung Enterprise SDK. The TOE does not include the user applications that run on top of the operating system, but does include controls that limit application behavior. The TOE is used as a mobile device within an enterprise environment where the configuration of the device is managed through a compliant device management solution.

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

4 Security Policy

This section summarizes the security functionality of the TOE:

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

4.1 Cryptographic support

The TOE includes a cryptographic module with CAVP 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, 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 of these cryptographic functions are also accessible as services to applications running on the TOE.

4.2 User data protection

The TOE controls access to system services by hosted applications, including the protection of the Trust Anchor Database. Additionally, the TOE protects user and other data through the use of encryption so that even if a device is physically lost, the data remains protected. The functionality provided by a KNOX container, if enabled, enhances the security of user data by providing an additional layer of separation between apps and data while the device is in use.

4.3 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 and the frequency of entering passwords is limited. When a configurable number of failures occurs, the TOE will be wiped to protect its contents. Passwords can be constructed using upper and lower case characters, numbers, and special characters. Password of up to 16 characters in length are supported. The TOE can also serve as an IEEE 802.1X supplicant and can use X509v3 certificates. It can validate certificates for EAP-TLS, TLS and IPsec exchanges.

4.4 Security management

The TOE provides all the interfaces necessary to manage the security functions identified throughout the Security Target as well as other functions commonly found in mobile devices. Many of the available functions are available to users of the TOE while others are restricted to administrators operating through a Mobile Device Management (MDM) solution once the TOE has been enrolled. Once the TOE has been enrolled in a MDM and is then un-enrolled, it will remove all MDM policies and disable CC mode.

4.5 Protection of the TSF

The TOE implements a number of features to protect itself to ensure the reliability and integrity of its security features. It protects data such as cryptographic keys so that they are not accessible or exportable. It also 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 (ASLR), and stack-based buffer overflow protections to minimize the potential to exploit application flaws. It can protect itself from modification by applications, as well as isolate the address spaces of applications from one another to protect those applications.

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 self-tests fail, the TOE will not enter 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 or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation.

4.6 TOE access

The TOE can be locked by the user or after a configured interval of inactivity thereby obscuring its display. The TOE also has the capability to display an advisory message (banner) when users unlock the TOE for use. The TOE is also able to attempt to connect to wireless networks as configured.

4.7 Trusted path/channels

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

5 Assumptions and Clarification of Scope

The Security Problem Definition, including the assumptions, may be found in the Protection Profile for Mobile Device Fundamentals, Version 2, 17 September 2014 (MDFPP). That information has not been reproduced here and the MDFPP 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 MDFPP 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 device needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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:
1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Mobile Device Fundamentals Protection Profile and performed by the evaluation team).

2. 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.
3. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

6 Documentation

The following documentation was used as evidence for the evaluation of the Samsung Galaxy S6 and S6 Edge:

- Samsung Android 5 on Galaxy Devices Guidance Documentation, version 2.1, March 26, 2015
- Samsung Android 5 on Galaxy Devices User Guidance Documentation, version 2.1, March 26, 2015

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

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report for Samsung Galaxy S6 and S6 Edge (MDFPP20), Version 0.2, March 31, 2015. A non-proprietary version of the tests performed and the evidence generated is summarized in the document: Assurance Activity Report (MDFPP20) for Samsung Electronics Co., LTD. Samsung Galaxy S and S6 Edge, Version 0.3, April 8, 2015.

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

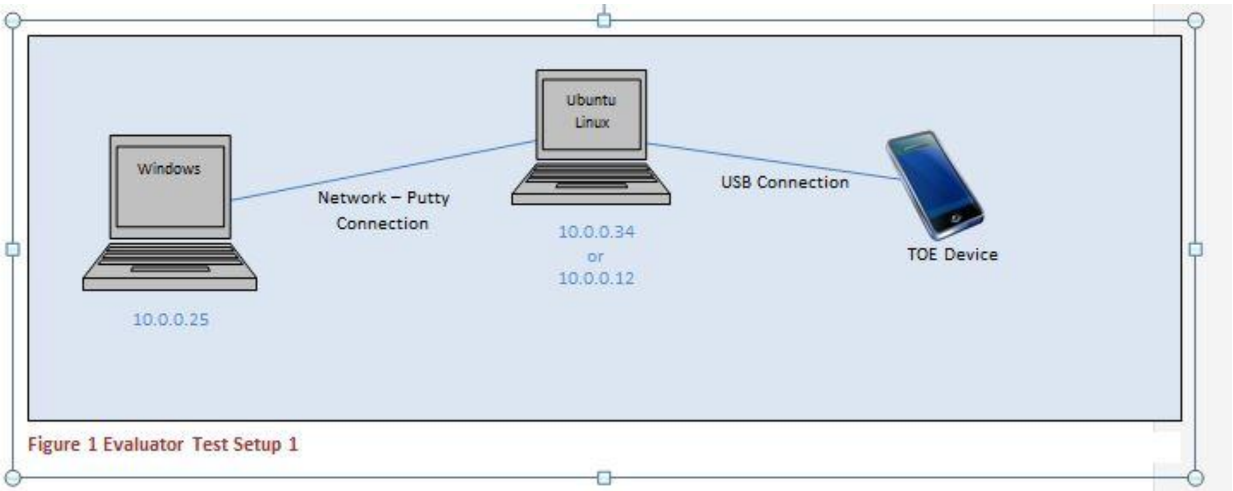

Figure 1 Evaluator Test Setup 1

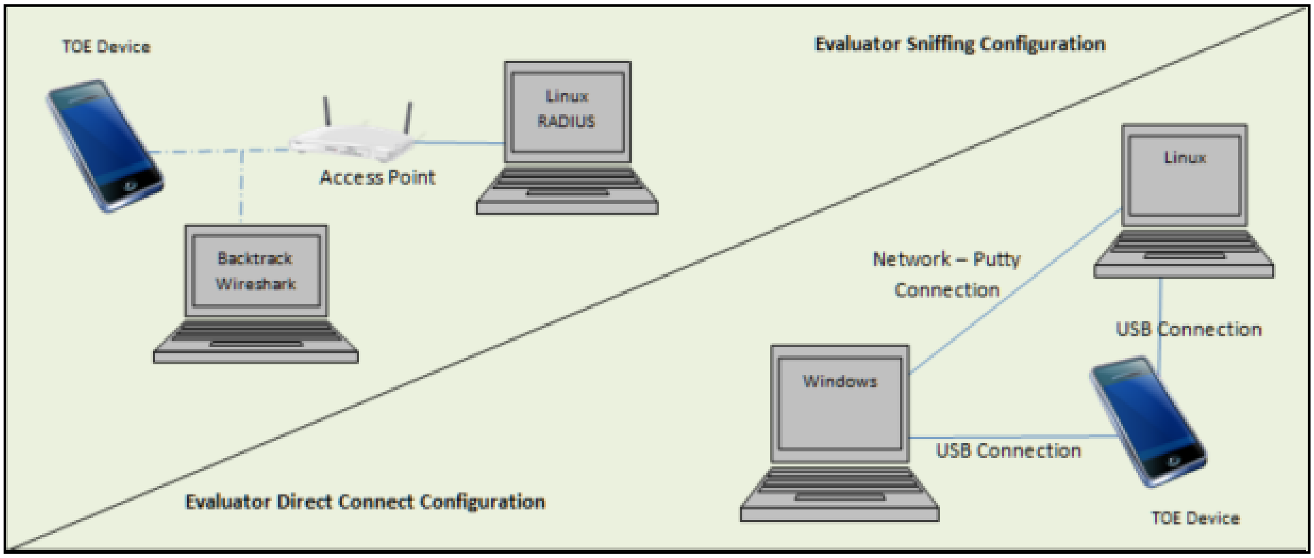

Figure 1 Evaluator Test Setup

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluated configuration consists of the Samsung Galaxy S6 and S6 Edge devices.

However, the evaluation team verified the product according the Samsung Android 5 on Galaxy Devices Guidance Documentation, version 2.1, March 26, 2015 document and ran the tests specified in the MDFPP.

To use the product in the evaluated configuration, the product must be configured as specified in Samsung Android 5 on Galaxy Devices Guidance Documentation, version 2.1, March 26, 2015.

8 Results of the Evaluation

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

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

8.1 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 S6 and S6 Edge products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

8.2 Evaluation of the Development (ADV)

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

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

8.3 Evaluation of the Guidance Documents (AGD)

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

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

8.4 Evaluation of the Life Cycle Support Activities (ALC)

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

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

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

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

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

8.6 Vulnerability Assessment Activity (VAN)

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

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

8.7 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.

9 Validator Comments/Recommendations

The evaluated configuration requires that software updates to the TOE be restricted to FOTA. The evaluators were unable to directly exercise this mechanism since it would have involved placing invalid updates on the live public servers that are currently in use by present customers. Hence, the evaluators had to take the products out of the evaluated configuration to test the update features.

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). Note that the guidance documentation used in the configuration of the Galaxy S6 and S6 Edge, is not for the versions tested. If newer documentation becomes available, regardless of labeling, it should not be used to configure the devices into CC Mode.

Note that the TOE user can configure and enable / disable a Google Backup feature to backup application data to the cloud. This backup is automatic when enabled; however the feature was not tested and no assertions can be made relative to the security of the backup feature. It cannot be assumed that backups are not occurring even when the feature is disabled.

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.

10 Annexes

Not applicable

11 Security Target

The Security Target is identified as *Samsung Electronics Co., Ltd. Samsung Galaxy S6 and S6 Edge (MDFPP20) Security Target, Version 0.5, April 8, 2015*.

12 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.

13 Bibliography

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

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

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

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

[4] Protection Profile for Mobile Device Fundamentals, Version 2, 17 September 2014.

[5] Samsung Android 5 on Galaxy Devices Guidance Documentation, version 2.1, March 26, 2015

[6] Assurance Activity Report (MDFPP20) for Samsung Electronics Co., LTD. Samsung Galaxy S and S6 Edge, Version 0.3, April 8, 2015

[7] Detailed Test Report for Samsung Galaxy S6 and S6 Edge (MDFPP20), Version 0.2, March 31, 2015

[8] Evaluation Technical Report for Samsung Galaxy S6 and S6 Edge (MDFPP20), Version 1.2, April 8, 2015