National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Samsung Electronics Co., Ltd.

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

Gyeonggi-do, 443-742 Korea

Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10)

Report Number: CCEVS-VR-10809-2017
Dated: June 15, 2017
Version: 0.4

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Stelios Melachrinoudis
The MITRE Corporation

Jerome Myers
The Aerospace Corporation

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 Devices on Android 7 (MDFPP30/WLANCEP10) solution provided by Samsung Electronics Co., Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in June 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the Protection Profile For Mobile Device Fundamentals, Version 3.0, 10 June 2016 and General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016.

The Target of Evaluation (TOE) is the Samsung Galaxy Devices on Android 7.

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

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

The technical information included in this report was obtained from the Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10) Security Target, version 0.3, May 30, 2017 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product

evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10) (Specific models identified in Section 3.1)
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 3.0, 10 June 2016 and General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016
ST	Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10) Security Target, version 0.3, May 30, 2017
Evaluation Technical Report	Evaluation Technical Report for Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10), version 0.4, June 8, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Samsung Electronics Co., Ltd.
Developer	Samsung Electronics Co., Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Stelios Melachrinoudis The MITRE Corporation
	Jerome Myers Aerospace Corporation

3 Architectural Information

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

The TOE is a mobile device based on Android 7.0 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 meet the following prerequisites 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 or a screen lock password required to decrypt data on boot.
- Revocation checking must be enabled.
- External storage must be encrypted.
- Password (non-container) recovery policy must not 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" if all the prerequisites have been met.
- 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 Workspace, which is part of the KNOX platform. 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 Workspace container created (and to create a KNOX Workspace container, one must purchase an additional license). Thus, the evaluation includes several KNOX-specific claims that apply to a KNOX Workspace container when created.

3.1 TOE Evaluated Configuration

There are different models of the TOE, the **Error! Reference source not found.**, and these models differ in their internal components (as described in the table below).

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

Device Name	Model Number	Chipset Vendor	CPU	Build Arch/ISA	Android Version	Kernel Version	Build Number
Galaxy S8	SM-G955F	System LSI	Exynos 8895	A64	7.0	4.4.13	NRD90M
Galaxy S8+	SM-G955A	Qualcomm	MSM8998	A64	7.0	4.4.16	NRD90M
Galaxy S7 Edge	SM-G935F	System LSI	Exynos 8890	A64	7.0	3.18.14	NRD90M
Galaxy S7 Edge	SM-G935A	Qualcomm	MSM8996	A64	7.0	3.18.31	NRD90M
Galaxy Tab S3	SM-T825Y	Qualcomm	MSM8996	A64	7.0	3.18.31	NRD90M
Galaxy S6 Edge	SM-G925V	System LSI	Exynos 7420	A64	7.0	3.10.61	NRD90M

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

V – Verizon Wireless,
P - Sprint,
R4 – US Cellular,
S – SK Telecom,
L – LG Uplus,
K - KT, Korea Telecom
A – AT&T,
T – T-Mobile,
C/F/I/Y – International

For each device there are specific models which are validated. This table lists the specific equivalence with the validated models.

Evaluated Device	Chipset Vendor	CPU	Equivalent Devices	Differences
Galaxy S8+	Qualcomm	MSM8998	Galaxy S8 (Qualcomm)	S8+ is larger
Galaxy S8+	Qualcomm	MSM8998	Galaxy S8 Active (Qualcomm)	Curved screen vs. Flat screen S7 Active has a IP68 & MIL-STD-810G certified body
Galaxy S8	System LSI	Exynos 8895	Galaxy S8 (System LSI)	S8+ is larger
Galaxy S7 Edge	Qualcomm	MSM8996	Galaxy S7 (Qualcomm)	Curved screen vs. Flat screen

Evaluated Device	Chipset Vendor	CPU	Equivalent Devices	Differences
Galaxy S7 Edge	Qualcomm	MSM8996	Galaxy S7 Active (Qualcomm)	Curved screen vs. Flat screen S7 Active has a IP68 & MIL-STD-810G certified body No fingerprint sensor
Galaxy S7 Edge	System LSI	Exynos 8890	Galaxy S7 (System LSI)	Curved screen vs. Flat screen
Galaxy S6 Edge	System LSI	Exynos 7420	Galaxy S6 Edge	Flat screen vs. Curved screen
Galaxy S6 Edge	System LSI	Exynos 7420	Galaxy S6 Edge+	Edge+ is larger
Galaxy S6 Edge	System LSI	Exynos 7420	Galaxy Note 5	Curved screen vs. Flat screen Note 5 is larger Note 5 includes stylus & functionality to take advantage of it for input (not security related)
Galaxy S6 Edge	System LSI	Exynos 7420	Galaxy S6 Active	Curved screen vs. Flat screen S6 Active has a IP68 & MIL-STD-810G certified body No fingerprint sensor

The full list of mobile devices which are supported by this evaluation are listed in this table.

Device Name	Base Model Number	Kernel Version	Build Number	Carrier Models
Galaxy S8 (Qualcomm)	SM-G950	4.4.16	NRD90M	U
Galaxy S8 (System LSI)	SM-G950	4.4.13	NRD90M	N, F
Galaxy S8 + (Qualcomm)	SM-G955	4.4.16	NRD90M	U
Galaxy S8 + (System LSI)	SM-G955	4.4.13	NRD90M	N, F
Galaxy S8 Active	SM-G892	4.4.16	NRD90M	A, None
Galaxy Tab S3	SM-T820	3.18.31	NRD90M	None
	SM-T825	3.18.31	NRD90M	N, Y, None
	SM-T827	3.18.31	NRD90M	V, A, R4
Galaxy S7 (Qualcomm)	SM-G930	3.18.31	NRD90M	T, P, R4, V, A
Galaxy S7 (System LSI)	SM-G930	3.18.14	NRD90M	F, S, K, L
Galaxy S7 Edge (Qualcomm)	SM-G935	3.18.31	NRD90M	A, T, P, R4, V
Galaxy S7 Edge (System LSI)	SM-G935	3.18.14	NRD90M	F, S, K, L
Galaxy S7 Active	SM-G891	3.18.31	NRD90M	A, None
Galaxy S6 Edge+	SM-G928	3.10.61	NRD90M	F, I, A, T, P, R4, V, S, K, L
Galaxy Note 5	SM-N920	3.10.61	NRD90M	I, A, T, P, R4, V, S, K, L

Galaxy S6	SM-G920	3.10.61	NRD90M	F, I, A, T, P, R4, V, S, K, L
Galaxy S6 Edge	SM-G925	3.10.61	NRD90M	F, I, A, T, P, R4, V, S, K, L
Galaxy S6 Active	SM-G890	3.10.61	NRD90M	A, None

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 storage. This functionality is combined with a number of on-device policies including local wipe, remote wipe, password complexity, automatic lock and privileged access to security configurations to prevent unauthorized access to the device and stored data.

The Samsung Enterprise Software Development Kit (SDK) builds on top of the existing Android security model by expanding the current set of security configuration of options to more than 600 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 Workspace container. The Enterprise can use policy controls to manage the device as a whole or the KNOX Workspace container specifically, as needed by the organization.

3.3 Physical Boundaries

The TOE is a multi-user mobile device based on Android (7.0) 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. When the TOE is used within an enterprise environment, the enterprise can manage the configuration of the mobile device 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 summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support

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

4.1 Security audit

The TOE is designed to be able to generate logs for a range of security relevant events. The TOE stores the logs locally so they can be accessed by an administrator or they can be exported to an MDM.

4.2 Cryptographic support

The TOE includes a cryptographic library 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 and key encryption keys) used by the TOE. Many of these cryptographic functions are also accessible as services to applications running on the TOE.

4.3 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 designed to protect user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected. The functionality provided by a KNOX Workspace container enhances the security of user data by providing an additional layer of separation between apps and data while the device is in use.

4.4 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 or Biometric Authentication Factor (BAF) 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 or re-enroll the biometric template. Passwords are obscured when entered so they cannot be read from the TOE's display and the frequency of entering passwords is limited and when a configured number of failures occurs, 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 between 4 and 16 characters are supported.

The TOE can also serve as an 802.1X supplicant and can use X509v3 and validate certificates for EAP-TLS, TLS and IPsec exchanges.

4.5 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. Many of the available functions are available to users of the TOE while many are restricted to administrators operating through a Mobile Device Management solution once the TOE has been enrolled. Once the TOE has been enrolled and then un-enrolled, it removes all MDM policies and disables CC mode.

4.6 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 particularly sensitive 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, 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 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 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 or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation.

4.7 TOE access

The TOE can be locked, obscuring its display, by the user or after a configured interval of inactivity. 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.

4.8 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.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in Protection Profile For Mobile Device Fundamentals, Version 3.0, 10 June 2016 (MDFPP30) and

General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016 (WLANCEP10). That information has not been reproduced here and the MDFPP30/WLANCEP10 should be consulted if there is interest in that material.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need 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 the and General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package Wireless Local Area Network Clients 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.
4. The functionality evaluated is scoped exclusively to the security functional requirements specified in the MDFPP30/WLANCEP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Samsung Android 7 on Galaxy Devices Guidance documentation, Version 3.0, June 1, 2017
- Samsung Android 7 on Galaxy Devices User Guidance Documentation, Version 3.0, April 18, 2017

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

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report for Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10), Version 0.3, June 7, 2017 (DTR) which is not

publically available. The *Assurance Activities Report for Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10), Version 0.4, June 8, 2017* (AAR), provides a non-proprietary overview of testing and the prescribed assurance activities.

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

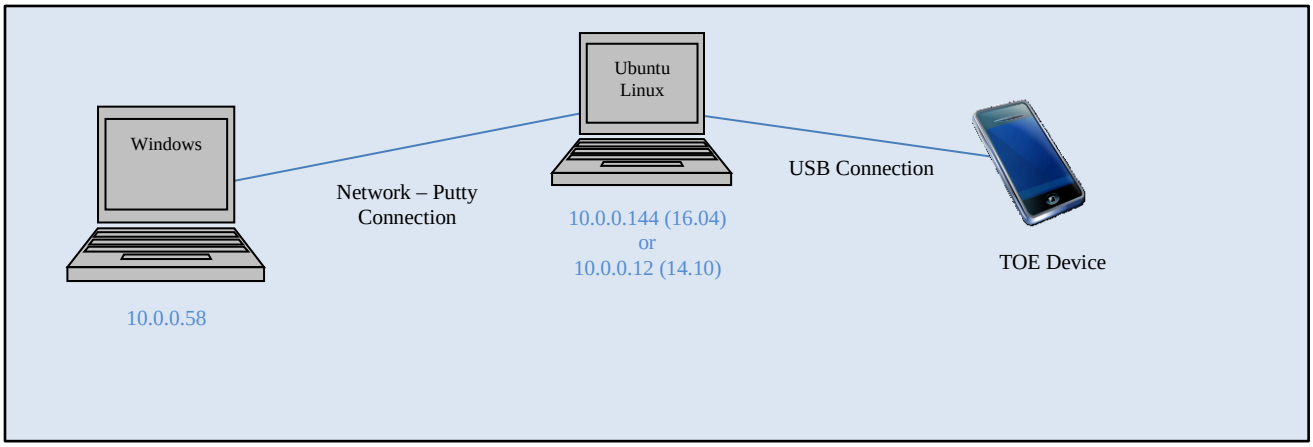

Figure 1 Evaluator Test Setup 1

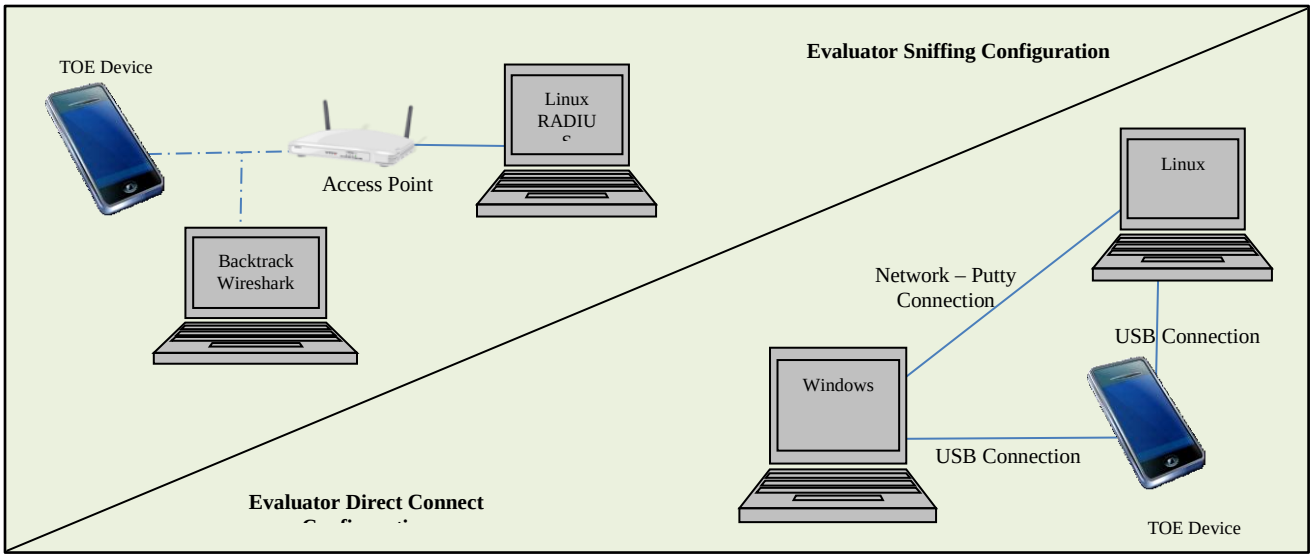

Figure 2 Evaluator Test Setup 2

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the Samsung Android 7 on Galaxy Devices Guidance documentation, Version 3.0, June 1, 2017 and Samsung Android 7 on Galaxy Devices User Guidance Documentation, Version 3.0, April 18, 2017 documents and ran the tests specified in the MDFPP30/WLANCEP10.

9 Evaluated Configuration

The evaluated configuration consists of the Samsung Galaxy Devices configured as specified in Samsung Android 7 on Galaxy Devices Guidance documentation, Version 3.0, June 1, 2017.

10 Results of the Evaluation

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

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10) TOE to be Part 2 extended, and to meet the SARs contained in the MDFPP30/WLANCEP10.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10) products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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

10.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the MDFPP30/WLANCEP10 related to the examination of the information contained in the TSS.

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

10.3 Evaluation of the Guidance Documents (AGD)

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

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

10.4 Evaluation of the Life Cycle Support Activities (ALC)

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

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

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the MDFPP30/WLANCEP10 and recorded the results in a Test Report, summarized in the AAR.

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

10.6 Vulnerability Assessment Activity (VAN)

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

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database

(http://www.kb.cert.org/vuls/) with the following search terms: Samsung S8, Galaxy S8, S8, Samsung, Knox, and Android.

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

10.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

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

The validators encourage the consumers of these products to understand the relationship between the products and any functionality that may be provided via Mobile Device Management (MDM) solutions. This evaluation neither covers, nor endorses, the use of any particular MDM solution; only the MDM interfaces of the products were exercised as part of the evaluation. In practice, the Samsung MDM is not available, though its settings could be managed via a suitable MDM and corresponding agent. Alternatively, Samsung has developed a downloadable application that can be utilized to put the device into CC mode – "CCMode.apk". The *Samsung Android 7 on Galaxy Devices Guidance Documentation* contains instructions on how the application can be acquired. As of the conclusion of this evaluation, an administrator can download the application directly from Samsung through https://docs.samsungknox.com/CCMode/CCMode_v1.2.zip or via the appropriate download link from https://www.samsungknox.com/en/article/common-criteria-mode. In addition, the

administrator can also download the latest guidance documentation and the list of applications provided with each validated device.

Over-The-Air (OTA) updates were not available during the evaluation; these are created by Google and the mobile device vendors, then distributed to the wireless carriers (Verizon, AT&T, etc.), for deployment to the respective devices via the carrier's network. Therefore, the OTA update functionality was not tested. Users and enterprise administrators should remain cognizant of OTA updates and the update cycles offered by the carriers.

There were several TRRT decisions and other considerations made throughout the course of this evaluation. Some were captured in TDs (TD 0180, TD 0194, and TD 0210) while others are either being captured in MDF PP v3.1 or limited to the current evaluation. Considerations not captured in TDs referring to biometrics requirements, as well as other TRRT queries, follow in the sections below.

11.1 TRRT decisions for Biometrics

MDF PP v3.0 currently mandates a few Assurance Activities for testing and TSS documentation that cannot be met as of the conclusion of this evaluation. Some of these issues are addressed in TDs (TD 0190 and TD 0210), while others are being addressed in MDF PP v3.1.

False Accept Rate (FAR) and False Reject Rate (FRR) testing as mandated in FIA_BMG_EXT.1.1 for MDF PP v3.0 only allows for live, online testing of fingerprint samples, but does not account for offline testing with previously generated fingerprint samples and templates that is performed by vendors throughout a product's lifecycle. More specifically, requiring the capture and use of 30,000 subjects for biometric FAR/FRR verification against a 1:10000 FAR requirement is not realistic for an evaluation.

Additionally, it is not explicitly mentioned that specific details regarding quality control, number of samples, test subjects, etc. can be made in a separate proprietary ST. A TRRT decision was made agreeing on an updated reference guide to FAR and FRR in Appendix I.1, as well as an updated Application Note for FIA_BMG_EXT.1.1 and corresponding Assurance Activity to address these issues. No TD is being issued; however, these changes will be addressed in MDF PP v3.1.

In FIA_PBA_EXT.1, the vendor selected "using a password as an additional factor" as a substitution for the "other circumstances" assignment. The validation team considers this substitution a valid refinement of the "using a PIN as an additional factor" selection per CC since a password can cover a larger key space than that of a PIN. Thus, the following statement in FIA_UAU.5.1, "if 'using a PIN as an additional factor' is selected in FDP_PBA_EXT.1.1, then 'hybrid' shall be selected", is being re-interpreted as being allowed to also include the clause, "or if 'using a password as an additional factor'". The TRRT agreed with this interpretation in its TRRT decision, but no TD is being issued; however, these changes will be addressed in MDF PP v3.1.

11.2 Additional considerations for Biometrics

Apart from TRRT decisions, a few other considerations need to be made when allowing for a biometric factor at initial configuration.

11.2.1 Clarification of Authentication Attempts at Lockscreen

When the max number of allowed "password failures" is set through the API, it also serves as the sum of authentication attempts allowed (biometric and password attempts) when a separate biometric factor is utilized at lockscreen. In CC mode, this value can be set from one to ten inclusive.

For example, if a value of ten is inputted to the setMaximumFailedPasswordsForWipe() function and only password is utilized as an authentication mechanism, only ten attempts at the password factor are allowed. However, if a biometric and password are both allowed as separate authentication mechanisms, then the same global failed authentication attempt counter is incremented regardless of which factor fails.

Once the failed attempt counter reaches ten, a device wipe takes place. Thus, there is only one counter for total authentication attempts with no counter for password attempts when determining whether a wipe takes place. As such, a wipe can still take place when using a biometric factor even when there are less than ten password attempts (for example, 9 attempts at biometric and 1 attempt at password).

Not all devices utilize the same number of allowed attempts for biometric for authentication.

For S7/S7 Edge devices, setting the sum of total authentication attempts allowed at lockscreen to values between two and nine inclusive sets the maximum number of biometric attempts allowed to be two less than this threshold (no discussion is included for a value of one). For example, if the total number of authentication attempts is set to nine, then a maximum of seven biometric attempts is allowed. Thus, at least two password attempts must be attempted before the device wipes. However, if the threshold for total authentication attempts is set to ten, then only five attempts at the biometric is allowed.

For all other devices evaluated, setting the threshold for maximum authentication attempts does not affect the maximum number of biometric or password attempts allowed at lockscreen individually; a single global authentication attempts counter is incremented until the threshold is reached to trigger a wipe.

11.2.2 Hybrid Authentication to the KNOX Container

In addition, hybrid authentication to the KNOX container (also referred to as multi-factor) does not precisely follow the definition in the MDF PP. Hybrid authentication is defined as "one where a user has to submit a combination of PIN and biometric samples with both to pass and without the user being made aware of which factor failed, if either fails."

In the evaluated configuration, a password is used in lieu of a PIN, but the user is made aware of whether the password or biometric fails. While the vendor notes in the TSS that "the

TOE's design ensures that no more than the configured maximum number of attempts is possible", compromise of the password still reduces the security of the authentication system (the SAFAR) to that of the weaker biometric authentication factor in the worst case. Parts e) and f) of the "password and fingerprint authentication example" in Appendix I.4 of MDF PP v3.0 (pgs 208-209) explain the risks of providing authentication feedback (i.e. whether the password or biometric failed) in hybrid authentication.

11.2.3 Traditional Risks Associated with Using Biometrics

Because hybrid or multi-factor authentication is not supported at lockscreen, it is recommended for customers and sponsors to understand and assume the risks provided when configuring the evaluated device to allow for a biometric factor separate from the password factor.

For this evaluation, biometric fingerprint has only been certified to the security strength of a four-digit numerical PIN (1:10000 FAR), which is much lower than that of a minimum 4-character password with 93 possible characters that can be used. CC evaluations providing for a stronger security strength for biometrics are currently infeasible to complete in a 3-6-month period. Thus, stronger claims must be assessed separately by specialized biometrics testing labs. In addition, the mitigation of threats of compromise to biometric templates, as well as system compromise through presentation attacks, is outside the scope of this evaluation because the corresponding objective requirements in the MDF PP have not been claimed.

11.3 Other TRRT Decisions

Three other TRRT decisions were made that did not lead to TDs.

A VPN client on a mobile device is only active when initiating a connection with the VPN Gateway. Because of this, even if the VPN Gateway is configured for aggressive mode, it will switch to main mode when it connects since the VPN client only supports main mode. Thus, the VPN gateway cannot connect using aggressive mode. Previous evaluations have required testing using aggressive mode, but the vendor and lab has maintained that it cannot be tested and the client does not have to accept connections initiated by the VPN Gateway. The TRRT agreed that the testing procedure to show the VPN client only supports main mode is acceptable, but is not issuing a TD; it will be addressed in the next version of the VPN Client EP.

For the testing of FIA_AFL_EXT.1, Test 3 states that "the evaluator shall ensure that the counter would be updated even if power to the device is cut immediately following notifying the TOE user if the authentication attempt was successful of not". The lab has maintained that because the battery cannot be removed from the phone, simply powering off the device is sufficient as there is no power source other than the battery. The TRRT agreed and has stated that only TSS documentation is required in this case. No TD is being issued; however, MDF PP v3.1 will address the change to only require TSS documentation when describing the actions that occur after authentication failure.

For FPT_JTA_EXT.1.1, the lab has maintained that even if the "control access by a signing key" selection is made, JTAG ports cannot be accessed since the mobile devices are released without pins or a socket to connect to. Even if provided, these pins or sockets are not easily accessible and would require disassembling or decomposing the device, which is likely to destroy or brick the devices. The TRRT agreed, stating that when "control access to a signing key" is selected, the vendor can provide evidence as to how access to the JTAG port is controlled without performing the test described. No TD is being issued; however, it is being addressed in MDF PP v3.1.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10) Security Target, Version 0.3, May 30, 2017*.

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.

- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

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

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

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

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Protection Profile For Mobile Device Fundamentals, Version 3.0, 10 June 2016 and General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016

[5] Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10) Security Target, Version 0.3, May 30, 2017 (ST)

[6] Assurance Activity Report for Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10), Version 0.4, June 8, 2017 (AAR)

[7] Detailed Test Report for Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10), Version 0.3, June 7, 2017 (DTR)

[8] Evaluation Technical Report for Samsung Galaxy Devices on Android 7 (MDFPP30/WLANCEP10), Version 0.4, June 8, 2017 (ETR)