National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Samsung Electronics Co., Ltd.

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

Gyeonggi-do, 443-742 Korea

Samsung Galaxy Devices on Android 8

Report Number:	**CCEVS-VR-10898-2018**
Dated:	**May 29, 2018**
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

John Butterworth
Joanne Fitzpatrick
Stelios Melachrinoudis
Linda Morrison

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 8 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 May 2018. 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 3.1, 16 June 2017, 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 and PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 05 October 2017.

The Target of Evaluation (TOE) is the Samsung Galaxy Devices on Android 8.

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 8 (MDFPP31/WLANCEP10/VPNC21) Security Target, Version 0.4, May 15, 2018 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 8 (Specific models identified in Section 3.1)
Protection Profile	Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017, 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 and PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 05 October 2017
ST	Samsung Galaxy Devices on Android 8 Security Target, Version 0.4, May 15, 2018
Evaluation Technical Report	Evaluation Technical Report for amsung Galaxy Devices on Android 8, version 0.4, May 22, 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Samsung Electronics Co., Ltd.
Developer	Samsung Electronics Co., Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	John Butterworth The MITRE Corporation Joanne Fitzpatrick The MITRE Corporation

Item	Identifier
	Stelios Melachrinoudis The MITRE Corporation Linda Morrison The MITRE Corporation Jerome Myers 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 device based on Android 8 with a built-in IPsec VPN client and modifications made to increase the level of security provided to end users and enterprises. The TOE is intended for use as part of an enterprise mobility solution providing mobile staff with enterprise connectivity.

The TOE includes a Common Criteria mode (or "CC mode") that an administrator can invoke using an MDM. The TOE must meet the following prerequisites in order for an administrator to transition the TOE to CC configuration.

- Require a screen lock password (swipe, PIN, pattern, accessibility (direction), or facial recognition screen locks are not allowed).
- The maximum password failure retry policy should be less than or equal to 50.
- 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 and password history 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.
- 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 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 Container, 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.

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

3.1 TOE Evaluated Platforms

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

Device Name	Model Number	Chipset Vendor	CPU	Build Arch/ISA	Android Version	Kernel Version	Build Number
Galaxy S9+	SM-G965F	Samsung	Exynos 9810	A64	8.0	4.9.65	R16NW
Galaxy S9+	SM-G965U	Qualcomm	SDM845	A64	8.0	4.9.59	R16NW
Galaxy S8	SM-G950F	Samsung	Exynos 8895	A64	8.0	4.4.13	R16NW
Galaxy S8+	SM-G955U	Qualcomm	MSM8998	A64	8.0	4.4.78	R16NW

Table 1 Evaluated Devices

In addition to the evaluated devices, the following device models are claimed as equivalent with a note about the differences between the evaluated device and the equivalent models.

Evaluated Device	CPU	Equivalent Devices	Differences
Galaxy S9+ (Qualcomm)	SDM845	Galaxy S9 (Qualcomm)	S9+ is larger
Galaxy S9+ (Samsung)	Exynos 9810	Galaxy S9 (Samsung)	S9+ is larger
Galaxy S8+ (Qualcomm)	MSM8998	Galaxy S8 (Qualcomm)	S8+ is larger
		Galaxy Note8 (Qualcomm)	Note8 includes S Pen & functionality to take advantage of it for input (not security related)
		Galaxy S8 Active	S8+ is larger S8 Active has a IP68 & MIL-STD-810G certified body
Galaxy S8 (Samsung)	Exynos 8895	Galaxy S8+ (Samsung)	S8+ is larger
		Galaxy Note8 (Samsung)	Note8 is larger Note8 includes S-Pen

Table 2 Equivalent Devices

In general, the devices include a final letter or number at the end of the name that denotes that the device is for a specific carrier or region (for example, U = US Carrier build and F = International, which were used during the evaluation). The following list of letters/numbers denotes the specific models that may be validated:

J – KDDI,
D – NTT Docomo,
U – All US Carriers (unified US model),
N – All Korean Carriers (unified Korean model),
F/C/I – International

For each device there are specific models which are validated. This table lists the specific carrier models that have the validated configuration (covering both evaluated and equivalent devices).

Device Name	Base Model Number	Carrier Models
Galaxy S9 (Qualcomm)	SM-G960	U, SC-02K*, SCV38*
Galaxy S9 (Samsung)	SM-G960	N, F
Galaxy S9+ (Qualcomm)	SM-G965	U
Galaxy S9+ (Samsung)	SM-G965	N, F
Galaxy Note8 (Qualcomm)	SM-N950	U, SC-01K*, SCV37*
Galaxy Note8 (Samsung)	SM-N950	N, F
Galaxy S8 (Qualcomm)	SM-G950	U
Galaxy S8 (Samsung)	SM-G950	N, F
Galaxy S8+ (Qualcomm)	SM-G955	U
Galaxy S8+ (Samsung)	SM-G955	N, F
Galaxy S8 Active	SM-G892	A, U, None

Table 3 Carrier Models

The carrier models marked by * are explicit model numbers for those carriers and do not follow the standard specified for other models. Where Carrier Models specifies “None” that means a device without a suffix is also a device that can be placed into a validated configuration.

3.2 TOE Architecture

The TOE combines with a Mobile Device Management solution (note that this evaluation does not include an MDM agent nor server) 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 reduces the risks that can be introduced through a Bring-Your-Own-Device (BYOD) model which can be extended to Corporate-Owned-Personally-Enabled (COPE) or other corporate-owned deployments.

Data on the TOE is protected through the implementation of Samsung On-Device Encryption (ODE) that 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 Knox Software Development Kit (SDK) builds on top of the existing Android security model by expanding the current set of security configuration options to more than 600 configurable policies and including additional security functionality such as application whitelisting and blacklisting.

The Knox Platform for Enterprise provides a set of flexible deployment options for Work environments, including the ability to enhance the BYOD or COPE models by creating a separate container for the Enterprise (the Workspace). Within the Knox Workspace, the Enterprise can provision separate applications and ensure they are kept separate from anything the user may do outside the Knox Workspace. The Enterprise can use policy controls to manage a Work environment on the device as a whole or within 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 8 that incorporates the Samsung Knox 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 includes an IPsec VPN client integrated into the firmware (as opposed to a downloadable application). Within an Enterprise environment, the Enterprise can manage the configuration of the mobile device, including the VPN client, 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 generates 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 multiple cryptographic libraries 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, EAP-TLS, IPsec, and HTTPS and 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 controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE protects 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 different categories of apps and data while the device is in use. The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

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. In addition, 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, 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 case 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 X.509v3 and validate certificates for EAP-TLS, TLS and IPsec exchanges. The TOE can also act as a client or server in an authenticated Bluetooth pairing. In addition to storing X.509 certificates used for IPsec connections, the TOE can also securely store pre-shared keys for VPN connections.

4.5 Security management

The TOE provides all the interfaces necessary to manage the security functions (including the VPN client) 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 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 also protects itself from modification by applications as well as isolates 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, HTTPS 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 the following documents:

- Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017, 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 and PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 05 October 2017

That information has not been reproduced here and the MDFPP31/WLANCEP10/VPNC21 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 MDFPP31/WLANCEP10/VPNC21 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Mobile Device Fundamentals Protection Profile and General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients and Virtual Private Network (VPN) Clients PP-Module and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the MDFPP31/WLANCEP10/VPNC21 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. Any non-security related functional capabilities of the TOE were not covered in this evaluation.
- While an MDM can be used in configuring the TOE into CC Mode, an MDM agent and server were not included and thus MDM functionality was not evaluated.
- The security functionality provided by the Knox Workspace container is limited to the Knox-specific claims made in this evaluation. All other functionality provided by the container is out of scope.

7 Documentation

The following documents were available with the TOE for evaluation:

- Samsung Android 8 on Galaxy Devices Administrator Guide, Version 4.0, May 15, 2018
- Samsung VPN Client on Galaxy Devices, Version 4.0, March 28, 2018

These are the only documents that should be trusted by the administrator in setting up the TOE into its evaluated configuration. Section 3.7 of the Samsung Android 8 Administrator Guide references procedures an end user must follow to ensure the TOE remains in the evaluated configuration (such as setting up a password). Device-specific documentation referenced by these documents (such as those references listed in Section 1.5 of the Samsung Android 8 Administrator Guide) serve as supplemental information for applying specific settings. These device-specific references are not to be used alone without consulting the two documents listed in this section.

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 Assurance Activity Report (MDFPP31/WLANCEP10/VPNC21) for Samsung Galaxy Devices on Android 8, Version 0.2, May 10, 2018 (AAR).

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the MDFPP31/WLANCEP10/VPNC21 including the tests associated with optional requirements. The AAR lists the tested devices in Section 1.1 (Device Equivalence) and provides a list of test tools and diagrams for the test environment in Section 3.4.1 (Independent Testing Conformance (ATE_IND.1)). More detailed results of testing can be found in the proprietary Detailed Test Report (DTR) prepared by the evaluator.

9 Evaluated Configuration

The evaluated configuration consists of the following series and models:

Device Name	Model Number	Chipset Vendor	CPU	Build Arch/ISA	Android Version	Kernel Version	Build Number
Galaxy S9+	SM-G965F	Samsung	Exynos 9810	A64	8.0	4.9.65	R16NW
Galaxy S9+	SM-G965U	Qualcomm	SDM845	A64	8.0	4.9.59	R16NW
Galaxy S8	SM-G950F	Samsung	Exynos 8895	A64	8.0	4.4.13	R16NW
Galaxy S8+	SM-G955U	Qualcomm	MSM8998	A64	8.0	4.4.78	R16NW

Table 4 Evaluated Devices

In addition to the evaluated devices, the following device models are claimed as equivalent with a note about the differences between the evaluated device and the equivalent models.

Evaluated Device	CPU	Equivalent Devices	Differences
Galaxy S9+ (Qualcomm)	SDM845	Galaxy S9 (Qualcomm)	S9+ is larger
Galaxy S9+ (Samsung)	Exynos 9810	Galaxy S9 (Samsung)	S9+ is larger
Galaxy S8+ (Qualcomm)	MSM8998	Galaxy S8 (Qualcomm)	S8+ is larger
		Galaxy Note8 (Qualcomm)	Note8 includes S Pen & functionality to take advantage of it for input (not security related)
		Galaxy S8 Active	S8+ is larger

			S8 Active has a IP68 & MIL-STD-810G certified body
Galaxy S8 (Samsung)	Exynos 8895	Galaxy S8+ (Samsung)	S8+ is larger
		Galaxy Note8 (Samsung)	Note8 is larger Note8 includes S-Pen

Table 5 Equivalent Devices

In general, the devices include a final letter or number at the end of the name that denotes that the device is for a specific carrier or region (for example, U = US Carrier build and F = International, which were used during the evaluation). The following list of letters/numbers denotes the specific models that may be validated:

J – KDDI,
D – NTT Docomo,
U – All US Carriers (unified US model),
N – All Korean Carriers (unified Korean model),
F/C/I – International

For each device there are specific models which are validated. This table lists the specific carrier models that have the validated configuration (covering both evaluated and equivalent devices).

Device Name	Base Model Number	Carrier Models
Galaxy S9 (Qualcomm)	SM-G960	U, SC-02K*, SCV38*
Galaxy S9 (Samsung)	SM-G960	N, F
Galaxy S9+ (Qualcomm)	SM-G965	U
Galaxy S9+ (Samsung)	SM-G965	N, F
Galaxy Note8 (Qualcomm)	SM-N950	U, SC-01K*, SCV37*
Galaxy Note8 (Samsung)	SM-N950	N, F
Galaxy S8 (Qualcomm)	SM-G950	U
Galaxy S8 (Samsung)	SM-G950	N, F
Galaxy S8+ (Qualcomm)	SM-G955	U
Galaxy S8+ (Samsung)	SM-G955	N, F
Galaxy S8 Active	SM-G892	A, U, None

Table 6 Carrier Models

The carrier models marked by * are explicit model numbers for those carriers and do not follow the standard specified for other models. Where Carrier Models specifies “None” that means a device without a suffix is also a device that can be placed into a validated configuration.

The products must be configured in accordance with the guidance listed in the Documentation section (Section 7 of this VR).

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 8 TOE to be Part 2 extended, and to meet the SARs contained in the MDFPP31/WLANCEP10/VPNC21.

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 8 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 MDFPP31/WLANCEP10/VPNC21 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 MDFPP31/WLANCEP10/VPNC21 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 proprietary 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 vulnerability analysis was performed on April 1, 2018.

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 Galaxy S9”, “Samsung S9”, “Samsung Galaxy S8”, “Samsung S8”, “Knox”, “Android”, “BoringSSL”, “strongswan”, “charon”.

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), Enterprise Device Management (EDM), and Enterprise Mobility Management (EMM) solutions (hereafter collectively referred to as MDM solutions). This evaluation neither covers, nor endorses, the use of any particular MDM solution; only the MDM-like interfaces of the products were exercised as part of the evaluation. In practice, the Samsung EDMapp and STIGtool are not available, though its settings could be managed via a suitable MDM solution and corresponding agent. Samsung does not intend to make the EDMApp and STIGtool available; however, the APIs used by these tools have been made available by Samsung. Per Section 2.3.2 of the Admin Guide, "this EDM should support the Samsung Knox APIs to enable the capabilities documented in this guide." Further, the Admin Guide states that the "Common Criteria Configuration section provides the specific information about the Knox APIs that are necessary to support this configuration…." Because the EDMApp and STIGtool apps are not available and do not intend to be made available, an a compatible MDM solution is required for the TOE to be placed in CC Mode, which in turn, places it in the evaluated configuration.

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.

Specific considerations referring to biometrics requirements follow in the sections below.

11.1 Additional considerations for Biometrics

A few considerations need to be made when allowing for a biometric factor at initial configuration.

11.1.1 Hybrid Authentication to the KNOX Container

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 H.4 of MDF PP v3.1 (pgs 180-181) explain the risks of providing authentication feedback (i.e. whether the password or biometric failed) in hybrid authentication.

11.1.2 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.

11.2 TRRT Requests and Technical Decisions

Four TRRT requests were made throughout the evaluation, two of which led to Technical Decisions (TD0301 and TD0303). These TRRT requests are as follows:

11.2.1 FIA_PSK_EXT.1 – No Practical Maximum

This issue concerns FIA_PSK_EXT.1 of the VPN Client PP-Module v2.1, which includes an Assurance Activity requiring the evaluator to test a pre-shared key above the maximum length. The concern raised by the lab was that while the vendor declared a maximum pre-shared key length of 64 characters in the SFR text, it is entirely possible to show that pre-shared key lengths greater than 64 characters can be used. In particular, the lab showed pre-shared keys over 1024 characters demonstrating successful connections. As a fix, the lab suggested that the "above the maximum" test be excluded or be optional.

After consultation with the IA SME, it was concluded that the "above the maximum" test should remain because there is no guarantee that pre-shared keys above the maximum length are preserved and may be truncated. Thus, it could create an interoperability issue when connecting to a different vendor product, as well as a usability issue where the user may assume they are getting a longer PSK than the declared maximum but is truncated. The vendor should explain what is happening with pre-shared keys with lengths greater than the maximum.

Thus, the TRRT disagreed with the suggestions in the request. Modifications to the VPN Client PP-Module to support testing ensuring the pre-shared key is not truncated beyond the declared maximum length are suggested and will be addressed in the next PP-Module update.

11.2.2 FCS_IPSEC_EXT.1.5 – IKEv1 With Only XAUTH

This issue concerns FCS_IPSEC_EXT.1.5 of the VPN Client PP-Module v2.1, which includes a selection for IKEv1 and a selection for XAUTH support, as well as applicable test cases. The corresponding test for "support for XAUTH" requires that if IKEv1 and XAUTH are supported, then IKEv1 must be tested with and without XAUTH. For this TOE, only a configuration of IKEv1 with XAUTH is supported; XAUTH cannot be turned off. The lab proposed that the Test Assurance Activities be revised to account for all corresponding combinations as appropriate.

The TRRT agreed that the TOE may, but is not required, to support IKEv1 with XAUTH and IKEv1 without XAUTH. Thus, the test would be revised to account for the various combinations.

The test was revised with the corresponding TRRT response reflected in TD0303, which is documented on the NIAP website under Technical Decisions.

11.2.3 FCS_CKM.1.1 – Generation vs. Import VPN Client Key

This issue concerns FCS_CKM.1.1 of the VPN Client PP-Module v2.1, which includes a requirement for key generation, particularly for IKE peer authentication. Although the requirement states that the VPN client or OS shall generate asymmetric keys for IKE peer authentication, it is unclear whether it allows these keys to be imported from the operational environment, especially for RSA or ECDSA as reflected in the TRRT request.

The TRRT disagreed that importing keys from the operational environment was allowed. Instead, the TRRT stated that the "intent of the IKE key generation requirement is for the key generation to be part of the evaluation. The TOE or its underlying OS (platform) must generate the keys and it is not acceptable to import the keys."

Thus, no changes to the VPN Client PP-Module were suggested.

11.2.4 FMT_SMF_EXT.3 SFR mismatch with AA

This issue concerns FMT_SMF_EXT.3 of the MDF PP v3.1, which includes a requirement to "provide a mechanism that allows users to view a list of currently authorized administrators and the management functions that each administrator is authorized to perform." The Assurance Activity requires that the evaluator should be able to view the list of policies that are currently in place from an administrator. The lab stated that the mobile device TOE may be unaware of specific policies from administrators even if the TOE is aware of the settings applied to the TOE. Instead, MDM agents and servers may likely be more aware of policies being applied to mobile device TOEs. As a result, the lab suggested removing the part of the Assurance Activity requiring the administrators to view specific policies.

The TRRT agreed with the request to remove the part of the test to require the administrator to view the list of policies in place. The response is captured in TD0301. It should be noted that TD0301 also includes an update for biometric FAR, which is separate from the issue for FMT_SMF_EXT.3 discussed in this subsection. NIAP is working on an update to the wording of Labgram #105/Valgram #125 to allow for the application of TDs that only apply in part. For example, a mobile device vendor could theoretically declare FMT_SMF_EXT.3 but not support biometrics.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Samsung Galaxy Devices on Android 8 (MDFPP31/WLANCEP10/VPNC21) Security Target, Version 0.4, May 15, 2018*.

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 3.1, 16 June 2017, 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 and PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 05 October 2017.

[5] Samsung Galaxy Devices on Android 8 (MDFPP31/WLANCEP10/VPNC21) Security Target, Version 0.4, May 15, 2018 (ST).

[6] Assurance Activity Report (MDFPP31/WLANCEP10/VPNC21) for Samsung Galaxy Devices on Android 8, Version 0.3, May 15, 2018 (AAR).

[7] Detailed Test Report (MDFPP31/WLANCEP10/VPNC21) for Samsung Galaxy Devices on Android 8, Version 0.3, May 22, 2018 (DTR).

[8] Evaluation Technical Report for Samsung Galaxy Devices on Android 8, Version 0.4, May 22, 2018 (ETR)