ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung Electronics Co., Ltd. Samsung Galaxy S7 Classified on Android 6 (MDFPP20)

Maintenance Update of Samsung Electronics Co., Ltd. Samsung Galaxy S7 Classified (MDFPP20)

Maintenance Report Number: CCEVS-VR-VID10739-2017a

Date of Activity: 27 June 2017

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;

Impact Analysis Report for Samsung Electronics Co., Ltd. Samsung Galaxy S7 Classified (MDFPP20), Version 1.3, April 28, 2017

Documentation reported as being updated:

- Samsung Electronics Co., Ltd. Samsung Galaxy S7 Classified (MDFPP20) Security Target, version 0.63, 2017/04/28

Assurance Continuity Maintenance Report:

Gossamer Security Solutions, on behalf of Samsung Electronics Co., Ltd., submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 28 April 2017. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes, and the security impact of the changes.

The IAR identifies the changes to the TOE, which include the clarification of device functionality as it relates to the Qualcomm hardware accelerator, patches for software updates for vulnerabilities, as well as other non-security claim relevant changes.

It was initially determined that the firmware for the Qualcomm Internal Cryptographic Engine (ICE) did not originally support 256-bit AES XTS keys for the On-Device Encryption (ODE) of internal storage media; instead the AES XTS encryption provided by Qualcomm only provided a 128-bit key and 128-bit tweak value, contradicting the lone 256-bit selections for FCS_CKM_EXT.2, FDP_DAR_EXT.1, and FCS_RBG_EXT.1. After this determination was made, 128-bit selection key selections were included for the non-Classified devices. To satisfy Classified requirements, 256-bit AES keys and tweak values for ODE encryption needed to be

incorporated on Classified devices. Thus, the firmware and ODE software from the Tab S3 branch, evaluated in VID 10809, were used in rebuilding the S7 branch of software with no modifications necessary (since the S7 software will not be deployed as an update to commercial devices—only Classified devices).

As a result, all mentions of 128-bit selections were removed from FCS_CKM_EXT.2 and both the TSS description of FCS_COP.1 and SFR and TSS description for FDP_DAR_EXT.1 have been updated. The reference to CBC for ODE was removed from FDP_DAR_EXT.1. Also, the FCS_COP.1 certificate listing for the Chipset hardware in the TSS has been updated to include newer CAVP certificates for AES 128/256 XTS, with the corresponding XTS certificate for the Exynos devices removed.

In addition to the selection and TSS content changes addressing AES encryption, patches for software updates for vulnerabilities are prepared as required by various policies and MDF requirements.

Non-security claim relevant changes outside the scope of the MDF evaluation were also claimed. These include disabling the SIM card as well as changes to various network and VPN-related settings, SE Android Policy Modifications, default settings, and exclusion of pre-installed apps.

The clarification of AES encryption for ODE as well as software updates for vulnerabilities listed above constitute the only security-based changes to the TOE.

The evaluation evidence consists of the Security Target and Impact Analysis Report (IAR). The Security Target and IAR include the model numbers affected, which is the Samsung Galaxy S7 Qualcomm.

Note that Samsung continually tracks bugs, vulnerabilities, and other defects reported in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the TOE.

Changes to TOE:

The specific device in question consists of the Galaxy S7 (Qualcomm). Except for the update to the Qualcomm ICE firmware and ODE to support 256-bit AES XTS keys and tweak values, the device has not changed in functionality; only the descriptions of the validated configuration have changed. The changes and effects based on ST modifications are summarized below.

1. Qualcomm ICE firmware exclusively providing 256-bit AES XTS keys and tweak values based on incorporating the Tab S3 branch (evaluated in VID 10809) into the S7 code for ODE.

Security Consideration	Assessment
The security relevant change made for the Classified device is to again support 256-bit AES encryption for the ODE	This is a security-relevant modification to the TOE. We will consider the impact by examining the individual requirements and TSS changesthemselves

services. As launched publically, the Qualcomm-based S7 devices utilized the Qualcomm ICE (Inline Cryptographic Engine) to provide encryption of the user data partition. It became clear later that the firmware in this version of ICE did not actually support 256-bit keys for XTS, but instead used 128-bit keys with a 128-bit tweak value. To provide support for 256-bit ODE on future devices, Qualcomm provided a firmware update for ICE that enabled the use of the AES XTS 256 capabilities of the hardware. The key generation component of the Qualcomm implementation limited key sizes to 128-bit. The update provided a new API where a key could be generated externally (in this case using BoringSSL) and be sent directly to the internal module for use. This new firmware API is available on all new Samsung devices using ICE (such as the Tab S3 and the Galaxy S8). This cannot be deployed to existing models though as it would require a factory reset to change the key size (there is no re-encrypt process to change the keys). The VID 10809 evaluation includes the Galaxy Tab S3 device. This device uses the same MSM8996 CPU as the S7 device used for Classified. To build the Classified device then, the firmware and ODE software from the Tab S3 branch to the Classified S7 branch with no modifications necessary (since this S7 software will not be deployed as an update to commercial devices). This updated firmware and ODE is being evaluated as part of VID 10809. While VID 10809 is being performed on Android 7, the firmware is independent of the OS installed on the device. The	(**bold underline indicates changes made or selections referenced)**. 1a) FCS_CKM_EXT.2: All DEKs shall be randomly generated with entropy corresponding to the security strength of AES key sizes of [**256**] bits. 1b) FCS_RBG_EXT.1.1: The TSF shall perform all deterministic random bit generation services in accordance with [NIST Special Publication 800-90A using [HMAC_DRBG (any), CTR_DRBG(AES)]]. 1c) FCS_RBG_EXT.1.2: The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [TSF-hardware-based noise source] with a minimum of [**256** bits] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate. 2) FCS_COP.1: Addition of AES 128/256 XTS CAVP certificates #3557/3555. 3) FDP_DAR_EXT.1.2: Encryption shall be performed using DEKs with AES in the [CBC, GCM, XTS] mode with key size [**256**] bits. Analysis of references 1a), 1b) and 1c): Change 1a) references FCS_CKM_EXT.2, but also depends on consistency with FCS_RBG_EXT.1, which corresponds to references 1b and 1c. These are being combined to a single set of references for completeness, starting from FCS_CKM_EXT.2. The Assurance Activities for FCS_CKM_EXT.2 state: "The evaluator shall review the TSS to determine how the functionality described by FCS_RBG_EXT.1 is invoked to generate DEKs. The evaluator uses the description of the RBG functionality in FCS_RBG_EXT.1 or documentation available for the operational environment to determine that the key size being requested is identical to the key size and mode to be used for the encryption/decryption of the data."

ODE software change brings the key generation for ICE in line with key generation for EXYNOS devices and older (pre-hardware accelerated) ODE software (the original ICE generated the key internally while all other ODE versions had a generated key provided to the module). All changes to the Security Target are focused on the FCS_CKM_EXT.2, FCP_COP.1 (in the TSS) and FDP_DAR_EXT.1 requirements and removing mentions of 128-bit encryption. Also the reference to CBC being used for ODE was also removed in FDP_DAR_EXT.1 as this is not the case in the TSS. In the FCS_COP.1 listing the explicitly CAVS certificate have been added for the chipset hardware table (and removed the list for the EXYNOS device). There are a few minor descriptive changes to note that this ST is for one specific device targeted to Classified, with the list of devices included in this update appropriately minimized to that list.	***Verdict*:** Analysis of FCS_CKM_EXT.2 states that the TOE RBGs "are capable of generating AES 256-bit DEKs…." In accordance with the Assurance Activity for FCS_CKM_EXT.2, the SFR, TSS, and Assurance Activity for FCS_RBG_EXT.1 were also analyzed. The TSS for FCS_RBG_EXT.1 states that Qualcomm guarantees 256 bits of entropy based on the output of DRBGs from 256-bit cryptographic algorithms (AES-256 and SHA-256). Thus, the description is consistent with that explained in FCS_CKM_EXT.2. The FCS_COP.1 certificates related to FCS_CKM_EXT.2 and FCS_RBG_EXT.1 are the same ones as those declared in the VID10739 evaluation, and thus remain valid. Therefore, all SFRs and TSS documentation affected by modifications to FCS_CKM_EXT.2 are adequately addressed by the changes made. The result for references 1a, 1b, and 1c is a PASS. <u>Analysis of reference 2):</u> Additional CAVP AES XTS certificates were added to FCS_COP.1(1) for the Chipset hardware, corresponding to #3557/3555. The certificates were checked and show that the Snapdragon 820 Inline Crypto Engine can perform encryption and description using both XTS_128 and XTS_256. Because 256-bit AES-XTS is claimed in both FCS_COP.1(1) and FDP_DAR_EXT.1.2, these new certificates are both valid and relevant to the evaluation. The result for reference 2 is a PASS. <u>Analysis of reference 3):</u> Reference 3) references FDP_EXT.EXT.1.2. The Assurance Activities state the following: For the TSS: "The evaluator shall verify that the TSS section of the ST indicates which data is protected by the DAR implementation and what data is considered TSF

	data. The evaluator shall ensure that this data includes all protected data." ***Verdict:*** The TSS addresses AES 256-bit encryption for the device under Assurance Maintenance. Therefore, the TSS changes address this Assurance Activity and are consistent with the selections declared in the SFR itself. The result is a PASS. For the AGD: "The evaluator shall review the AGD guidance to determine that the description of the configuration and use of the DAR protection does not require the user to perform any actions beyond configuration and providing the authentication credential. The evaluator shall also review the AGD guidance to determine that the configuration does not require the user to identify encryption on a per-file basis." ***Verdict:*** The configuration and functionality of the DAR protection does not change from the user's point of view, regardless of the number of bits in key size for the keys themselves, using AES. The result is a PASS. For the testing: "The evaluator shall enable encryption according to the AGD guidance. The evaluator shall create user data (non-system) either by creating a file or by using an application. The evaluator shall use a tool provided by the developer to verify that this data is encrypted when the product is powered off, in conjunction with Test 1 for FIA_UAU_EXT.1." ***Verdict:*** The test assurance activity does not verify how many bits of AES are used for DAR protection; only that the DAR protection is functional as driven by encryption. However, since the requirement has changed to support 256-bit encryption exclusively, it needs to be shown that all modes are supported, including XTS. To address this, the vendor incorporated the Samsung Galaxy Tab S3 firmware and ODE software update into the code branch implementing

	ODE for the Samsung Galaxy S7. Changes in overall code must be tested for an evaluation to pass. Testing using the new code was performed in VID 10809, which was completed on June 15, 2017. Because the software in both evaluations is identical for the implementation of ODE, as well as the hardware through the equivalency argument given in the IAR, the test will still pass if an evaluation team were to repeat it. The result is a PASS.

2. General Security Updates

Security Consideration	Assessment
The devices receive regular updates to maintain the overall security of the system as expected under a Common Criteria evaluation. Samsung works with Google to create update packages on a monthly basis for deployment (this is the SMR listed below). Samsung reviews the CVE database and prepares patches for applicable vulnerabilities on a regular basis and adds these into the SMRs for deployment during these updates.	This is consistent with all applicable NIAP policies and MDF requirements related to vulnerabilities. Original assurance is maintained.

3. SIM card disabled

Security Consideration	Assessment
The phone will not recognize a SIM when installed, and will not activate any cellular connectivity. All pop-ups related to the SIM and the SIM tray (including the notice to ensure it is inserted tightly to protect against water damage) will not appear. The device is intended to be operated only on wired or Wi-Fi networks	This is not security relevant because the claimed and tested MDF functionality remains the same.

4. Network-related settings

Security Consideration	Assessment
API to support WLAN Interface MTU to be set to less than 1500 bytes	This is not security relevant because the claimed and tested MDF functionality remains the same.

API to be able to disable Ethernet	This is not security relevant because the claimed and tested MDF functionality remains the same.

5. VPN-related settings

Security Consideration	Assessment
Always-on VPN configuration can support multiple DNS entries instead of a single entry	This is not security relevant because the claimed and tested MDF functionality remains the same.
Using a custom SDK, an API is provided to change the timeout range for the VPN connection to between 1 and 10 seconds	This is not security relevant because the claimed and tested MDF functionality remains the same.
VPN client can connect without performing a revocation check on the server certificate	This is specific to the VPN client and not revocation checking on the device as a whole. Thus, it does not change the claims in the Security Target about the device performing revocation checking otherwise (such as on a TLS connection). As a result, the claimed and tested MDF functionality remains the same.
IPsec MTU can be changes from the default of 1350 bytes	This is not security relevant because the claimed and tested MDF functionality remains the same.
KnoxVPNSampleService.apk will be preloaded to enable VPN Profile Switching and the integration of the Samsung validated VPN into the Knox VPN framework	KnoxVPNSampleService.apk is a pre-installed app. Pre-installed apps are provided by device manufacturers, OS developers, and mobile carriers. They provide capabilities outside of scope and do not provide security functionality mandated by the MDF PP. Because AVA_VAN.1 limits the scope of vulnerability search activities, the original assurance of the product is not affected.

6. SE Android Policy Modifications

Security Consideration	Assessment
Policies modified to ensure Quark Shield can operate properly	This is not security relevant because the claimed and tested MDF functionality remains the same.

SPD update is blocked	This is not security relevant because the claimed and tested MDF functionality remains the same.
Policy changes [specific to policyloader_app]	This is not security relevant because the claimed and tested MDF functionality remains the same.
Additional entries on seapp_context file	This is not security relevant because the claimed and tested MDF functionality remains the same.

7. Changed Default settings when device is first turned on (different from Commercial device)

Security Consideration	**Assessment**
o Wi-Fi ☐ Wi-Fi: off o NFC and Payment ☐ NFC and Payment: off ☐ Android Beam: off o More Connection Settings ☐ Nearby Device Scanning: off ☐ Printing > Samsung Print Services Plugin: Off o Notifications: All off o Display ☐ Screen timeout: 1 minute ☐ Always on Display: off o Advanced Features ☐ Quick Launch Camera: Off ☐ Pop-up view gesture: Off ☐ Smart capture: Off ☐ Palm swipe to capture: Off ☐ Direct call: Off ☐ Smart alert: Off ☐ Easy mute: Off o Lock Screen and Security ☐ Info and App shortcuts > App shortcuts > Left shortcut: Off ☐ Info and App shortcuts > App shortcuts > Right shortcut: Off ☐ Notifications on Lock Screen > Content on lock screen: Hide Content ☐ Notifications on Lock Screen > All apps: Off ☐ Other Security Settings > Make passwords visible: Off	This is not security relevant because the claimed and tested MDF functionality remains the same.

☐ Other Security Settings > Usage Data Access > More: Show system apps : All Off o Privacy and Safety ☐ Location: off o Developer Mode (these cannot be set by default; APIs will be provided to disable them) ☐ Developer Mode ☐ Stay Awake ☐ USB Debugging ☐ Verify USB ☐ All other settings under Developer Mode Off	

8. Pre-installed apps

Security Consideration	**Assessment**
The following normally pre-installed apps not included: o Facebook (com.facebook.appmanager) o Dictionary (com.sec.android.app.dictionary) o Gear VR Services (com.samsung.android.hmt.vrsvc, com.samsung.android.app.vrsetupwizard, com.samsung.android.app.vrsetupwizardstub, com.samsung.android.hmt.vrshell, com.samsung.android.vrsystem) o Instagram (com.instagram.android) o S Voice (com.samsung.voiceserviceplatform) o Samsung Pay (com.samsung.android.spay, com.samsung.android.spayfw) o Theme store (com.samsung.android.themestore) o WhatsApp (com.whatsapp)	Pre-installed apps are provided by device manufacturers, OS developers, and mobile carriers. They provide capabilities outside of scope and do not provide security functionality mandated by the MDF PP. Therefore, the removal of these pre-installed apps does not affect the original assurance of the product.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security. It was determined that the changes affected the documentation of a few requirements as well as CAVP certificates. The Qualcomm ICE firmware and ODE implementation were also affected. Thus, additional testing was required to address the inclusion of 256-bit AES-XTS keys and tweak values since implementation changed from the original evaluation. This testing would be addressed in VID 10809. The equivalency argument in the IAR referencing testing for this updated firmware

and ODE was found to be acceptable. No additional testing is required to address the modified ICE firmware and ODE implementation, and thus, the impact upon security was found to be minor.

Furthermore, no additional testing is required based on other documentation changes described above because the test Assurance Activities are already addressed by the original testing performed during the evaluation and by the valid CAVP certificates being declared. Because the resulting documentation was found to be complete and correct within the guidelines of the PP and without the need for additional testing from what was performed previously, the impact upon security was found to be minor.

In addition, the mobile device vendor reported having conducted a vulnerability search update that located no new vulnerabilities up to the end of the previous month as reflected by update newsletters by the platform and mobile device vendors. Further, it was also reported that the vendor did regression testing and that the changes, collectively, had no security impact on the TOE.

Therefore, CCEVS agrees that the original assurance is maintained for the product.