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

Maintenance Update of Samsung Electronics Co., Ltd. Samsung Galaxy S7 on Android 6 (MDFPP20)

Maintenance Report Number: CCEVS-VR-VID10739-2017

Date of Activity: 11 April 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 on Android 6 (MDFPP20), Version 1.2b, April 4, 2017

Documentation reported as being updated:

- Samsung Electronics Co., Ltd. Samsung Galaxy S7 on Android 6 (MDFPP20) Security Target, version 0.62, 2017/04/10

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 4 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, as well as the patches for software updates for vulnerabilities.

It was determined that the Qualcomm hardware accelerator did not provide 256-bit keys for 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. Addressing this inconsistency requires that additional 128-bit selections be incorporated with the above requirements for clarification. Specific to the Assurance Maintenance for this evaluation, it also required stating that a SHA-256 HASH_DRBG, provided by the Qualcomm Application Processor

(AP) was used in FCS_RBG_EXT.1, as well as listing additional CAVP certificate numbers for HASH_DRBG in the TSS of FCS_COP.1. The TSS descriptions were also updated to this effect for the Qualcomm versions of the S7/S7 Edge as using AES-128 XTS for ODE encryption while all other devices use AES-256 XTS for ODE.

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.

The two updates 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 are the Samsung Galaxy S7 devices (S7 Qualcomm, S7 Edge Qualcomm, and S7 Active 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 devices in question consist of three Samsung Galaxy S7 models: The Galaxy S7 (Qualcomm), the Galaxy S7 Edge (Qualcomm), and the S7 Active (Qualcomm). The devices themselves have 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 hardware accelerator providing 128-bit AES XTS keys and 128-bit tweak values, rather than 256-bit keys.

Security Consideration	Assessment
It was determined after the evaluation that the Qualcomm hardware accelerator did not actually provide a 256-bit key for the ODE encryption of the internal storage media. The AES XTS encryption provided by Qualcomm in their ICE (In-line Cryptographic Engine) module only provided a 128-bit key and a 128-bit tweak value. This is not applicable on any other model included in the evaluation and is specific to the chipset implementation at the time of the device launch. To properly clarify this position, the requirements FCS_CKM_EXT.2,	This is a security-relevant modification to the TOE. We will consider the impact by examining the individual requirements themselves (**bold underline indicates changes made)**. 1a) FCS_CKM_EXT.2: All DEKs shall be randomly generated with entropy corresponding to the security strength of AES key sizes of [**128**, 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 [**Hash_DRBG(any),** HMAC_DRBG (any), CTR_DRBG(AES)]].

FDP_DAR_EXT.1 and FCS_RBG_EXT.1 have been updated to show that 128-bit AES keys may be generated and used. In addition, the TSS was further clarified in FCP_COP.1 to list the certifications for the DRBG used on the Galaxy S7 Qualcomm devices. The TSS descriptions have been updated to reflect this with a specific notation in the FDP_DAR_EXT.1 stating that the Qualcomm versions of the S7/S7 Edge/S7 Active use AES-128 XTS for ODE while all other devices use AES-256 XTS for ODE.	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 [**128,** 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) FDP_DAR_EXT.1.2: Encryption shall be performed using DEKs with AES in the [CBC, GCM, XTS] mode with key size [**128**, 256] bits. Analysis of changes 1a), 1b) and 1c): Change 1a) references FCS_CKM_EXT.2, but also depends on consistency with FCS_RBG_EXT.1, which corresponds to changes 1b and 1c. These are being combined to a single set of changes 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." ***Verdict*:** Analysis of FCS_CKM_EXT.2 states that the TOE RBGs "are capable of generating both AES 128-bit and 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 to generate the 128-bit ODE DEK, Qualcomm processors on Galaxy S7 devices use the "SHA-256 HASH_DRBG function which uses the TOE-hardware-based noise source as input." Thus, a 128-bit ODE DEK can be generated; however, to claim an additional variant of DRBG compared to what was declared previously in the original evaluation,

	certificates listed in the TSS of FCS_COP.1 must reflect this change. The other Assurance Activities in FCS_RBG_EXT.1 are dependent on the content of the Entropy Assessment Report (EAR), which is unchanged and doesn't apply as the entropy generation is unaffected; and the corresponding CAVP certificates, which are applicable. The selections made in FCS_RBG_EXT.1 are consistent with content in the TSS. In the TSS for FCS_COP.1, Qualcomm Application Processor (AP) CAVP certificates for DRBG SHA-256 HASH_DRBG and SHA-256 were added, corresponding to #885 for DRBG, as well as #2908 and #2930 for SHA-256. Because SHA-256 is already selected in FCS_COP.1(2), content in the SFR itself, as well as other documentation apart from the TSS, is unaffected, since valid CAVP certificates exist to address the Testing portion of the Assurance Activity. Therefore, all SFRs and TSS documentation affected by modifications to FCS_CKM_EXT.2 are adequately addressed by the changes made. The result for changes 1a, 1b, and 1c is a PASS. <u>Analysis of change 2):</u> Change 2) 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-128 XTS encryption and the use of AES-128 XTS for ODE as it relates to Galaxy S7 Qualcomm devices, as well as AES 256-bit encryption for all other devices. 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. If it could be shown during the evaluation that the DAR protection was functional and the overall product functionality hasn't changed from a user's point-of-view, then 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).	This is consistent with all applicable NIAP policies and MDF requirements related to vulnerabilities. Original assurance is maintained.

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.	

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. Additional testing is not required as a result of the changes because the test Assurance Activities based on the current documentation 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.