ASSURANCE CONTINUITY MAINTENANCE REPORT FOR LG Electronics Inc. G4 Smartphone (MDFPP11)

Maintenance Update of LG Electronics Inc. G4 Smartphone (MDFPP11)

Maintenance Report Number: CCEVS-VR-VID10626-2017

Date of Activity: 21 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 LG Electronics, Inc. G4 Smartphone, Revision 1.2, April 12, 2017

Documentation reported as being updated:

- LG Electronics Inc. G4 Smartphone (MDFPP11) Security Target, version 1.6, 2017/04/04

Assurance Continuity Maintenance Report:

Gossamer Security Solutions, on behalf of LG Electronics Inc, submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 12 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 chipset, as well as the patches for software updates for vulnerabilities.

It was determined that the Qualcomm chip did not provide 256-bit encryption support for Data-At-Rest (DAR) encryption as first understood. The Qualcomm chip only provides a 128-bit key in their Inline Crypto Engine (ICE) module, contradicting the lone 256-bit selections for FCS_CKM_EXT.2 and FDP_DAR_EXT.1, as well as the TSS documentation for FCS_RBG_EXT.1. Addressing this inconsistency requires the removal of 256-bit DAR encryption protection claims, specifically, that additional 128-bit selections and any applicable documentation be incorporated with the above requirements for clarification. Specific to the Assurance Maintenance for this evaluation, it also required stating that a 128-bit AES CTR_DRBG, provided by the Qualcomm Application Processor (AP) was used in FCS_RBG_EXT.1. No additional CAVP certificates needed to be declared because of this change.

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 device affected (the LG G4), so it applies to LG G4 Qualcomm models listed in the ST.

Note that LG continually tracks Android and other vulnerabilities reported by Google and in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the TOE, as confirmed by the lab and documented in the IAR.

Changes to TOE:

The specific device in question consists of the LG G4, which includes a Qualcomm processor, thus applying to all models listed in the ST. The device and models 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. The Qualcomm chip in the TOE does not provide the 256-bit encryption support for Data at Rest device encryption as first understood. The Qualcomm chip only provides a 128-bit key in their ICE module.

Security Consideration	Assessment
The TOE has not been modified. The Qualcomm chip in the TOE does not provide the 256-bit encryption support for Data at Rest device encryption as first understood. The Qualcomm chip only provides a 128-bit key in their ICE module. As such, the Security Target has been updated to remove 256-bit Data at Rest for device encryption protection claims. To address these Qualcomm chip clarifications no requirements were changed in the Security Target. The description of FCS_CKM_EXT.2 was updated to clarify the user data partition encryption is 128-bits. The FDP_DAR_EXT.1 description was also updated to reflect 128-bit XTS mode of	This is a security-relevant modification to the TOE. We will consider the impact by examining the individual requirements themselves. While no changes were made to the requirements themselves, the TSS Assurance Activities for the following requirements have changed, so this full examination applies. 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)]].

AES. An explanation of why the selection of 128-bits was not made was for FCS_RBG_EXT.1 was added to the TSS. Also in the TSS section for FCS_RBG_EXT.1, a clarification was made in item 2 that the TOE uses a 128-bit AES CTR_DRBG.	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) FDP_DAR_EXT.1.2: Encryption shall be performed using DEKs with AES in the [CBC] mode with key size [128, 256] bits. <ins>Analysis of 1a), 1b) and 1c):</ins> 1a) references FCS_CKM_EXT.2, but also depends on consistency with FCS_RBG_EXT.1, which corresponds to 1b) and 1c). These are being combined to a single set of requirements to analyze 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 "when generating the TOE's own Data At Rest encryption key (for protection of the user data partition), the TOE uses its AES-128 CTR_DRBG provided in the Application Processor to generate a 128-bit AES XTS key." 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 "while the TOE includes implementations of three DRBG variants (and supports all options within each variant), the TOE (and its current system level applications) make use of an AES-256 CTR_DRBG

	and AES-128 CTR_DRBG.” At this point, one can make the argument that a missing 128-bit selection for FCS_RBG_EXT.1 would violate exact conformance because of the inconsistency with the TSS description above; however, the lab has addressed this with the following explanation: “The FCS_RBG_EXT.1 requirement does not include a 128-bit selection for its data protection as the 256-bit addresses the superset of cases in the requirements. As the PP indicates in its application notes for FCS_RBG_EXT.1 *‘For the selection in FCS_RBG_EXT.1.2, the ST author selects the appropriate number of bits of entropy that corresponds to the greatest security strength of the algorithms included in the ST. Security strength is defined in Tables 2 and 3 of NIST SP 800-57A. For example, if the implementation includes 2048-bit RSA (security strength of 112 bits), AES 128 (security strength 128 bits), and HMAC-512 (security strength 256 bits), then the ST author would select 256 bits.’*” The explanation above addresses the inconsistency concern one would raise up to this point of the analysis. 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, the CAVP certificates are unaffected and based on the updated TSS descriptions, it can be concluded that valid CAVP certificates still exist to address the Testing portion of the Assurance Activity. Therefore, all SFRs and TSS documentation affected by DAR key size starting from FCS_CKM_EXT.2 are adequately addressed by the changes made. The result for 1a, 1b, and 1c is a PASS.

	Analysis of 2): 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 the AES 128-bit DEK for with XTS feedback mode to encrypt the DAR partition. 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, since it would yield the same result using the same text. The result is a PASS.

2. General Security Updates

Security Consideration	**Assessment**
This section updates the vulnerability analysis since the last completed evaluation for the TOE. Note the vendor has also applied all Android patches through the date of this IAR.	This is consistent with all applicable NIAP policies and MDF requirements related to vulnerabilities. Original assurance is maintained.

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. 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 applied all Android patches through the date of this IAR as reflected by update notes and newsletters by the platform and mobile device vendors. Further, it was also reported that the lab did a vulnerability analysis and that the changes, collectively, had no security impact on the TOE.

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