# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR LG Electronics G3 Smartphone with Lollipop OS

## Maintenance Update of LG Electronics G3 Smartphone with Lollipop OS

**Maintenance Report Number:** CCEVS-VR-VID10621-2015a

**Date of Activity**: 30 June 2015

**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. G3 Smartphone Lollipop OS Revision 1.1, June 30, 2015.

**Documentation Updated**: (List all documentation updated)

**Security Target:** LG Electronics Inc. G3 Smartphone (MDFPP11) Security Target, Version 1.5, March 19, 2015**.** Changes in the Security Target are:

- Updated identification of ST and maintained TOE.
- Updated to remove references to the Bouncy Castle cryptographic library and reference the new Admin Guide.
- Updated to correct a kernel Random Number Generator (RNG) CAVP reference.

**Guidance Documentation**: LG Electronics Inc. G3 Administrator Guidance, version 1.3, March 26, 2015. Changes in the maintained guidance documentation include.

- Updated document to version 1.4
- Removed references to the Bouncy Castle cryptographic library.

**Assurance Continuity Maintenance Report:**

Gossamer CCTL submitted an Impact Analysis Report (IAR) for the LG G3 Smartphone with Lollipop OS to the CCEVS for approval, and provided an updated package in June 2015. 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.

**Changes to TOE:**

No changes were made to the TOE software as initially validated. The TOE provides several evaluated cryptographic service providers (CSPs) that can be used to develop secure software targeting the evaluated configuration. The device's Bouncy Castle CSP, which is used to provide cryptographic services to user-mode applications, does not meet recent, more stringent health requirements levied by NIST. The Bouncy Castle CSP is still available as part of the TOE, but its use by software developers is discouraged. Software developers must use the cryptographic services provided by the other approved CSPs available on the device when developing software targeting the evaluated configuration. Software developers should consult the LG Electronics Inc. G3 Administrator Guidance, Version 1.4 for instructions and sample code for developing software using the device's approved CSPs.

**Equivalency Discussion**

No changes were made to the TOE software as initially validated.

**Summary of Product Changes:**

No changes were made to the TOE software as initially validated.

**Regression Tests**:

No regression tests were conducted because the TOE has not changed.

**Conclusion:**

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found the changes to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.