National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

LG Electronics Inc.

20 Yoido-dong, Youngdungpogu, Seoul 152-721, Korea

LG Electronics Inc. G4 Smartphone

Report Number: CCEVS-VR-VID10626-2015
Dated: July 1, 2015
Version: 1.0

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

Jerry Myers
Ken Stutterheim
Aerospace Corporation

Sheldon Durrant
Stelios Melachrinoudis
MITRE Corporation

Common Criteria Testing Laboratory

James Arnold
Tammy Compton
Khai Van
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 LG G4 Smartphone solution provided by LG Electronics Inc. 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 June 2015. 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.

The Target of Evaluation (TOE) is the LG G4 Smartphone with a Qualcomm Snapdragon 808 (MSM8992) processor.

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 Gossamer Security Solutions evaluation team concluded that the TOE met Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the LG Electronics Inc. G4 Smartphone (MDFPP11) Security Target and analysis performed by the evaluation 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:	LG Electronics Inc. G4 Smartphone with a Qualcomm Snapdragon 808 (MSM8992) processor
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 1.1, 12 February 2014
ST:	LG Electronics Inc. G4 Smartphone (MDFPP11) Security Target, Version 1.4, May 27, 2015
Evaluation Technical Report	Evaluation Technical Report for LG Electronics Inc. G4 Smartphone (MDFPP11), Version 0.2, July 1, 2015
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	LG Electronics Inc.
Developer	LG Electronics Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Jerry Myers, The Aerospace Corporation
	Ken Stutterheim, The Aerospace Corporation

Item	Identifier
	Sheldon Durrant, The MITRE Corporation
	Stelios Melachrinoudis, The MITRE 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 used to support enterprises and individual users alike. Based upon Android 5.1 and improved by LG, the TOE provides wireless connectivity and an execution environment for mobile applications

The TOE provides a rich Application Programming Interface (API) to mobile applications and allows users installing an application to either approve or reject an application based upon the API access that the application requires.

The TOE also provides users with the ability to protect Data-At-Rest with AES encryption, including all user and mobile application data stored in the user's data partition. The TOE affords special protection to all user and application cryptographic keys stored in the TOE. Moreover, the TOE provides users the ability to AES encrypt data and files stored on an SD Card inserted into the device.

Finally, the TOE interacts with a Mobile Device Management solution to allow enterprise control of the configuration and operation of the device so as to ensure adherence to enterprise-wide policies.

3.1 TOE Evaluated Configuration

The evaluated configuration for the LG G4 Smartphone contains 32GB of internal Flash storage, 3GB of memory, and a Qualcomm Snapdragon 808 (MSM8992) processor and comes in the following different carrier versions.

Product	Carrier	Security Software Version	OS version	Build number
LG G4 H810	AT&T	MDF v1.1 Release 5	Android 5.1	LMY47D
LG G4 VS986	Verizon	MDF v1.1 Release 5	Android 5.1	LMY47D
LG G4 LS991	Sprint	MDF v1.1 Release 5	Android 5.1	LMY47D
LG G4 H811	T-Mobile	MDF v1.1 Release 5	Android 5.1	LMY47D

NOTE: Carrier specific versions of the evaluated product are released based upon that carrier's own schedule, so some carriers may not have released the evaluated version of the TOE by the time this report is published. Therefore, consumers should ensure that they have the evaluated version of the product software.

3.2 Physical Boundaries

The TOE's physical boundary is the physical perimeter of its enclosure (without the rear access cover present, so that one can access and replace the device's battery, SIM, and SD Card).

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security Management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Cryptographic support

The TOE includes cryptographic modules with FIPS 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 and HTTPS and also to encrypt Data-At-Rest (including the generation and protection of keys and key encryption keys) used by the TOE. Many of these cryptographic functions are also accessible as services to applications running on the TOE.

4.2 User data protection

The TOE is designed to control access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE is designed to protect user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected.

4.3 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 (i.e., Password Authentication Factor) must be correctly entered to unlock the TOE. Also, even when the TOE is unlocked the password must be re-entered to change the password. Passwords are obscured when entered so they cannot be read from the TOE's display and 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 cases characters, numbers, and special characters and passwords up to 14 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 HTTPS exchanges.

4.4 Security management

The TOE provides all the interfaces necessary to manage the security functions 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 (MDM) solution once the TOE has been enrolled. Once the TOE has been enrolled and then un-enrolled, it will remove Enterprise applications, remove MDM policies, and disable CC mode.

4.5 Protection of the TSF

The TOE implements a number of features designed 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 is also designed to protect itself from modification by applications as well as to isolate 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 as all applications must have signatures (even if self-signed).

4.6 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 administrator-specified (using an MDM) advisory message (banner) when the user unlocks the TOE for the first use after reboot. The TOE is also able to attempt to connect to wireless networks as configured.

4.7 Trusted path/channels

The TOE supports the use of IEEE 802.11-2012, IEEE 802.1X, and EAP-TLS to secure communications channels between itself and other trusted network devices.

5 Assumptions and Clarification of Scope

The Security Problem Definition, including the assumptions, may be found in the Protection Profile For Mobile Device Fundamentals, Version 1.1, 12 February 2014 (MDFPP). That information has not been reproduced here; the MDFPP 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 MDFPP 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.

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:

1. 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 performed by the evaluation team).
2. 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.
3. 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.

6 Documentation

The following documentation was used as evidence for the evaluation of the LG G4 Smartphone:

- LG Electronics Inc. G4 Administrator Guidance, version 0.3, June 1, 2015

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

7 IT Product Testing

The detailed tests performed by the developer and the Evaluation Team were provided in proprietary format to the validation team in the Detailed Test Report for LG G4 Smartphone (MDFPP11), Version 0.2, June 1, 2015. The non-proprietary version of the testing evidence is included in the Assurance Activity Report for LG G4 Smartphone (MDFPP11) Version 0.2, July 1, 2015.

The following diagrams depict the test environments used by the evaluators.

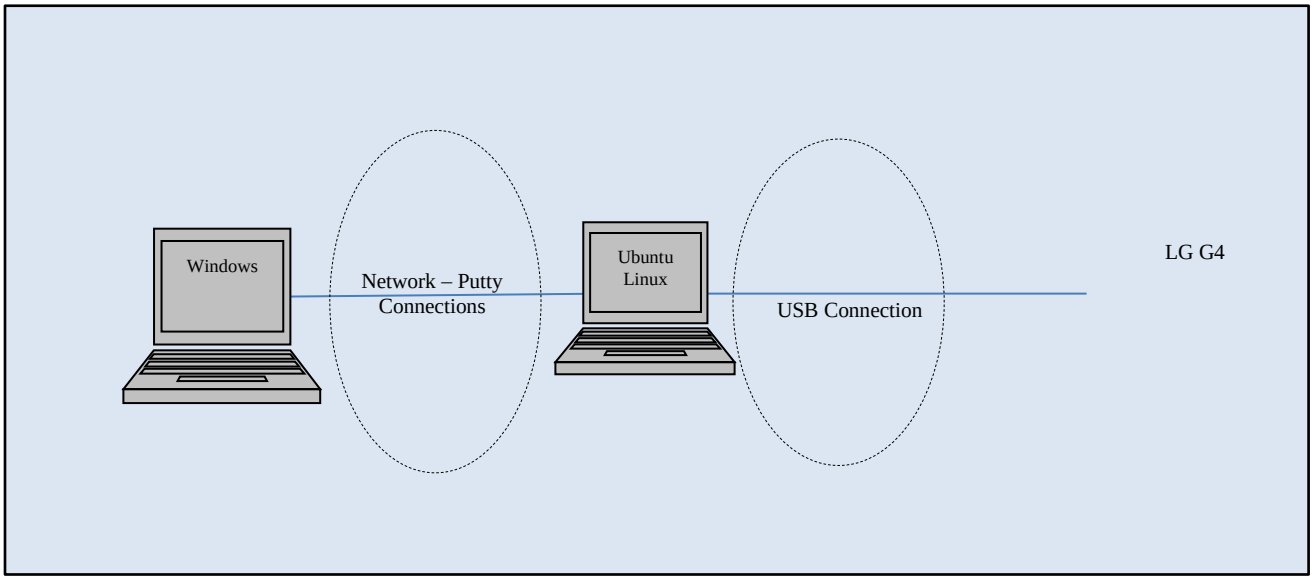

Figure 1 Developer Test Setup

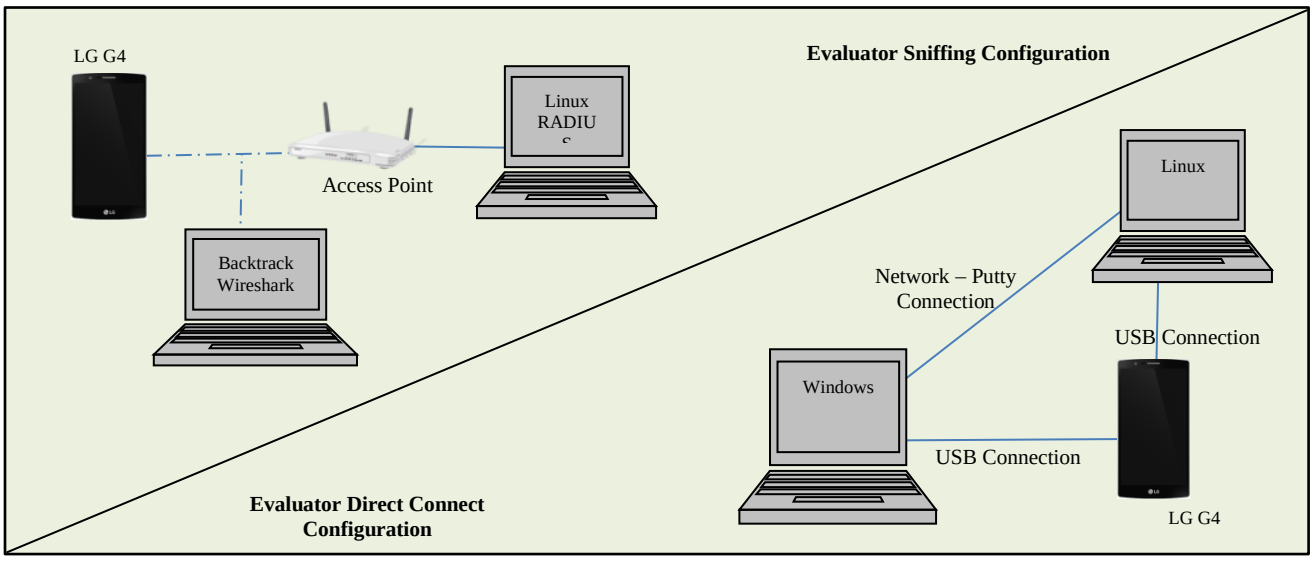

Figure 2 Evaluator Test Setup

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the LG Electronics Inc. G4 Administrator Guidance, version 0.3, June 1, 2015 document and ran the tests specified in the MDFPP.

8 Evaluated Configuration

The evaluated configuration consists of the LG G4 Smartphone devices.

To use the product in the evaluated configuration, the product must be configured as specified in LG Electronics Inc. G4 Administrator Guidance, version 0.3, June 1, 2015.

9 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 EAL1 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 Product Name TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 1).

9.1 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 LG G4 Smartphone product 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.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 1 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 MDFPP 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.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 1 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.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 1 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.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the MDFPP and recorded the results in a Test Report, summarized in the Assurance Activities Report.

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.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities. The search identified some general Android vulnerabilities which were addressed by the vendor prior to the completion of the evaluation.

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.

9.7 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.

10 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.

It should be noted that if a suitable Mobile Device Management tool for enterprise level configuration and control of the deployed devices is not available, the vendor provides a standalone application that can be used to place the devices into CC mode individually.

The evaluated product covers core functionality that is common to several carriers. Each carrier adapts the product for its infrastructure in a manner that does not impact the

evaluated functionality. The carrier specific versions of the evaluated product are released based upon that carrier's own schedule, so some carriers may not have released the evaluated version of the TOE by the time this report is published. Consumers should ensure that they have the evaluated version of the product software as it includes the vulnerability fixes as identified by the evaluation. The evaluated product version is: Security Software Version MDF v1.1, Release 4; Build number: LMY47D

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.

Shortly before the evaluation completed a new denial of service vulnerability was identified that applied to this and most other Android mobile devices with comparable functionality. The vendor will be addressing the issue as soon as Google pushes out a patch to the Android community. Users should follow their local polices for updates utilizing the trusted update feature of the evaluated product to apply patches.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as *LG Electronics Inc. G4 Smartphone (MDFPP11) Security Target, Version 1.4, May 27, 2015*.

13 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.

14 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 2102.

[4] Protection Profile for Mobile Device Fundamentals, Version 1.1, 12 February 2014.

[5] Assurance Activity Report for LG G4 Smartphone (MDFPP11) Version 0.2, July 1, 2015

[6] LG Electronics Inc. G4 Smartphone (MDFPP11) Security Target, Version 1.4, May 27, 2015