National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
LG Electronics Inc.
LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6)

Report Number:	**CCEVS-VR-10912-2018**
Dated:	**December 14, 2018**
Version:	**0.3**

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

John Butterworth
Michelle Carlson
Jenn Dotson
Stelios Melachrinoudis
The MITRE Corporation
McLean, VA

Kenneth Stutterheim
The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
Raymond Smoley
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 Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) 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 December 2018. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. Those reports are summarized in the publicly available Assurance Activity Report (AAR) for this evaluation. 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, Version 3.1, 16 June 2017 (MDFPP31) and the Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016 (WLANCEP10).

The Target of Evaluation (TOE) is the LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6). The 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 technical information included in this report was obtained from the LG Electronics Inc. LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) (MDFPP31/WLANCEP10) Security Target, version 0.6, November 26, 2018 and analysis performed by the Validation 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 Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) (Specific models identified in Section 3.1)
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 3.1, 16 June 2017 (MDFPP31) and the Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016 (WLANCEP10)
ST	LG Electronics Inc. LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) Security Target, version 0.6, November 26, 2018
Evaluation Technical Report	Evaluation Technical Report for LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6), version 0.3, December 3, 2018
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.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	John Butterworth, MITRE Corporation Michelle Carlson, MITRE Corporation Jenn Dotson, MITRE Corporation Stelios Melachrinoudis, MITRE Corporation Kenneth Stutterheim, The Aerospace 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 that can support both enterprises and individual users. Based upon Android 8.0 with 4.9, 4.4, and 3.18 Linux kernels in the ThinQ, V30, and G6 devices respectively, and improved by LG (for example, by adding NIST approved cryptographic algorithms, strengthening X.509 certificate checking, bolstering keystore protection, and applying security patches) to meet the MDFPP requirements, the TOE provides wireless connectivity and provides an execution environment for mobile applications.

The TOE allows basic telephony features (make and receive phone calls, send and receive SMS/MMS messages) as well as advanced network connectivity (allowing connections to both 802.11 Wi-Fi and 2G/3G/4G LTE mobile data networks). The TOE supports using client certificates to connect to access points offering WPA2 networks with 802.1x/EAP-TLS, or alternatively connecting to cellular base stations when utilizing mobile data.

The TOE offers mobile applications an Application Programming Interface (API) including those provided by the Android framework and through extensions to the Android DevicePolicyManager API by LG.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

Product	Carrier	Security SW Version	OS version	Build number	WFA Cert#
LG G7 ThinQ G710VM	Verizon	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76595
LG G7 ThinQ G710PM	Sprint	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76600
LG G7 ThinQ G710TM	T-Mobile	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76597
LG G7 ThinQ G710ULM	Open	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76840
LG V35 ThinQ V350AWM / LG	AT&T	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76799 WFA76601

Product	Carrier	Security SW Version	OS version	Build number	WFA Cert#
V35+ ThinQ V350AWA					
LG V35 ThinQ V350ULM	Open	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76841
LG V30 H931	AT&T	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72469
LG V30 VS996	Verizon	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72468
LG V30+ LS998U	Sprint	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72470
LG V30 H932	T-Mobile	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72471
LG V30 US998 LG V30+ US998U	Open, U.S. Cellular, LRA	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72472
LG G6 H871	AT&T	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69452
LG G6 VS988	Verizon	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69251
LG G6 LS993	Sprint	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69457
LG G6 H872	T-Mobile	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69454
LG G6 US997	Open, U.S. Cellular, LRA	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69455

During the evaluation, Gossamer utilized a Verizon model of each phone for all testing.

Furthermore, one must configure the TOE into its Common Criteria Mode in order to utilize the TOE in its evaluated configuration. As described in the Admin Guide, one must select the following options to configure the TOE into Common Criteria Mode:

1. Enable the password on the lock-screen (done by an MDM Agent or by the user through the UI)
2. Enable SD card encryption (via MDM Agent or UI)
3. Set CC mode (using an MDM API either through an MDM Agent or through the standalone app referenced in the Admin Guide)

Doing this ensures that the phone complies with the MDFPP requirements (for example restricting TLS/HTTPS ciphersuites, disallowing ‘Download Mode’, disabling ‘Smart Lock’, disallowing VPN split-tunneling).

Please refer to the Admin Guide for more details on how to accomplish the necessary configuration steps.

3.2 TOE Architecture

The TOE provides a rich API to mobile applications and provides users installing an application the option to either approve or reject an application based upon the API access that the application requires (or to grant applications access at runtime).

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 uses a key hierarchy that combines a REK with the user's password to provide 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 can interact with a Mobile Device Management system (not part of this evaluation) to allow enterprise control of the configuration and operation of the device so as to ensure adherence to enterprise-wide policies (for example, enabling CC mode, or restricting use of the device's camera, etc.).

The TOE includes several different levels of execution including (from lowest to highest) hardware, a Trusted Execution Environment, Android's Linux kernel, Android's user space, Android's Android Runtime (ART) environment for mobile applications, and the mobile applications themselves.

3.3 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 summaries 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 components (including its BoringSSL library, its Kernel Loadable Cryptographic module, and its Application Processor) with CAVP 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 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 controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE protects user and other sensitive data using encryption so that even if a device is physically lost, the data remains protected. The TOE supports Android for Work profiles to provide additional separation between application and application data belonging to the Android for Work profile. Please see the Admin Guide for additional details regarding how to set up and use Android for Work profiles.

4.3 Identification and authentication

The TOE supports features related to identification and authentication. From a user perspective, except for FCC mandated (making phone calls to an emergency number) or non-sensitive functions (e.g., choosing the keyboard input method or taking screen shots), a password (i.e., Password Authentication Factor) must be correctly entered to unlock the TOE. Also, even if 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. The frequency of password entry is limited and when a configured number of password entry 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. Password lengths up to 16 characters are supported.

The TOE can also serve as an IEEE 802.1X supplicant and can both use X.509v3 and validate certificates for EAP-TLS, TLS, and HTTPS exchanges.

4.4 Security management

The TOE provides the interfaces necessary to manage the security functions identified throughout the 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 others are restricted to administrators who may be operating through a Mobile Device Management solution if the TOE has been enrolled. Once the TOE has been enrolled and is then later un-enrolled, it will remove Enterprise applications, MDM policies, and disable CC mode.

4.5 Protection of the TSF

The TOE implements functions to ensure the reliability and integrity of its security features. It protects sensitive data such as cryptographic keys so that they are not accessible or exportable. It provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). The TOE 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 protects against modification by applications and will 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 self-tests fail, the TOE will not enter into its operational mode. It 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 functionality 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 either by the user or after a configured interval of inactivity thereby obscuring its display. The TOE also has the capability to display an administrator specified (using the TOE's MDM API) 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, 802.1X, and EAP-TLS to secure communications channels between itself and other trusted network devices.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile For Mobile Device Fundamentals, Version 3.1, 16 June 2017 and the Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016 (WLANCEP10)

That information has not been reproduced here and the MDFPP31/WLANCEP10 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 MDFPP31/WLANCEP10 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.

6 Clarification of Scope

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:

- 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 the Wireless Local Area Network Clients Extended Package and performed by the evaluation team).
- 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.
- 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.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the MDFPP31/WLANCEP10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.
- Android for Work functionality can be used to account for BYOD scenarios where personal data and Enterprise data are separated; however, it is not required for compliance to the PPs. Therefore, its use is out of scope and it has not been evaluated.

7 Documentation

The following documents were available with the TOE for evaluation:

- LG Electronics Inc. LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) Guidance Documentation, Version 0.2, October 12, 2018

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the LG Electronics Inc. LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) Guidance Documentation, Version 0.2, October 12, 2018. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report (MDFPP31/WLANCEP10) for LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6), Version 0.3, November 30, 2018 (DTR), as summarized in the evaluation Assurance Activity Report.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the MDFPP31/WLANCEP10 including the tests associated with optional requirements.

8.3 Test Environment

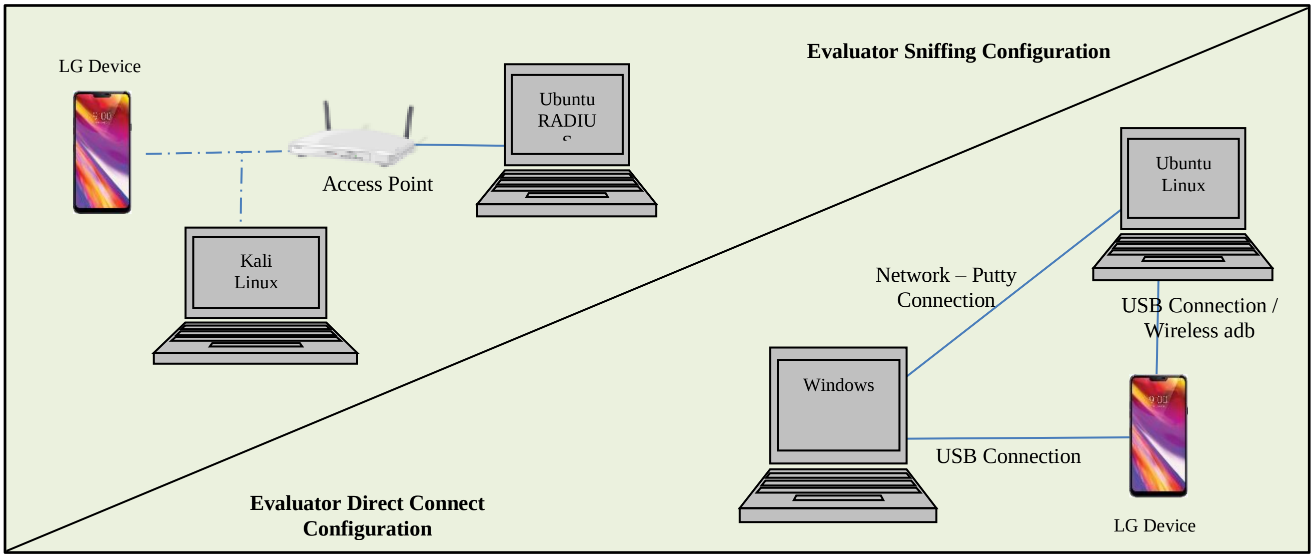

Figure 1 Evaluator Test Setup

8.4 Testing Tools

- Standard Windows utilities (e.g., notepad, snip tool)
- Putty version 2013-11-27:r10097
- HxD (Hexeditor) version 1.7.7.0
- LGUP version 1.15
- adb (Android Debug Bridge) version 1.0.31
- Wireshark version 2.6.1
- OpenSSL version 1.0.2g-fips
- freeradius version 3.0.15
- strongswan version 5.1.2.0
- micro-httpd
- tcpdump

- adb (Android Debug Bridge) version 1.0.39
- Evaluator developed test scripts
- Developer provided TOE device apps (*.apk files) and scripts (*.sh files) – the developer created a number of apps and scripts for the purpose of testing the TOE devices. *The scripts, complied apps, and app source files were provided to the evaluators. Each applicable app and script is identified in the context of relevant test cases – the scripts are included verbatim and the apps are described (based on evaluator use and examination of app sources).*
- airmon-ng
- Wireshark version 1.12.3
- Mobile Device Management app LGMDMClient7_1_16_debug.apk

9 Evaluated Configuration

The evaluated configuration consists of the following series and models:

Product	Carrier	Security SW Version	OS version	Build number	WFA Cert#
LG G7 ThinQ G710VM	Verizon	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76595
LG G7 ThinQ G710PM	Sprint	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76600
LG G7 ThinQ G710TM	T-Mobile	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76597
LG G7 ThinQ G710ULM	Open	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76840
LG V35 ThinQ V350AWM / LG V35+ ThinQ V350AWA	AT&T	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76799 WFA76601
LG V35 ThinQ V350ULM	Open	MDF v3.1 Release 3	Android 8.0	OPR1.170623.032	WFA76841
LG V30 H931	AT&T	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72469
LG V30 VS996	Verizon	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72468
LG V30+ LS998U	Sprint	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72470
LG V30 H932	T-Mobile	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72471
LG V30 US998 LG V30+ US998U	Open, U.S. Cellular, LRA	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA72472
LG G6 H871	AT&T	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69452
LG G6 VS988	Verizon	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69251
LG G6 LS993	Sprint	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69457
LG G6 H872	T-Mobile	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69454
LG G6 US997	Open, U.S.	MDF v3.1 Release 2.1	Android 8.0	OPR1.170623.032	WFA69455

Product	Carrier	Security SW Version	OS version	Build number	WFA Cert#
	Cellular, LRA				

10 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 assurance activities and 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 Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) TOE to be Part 2 extended, and to meet the SARs contained in the MDFPP31/WLANCEP10.

10.1 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 Android 8 device (G7 ThinQ, V35 ThinQ, V30, G6) products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each 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 evaluation team performed the assurance activities specified in the MDFPP31/WLANCEP10 related to the examination of the information contained in the TSS.

The validators 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.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each 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 validators 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.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators 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.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the MDFPP31/WLANCEP10 and recorded the results in a Test Report, summarized in the AAR.

The validators 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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and the Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 9/5/2018 using the following search terms:

"LG", "LGE", "Judy", "LG Judy", "LG V30", "V30", "BoringSSL", "Android", "Android 8", "Kernel Loadable Cryptographic Module", "Application Processor Cryptographic", "Kernel Loadable Cryptographic Module Algorithm", "Application Processor Cryptographic Algorithm", “LG Lucy”, “LG Joan”, “LG V30”, “LG G6” , “G6”, “V30”.

The validators 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.

10.7 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.

11 Validator Comments/Recommendations

The validators suggest that the consumer pay attention to the evaluated configuration of the appliances as the functionality that was evaluated was scoped exclusively to the security functional requirements specified in the Security Target. For example, although mentioned in the configuration guide and available on the devices, the LG VPN client was not part of this evaluation.

Additionally, the validators encourage the consumers of these products to understand the relationship between the products and any functionality that may be provided via Mobile Device Management solutions. This evaluation neither covers nor endorses the use of any particular MDM solution and only the MDM interfaces of the products were exercised as part of the evaluation.

As tested, the LG Android 8 devices utilized security software MDF v3.1 Release 3. No earlier or later versions of the software were tested, and hence their use would place the device outside the evaluated configuration. Mobile devices may come preloaded with software from both the vendor and carrier. That software was not evaluated and therefore no claims can be made as to their effectiveness nor to its correct operation.

In practice, the LG MDM is not available, though the TOE settings could be managed via a suitable MDM and corresponding agent. Alternatively, LG has developed a downloadable application that can be utilized to put the device into CC mode – MDM Test.apk. The LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) Guidance Documentation contains instructions on how the application can be acquired. As of the conclusion of this evaluation, an administrator can send an e-mail to support-enterprise-mobility@lge.com to request the application.

Over-The-Air (OTA) updates were not available during the evaluation; these are created by Google and the mobile device vendors, then distributed to the wireless carriers (Verizon, AT&T, etc.), for deployment to the respective devices via the carrier's network. Therefore, the OTA update functionality was not directly tested. The TOE, in its evaluated CC mode, prevents a user from installing a new software image via USB, as CC mode prevents the phone from entering its download mode during boot. Thus, in CC mode, the phone can only update via Firmware Over The Air (FOTA). The update can be made available by the carrier, but the administrator/enterprise administrator would still need to evaluate and approve the installation of the update.

The consumer should note that the LG G6 model supports Address Space Layout Randomization (ASLR) to applications but not ASLR to the kernel.

When FCS_CKM_EXT.5 was tested, the audit record for "Failure of the wipe" showed a date that was not within the timeframe of the evaluation. The lab confirmed that this information represents the date of the kernel and does not represent the current date that the audit record was generated.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *LG Electronics Inc. LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) (MDFPP31/WLANCEP10) Security Target, Version 0.6, November 26, 2018*.

14 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.

15 **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 2012.

[4] Protection Profile For Mobile Device Fundamentals, Version 3.1, 16 June 2017 and the Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016 (WLANCEP10).

[5] LG Electronics Inc. LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) (MDFPP31/WLANCEP10) Security Target, Version 0.6, November 26, 2018 (ST).

[6] Assurance Activity Report (MDFPP31/WLANCEP10) for LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6), Version 0.3, December 3, 2018 (AAR).

[7] Detailed Test Report (MDFPP31/WLANCEP10) for LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6), Version 0.3, November 30, 2018 (DTR).

[8] Evaluation Technical Report for LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6), Version 0.3, December 3, 2018 (ETR)

[9] LG Electronics Inc. LG Android 8 devices (G7 ThinQ, V35 ThinQ, V30, G6) Guidance Documentation, Version 0.2, October 12, 2018