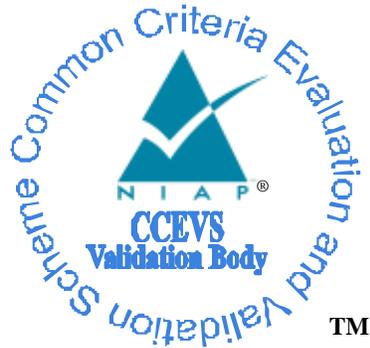


National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

LG Electronics Inc.

20 Yoido-dong, Youngdungpogu

Seoul 152-721, Korea

LG V20 and G5 Smartphones

Report Number: CCEVS-VR-10758-2016
Dated: November 10, 2016
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

Patrick Mallett, PhD
MITRE Corporation

Jerome Myers, PhD
Aerospace Corporation

Common Criteria Testing Laboratory

Jim Arnold
Tammy Compton
Cornelius Haley
Raymond Smoley
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1	Executive Summary	1
2	Identification	1
3	Architectural Information	3
3.1	TOE Evaluated Platforms	3
3.2	TOE Architecture.....	3
3.3	Physical Boundaries.....	4
4	Security Policy	4
4.1	Cryptographic support	4
4.2	User data protection	4
4.3	Identification and authentication.....	4
4.4	Security management.....	5
4.5	Protection of the TSF.....	5
4.6	TOE access.....	5
4.7	Trusted path/channels	6
5	Assumptions and Clarification of Scope.....	6
6	Documentation.....	6
7	IT Product Testing	6
7.1	Developer Testing.....	7
7.2	Evaluation Team Independent Testing	7
8	Evaluated Configuration	7
9	Results of the Evaluation	7
9.1	Evaluation of the Security Target (ASE).....	7
9.2	Evaluation of the Development (ADV).....	8
9.3	Evaluation of the Guidance Documents (AGD).....	8
9.4	Evaluation of the Life Cycle Support Activities (ALC).....	8
9.5	Evaluation of the Test Documentation and the Test Activity (ATE)	8
9.6	Vulnerability Assessment Activity (VAN).....	8
9.7	Summary of Evaluation Results.....	9
10	Validator Comments/Recommendations	9
11	Annexes.....	9
12	Security Target.....	9
13	Glossary	9
14	Bibliography	10

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of LG V20 and G5 Smartphones 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 November 2016. 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 EAL 1.

The Target of Evaluation (TOE) is the LG V20 and G5 Smartphones.

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 Common Criteria requirements for Evaluation Assurance Level (EAL) 1.

The technical information included in this report was obtained from the LG Electronics Inc. V20 and G5 Smartphones Security Target, version 0.4, October 26, 2016 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) for Evaluation Assurance Level (EAL) 1 through 4 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 V20 and G5 Smartphones (Specific models identified in Section 3.1)
Protection Profile	Protection Profile For Mobile Device Fundamentals, Version 2.0, 17 September 2014
ST	LG V20 and G5 Smartphones Security Target, version 0.4, October 26, 2016
Evaluation Technical Report	Evaluation Technical Report for LG V20 and G5 Smartphones, version 0.3, November 10, 2016
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	Patrick Mallett, MITRE Corporation Jerome Myers, 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 designed to support enterprises and individual users alike. Based upon Android 7.0 and improved by LG, the TOE provides wireless connectivity and provides an execution environment for mobile applications.

3.1 TOE Evaluated Platforms

The evaluated configuration for the V20 and G5 Smartphones comes in the following different carrier versions:

Product	Carrier	Security SW Version	OS version	Build number	WFA Cert#
LG V20 H910	AT&T	MDF v2.0 Release 4	Android 7.0	NRD90M	66750
LG V20 VS995	Verizon	MDF v2.0 Release 4	Android 7.0	NRD90M	66702
LG V20 LS997	Sprint	MDF v2.0 Release 4	Android 7.0	NRD90M	66752
LG V20 H918	T-Mobile	MDF v2.0 Release 4	Android 7.0	NRD90M	66773
LG V20 US996	Open	MDF v2.0 Release 4	Android 7.0	NRD90M	66771
LG G5 H820	AT&T	MDF v2.0 Release 4	Android 7.0	NRD90U	63786
LG G5 VS987	Verizon	MDF v2.0 Release 4	Android 7.0	NRD90U	63656
LG G5 LS992	Sprint	MDF v2.0 Release 4	Android 7.0	NRD90U	63797
LG G5 H830	T-Mobile	MDF v2.0 Release 4	Android 7.0	NRD90U	63768

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 TOE Architecture

The TOE provides a rich API to mobile applications and provides 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 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.

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 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 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 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. 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 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 16 characters are supported.

The TOE can also serve as an 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 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 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 802.11-2012, 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 2.0, 17 September 2014 (MDFPP20). That information has not been reproduced here; the MDFPP20 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 MDFPP20 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 documents were available with the TOE for evaluation:

- LG Electronics Inc. LG Android 7 devices (V20, G5) Guidance Documentation

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report (MDFPP20) for V20 and G5 Smartphones, version 0.3, November 9, 2016 (DTR).

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 a Common Criteria Certification document and ran the tests specified in the MDFPP20 including the tests associated with optional requirements.

8 Evaluated Configuration

The evaluated configuration consists of the following series and models:

Product	Carrier	Security SW Version	OS version	Build number	WFA Cert#
LG V20 H910	AT&T	MDF v2.0 Release 4	Android 7.0	NRD90M	66750
LG V20 VS995	Verizon	MDF v2.0 Release 4	Android 7.0	NRD90M	66702
LG V20 LS997	Sprint	MDF v2.0 Release 4	Android 7.0	NRD90M	66752
LG V20 H918	T-Mobile	MDF v2.0 Release 4	Android 7.0	NRD90M	66773
LG V20 US996	Open	MDF v2.0 Release 4	Android 7.0	NRD90M	66771
LG G5 H820	AT&T	MDF v2.0 Release 4	Android 7.0	NRD90U	63786
LG G5 VS987	Verizon	MDF v2.0 Release 4	Android 7.0	NRD90U	63656
LG G5 LS992	Sprint	MDF v2.0 Release 4	Android 7.0	NRD90U	63797
LG G5 H830	T-Mobile	MDF v2.0 Release 4	Android 7.0	NRD90U	63768

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 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 V20 and G5 Smartphone products 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 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 MDFPP20 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 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 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 ran the set of tests specified by the assurance activities in the MDFPP20 and recorded the results in a Test Report, summarized in the AAR.

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 performed a public search for vulnerabilities and did not discover any public issues with the TOE.

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

All of the validators observations are covered by the restrictions specified in the Clarification of Scope section of this report. The validators have no supplemental comments.”

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *LG V20 and G5 Smartphones (MDFPP20) Security Target, Version 0.4, October 26, 2016.*

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 2.0, 17 September 2014
- [5] LG V20 and G5 Smartphones (MDFPP20) Security Target, Version 0.4, October 26, 2016 (ST)
- [6] Assurance Activity Report (MDFPP20) for V20 and G5 Smartphones, Version 0.3, November 10, 2016 (AAR)
- [7] Detailed Test Report (MDFPP20) for V20 and G5 Smartphones, Version 0.2, November 9, 2016 (DTR)
- [8] Evaluation Technical Report for LG V20 and G5 Smartphones, Version 0.3, November 10, 2016 (ETR)