National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

™

Validation Report

Protection Profile for Mobile Device Fundamentals, Version 3.0, June 10, 2016

Report Number:	**CCEVS-VR-PP-0032**
Dated:	**24 May 2017**
Version:	**1.0**

ACKNOWLEDGEMENTS

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Security Requirements for Mobile Device Fundamentals (version 3.0) Protection Profile, also referred to as the Mobile Device Protection Profile (MDFPP30). It presents a summary of the MDFPP30 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the MDFPP30 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the LG Electronics Inc. G6 Smartphone. The evaluation was performed by the Gossamer Security Solutions Inc. Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in May 2017. This evaluation addressed the base requirements of the MDFPP30, as well as a few of the additional requirements contained in Appendices C and D.

Additional review of the PP to confirm that it meets the claimed APE assurance requirements was performed independently by the VR author as part of the completion of this VR.

The evaluation determined that the MDFPP v.3.0 is both Common Criteria Part 2 Extended and Part 3 Extended. The PP 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). Because the ST contains only material drawn directly from the MDFPP30, performance of the majority of the ASE work units serves to satisfy the APE work units as well.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the MDFPP30 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity report are consistent with the evidence produced.

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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the MDFPP30 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the G6 Smartphone, provided by LG Electronics Inc. The evaluation was performed by the Gossamer Security Solutions Inc. Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in May 2017.

The MDFPP30 contains a set of "base" requirements that all conformant STs must include, and in addition, contains "Optional," "Selection-based," and "Objective" requirements. Optional

requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based upon the selections made in the base requirements and the capabilities of the TOE. Objective requirements are those that that specify security functionality that is desirable but is not explicitly required by the PP. The vendor may choose to include such requirements in the ST and still claim conformance to this PP.

Because these discretionary requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the MDFPP30 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the MDFPP30.

Protection Profile	*Protection Profile for Mobile Device Fundamentals, Version 3.0, 17 June 2016*
ST (Base)	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target, Version 0.3, February 28, 2017
Assurance Activity Report (Base)	Assurance Activity Report (MDFPP30/WLANCEP10) for LG Electronics G6 Smartphone, Version 0.3, April 24, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Gossamer Security Solutions Inc., Catonsville, MD. USA
CCEVS Validators	Joanne Fitzpatrick, MITRE
	Stelios Melachrinoudis, MITRE
	Jean Petty, MITRE

3 MDFPP Description

The MDFPP30 specifies information security requirements for mobile devices for use in an enterprise and describes these essential security services provided by the mobile device that serves as a foundation for a secure mobile architecture. A mobile device in the context of this Protection Profile is a device which is composed of a hardware platform and its system software. The device typically provides wireless connectivity and may include software for functions like secure messaging, email, web, VPN connection, and VoIP (Voice over IP), for access to the protected enterprise network, enterprise data and applications, and for communicating with other mobile devices. Examples of a mobile device that should claim conformance to this Protection Profile include smartphones, tablet computers, and other mobile devices with similar capabilities.

Compliant TOEs will provide essential services, such as cryptographic services, data-at-rest protection, and key storage services to support the secure operation of applications on the

device and include functionality that addresses threats to the TOE and implements policies that are imposed by law or regulation. Additional security features such as security policy enforcement, application mandatory access control, anti-exploitation features, user authentication, and software integrity protection are implemented in order to address threats. It is expected that a typical deployment would also include either third-party or bundled components that provide:

● Data in transit protection (e.g. VPN Client, VoIP Client, Web Browser)
● Security policy management (e.g. MDM System)

The mobile device may be operated in a number of use cases. In addition to providing essential security services, the mobile device includes the necessary security functionality to support configurations for these various use cases. Each use case may require additional configuration and applications to achieve the desired security.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: Assumptions

Assumption Name	Assumption Definition
A.CONFIG	It is assumed that the TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.
A.NOTIFY	It is assumed that the mobile user will immediately notify the administrator if the Mobile Device is lost or stolen.
A.PRECAUTION	It is assumed that the mobile user exercises precautions to reduce the risk of loss or theft of the Mobile Device.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.EAVESDROP	If positioned on a wireless communications channel or elsewhere on the network, attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints.
T.NETWORK	An attacker may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints.
T.PHYSICAL	Loss of confidentiality of user data and credentials may be a result of an attacker gaining physical access to a Mobile Device.

Threat Name	Threat Definition
T.FLAWAPP	Malicious or exploitable code could be used knowingly or unknowingly by a developer, possibly resulting in the capability of attacks against the platform's system software.
T.PERSISTENT	An attacker gains and continues to have access the device, resulting it loss of integrity and possible control by both an adversary and legitimate owner.

4.3 Organizational Security Policies

No organizational policies have been identified that are specific to Mobile Devices.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 3: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.COMMS	The TOE will provide the capability to communicate using one (or more) standard protocols as a means to maintain the confidentiality of data that are transmitted outside of the TOE.
O.STORAGE	The TOE will provide the capability to encrypt all user and enterprise data and authentication keys to ensure the confidentiality of data that it stores.
O.CONFIG	The TOE will provide the capability to configure and apply security policies. This ensures the Mobile Device can protect user and enterprise data that it may store or process.
O.AUTH	The TOE will provide the capability to authenticate the user and endpoints of a trusted path to ensure they are communicating with an authorized entity with appropriate privileges.
O.INTEGRITY	The TOE will provide the capability to perform self-tests to ensure the integrity of critical functionality, software/firmware and data has been maintained. The TOE will also provide a means to verify the integrity of downloaded updates.
O.PRIVACY	The TOE will provide separation and privacy between user activities.

The following table contains objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

Environmental Security Obj.	TOE Security Objective Definition
OE.CONFIG	TOE administrators will configure the Mobile Device security functions correctly to create the intended security policy.
OE.NOTIFY	The Mobile User will immediately notify the administrator if the Mobile Device is lost or stolen.
OE.PRECAUTION	The Mobile User exercises precautions to reduce the risk of loss or theft of the Mobile Device.

5 Requirements

As indicated above, requirements in the MDFPP30 are comprised of the "base" requirements and additional requirements that are conditionally optional. The following are table contains the "base" requirements that were validated as part of the LG Electronics Inc. G6 Smartphone evaluation activity referenced above.

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FAU_STG.1: Audit Storage Protection	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FAU_STG.4: Prevention of Audit Data Loss	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
FCS: Cryptographic Support	FCS_CKM.1 Cryptographic Key Generation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_CKM.2(1): Cryptographic Key Establishment	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_CKM.2(2): Cryptographic Key Establishment (While Device Is Locked)	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_CKM_EXT.1: Extended: Cryptographic Key Support	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_CKM_EXT.2: Extended: Cryptographic Key Random Generation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_CKM_EXT.3: Extended: Cryptographic Key Generation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_CKM_EXT.4: Extended: Key Destruction	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_CKM_EXT.5: Extended: TSF Wipe	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_CKM_EXT.6: Extended: Salt Generation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_COP.1(1): Cryptographic Operation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_COP.1(2): Cryptographic Operation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
	FCS_COP.1(3): Cryptographic Operation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_COP.1(4): Cryptographic Operation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_COP.1(5): Cryptographic Operation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_HTTPS_EXT.1: Extended: HTTPS Protocol	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_IV_EXT.1: Extended: Initialization Vector Generation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_SRV_EXT.1: Extended: Cryptographic Algorithm Services	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_STG_EXT.1: Extended: Cryptographic Key Storage	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_STG_EXT.2: Extended: Encrypted Cryptographic Key Storage	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_STG_EXT.3: Extended: Integrity of Encrypted Key Storage	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FCS_TLSC_EXT.1: Extended: TLS Protocol	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
FDP: User Data Protection	FDP_ACF_EXT.1: Extended: Security Access Control	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FDP_DAR_EXT.1: Extended: Protected Data Encryption	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FDP_DAR_EXT.2: Extended: Sensitive Data Encryption	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FDP_IFC_EXT.1: Extended: Subset Information Flow Control	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FDP_STG_EXT.1: Extended: User Data Storage	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FDP_UPC_EXT.1: Extended: Inter-TSF User Data Transfer Protection	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_AFL_EXT.1: Authentication Failure Handling	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_BLT_EXT.1: Extended: Bluetooth User Authorization	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_BLT_EXT.2: Extended: Bluetooth Mutual Authentication	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_BLT_EXT.3: Extended: Rejection of Duplicate Bluetooth Connections	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_BLT_EXT.4: Extended: Secure Simple Pairing	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_PMG_EXT.1: Extended: Password Management	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_TRT_EXT.1: Extended: Authentication Throttling	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_UAU.5: Multiple Authentication Mechanisms	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_UAU.6(1): Re-Authentication	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_UAU.6(2): Re-Authentication	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_UAU.7: Protected Authentication Feedback	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_UAU_EXT.1: Extended: Authentication for Cryptographic Operation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_UAU_EXT.2: Extended: Timing of Authentication	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_X509_EXT.1: Extended: Validation of Certificates	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_X509_EXT.2: Extended: X509 Certificate Authentication	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_X509_EXT.3: Extended: Request Validation of Certificates	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
FMT: Security Management	FMT_MOF_EXT.1: Extended: Management of Security Functions Behavior	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
	FMT_SMF_EXT.1: Extended: Specification of Management Functions	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FMT_SMF_EXT.2: Extended: Specification of Remediation Actions	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
FPT: Protection of the TSF	FPT_AEX_EXT.1: Extended: Anti-Exploitation Services (ASLR)	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_AEX_EXT.2: Extended: Anti-Exploitation Services (Memory Page Permissions)	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_AEX_EXT.3: Extended: Anti-Exploitation Services (Overflow Protection)	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_AEX_EXT.4: Extended: Domain Isolation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_JTA_EXT.1: Extended: JTAG Disablement	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_KST_EXT.1: Extended: Key Storage	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_KST_EXT.2: Extended: No Key Transmission	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_KST_EXT.3: Extended: No Plaintext Key Export	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_NOT_EXT.1: Extended: Self-Test Notification	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_STM.1: Reliable Time Stamps	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_TST_EXT.1: Extended: TSF Cryptographic Functionality Testing	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_TST_EXT.2: Extended: TSF Integrity Checking	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_TUD_EXT.1: Extended: Trusted Update: TSF Version Query	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_TUD_EXT.2: Extended: TSF Update Verification	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
FTA: TOE Access	FTA_SSL_EXT.1: Extended: TSF- and User-Initiated Locked State	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
FTP: Trusted Path/Channels	FTP_ITC_EXT.1: Extended: Trusted Channel Communications	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

The following table contains the "**Optional**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_UAU_EXT.4: Secondary User Authentication	

The following table contains the "**Selection-Based**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM_EXT.1 [1.4]: Extended: Cryptographic Key Support (REK)	
	FCS_DTLS_EXT.1: Extended: DTLS Protocol	
	FCS_TLSC_EXT.1 [1.5]: Extended: TLS Protocol	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
FDP: User Data Protection	FDP_ACF_EXT.1 [1.4]: Extended: Security Access Control	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FDP_BCK_EXT.1 Extended: Application Backup	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FDP_PBA_EXT.1 Extended: Storage of Critical Biometric Parameters	
FIA: Identification and Authentication	FIA_BMG_EXT.1: Accuracy of Biometric Authentication	
FPT: Protection of the TSF	FPT_TST_EXT.2 [2.2]: Extended: TSF Integrity Testing	
	FPT_TUD_EXT.2 [2.6]: Extended: Trusted Update Verification	

The following table contains the "**Objective**" requirements contained in Appendix D, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are not currently mandated by the PP but

specify security functionality that is desirable, and are expected to transition from objective requirements to baseline requirements in future versions of the PP.

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_SAR.1: Audit Review	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FAU_SEL.1: Selective Audit	
FCS: Cryptographic Services	FCS_CKM_EXT.7: Extended: Bluetooth Key Generation	
	FCS_RBG_EXT.1 [1.4]: Extended: Cryptographic Operation (Random Bit Generation)	
	FCS_RBG_EXT.2: Extended: Cryptographic Operation (Random Bit Generation)	
	FCS_SRV_EXT.1 [1.2]: Extended: Cryptographic Algorithm Services	
	FCS_TLSC_EXT.1 [1.6, 1.7, 1.8]: Extended: TLS Client Protocol	
FDP: User Data Protection	FDP_ACF_EXT.1 [1.3]: Extended: Security Attribute Based Access Control	
	FDP_BLT_EXT.1: Extended: Limitation of Bluetooth Device Access	
FIA: Identification and Authentication	FIA_BLT_EXT.1 [1.2]: Extended: Bluetooth User Authorization	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FIA_BLT_EXT.5: Extended: Bluetooth Authentication – Secure Connections Only	
	FIA_BMG_EXT.2: Extended: Biometric Enrollment	
	FIA_BMG_EXT.3: Extended: Biometric Verification	
	FIA_BMG_EXT.4: Extended: Biometric Templates	
	FIA_BMG_EXT.5: Extended: Handling Unusual Biometric Templates	
	FIA_BMG_EXT.6: Extended: Spoof Detections for Biometrics	
	FIA_X509_EXT.2 [2.3, 2.4]: Extended: X509 Certificate Authentication	
	FIA_X509_EXT.4: Extended: X509 Certificate Enrollment	
FMT: Security Management	FMT_SMF_EXT.3: Extended: Current Administrator	
FPT: Protection of the TSF	FPT_AEX_EXT.1 [1.3, 1.4]: Extended: Anti-Exploitation Services (ASLR)	
	FPT_AEX_EXT.2 [2.2]: Extended: Anti-Exploitation Services (Memory Page Permissions)	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
	FPT_AEX_EXT.3 [3.2]: Extended: Anti-Exploitation Services (Overflow Protection)	
	FPT_BBD_EXT.1: Extended: Application Processor Mediation	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	FPT_BLT_EXT.1: Extended: Limitation of Bluetooth Profile Support	
	FPT_NOT_EXT.1 [1.2]: Extended: Self-Test Notification	
	FPT_TUD_EXT.2 [2.5, 2.7]: Extended: Trusted Update Verification	
FTA: TOE Access	FTA_TAB.1: Default TOE Access Banners	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
FTP: Trusted Path/Channels	FTP_BLT_EXT.1: Extended: Bluetooth Encryption	
	FTP_BLT_EXT.2: Extended: Bluetooth Encryption	

6 Assurance Requirements

The following are the assurance requirements contained in the MDFPP30:

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	ASE_ECD.1: Extended Components Definition	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	ASE_INT.1: ST Introduction	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	ASE_OBJ.1: Security Objectives for the Operational Environment	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	ASE_REQ.1: Stated Security Requirements	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	ASE_SPD.1: Security Problem Definition	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	ASE_TSS.1: TOE Summary Specification	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
ADV: Development	ADV_FSP.1 Basic Functional Specification	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

AGD: Guidance documents	AGD_OPE.1: Operational User Guidance	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	AGD_PRE.1: Preparative Procedures	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	ALC_CMS.1: TOE CM Coverage	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
	ALC_TSU_EXT: Timely Security Updates	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
ATE: Tests	ATE_IND.1: Independent Testing - Sample	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

7 Results of the evaluation

Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
APE_ECD.1	Pass	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
APE_INT.1	Pass	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
APE_OBJ.2	Pass	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target
APE_REQ.1	Pass	LG Electronics Inc. G6 Smartphone (MDFPP30/WLANCEP10) Security Target

8 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 as interpreted by the supplemental guidance in the MDFPP Assurance Activities to determine whether or not the claims made are justified.

- **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.

9   Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1]   Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 4, dated: September 2012.

[2]   Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 4, dated: September 2012.

[3]   Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 4, dated: September 2012.

[4]   Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 4, dated: September 2012.

[5]   Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6]   Gossamer Security Solutions, *Assurance Activity Report for G6 Smartphone*, Version 0.3, April 24, 2017.

[7]   Gossamer Security Solutions, *LG Electronics Inc. G6 Smartphone (MDFPP30) Security Target*, Version 0.3, February 28, 2017.

[8]   Protection Profile for Mobile Device Fundamentals, Version 3.0, 17 June 2016