National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Protection Profile for Mobile Device Fundamentals, Version 3.1, June 16, 2017

Report Number:	**CCEVS-VR-PP-0041**
Dated:	**16 November 2017**
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

Common Criteria Testing Laboratory

Gossamer Security Solutions, Inc.
Catonsville, Maryland

Table of Contents

Table of Tables

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 3.1) Protection Profile (PP), also referred to as the Mobile Device Protection Profile (MDFPP31). It presents a summary of the MDFPP31 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the MDFPP31 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.V30 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 November 2017. This evaluation addressed the base requirements of the MDFPP31, as well as a few of the additional requirements contained in Appendices B and C.

An additional review of the PP was performed independently by the Validation Report (VR) author as part of the completion of this VR, to confirm that it meets the claimed APE assurance requirements.

The evaluation determined that the MDFPP31 is both Common Criteria Part 2 Extended and Part 3 Extended. The PP identified in this VR has been evaluated at a NIAP approved CCTL 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). The ST contains material drawn directly from the MDFPP31 as well as the Extended Package for Wireless LAN Client Version 1.0. Evaluation of the ST materials that relate to MDFPP31 as part of completing 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 MDFPP31 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 (AAR) 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 CCTLs. CCTLs evaluate products against PPs that contain Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

To be thorough and efficient, the evaluation of the MDFPP31 was performed concurrent with the first product evaluation against the PP. The Target of Evaluation (TOE) was the V30 Smartphone, created by LG Electronics Inc. The evaluation was performed by the Gossamer Security Solutions Inc. CCTL in Catonsville, Maryland, United States of America, and was completed in November 2017.

The MDFPP31 contains a set of "base" requirements that all conformant STs must include, and additionally 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 MDFPP31 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 of the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP and subsequent evaluations that address additional optional requirements in the MDFPP31.

Protection Profile	*Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017*
ST (Base)	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target, Version 0.6, November 1, 2017
Assurance Activity Report (Base)	Assurance Activity Report (MDFPP31/WLANCEP10) for LG Electronics V30 Smartphone, Version 0.5, November 1, 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, The MITRE Corporation
	Stelios Melachrinoudis, The MITRE Corporation
	John Butterworth, The MITRE Corporation
	Kenneth Stutterheim, The Aerospace Corporation

3 MDFPP Description

The MDFPP31 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 PP 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 Voice over IP (VoIP), 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 PP 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	An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints.
T.NETWORK	An attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints in order to compromise the Mobile Device. These attacks include malicious software update of any applications or system software on the device. These attacks also include malicious web pages or email

Threat Name	Threat Definition
	attachments, which are usually delivered to devices over the network.
T.PHYSICAL	An attacker, with physical access, may attempt to access user data on the Mobile Device including credentials. These physical access threats may involve attacks, which attempt to access the device through external hardware ports, impersonate the user authentication mechanisms, through its user interface, and also through direct and possibly destructive access to its storage media. Note: Defending against device re-use after physical compromise is out of scope for this protection profile.
T.FLAWAPP	Applications loaded onto the Mobile Device may include malicious or exploitable code. This code could be included intentionally or unknowingly by the developer, perhaps as part of a software library. Malicious apps may attempt to exfiltrate data to which they have access. They may also conduct attacks against the platform's system software, which will provide them with additional privileges and the ability to conduct further malicious activities. Malicious applications may be able to control the device's sensors (GPS, camera, microphone) to gather intelligence about the user's surroundings even when those activities do not involve data resident or transmitted from the device. Flawed applications may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.
T.PERSISTENT	Persistent presence on a device by an attacker implies that the device has lost integrity and cannot regain it. The device has likely lost this integrity due to some other threat vector, yet the continued access by an attacker constitutes an on-going threat in itself. In this case, the device and its data may be controlled by an adversary as well as by its 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	To address the network eavesdropping (T.EAVESDROP) and network attack (T.NETWORK) threats, concerning wireless transmission of Enterprise and user data and configuration data between the TOE and remote network entities, conformant TOEs will use a trusted communication path. The TOE will be capable of communicating using one (or more) of these standard protocols: IPsec, DTLS, TLS, HTTPS, or Bluetooth. The protocols are specified by RFCs that offer a variety of implementation choices. Requirements have been imposed on some of these choices (particularly those for cryptographic primitives) to provide interoperability and resistance to cryptographic attack.

TOE Security Obj.	TOE Security Objective Definition
	While conformant TOEs must support all of the choices specified in the ST including any optional SFRs defined in this PP, they may support additional algorithms and protocols. If such additional mechanisms are not evaluated, guidance must be given to the administrator to make clear the fact that they were not evaluated.
O.STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of a Mobile Device (T.PHYSICAL), conformant TOEs will use data-at-rest protection. The TOE will be capable of encrypting data and keys stored on the device and will prevent unauthorized access to encrypted data.
O.CONFIG	To ensure a Mobile Device protects user and enterprise data that it may store or process, conformant TOEs will provide the capability to configure and apply security policies defined by the user and the Enterprise Administrator. If Enterprise security policies are configured these must be applied in precedence of user specified security policies.
O.AUTH	To address the issue of loss of confidentiality of user data in the event of loss of a Mobile Device (T.PHYSICAL), users are required to enter an authentication factor to the device prior to accessing protected functionality and data. Some non-sensitive functionality (e.g., emergency calling, text notification) can be accessed prior to entering the authentication factor. The device will automatically lock following a configured period of inactivity in an attempt to ensure authorization will be required in the event of the device being lost or stolen. Authentication of the endpoints of a trusted communication path is required for network access to ensure attacks are unable to establish unauthorized network connections to undermine the integrity of the device. Repeated attempts by a user to authorize to the TSF will be limited or throttled to enforce a delay between unsuccessful attempts.
O.INTEGRITY	To ensure the integrity of the Mobile Device is maintained conformant TOEs will perform self-tests to ensure the integrity of critical functionality, software/firmware and data has been maintained. The user shall be notified of any failure of these self-tests. This will protect against the threat T.PERSISTENT. To address the issue of an application containing malicious or flawed code (T.FLAWAPP), the integrity of downloaded updates to software/firmware will be verified prior to installation/execution of the object on the Mobile Device. In addition, the TOE will restrict applications to only have access to the system services and data they are permitted to interact with. The TOE will further protect against malicious applications from gaining access to data they are not authorized to access by randomizing the memory layout.
O.PRIVACY	In a BYOD environment, a personally-owned mobile device is used for both personal activities and enterprise data. Enterprise management solutions may have the technical capability to monitor and enforce security policies on the device. However, the

TOE Security Obj.	TOE Security Objective Definition
	privacy of the personal activities and data must be ensured. In addition, since there are limited controls that the enterprise can enforce on the personal side, separation of personal and enterprise data is needed. This will protect against the T.FLAWAPP and T.PERSISTENT threats.

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.

4.5 Requirements

As indicated above, requirements in the MDFPP31 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. V30 Smartphone evaluation activity referenced above.

Table 5: Base Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FAU_STG.1: Audit Storage Protection	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FAU_STG.4: Prevention of Audit Data Loss	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FCS: Cryptographic Support	FCS_CKM.1 Cryptographic Key Generation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_CKM.2(1): Cryptographic Key Establishment	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_CKM.2(2): Cryptographic Key Establishment (While Device Is Locked)	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_CKM_EXT.1: Cryptographic Key Support	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_CKM_EXT.2: Extended: Cryptographic Key Random Generation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
	FCS_CKM_EXT.3: Extended: Cryptographic Key Generation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_CKM_EXT.4: Key Destruction	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_CKM_EXT.5: TSF Wipe	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_CKM_EXT.6: Salt Generation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_COP.1(1): Cryptographic Operation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_COP.1(2): Cryptographic Operation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_COP.1(3): Cryptographic Operation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_COP.1(4): Cryptographic Operation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_COP.1(5): Cryptographic Operation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_HTTPS_EXT.1: HTTPS Protocol	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_IV_EXT.1: Extended: Initialization Vector Generation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_SRV_EXT.1: Cryptographic Algorithm Services	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_STG_EXT.1: Cryptographic Key Storage	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_STG_EXT.2: Encrypted Cryptographic Key Storage	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_STG_EXT.3: Integrity of Encrypted Key Storage	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FCS_TLSC_EXT.1: TLS Protocol	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
FDP: User Data Protection	FDP_ACF_EXT.1: Security Access Control	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FDP_DAR_EXT.1: Protected Data Encryption	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FDP_DAR_EXT.2: Sensitive Data Encryption	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FDP_IFC_EXT.1: Subset Information Flow Control	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FDP_STG_EXT.1: User Data Storage	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FDP_UPC_EXT.1: Inter-TSF User Data Transfer Protection	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FIA: Identification and Authentication	FIA_AFL_EXT.1: Authentication Failure Handling	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_BLT_EXT.1: Bluetooth User Authorization	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_BLT_EXT.2: Bluetooth Mutual Authentication	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_BLT_EXT.3: Extended: Rejection of Duplicate Bluetooth Connections	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_BLT_EXT.4: Secure Simple Pairing	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_PMG_EXT.1: Password Management	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_TRT_EXT.1: Authentication Throttling	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_UAU.5: Multiple Authentication Mechanisms	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_UAU.6: Re-Authentication	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_UAU.7: Protected Authentication Feedback	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_UAU_EXT.1: Authentication for Cryptographic Operation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
	FIA_UAU_EXT.2: Timing of Authentication	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_X509_EXT.1: Validation of Certificates	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_X509_EXT.2: X509 Certificate Authentication	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FIA_X509_EXT.3: Request Validation of Certificates	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FMT: Security Management	FMT_MOF_EXT.1: Management of Security Functions Behavior	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FMT_SMF_EXT.1: Specification of Management Functions	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FMT_SMF_EXT.2: Specification of Remediation Actions	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FPT: Protection of the TSF	FPT_AEX_EXT.1: Anti-Exploitation Services (ASLR)	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_AEX_EXT.2: Anti-Exploitation Services (Memory Page Permissions)	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_AEX_EXT.3: Anti-Exploitation Services (Overflow Protection)	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_AEX_EXT.4: Domain Isolation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_JTA_EXT.1: JTAG Disablement	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_KST_EXT.1: Key Storage	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_KST_EXT.2: No Key Transmission	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_KST_EXT.3: No Plaintext Key Export	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_NOT_EXT.1: Self-Test Notification	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_STM.1: Reliable Time Stamps	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
	FPT_TST_EXT.1: TSF Cryptographic Functionality Testing	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_TST_EXT.2(1): TSF Integrity Checking	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_TUD_EXT.1: Trusted Update: TSF Version Query	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_TUD_EXT.2: TSF Update Verification	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FTA: TOE Access	FTA_SSL_EXT.1: TSF- and User-Initiated Locked State	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FTP: Trusted Path/Channels	FTP_ITC_EXT.1: Trusted Channel Communications	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target

The following table contains the "**Optional**" requirements contained in Appendix A, 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.

Table 6: Optional Requirements

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

The following table contains the "**Selection-Based**" 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.

Table 7: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_CKM_EXT.7: Cryptographic Key Support (REK)	PP Evaluation
	FCS_DTLS_EXT.1: DTLS Protocol	PP Evaluation
	FCS_TLSC_EXT.2: TLS Protocol	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FDP: User Data Protection	FDP_ACF_EXT.2: Security Access Control	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FDP_PBA_EXT.1: Storage of Critical Biometric Parameters	PP Evaluation

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_BMG_EXT.1: Accuracy of Biometric Authentication	PP Evaluation
FPT: Protection of the TSF	FPT_TST_EXT.3 TSF Integrity Testing	PP Evaluation
	FPT_TUD_EXT.3 Trusted Update Verification	PP Evaluation

The following table contains the "**Objective**" 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 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.

Table 8: Objective Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_SAR.1: Audit Review	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	FAU_SEL.1: Selective Audit	PP Evaluation
FCS: Cryptographic Services	FCS_CKM_EXT.8: Bluetooth Key Generation	PP Evaluation
	FCS_RBG_EXT.2 Cryptographic Operation (Random Bit Generation)	PP Evaluation
	FCS_RBG_EXT.3: Cryptographic Operation (Random Bit Generation)	PP Evaluation
	FCS_SRV_EXT.2 Cryptographic Algorithm Services	PP Evaluation
	FCS_TLSC_EXT.3: TLS Client Protocol	PP Evaluation
FDP: User Data Protection	FDP_ACF_EXT.3: Security Attribute Based Access Control	PP Evaluation
	FDP_BLT_EXT.1: Limitation of Bluetooth Device Access	PP Evaluation
	FDP_BCK_EXT.1: Application Backup	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FIA: Identification and Authentication	FIA_BLT_EXT.5: Bluetooth Authentication – Secure Connections Only	PP Evaluation
	FIA_BLT_EXT.6: Bluetooth User Authorization	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	FIA_BMG_EXT.2: Biometric Enrollment	PP Evaluation
	FIA_BMG_EXT.3: Biometric Verification	PP Evaluation
	FIA_BMG_EXT.4: Biometric Templates	PP Evaluation
	FIA_BMG_EXT.5: Handling Unusual Biometric Templates	PP Evaluation
	FIA_BMG_EXT.6: Spoof Detections for Biometrics	PP Evaluation
	FIA_X509_EXT.4: X509 Certificate Enrollment	PP Evaluation
	FIA_X509_EXT.5: X509 Certificate Enrollment	PP Evaluation
FMT: Security Management	FMT_SMF_EXT.3: Current Administrator	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
FPT: Protection of the TSF	FPT_AEX_EXT.5: Anti-Exploitation Services (ASLR)	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	FPT_AEX_EXT.6: Anti-Exploitation Services (Memory Page Permissions)	PP Evaluation
	FPT_AEX_EXT.7: Anti-Exploitation Services (Overflow Protection)	PP Evaluation
	FPT_BBD_EXT.1: Application Processor Mediation	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
	FPT_BLT_EXT.1: Limitation of Bluetooth Profile Support	PP Evaluation
	FPT_NOT_EXT.2: Self-Test Notification	PP Evaluation
	FPT_TST_EXT.2(2): TSF Integrity Checking	PP Evaluation
	FPT_TUD_EXT.4: Trusted Update Verification	PP Evaluation
FTA: TOE Access	FTA_TAB.1: Default TOE Access Banners	LG Electronics Inc. V30 Smartphone (MDFPP31/ WLANCEP10) Security Target
FTP: Trusted Path/Channels	FTP_BLT_EXT.1: Bluetooth Encryption	PP Evaluation
	FTP_BLT_EXT.2: Bluetooth Encryption	PP Evaluation

5 Assurance Requirements

The following are the assurance requirements contained in the MDFPP31:

Table 9: Assurance Requirements

Requirement Class	Requirement Component	Verified By
ASE: Security Target	ASE_CCL.1: Conformance Claims	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	ASE_ECD.1: Extended Components Definition	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	ASE_INT.1: ST Introduction	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	ASE_OBJ.1: Security Objectives for the Operational Environment	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	ASE_REQ.1: Stated Security Requirements	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	ASE_SPD.1: Security Problem Definition	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	ASE_TSS.1: TOE Summary Specification	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
ADV: Development	ADV_FSP.1 Basic Functional Specification	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target

Requirement Class	Requirement Component	Verified By
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	AGD_PRE.1: Preparative Procedures	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	ALC_CMS.1: TOE CM Coverage	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
	ALC_TSU_EXT: Timely Security Updates	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
ATE: Tests	ATE_IND.1: Independent Testing - Sample	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target

6 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.

Table 10: Evaluation Results

APE Requirement	Evaluation Verdict	Verified By
APE_CCL.1	Pass	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
APE_ECD.1	Pass	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
APE_INT.1	Pass	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
APE_OBJ.2	Pass	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target
APE_REQ.1	Pass	LG Electronics Inc. V30 Smartphone (MDFPP31/WLANCEP10) Security Target

7 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.

8 Bibliography

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

[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 V30 Smartphone*, Version 0.5, November 1, 2017.

[7] Gossamer Security Solutions, *LG Electronics Inc. V30 Smartphone (MDFPP31) Security Target*, Version 0.6, November 1, 2017.

[9] Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017