# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme



TM

# Validation Report

# Protection Profile for Mobile Device Fundamentals, Version 2.0, September 17th, 2014

## ACKNOWLEDGEMENTS

### <u>Common Criteria Testing Laboratory</u>

# 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 2.0) Protection Profile, also referred to as the Mobile Device Protection Profile (MDFPP20).  It presents a summary of the MDFPP20 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the MDFPP20 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 Boeing Black.   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 February 2015. This evaluation addressed the base requirements of the MDFPP20, as well as a few of the additional requirements contained in Appendices C and D.

The information in this report is largely derived from Evaluation Technical Report (ETR), written by the Gossamer Security Solutions CCTL. 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.2.0 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 MDFPP20, performance of the majority of the ASE work units serves to satisfy the APE work units as well.  Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

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 MDFPP20 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the evaluation technical 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 MDFPP20 was performed concurrent with the first product evaluation against the PP.  In this case the TOE for this first product was the Boeing Black, provided by The Boeing Company.  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 February 2015.

The MDFPP20 contains a set of "base" requirements that all conformant STs must include, and in addition, contains both "Selection-based" and "Objective" requirements. 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 optional 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 MDFPP20 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 MDFPP20.

| | |
|---|---|
| **Protection Profile** | *Protection Profile for Mobile Device Fundamentals, Version 2.0, 17 September 2015* |
| **ST (Base)** | The Boeing Company Boeing Black (MDFPP20) Security Target, Version 1.1, March 2, 2015 |
| **Evaluation Technical Report (Base)** | Evaluation Technical Report (MDFPP20) For Boeing Black, Version 0.3, February 20, 2015 |
| **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** | Kenneth Elliott, The Aerospace Corporation |
| | Dr. Jerome Myers, The Aerospace Corporation |
| | Ken Stutterheim, The Aerospace Corporation |
| | Stelios Melachrinoudis, MITRE Corporation |

# 3  MDFPP Description

The MDFPP20 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: TOE 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 |
|---|---|

| 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. |
| 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. |

The following table contains objectives for the Operational Environment.

**Table 4: Security Objectives for the Operational Environment**

| Environmental Security Obj. | TOE Security Objective Definition |
|---|---|

| 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 MDFPP20 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 Boeing evaluation activity referenced above.

| Requirement Class | Requirement Component |
|---|---|
| **FCS: Cryptographic Support** | FCS_CKM.1(1): Cryptographic Key Generation |
| | FCS_CKM.1(2): Cryptographic Key Generation |
| | FCS_CKM.2(1): Cryptographic Key Establishment |
| | FCS_CKM.2(2): Cryptographic Key Distribution |
| | FCS_CKM_EXT.1: Extended: Cryptographic Key Support |
| | FCS_CKM_EXT.2: Extended: Cryptographic Key Random Generation |
| | FCS_CKM_EXT.3: Extended Cryptographic Key Distribution |
| | FCS_CKM_EXT.4: Extended: Key Destruction |
| | FCS_CKM_EXT.5: Extended: TSF Wipe |
| | FCS_CKM_EXT.6: Extended: Salt Generation |
| | FCS_COP.1(1): Cryptographic Operation |
| | FCS_COP.1(2): Cryptographic Operation |
| | FCS_COP.1(3): Cryptographic Operation |
| | FCS_COP.1(4): Cryptographic Operation |
| | FCS_COP.1(5): Cryptographic Operation |
| | FCS_HTTPS_EXT.1: Extended: HTTPS Protocol |
| | FCS_IV_EXT.1: Extended: Initialization Vector Generation |
| | FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation) |
| | FCS_SRV_EXT.1: Extended: Cryptographic Algorithm Services |
| | FCS_STG_EXT.1: Extended: Cryptographic Key Storage |
| | FCS_STG_EXT.2: Extended: Encrypted Cryptographic Key Storage |
| | FCS_STG_EXT.3: Extended: Integrity of Encrypted Key Storage |
| | FCS_TLSC_EXT.1: Extended: EAP TLS Protocol |
| | FCS_TLSC_EXT.2: Extended: TLS Protocol |
| **FDP: User Data Protection** | FDP_ACF_EXT.1: Extended: Security Access Control |
| | FDP_DAR_EXT.1: Extended: Data-At-Rest Protection |
| | FDP_IFC_EXT.1: Extended: Protected Data Encryption |
| | FDP_STG_EXT.1: Extended: User Data Storage |
| | FDP_UPC_EXT.1: Extended: Inter-TSF User Data Transfer Protection |
| **FIA: Identification and Authentication** | FIA_AFL_EXT.1: Extended: Authentication Failure Handling |
| | FIA_BLT_EXT.1: Extended: Bluetooth User Authorization |
| | FIA_PAE_EXT.1: Extended: PAE Authentication |

| Requirement Class | Requirement Component |
|---|---|
| | FIA_PMG_EXT.1: Extended: Password Management |
| | FIA_TRT_EXT.1: Extended: Authentication Throttling |
| | FIA_UAU.7: Protected Authentication Feedback |
| | FIA_UAU_EXT.1: Extended: Authentication for Cryptographic Operation |
| | FIA_UAU_EXT.2: Extended: Timing of Authentication |
| | FIA_UAU_EXT.3: Extended: Re-Authentication |
| | FIA_X509_EXT.1: Extended: Validation of Certificates |
| | FIA_X509_EXT.2: Extended: X509 Certificate Authentication |
| | FIA_X509_EXT.3: Extended: Request Validation of Certificates |
| **FMT: Security Management** | FMT_MOF_EXT.1: Extended: Management of Security Functions Behavior |
| | FMT_SMF_EXT.1: Extended: Specification of Management Functions |
| | FMT_SMF_EXT.2: Extended: Specification of Remediation Actions |
| **FPT: Protection of the TSF** | FPT_AEX_EXT.1: Extended: Anti-Exploitation Services (ASLR) |
| | FPT_AEX_EXT.2: Extended: Anti-Exploitation Services (Memory Page Permissions) |
| | FPT_AEX_EXT.3: Extended: Anti-Exploitation Services (Stack Overflow Protection) |
| | FPT_AEX_EXT.4: Extended: Domain Isolation |
| | FPT_KST_EXT.1: Extended: Key Storage |
| | FPT_KST_EXT.2: Extended: No Key Transmission |
| | FPT_KST_EXT.3: Extended: No Plaintext Key Export |
| | FPT_NOT_EXT.1: Extended: Self-Test Notification |
| | FPT_STM.1:: Reliable Time Stamps |
| | FPT_TST_EXT.1: Extended: TSF Cryptographic Functionality Testing |
| | FPT_TST_EXT.2: Extended: TSF Integrity Testing |
| | FPT_TUD_EXT.1: Extended: Trusted Update: TSF Version Query |
| | FPT_TUD_EXT.2: Extended: Trusted Update Verification |
| **FTA: TOE Access** | FTA_SSL_EXT.1: Extended: TSF- and User Initiated Locked State |
| | FTA_WSE_EXT.1: Extended: Wireless Network Access |
| **FTP: Trusted Path/Channels** | FTP_ITC_EXT.1: Extended: Trusted Channel Communication |

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 | |
| | FCS_DTLS_EXT.1: Extended: DTLS Protocol | |
| | FCS_TLSC_EXT.1 [1.5]: Extended: EAP-TLS Protocol | |
| | FCS_TLSC_EXT.2 [2.5]: Extended: TLS | |

| Requirement Class | Requirement Component | Verified By |
|---|---|---|
| | Protocol | |
| 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_GEN.1: Audit Data Generation | |
| | FAU_SAR.1: Audit Review | |
| | FAU_SEL.1: Selective Audit | |
| | FAU_STG.1: Audit Storage Protection | |
| | FAU_STG.4: Prevention of Audit Data Loss | |
| FCS: Cryptographic Services | FCS_CKM.1(3): Cryptographic Key Generation | |
| | FCS_CKM_EXT.7: Extended: Bluetooth Key Generation | |
| | FCS_RBG_EXT.1 [1.4, 1.5]: Extended: Cryptographic Operation (Random Bit Generation) | |
| | FCS_SRV_EXT.1 [1.2]: Extended: Cryptographic Algorithm Services | |
| | FCS_TLSC_EXT.1 [1.6-1.8]: Extended: EAP-TLS Protocol | |
| | FCS_TLSC_EXT.2 [2.6-2.8]: Extended: TLS 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 | |
| | FDP_DAR_EXT.2: Extended: Sensitive Data Encryption | |
| FIA: Identification and Authentication | FIA_BLT_EXT.1 [1.2]: Extended: Bluetooth User Authorization | |
| | FIA_BLT_EXT.2: Extended: Bluetooth Authentication | |
| | FIA_X509_EXT.2 [2.3, 2.4]: Extended: X509 Certificate Authentication | |
| | FIA_X509_EXT.4: Extended: X509 Certificate Enrollment | |
| FPT: Protection of the | FPT_AEX_EXT.1 [1.3, 1.4]: Extended: | |

| Requirement Class | Requirement Component | Verified By |
|---|---|---|
| **TSF** | Anti-Exploitation Services (ASLR) | |
| | FPT_AEX_EXT.2 [2.2]: Extended: Anti-Exploitation Services (Memory Page Permissions) | |
| | FPT_AEX_EXT.3 [3.2]: Extended: Anti-Exploitation Services (Overflow Protection) | |
| | FPT_BBD_EXT.1: Extended: Application Processor Mediation | Boeing Black, February 2015 |
| | FPT_BLT_EXT.1: Extended: Limitation of Bluetooth Profile Support | |
| | FPT_NOT_EXT.1 [1.2, 1.3]: 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 | Boeing Black, February 2015 |

# 6 Assurance Requirements

The following are the assurance requirements contained in the MDFPP20:

| Requirement Class | Requirement Component |
|---|---|
| **ASE: Security Target** | ASE_CCL.1: Conformance Claims |
| | ASE_ECD.1: Extended Components Definition |
| | ASE_INT.1: ST Introduction |
| | ASE_OBJ.1: Security Objectives for the Operational Environment |
| | ASE_REQ.1: Stated Security Requirements |
| | ASE_SPD.1: Security Problem Definition |
| | ASE_TSS.1: TOE Summary Specification |
| **ADV: Development** | ADV_FSP.1 Basic Functional Specification |
| **AGD: Guidance documents** | AGD_OPE.1: Operational User Guidance |
| | AGD_PRE.1: Preparative Procedures |
| **ALC: Life-cycle support** | ALC_CMC.1: Labeling of the TOE |
| | ALC_CMS.1: TOE CM Coverage |
| | ALC_TSU_EXT: Timely Security Updates |
| **ATE: Tests** | ATE_IND.1: Independent Testing - Sample |
| **AVA: Vulnerability Assessment** | AVA_VAN.1: Vulnerability Survey |

# 7 Results of the evaluation

The CCTL produced an ETR that contained the following results. 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 |
|---|---|

| APE_CCL.1 | Pass |
|---|---|
| APE_ECD.1 | Pass |
| APE_INT.1 | Pass |
| APE_OBJ.2 | Pass |
| APE_REQ.1 | Pass |

# 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 2, dated: September 2007.

[2]	Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3]     Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4]     Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[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. *Evaluation Technical Report (MDFPP20) For Boeing Black,* Version 0.3, February 20, 2015.

[7]     Gossamer Security Solutions. *The Boeing Company Boeing Black (MDFPP20) Security Target*, Version 1.1. March 2, 2015.

[8]     Protection Profile for Mobile Device Fundamentals, Version 2.0, 17 September 2014.