National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients

Version 1.0

2022-10-11

Report Number:	**CCEVS-VR-PP-0098**
Dated:	**November 8, 2024**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGMENTS

<u>Common Criteria Testing Laboratory</u>

Base and Additional Requirements

Gossamer Security Solutions
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients, Version 1.0 (CFG_MDF-BT-WLANC_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Protection Profile for Mobile Device Fundamentals, Version 3.3 (PP_MDF_V3.3) Base-PP, PP-Module for Bluetooth, Version 1.0 (MOD_BT_V1.0), and PP-Module for WLAN Clients, Version 1.0 (MOD_WLANC_V1.0). It presents a summary of the CFG_MDF-BT-WLANC_V1.0 and the evaluation results.

Gossamer Security Solutions, located in Columbia, Maryland, performed the evaluation of the CFG_MDF-BT-WLANC_V1.0 and the PP_MDF_V3.3 Base-PP, MOD_BT_V1.0, and MOD_WLANC_V1.0 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was the Zebra Devices on Android 13 (Zebra Android 13).

This evaluation addressed the base security functional requirements of PP_MDF_V3.3 Base-PP, MOD_BT_V1.0, and MOD_WLANC_V1.0 as part of CFG_MDF-BT-WLANC_V1.0. The PP-Modules define additional requirements, some of which the Zebra Android 13 evaluation claimed. The Validation Report (VR) author independently performed an additional review of the PP-Configuration, Base PP, and PP-Modules as part of the completion of this VR, to confirm they meet the claimed APE and ACE requirements.

The evaluation determined the CFG_MDF-BT-WLANC_V1.0 is both Common Criteria Part 2 Extended and Part 3 Extended. An accredited Information Technology Security Evaluation Facility (ITSEF) evaluated the PP-Configuration, Base-PP, and PP-Modules identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Revision 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 5). The Security Target (ST) includes material from the PP_MDF_V3.3, MOD_BT_V1.0, and MOD_WLANC_V1.0; completion of the ASE workunits satisfied the APE workunits for PP_MDF_V3.3 and the ACE workunits for the PP-Modules, but only for the materials defined in the PP-Modules, and only when the PP-Modules are in the defined PP-Configuration.

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

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 Profiles (PPs) and PP-Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 workunits specific to the technology described by the PP or PP-Modules. Products may only be evaluated against PP-Modules when a PP-Configuration is defined to include the PP-Modules with at least one corresponding Base-PP.

To promote thoroughness and efficiency, the evaluation of the CFG_MDF-BT-WLANC_V1.0, PP_MDF_V3.3, MOD_BT_V1.0, and MOD_WLANC_V1.0, was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Zebra Android 13, performed by Gossamer Security Solutions in Columbia, MD.

This evaluation addressed the base security functional requirements of PP_MDF_V3.3, MOD_BT_V1.0, and MOD_WLANC_V1.0 as part of CFG_MDF-BT-WLANC_V1.0. The PP-Modules define additional requirements, some of which the Zebra Android 13 evaluation claimed.

PP_MDF_V3.3, MOD_BT_V1.0, and MOD_WLANC_V1.0 contain a set of base requirements that all conformant STs must include, and additionally contain optional, objective, implementation-based, and selection-based requirements. Optional requirements are those that may be claimed or omitted at the product vendor’s discretion. Objective requirements are not currently prescribed by these PP-Modules but are expected to be included in future versions of the PP-Modules. Vendors planning to have evaluations performed against future products are encouraged to plan for these objective requirements to be met. Implementation-based requirements are those that are dependent on the TOE implementing a particular function. Selection-based requirements are those that must be included based upon the selections made in other requirements and the abilities of the TOE.

The VR author evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ workunits performed against the PP-Modules. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the CFG_MDF-BT-WLANC_V1.0 were evaluated.

The following identifies the PP-Modules in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against these PP-Modules.

PP-Configuration	PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients, Version 1.0, 2022-10-11
Base-PP	Protection Profile for Mobile Device Fundamentals, Version 3.3, 2022-09-12 (PP_MDF_V3.3)
Modules in PP-Configuration	PP-Module for Bluetooth, Version 1.0, 2021-04-15 (MOD_BT_V1.0) PP-Module for WLAN Clients, Version 1.0, 2022-03-31 (MOD_WLANC_V1.0)
ST (Base)	Zebra Devices on Android 13 Security Target, Version 0.4, 07/26/2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Gossamer Security Solutions Columbia, MD

3 CFG_MDF-BT-WLANC_V1.0 Description

CFG_MDF-BT-WLANC_V1.0 is a PP-Configuration that combines the following.

- Protection Profile for Mobile Device Fundamentals, Version 3.3 (PP_MDF_V3.3)
- PP-Module for Bluetooth, Version 1.0 (MOD_BT_V1.0)
- PP-Module for WLAN Clients, Version 1.0 (MOD_WLANC_V1.0)

This PP-Configuration is for a mobile device that includes Bluetooth and WLAN client abilities according to the requirements of the PP-Configuration.

A Bluetooth device is a communications standard for short-range wireless transmissions, which is implemented in many commercial devices. It is a logical component that executes on an end-user personal computing or mobile device. In the context of CFG_MDF-BT-WLANC_V1.0, a Bluetooth device relies on an operational environment for its execution domain and proper usage.

A WLAN client is a component executing on a device that allows for 802.11 network connectivity. In the context of CFG_MDF-BT-WLANC_V1.0, the mobile device includes the hardware and software needed to function as a WLAN client.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_MDF-BT-WLANC_V1.0.

Table 1: Assumptions

Assumption Name	**Assumption Definition**
From PP_MDF_V3.3	
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.
A.PROPER_USER	Mobile Device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.
From MOD_BT_V1.0	
No additional assumptions defined in MOD_BT_V1.0.	
From MOD_WLANC_V1.0	
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_MDF-BT-WLANC_V1.0.

Table 2: Threats

Threat Name	**Threat Definition**
From PP_MDF_V3.3	
T.MALICIOUS_APP	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.NETWORK_ATTACK	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

Threat Name	Threat Definition
	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 attachments, which are usually delivered to devices over the network.
T.NETWORK_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.PERSISTENT_PRESENCE	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.
T.PHYSICAL_ACCESS	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.
From MOD_BT_V1.0	
This PP-Module defines no additional threats beyond those defined in the base PPs. Note however that the SFRs defined in this PP-Module will assist in the mitigation of T.NETWORK_EAVESDROP and T.NETWORK_ATTACK in the Base-PP. Note: While the Bluetooth functionality does not introduce new threats, it does introduce new ways to exploit existing threats.	
From MOD_WLANC_V1.0	
T.TSF_FAILURE	Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_MDF-BT-WLANC_V1.0.

Table 3: Organizational Security Policies

OSP Name	**OSP Definition**
From PP_MDF_V3.3	
No OSPs defined in PP_MDF_V3.3.	
From MOD_BT_V1.0	
No OSPs defined in MOD_BT_V1.0.	
From MOD_VPNC_V2.4	
No OSPs defined in MOD_VPNC_V2.4.	
From MOD_WLANC_V1.0	
No OSPs defined in MOD_WLANC_V1.0.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_MDF-BT-WLANC_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	**TOE Security Objective Definition**
From PP_MDF_V3.3	
O.AUTH	To address the issue of loss of confidentiality of user data in the event of loss of a Mobile Device (T.PHYSICAL_ACCESS), 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.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.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

TOE Security Objective	TOE Security Objective Definition
	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.MALICIOUS_APP), 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 (use cases 3 and 4), 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 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.MALICIOUS_APP and T.PERSISTENT_PRESENCE threats.
O.PROTECTED_COMMS	To address the network eavesdropping (T.NETWORK_EAVESDROP) and network attack (T.NETWORK_ATTACK) threats described in Section 3.1 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 must be capable of communicating using mutually authenticated TLS, EAP-TLS, HTTPS, 802.1X, and 802.11-2012. The TOE may optionally communicate using these standard protocols: IPsec, mutually-authenticated DTLS, or Bluetooth. These 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. 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_ACCESS), 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.
From MOD_BT_V1.0	
This PP-Module defines no additional TOE security objectives beyond those defined in the Base-PP. However, the SFRs defined in this PP-Module will assist in the achievement of O.PROTECTED_COMMS in the Base-PP.	
From MOD_WLANC_V1.0	
O.AUTH_COMM	The TOE will provide a means to ensure that it is communicating with an authorized access point and not some other entity pretending to be

TOE Security Objective	TOE Security Objective Definition
	an authorized access point, and will provide assurance to the access point of its identity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE will provide or use cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of data that are transmitted outside the TOE and its host environment.
O.SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to allow administrators to be able to configure the TOE.
O.WIRELESS_ACCESS_POINT_CONNECTION	The TOE will provide the capability to restrict the wireless access points to which it will connect.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_MDF-BT-WLANC_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_MDF_V3.3	
OE.CONFIG	TOE administrators will configure the Mobile Device security functions correctly to create the intended security policy.
OE.DATA_PROPER_USER	Administrators take measures to ensure that mobile device users are adequately vetted against malicious intent and are made aware of the expectations for appropriate use of the device.
OE.NOTIFY	The Mobile User will immediately notify the administrator if the Mobile Device is lost or stolen.
OE.PRECAUTION	The mobile device user exercises precautions to reduce the risk of loss or theft of the Mobile Device.
From MOD_BT_V1.0	
No additional operational environment objectives defined in MOD_BT_V1.0.	
From MOD_WLANC_V1.0	
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.TRUSTED_ADMIN	TOE administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 Functional Requirements

As indicated above, CFG_MDF-BT-WLANC_V1.0 includes PP_MDF_V3.3, MOD_BT_V1.0, and MOD-WLANC_V1.0.

Requirements in MOD_BT_V1.0 and MOD-WLANC_V1.0 are comprised of the “base” requirements, additional requirements that are selection-based or objective, and additional requirements that are dependent on the Base-PP that the PP-Modules are used with. The following table contains the “base” requirements that were validated as part of the Zebra Android 13 evaluation activities referenced above as well as the additional requirements that depend on the Base-PP that is claimed. In the case of the Zebra Android 13 evaluation, only those that apply when PP_MDF_V3.3 is the Base-PP were claimed by the TOE; those associated with other Base-PPs did not apply and have been evaluated through evaluation of the PP-Module workunits.

Table 6 defines the mandatory requirements for each component in CFG_MDF-BT-WLANC_V1.0. This includes requirements that all conformant products must claim, requirements in PP_MDF_V3.3 that are modified by a PP-Module (e.g. by forcing that a certain selection be made or that a certain optional requirement must be included), and requirements that are mandatory for a PP-Module depending on what Base-PP the PP-Module is extending.

Table 6: Mandatory Security Functional Requirements

Requirement Class	Requirement Component	Verified By
PP_MDF_V3.3		
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Zebra Android 13
	FAU_SAR.1: Audit Review	Zebra Android 13
	FAU_STG.1: Audit Storage Protection	Zebra Android 13
	FAU_STG.4: Prevention of Audit Data Loss	Zebra Android 13
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Zebra Android 13
	FCS_CKM.2/LOCKED: Cryptographic Key Establishment	Zebra Android 13
	FCS_CKM.2/UNLOCKED: Cryptographic Key Establishment	Zebra Android 13
	FCS_CKM_EXT.1: Cryptographic Key Support	Zebra Android 13
	FCS_CKM_EXT.2: Cryptographic Key Random Generation	Zebra Android 13
	FCS_CKM_EXT.3: Cryptographic Key Generation	Zebra Android 13
	FCS_CKM_EXT.4: Key Destruction	Zebra Android 13
	FCS_CKM_EXT.5: TSF Wipe	Zebra Android 13
	FCS_CKM_EXT.6: Salt Generation	Zebra Android 13
	FCS_COP.1/CONDITION: Cryptographic Operation	Zebra Android 13
	FCS_COP.1/ENCRYPT: Cryptographic Operation	Zebra Android 13
	FCS_COP.1/HASH: Cryptographic Operation	Zebra Android 13

Requirement Class	Requirement Component	Verified By
	FCS_COP.1/KEYHMAC: Cryptographic Operation	Zebra Android 13
	FCS_COP.1/SIGN: Cryptographic Operation	Zebra Android 13
	FCS_HTTPS_EXT.1: HTTPS Protocol	Zebra Android 13
	FCS_IV_EXT.1: Initialization Vector Generation	Zebra Android 13
	FCS_RBG_EXT.1: Random Bit Generation	Zebra Android 13
	FCS_SRV_EXT.1: Cryptographic Algorithm Services	Zebra Android 13
	FCS_STG_EXT.1: Cryptographic Key Storage	Zebra Android 13
	FCS_STG_EXT.2: Encrypted Cryptographic Key Storage	Zebra Android 13
	FCS_STG_EXT.3: Integrity of Encrypted Key Storage	Zebra Android 13
FDP: User Data Protection	FDP_ACF_EXT.1: Access Control for System Services	Zebra Android 13
	FDP_DAR_EXT.1: Protected Data Encryption	Zebra Android 13
	FDP_DAR_EXT.2: Sensitive Data Encryption	Zebra Android 13
	FDP_IFC_EXT.1: Subset Information Flow Control	Zebra Android 13
	FDP_STG_EXT.1: User Data Storage	Zebra Android 13
	FDP_UPC_EXT.1/APPS: Inter-TSF User Data Transfer Protection (Applications)	Zebra Android 13
FIA: Identification and Authentication	FIA_AFL_EXT.1: Authentication Failure Handling	Zebra Android 13
	FIA_PMG_EXT.1: Password Management	Zebra Android 13
	FIA_TRT_EXT.1: Authentication Throttling	Zebra Android 13
	FIA_UAU.5: Multiple Authentication Mechanisms	Zebra Android 13
	FIA_UAU.6/CREDENTIAL: Re-Authenticating (Credential Change)	Zebra Android 13
	FIA_UAU.6/LOCKED: Re-Authenticating (TSF Lock)	Zebra Android 13
	FIA_UAU.7: Protected Authentication Feedback	Zebra Android 13
	FIA_UAU_EXT.1: Authentication for Cryptographic Operation	Zebra Android 13
	FIA_UAU_EXT.2: Timing of Authentication	Zebra Android 13

Requirement Class	Requirement Component	Verified By
	FIA_X509_EXT.1: X.509 Validation of Certificates	Zebra Android 13
	FIA_X509_EXT.2: X.509 Certificate Authentication	Zebra Android 13
	FIA_X509_EXT.3: Request Validation of Certificates	Zebra Android 13
FMT: Security Management	FMT_MOF_EXT.1: Management of Security Functions Behavior	Zebra Android 13
	FMT_SMF.1: Specification of Management Functions	Zebra Android 13
	FMT_SMF_EXT.2: Specification of Remediation Actions	Zebra Android 13
FPT: Protection of the TSF	FPT_AEX_EXT.1: Application Address Space Layout Randomization	Zebra Android 13
	FPT_AEX_EXT.2: Memory Page Permissions	Zebra Android 13
	FPT_AEX_EXT.3: Stack Overflow Protection	Zebra Android 13
	FPT_AEX_EXT.4: Domain Isolation	Zebra Android 13
	FPT_JTA_EXT.1: JTAG Disablement	Zebra Android 13
	FPT_KST_EXT.1: Key Storage	Zebra Android 13
	FPT_KST_EXT.2: No Key Transmission	Zebra Android 13
	FPT_KST_EXT.3: No Plaintext Key Export	Zebra Android 13
	FPT_NOT_EXT.1: Self-Test Notification	Zebra Android 13
	FPT_STM.1: Reliable Time Stamps	Zebra Android 13
	FPT_TST_EXT.1: TSF Cryptographic Functionality Testing	Zebra Android 13
	FPT_TST_EXT.2/PREKERNEL: TSF Integrity Checking (Pre-Kernel)	Zebra Android 13
	FPT_TUD_EXT.1: TSF Version Query	Zebra Android 13
	FPT_TUD_EXT.2: TSF Update Verification	Zebra Android 13
	FPT_TUD_EXT.3: Application Signing	Zebra Android 13
FTA: TOE Access	FTA_SSL_EXT.1: TSF- and User-Initiated Locked State	Zebra Android 13
	FTA_TAB.1: Default TOE Access Banners	Zebra Android 13

Requirement Class	Requirement Component	Verified By
FTP: Trusted Path/Channels	FTP_ITC_EXT.1: Trusted Channel Communication	Zebra Android 13
From MOD_BT_V1.0		
Modified SFRs when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
FMT: Security Management	FMT_SMF_EXT.1: Specification of Management Functions	Zebra Android 13 – *Note that the MDF PP identifies this SFR as FMT_SMF.1*
Additional SFRs when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
FMT: Security Management	FMT_SMF_EXT.1/BT: Specification of Management Functions	Zebra Android 13
Modified SFRs when the Protection Profile for General Purpose Operating Systems is the Base-PP		
FMT: Security Management	FMT_MOF_EXT.1: Management of Security Functions Behavior	Module Evaluation
	FMT_SMF_EXT.1: Specification of Management Functions	Module Evaluation
Additional SFRs when the Protection Profile for General Purpose Operating Systems is the Base-PP		
FMT: Security Management	FMT_MOF_EXT.1/BT: Management of Security Functions Behavior	Module Evaluation
	FMT_SMF_EXT.1/BT: Specification of Management Functions	Module Evaluation
From MOD_WLANC_V1.0		
Modified SFRs when the Protection Profile for General Purpose Operating Systems is the Base-PP		
There are no modified SFRs when the General Purpose Operating Systems is the Base-PP.		
Additional SFRs when the Protection Profile for General Purpose Operating Systems is the Base-PP		
There are no additional SFRs when the General Purpose Operating Systems is the Base-PP.		
Modified SFRs when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
There are no modified SFRs when the Mobile Device Fundamentals is the Base-PP.		
Additional SFRs when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
There are no additional SFRs when the Mobile Device Fundamentals is the Base-PP.		

Table 7: Mandatory PP-Module SFRs

Requirement Class	Requirement Component	Verified By
From MOD_BT_V1.0		
FAU: Security Audit	FAU_GEN.1/BT: Audit Data Generation (Bluetooth)	Zebra Android 13
FCS: Cryptographic Support	FCS_CKM_EXT.8: Bluetooth Key Generation	Zebra Android 13
FIA: Identification and Authentication	FIA_BLT_EXT.1: Bluetooth User Authorization	Zebra Android 13
	FIA_BLT_EXT.2: Bluetooth Mutual Authentication	Zebra Android 13
	FIA_BLT_EXT.3: Rejection of Duplicate Bluetooth Connections	Zebra Android 13
	FIA_BLT_EXT.4: Secure Simple Pairing	Zebra Android 13
	FIA_BLT_EXT.6: Trusted Bluetooth Device User Authorization	Zebra Android 13
	FIA_BLT_EXT.7: Untrusted Bluetooth Device User Authorization	Zebra Android 13
FTP: Trusted Path/Channels	FTP_BLT_EXT.1: Bluetooth Encryption	Zebra Android 13
	FTP_BLT_EXT.2: Persistence of Bluetooth Encryption	Zebra Android 13
	FTP_BLT_EXT.3/BR: Bluetooth Encryption Parameters (BR/EDR)	Zebra Android 13
From MOD_WLANC_V1.0		
FAU: Security Audit	FAU_GEN.1/WLAN: Audit Data Generation (Wireless LAN)	Zebra Android 13
FCS: Cryptographic Support	FCS_CKM.1/WPA: Cryptographic Key Generation (Symmetric Keys for WPA2/WPA3 Connections)	Zebra Android 13
	FCS_CKM.2/WLAN: Cryptographic Key Distribution (Group Temporal Key for WLAN)	Zebra Android 13
	FCS_TLSC_EXT.1/WLAN: TLS Client Protocol (EAP-TLS for WLAN)	Zebra Android 13
	FCS_WPA_EXT.1: Supported WPA Versions	Zebra Android 13
FIA: Identification and Authentication	FIA_PAE_EXT.1: Port Access Entity Authentication	Zebra Android 13
	FIA_X509_EXT.1/WLAN: X.509 Certificate Validation	Zebra Android 13
	FIA_X509_EXT.2/WLAN: X.509 Certificate Authentication (EAP-TLS for WLAN)	Zebra Android 13

Requirement Class	Requirement Component	Verified By
	FIA_X509_EXT.6: X.509 Certificate Storage and Management	Zebra Android 13
FMT: Security Management	FMT_SMF.1/WLAN: Specification of Management Functions (WLAN Client)	Zebra Android 13 (Incorrectly named in the ST as FMT_SMF_EXT.1/WLAN)
FPT: Protection of the TSF	FPT_TST_EXT.3/WLAN: TSF Cryptographic Functionality Testing (WLAN Client)	Zebra Android 13
FTA: TOE Access	FTA_WSE_EXT.1: Wireless Network Access	Zebra Android 13
FTP: Trusted Path/Channels	FTP_ITC.1/WLAN: Trusted Channel Communication (Wireless LAN)	Zebra Android 13

The following table contains the "**Optional**" requirements contained in Appendix A.1, and an indication of how those requirements were evaluated (from the list in the Identification section). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
PP_MDF_V3.3		
FIA: Identification and Authentication	FIA_UAU_EXT.4: Secondary User Authentication	PP Evaluation
From MOD_BT_V1.0		
The MOD_BT_V1.0 does not define any additional optional requirements.		
From MOD_WLANC_V1.0		
The MOD_WLANC_V1.0 does not define any additional optional requirements.		

The following table contains the "**Objective**" requirements contained in Appendix A.2, and an indication of what evaluation those requirements were verified in (from the list in the Identification section). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
PP_MDF_V3.3		
FAU: Security Audit	FAU_SEL.1: Selective Audit	PP Evaluation
FCS: Cryptographic Support	FCS_RBG_EXT.2: Random Bit Generator State Preservation	PP Evaluation
	FCS_RBG_EXT.3: Support for Personalization String	PP Evaluation

Requirement Class	Requirement Component	Verified By
	FCS_SRV_EXT.2: Cryptographic Key Storage Services	Zebra Android 13 (Incorrectly named in the ST as Cryptographic Algorithm Services)
FDP: User Data Protection	FDP_ACF_EXT.3: Security Attribute Based Access Control	PP Evaluation
	FDP_BCK_EXT.1: Application Backup	PP Evaluation
	FDP_BLT_EXT.1: Limitation of Bluetooth Device Access	PP Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.4: X.509 Certificate Enrollment	PP Evaluation
	FIA_X509_EXT.5: X.509 Certificate Requests	PP Evaluation
FMT: Security Management	FMT_SMF_EXT.3: Current Administrator	Zebra Android 13
FPT: Protection of the TSF	FPT_AEX_EXT.5: Kernel Address Space Layout Randomization	Zebra Android 13
	FPT_AEX_EXT.6: Write or Execute Memory Page Permissions	PP Evaluation
	FPT_AEX_EXT.7: Heap Overflow Protection	PP Evaluation
	FPT_BBD_EXT.1: Application Processor Mediation	Zebra Android 13
	FPT_BLT_EXT.1: Limitation of Bluetooth Profile Support	PP Evaluation
	FPT_NOT_EXT.2: Software Integrity Verification	PP Evaluation
	FPT_TST_EXT.2/POSTKERNEL: TSF Integrity Checking (Post-Kernel)	Zebra Android 13
	FPT_TUD_EXT.5: Application Verification	PP Evaluation
	FPT_TUD_EXT.6: Trusted Update Verification	Zebra Android 13
From MOD_BT_V1.0		
FIA: Identification and Authentication	FIA_BLT_EXT.5: Bluetooth Secure Connections	Module Evaluation
From MOD_WLANC_V1.0		
The MOD_WLANC_V1.0 does not define any additional objective requirements.		

The following table contains the “**Implementation-based**” requirements contained in Appendix A.3, and an indication of what evaluation those requirements were verified in (from the list in the Identification section). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through “Module Evaluation.”

Table 10: Implementation-based Requirements

Requirement Class	Requirement Component	Verified By
PP_MDF_V3.3		
FDP: User Data Protection	FDP_UPC_EXT.1/BLUETOOTH: Inter-TSF User Data Transfer Protection (Bluetooth)	Zebra Android 13
From MOD_BT_V1.0		
The MOD_BT_V1.0 does not define any additional implementation-based requirements.		
From MOD_WLANC_V1.0		
The MOD_WLANC_V1.0 does not define any additional implementation-based requirements.		

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). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 11: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
PP_MDF_V3.3		
FCS: Cryptographic Support	FCS_CKM_EXT.7: Cryptographic Key Support (REK)	PP Evaluation
FDP: User Data Protection	FDP_ACF_EXT.2: Access Control for System Resources	Zebra Android 13 (Incorrectly named in the ST as Security access control)
FPT: Protection of the TSF	FPT_TST_EXT.3: TSF Integrity Testing	PP Evaluation
	FPT_TUD_EXT.4: Trusted Update Verification	PP Evaluation
From MOD_BT_V1.0		
FTP: Trusted Path/Channels	FTP_BLT_EXT.3/LE: Bluetooth Encryption Parameters (LE)	Zebra Android 13
From MOD_WLANC_V1.0		
FCS: Cryptographic Support	FCS_TLSC_EXT.2/WLAN: TLS Client Support for Supported Groups Extension (EAP-TLS for WLAN)	Zebra Android 13

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_MDF_V3.3. The SARs defined in that PP are applicable to MOD_BT_V1.0 and MOD-WLANC_V1.0, as well as CFG_MDF-BT-WLANC_V1.0 as a whole.

7 Results of the Evaluation

Note that for APE and ACE elements and workunits identical to ASE elements and workunits, the lab performed the ACE workunits concurrent to the ASE workunits.

Table 12: Evaluation Results: PP_MDF_V3.3

APE Requirement	Evaluation Verdict	Verified By
APE_INT.1	Pass	PP Evaluation
APE_CCL.1	Pass	PP Evaluation
APE_SPD.1	Pass	PP Evaluation
APE_OBJ.1	Pass	PP Evaluation
APE_ECD.1	Fail	PP Evaluation
APE_REQ.1	Pass	PP Evaluation

Table 13: Evaluation Results: MOD_BT_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module Evaluation
ACE_CCL.1	Pass	Module Evaluation
ACE_SPD.1	Pass	Module Evaluation
ACE_OBJ.1	Pass	Module Evaluation
ACE_ECD.1	Pass	Module Evaluation
ACE_REQ.1	Pass	Module Evaluation
ACE_MCO.1	Pass	Module Evaluation

Table 14: Evaluation Results: MOD_WLANC_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module Evaluation
ACE_CCL.1	Pass	Module Evaluation
ACE_SPD.1	Pass	Module Evaluation
ACE_OBJ.1	Pass	Module Evaluation
ACE_ECD.1	Fail	Module Evaluation
ACE_REQ.1	Pass	Module Evaluation
ACE_MCO.1	Pass	Module Evaluation

Table 15: Evaluation Results: CFG_MDF-BT-WLANC_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_CCO.1	Pass	PP-Config Evaluation

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 unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_BT_V1.0 and MOD-WLANC_V1.0 Evaluation Activities to determine whether 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.
- **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 the CCEVS Validation Body uses that leads to the issuance 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 VR.

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients, Version 1.0, 2022-10-24.

[6] Protection Profile for Mobile Device Fundamentals, Version 3.3, 2022-09-12.

[7] PP-Module for Bluetooth, Version 1.0, 2021-04-15.

[8] PP-Module for WLAN Clients, Version 1.0, 2022-03-31.

[9] Zebra Devices on Android 13 Security Target, Version 0.4, 07/26/2024.