National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Zebra Devices on Android 14

Report Number: CCEVS-VR-VID11631-2025
Dated: October 9, 2025
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

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Sheldon Durrant
Randy Heimann
Lisa Mitchell
Linda Morrison
Clare Parran
Lori Sarem
The MITRE Corporation

Common Criteria Testing Laboratory

Nate Feldman
Raymond Smoley
Rizheng Sun
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This Validation Report (VR) documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Zebra Devices on Android 14 solution provided by Zebra Technologies Corporation. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in October 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements of the *PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients*, Version 1.0, 11 October 2022 (CFG_MDF-BT-WLANC_V1.0) which includes the Base PP: *Mobile Device Fundamentals,* Version 3.3, 12 September 2022 (MDF33) with the *PP-Module for Bluetooth*, Version 1.0, 15 April 2021 (BT10) and the *PP-Module for WLAN Clients*, Version 1.0, 31 March 2022 (WLANC10) plus the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 (PKGTLS11).

The Target of Evaluation (TOE) is the Zebra Devices on Android 14.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Zebra Devices on Android 14 Security Target*, version 0.5, October 7, 2025 and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Zebra Devices on Android 14 (Specific models identified in Section 8)
Protection Profile	*PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients*, Version 1.0, 11 October 2022 (CFG_MDF-BT-WLANC_V1.0) which includes the Base PP: *Mobile Device Fundamentals*, Version 3.3, 12 September 2022 (MDF33) with the *PP-Module for Bluetooth*, Version 1.0, 15 April 2021 (BT10) and the *PP-Module for WLAN Clients*, Version 1.0, 31 March 2022 (WLANC10) plus the *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 (PKGTLS11)
ST	*Zebra Devices on Android 14 Security Target*, version 0.5, October 7, 2025
Evaluation Technical Report	*Evaluation Technical Report for Zebra Devices on Android 14*, version 0.3, October 7, 2025
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor & Developer	Zebra Technologies Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD

Item	Identifier
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Randy Heimann, Lisa Mitchell, Linda Morrison, Clare Parran, Lori Sarem

3 Architectural Information

Note: The following architectural description is based on the description presented in the ST.

The TOE is Zebra Devices on Android 14.

The Zebra Devices are handheld computing devices utilizing the Qualcomm-based chipsets, angled rear-facing barcode reader, optional stylus pen, and battery that is warm-swappable. The Devices use the Android operating system, providing access to applications from the Google Play store or Zebra's partners. The Devices feature built-in multi-carrier 4G LTE and FirstNet Ready with Band 14, voice capabilities, and dual SIM cards. The TOE supports using client certificates to connect to access points offering WPA2/WPA3 networks with 802.1x/EAP-TLS or alternatively connecting to cellular base stations when utilizing mobile data.

3.1 TOE Evaluated Platforms

Details regarding the evaluated configuration are provided in Section 8 below.

3.2 TOE Architecture

The TOE provides a rich API to mobile applications and provides users installing an application the option to either approve or reject an application based upon the API access that the application requires (or to grant applications access at runtime).

The TOE also provides users with the ability to protect Data-At-Rest with AES encryption, including all user and mobile application data stored in the user's data partition. The TOE uses a key hierarchy that combines a REK with the user's password to provide protection to all users and application cryptographic keys stored in the TOE.

Finally, the TOE can interact with a Mobile Device Management (MDM) system (not part of this evaluation) to allow enterprise control of the configuration and operation of the device so as to ensure adherence to enterprise-wide policies (for example, restricting use of a corporate provided device's camera, forced configuration of maximum login attempts, pulling of audit logs off the TOE, etc.) as well as policies governing enterprise applications and data. An MDM is made up of two parts: the MDM agent and MDM server. The MDM Agent is installed on the phone/mobile computer as an administrator with elevated permissions (allowing it to change the relevant settings on the phone/device) while the MDM Server is used to issue the commands to the MDM Agent. Neither portion of the MDM process is considered part of the TOE, and therefore not being directly evaluated.

The TOE includes several different levels of execution including (from lowest to highest): hardware, a Trusted Execution Environment (TEE) which is used to store cryptographic keys, Android's Linux kernel which perform low-lev android OS functions, and Android's user space, which provides APIs allowing applications to leverage the cryptographic functionality of the device.

3.3 Physical Boundaries

The TOE's physical boundary is the physical perimeter of its enclosure. The TOE runs Android as its software/OS, executing on a Qualcomm Snapdragon processor. The TOE does not include the user applications that run on top of the operating system but does include controls that limit application behavior. Further, the device provides support for downloadable MDM agents to be installed to limit or permit different functionality of the device. There is no built-in MDM agent pre-installed on the device.

The TOE communicates and interacts with 802.11-2012 Access Points and mobile data networks to establish network connectivity, and through that connectivity interacts with MDM servers that allow administrative control of the TOE.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Security management
6. Protection of the TSF
7. TOE access
8. Trusted path/channels

4.1 Security audit

The TOE implements a security log and logcat that are each stored in a circular memory buffer. An MDM agent can read/fetch the security logs, can retrieve logcat logs, and then handle appropriately (potentially storing the log to Flash or transmitting its contents to the MDM server). These log methods meet the logging requirements outlined by FAU_GEN.1 in MDFPPv3.3. Please see the Security audit section 6.1 in the ST for further information and specifics.

4.2 Cryptographic support

The TOE includes multiple cryptographic libraries with CAVP certified algorithms for a wide range of cryptographic functions including the following: asymmetric key generation and establishment, symmetric key generation, encryption/decryption, cryptographic hashing and keyed-hash message authentication. These functions are supported with suitable random bit generation, key derivation, salt generation, initialization vector generation, secure key storage, and key and protected data destruction. These primitive cryptographic functions may be used to implement security protocols such as TLS, EAP-TLS, IPsec, and HTTPS and to encrypt the media (including the generation and protection of data and key encryption keys) used by the TOE. Many of these cryptographic functions are also accessible as services to applications running on the TOE allowing application developers to ensure their application meets the required criteria to remain compliant to MDFPP standards.

4.3 User data protection

The TOE controls access to system services by hosted applications, including protection of the Trust Anchor Database. Additionally, the TOE protects user and other sensitive data using File-Based Encryption (FBE) so that even if a device is physically lost, the data remains protected. The TOE's evaluated configuration supports Android Enterprise profiles to provide additional separation between application and application data belonging to the Enterprise profile. Please see the Admin Guide for additional details regarding how to set up and use Enterprise profiles.

4.4 Identification and authentication

The TOE supports a number of features related to identification and authentication. From a user perspective, except for FCC mandated (making phone calls to an emergency number) or non-sensitive functions (e.g., choosing the keyboard input method or taking screen shots), a password (i.e., Password Authentication Factor) must be correctly entered to unlock the TOE. Also, even when unlocked, the TOE requires the user re-enter the password to change the password. Passwords are obscured when entered so they cannot be read from the TOE's display and the frequency of entering passwords is limited and when a configured number of failures occurs, the TOE will be wiped to protect its contents. Passwords can be constructed using upper and lower cases characters, numbers, and special characters and passwords up to 16 characters are supported.

The TOE can also serve as an 802.1X supplicant and can both use and validate X.509v3 certificates for EAP-TLS, TLS, and HTTPS exchanges.

4.5 Security management

The TOE provides all the interfaces necessary to manage the security functions identified throughout the ST as well as other functions commonly found in mobile devices. Many of the available functions are available to users of the TOE while many are restricted to administrators operating through a Mobile Device Management solution once the TOE has been enrolled.

4.6 Protection of the TSF

The TOE implements a number of features to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as cryptographic keys so that they are not accessible or exportable through the use of the application processor's hardware. The TOE disallows all read access to the Root Encryption Key (REK) and retains all keys derived from the REK within its Trusted Execution Environment (TEE). Application software can only use keys derived from the REK by reference and receive the result.

The TOE also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability). It enforces read, write, and execute memory page protections, uses address space layout randomization, and stack-based buffer overflow protections to minimize the potential to exploit application flaws. It also protects itself from modification by applications as well as isolates the address spaces of applications from one another to protect those applications.

The TOE includes functions to perform self-tests and software/firmware integrity checking so that it might detect when it is failing or may be corrupt. If any self-tests fail, the TOE will not go into an operational mode. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE. Digital signature checking also extends to verifying applications prior to their installation as all applications must have signatures (even if self-signed).

4.7 TOE access

The TOE can be locked, obscuring its display, by the user or after a configured interval of inactivity. The TOE also has the capability to display an administrator specified (using the TOE's MDM API) advisory message (banner) when the user unlocks the TOE for the first use after reboot.

The TOE is also able to attempt to connect to wireless networks as configured.

4.8 Trusted path/channels

The TOE supports the use of IEEE 802.11-2012, 802.1X, and EAP-TLS and TLS, HTTPS to secure communications channels between itself and other trusted network devices.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *Mobile Device Fundamentals*, Version 3.3, 12 September 2022 (MDF33)
- *PP-Module for Bluetooth*, Version 1.0, 15 April 2021 (BT10)
- *PP-Module for WLAN Clients*, Version 1.0, 31 March 2022 (WLANC10)
- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 (PKGTLS11)

That information has not been reproduced here and the MDF33/BT10/WLANC10/PKGTLS11 should be consulted if there is interest in that material.

5.2 Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the MDF33/BT10/WLANC10/PKGTLS11 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Mobile Device Fundamentals Protection Profile with the Bluetooth and WLAN Clients Modules plus the TLS Package and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Mobile Device models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the MDF33/BT10/WLANC10/PKGTLS11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- *Android 14 Common Criteria Administrator Guidance for Zebra Devices (SD660/SM6375/ QCM6490/QCM5430/ QCM4490/)*, Version 0.3, October 7, 2025

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary *Detailed Test Report for Zebra Devices on Android 14*, Version 0.3, October 7, 2025 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the MDF33/BT10/WLANC10/PKGTLS11 including the tests associated with optional requirements.

8 Evaluated Configuration

The TOE encompasses mobile devices that support enterprises and individual users alike and this evaluation tested the following Mobile Handhelds models and versions.

Product	Model #	CPU	Arch	Kernel	Android OS version	Security Patch Level
660 Mobile Handhelds	TC52ax, TC57, TC26, MC9300	Qualcomm SDM660	ARMv8	4.19	Android 14.0	September 2025
6490 Mobile Handhelds	TC58	Qualcomm QCM6490	ARMv8	5.4	Android 14.0	September 2025
6375 Mobile Handhelds	ET40, ET45, TC15	Qualcomm SM6375	ARMv8	5.4	Android 14.0	September 2025
4490 Mobile Handheld	TC53e, TC58e, MC9400	Qualcomm QCM4490	ARMv8	5.10	Android 14.0	September 2025

The following other, equivalent models are included in the evaluation as they utilize the same hardware components and same image, CPU, architecture, kernel version, Android version, and patch version as the above devices (i.e., each CPU model has one image). The QCS4490 CPU is equivalent to the QCM4490 CPU and the QCM5430 CPU is equivalent to the QCM6490. In both cases, the CPUs have the same instruction set.

Model #	CPU	Wireless Chipset	Cellular	WiFi 6 support	Description
SDM660 Devices with WCN3990					
CC600	SDM660	WCN3990	WLAN	No	5” Customer concierge interactive tablet-style kiosk device
CC6000	SDM660	WCN3990	WLAN	No	10” Customer concierge interactive tablet-style kiosk device
ET51	SDM660	WCN3990	WLAN	No	8”/10” tablet
ET56	SDM660	WCN3990	WWAN Data Only	No	8”/10” tablet
L10A	SDM660	WCN3990	WWAN Data Only	No	10” Ultra Rugged WWAN tablet
MC20	SDM660	WCN3990	WLAN	No	4” Keypad WLAN device for Japanese Market
MC9300	SDM660	WCN3990	WLAN	No	4.3” Ultra-rugged keypad WLAN device
PS20	SDM660	WCN3990	WLAN	No	4” Personal Shopper assistant
TC52	SDM660	WCN3990	WLAN	No	5” Phone
TC52-HC	SDM660	WCN3990	WLAN	No	5” Phone made form healthcare grade plastics
TC52x	SDM660	WCN3990	WLAN	No	5” Phone
TC52x-HC	SDM660	WCN3990	WLAN	No	5” Phone made form healthcare grade plastics
TC57	SDM660	WCN3990	WWAN/ Cellular	No	5” Phone
TC57x	SDM660	WCN3990	WWAN/ Cellular	No	5” Phone
TC72	SDM660	WCN3990	WLAN	No	4.7” Ultra rugged Phone
TC77	SDM660	WCN3990	WWAN/ Cellular	No	4.7” Ultra rugged Phone
TC83	SDM660	WCN3990	WLAN	No	4” Ultra rugged Touch Computer / Gun Handler phone
VC83	SDM660	WCN3990	WLAN	No	8” / 10” Vehicle Mounted Computer
WT6300	SDM660	WCN3990	WLAN	No	3.2” Advanced glove-optimized rugged wearable device
EC30	SDM660	WCN3990	WLAN	No	3” Portable, lightweight phone
EC50	SDM660	WCN3990	WLAN	No	5” Enterprise Mobile computer with optional integrated scanner
EC55	SDM660	WCN3990	WWAN/ Cellular	No	5” Enterprise Mobile computer with optional integrated scanner
MC2200	SDM660	WCN3990	WLAN	No	4” Touch computer / gun handler
MC2700	SDM660	WCN3990	WWAN/ Cellular	No	4” Touch computer / gun handler
MC3300x	SDM660	WCN3990	WLAN	No	4” Touch computer / gun handler
MC33xR	SDM660	WCN3990	WLAN	No	4” Touch computer / gun handler with RFID

Model #	CPU	Wireless Chipset	Cellular	WiFi 6 support	Description
SDM660 Devices with WCN3980					
TC21	SDM660	WCN3980	WLAN	No	5” Phone
TC21-HC	SDM660	WCN3980	WLAN	No	5” Phone made from healthcare grade plastics
TC26	SDM660	WCN3980	WWAN/ Cellular	No	5” Phone
TC26-HC	SDM660	WCN3980	WWAN/ Cellular	No	5” Phone made form healthcare grade plastics
SDM660 Devices with BCM43752					
TC52ax	SDM660	BCM43752	WLAN	Yes	5” Phone
MC33ax	SDM660	BCM43752	WLAN	Yes	4” Touch computer / gun handler
QCM4490/QCS4490 Devices with WCN6856					
MC3400	QCM4490	WCN6856	WLAN	Yes	4.0” Gun, straight shooter scanning device
MC3450	QCM4490	WCN6856	WWAN	Yes	4.0” Gun, straight shooter scanning device
MC9400	QCM4490	WCN6856	WLAN	Yes	4.3” Ultra Rugged Pistol Grip device
MC9450	QCM4490	WCN6856	WWAN	Yes	4.3” Ultra Rugged Pistol Grip device
PS30	QCM4490	WCN6856	WLAN	Yes	4.7” Shopping device,
TC53e	QCM4490	WCN6856	WLAN	Yes	6” Phone
TC58e	QCM4490	WCN6856	WWAN	Yes	6” Phone
FR55 / FR55S	QCS4490	WCN6856 / SDR435 (WWAN)	WWAN	Yes	True Hot swap, NFC, Secure Element, SAM phone
WT5400	QCS4490	WCN6856	WLAN	Yes	4.7” Wearable
WT6400	QCS4490	WCN6856	WLAN	Yes	4.7” Wearable
QCM5430 Devices with WCN6856					
HC20	QCM5430	WCN6856	WLAN	Yes	6” Phone made from healthcare plastics
HC50	QCM5430	WCN6856	WLAN	Yes	6” Phone made from healthcare plastics
TC22	QCM5430	WCN6856	WLAN	Yes	6” Phone
TC27	QCM5430	WCN6856	WWAN/ Cellular	Yes	6” Phone
TC22R	QCM5430	WCN6856 (WIFI)	WLAN only	Yes	6” Gun style phone with NFC
TC27R	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	6” Gun style phone with NFC
EM45	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	6.7” Phone with 5G Sub6, NFC, BLE 5.3
TC73-5430	QCM5430	WCN6856	WLAN	Yes	Phone (Nazare)
TC78-5430	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	Phone (Nazare)
KC50S	QCM5430	WCN6856	WLAN	Yes	22” & 15” Tablet with NFC
KC50L	QCM5430	WCN6856	WLAN	Yes	22” & 15” Tablet with NFC
HC25	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	22” & 15” Tablet with NFC
HC55	QCM5430	WCN6856 (WIFI) SDR735 (WWAN, GPS)	WWAN	Yes	22” & 15” Tablet with NFC
ZEC500	QCM5430	WCN6856	WLAN	Yes	Wireless WSC, Kisok box - Android device without an embedded display or battery
SM6375 Devices with BCM43752					

Model #	CPU	Wireless Chipset	Cellular	WiFi 6 support	Description
ET40	SM6375	BCM43752	WLAN	Yes	8"/ 10" Tablet with NFC PN7160
ET40HC	SM6375	BCM43752	WLAN	Yes	8"/ 10" Tablet made from Healthcare grade plastics, NFC PN7160
ET45	SM6375	BCM43752	WWAN Data Only	Yes	8"/ 10" Tablet with NFC PN7160
ET45HC	SM6375	BCM43752	WWAN Data Only	Yes	8"/ 10" Tablet made from Healthcare grade plastics, NFC PN7160
SM6375 with WCN3988					
TC15	SM6375	WCN3988	WWAN/ Cellular	No	6.5" Phone with NFC PN557
TN28	SM6375	WCN3988	WWAN/ Cellular	No	6.5" Phone with NFC PN557
QCM6490 Devices with WCN6856					
ET60	QCM6490	WCN6856	WLAN	Yes	10” Tablet
ET65	QCM6490	WCN6856	WWAN Data Only	Yes	10” Tablet
TC53	QCM6490	WCN6856	WLAN	Yes	6” Phone
TC58	QCM6490	WCN6856	WWAN/ Cellular	Yes	6” Phone
TC73	QCM6490	WCN6856	WLAN	Yes	6” Phone
TC78	QCM6490	WCN6856	WWAN/ Cellular	Yes	6” Phone

The above models may represent additional model-specific SKUs which vary by screen-size, RAM / Storage Capacity, battery capacity, base vs premium materials. The Bluetooth MAP profile is not supported on devices without Cellular capabilities.

Some of the claimed SKUs [e.g., TC58e, TC53e] are equipped with Strongbox capabilities; however, the scope of the evaluation does not encompass the validation of this functionality and its use is not supported within the evaluated configuration.

Some features and settings must be enabled for the TOE to operate in its evaluated configuration. The following features and settings must be enabled:

1. Require a lockscreen password
2. Disable Smart Lock
3. Enable Encryption of Wi-Fi and Bluetooth secrets by enabling ‘niap_mode’
4. Disable Debugging Features (Developer options)
5. Disable installation of applications from unknown sources
6. Enable Audit Logging

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The Evaluation team determined the Devices on Android 14 TOE to be Part 2 extended, and to meet the SARs contained in the MDF33/BT10/WLANC10/PKGTLS11.

9.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Zebra Devices on Android 14 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the Evaluation team performed the assurance activities specified in the MDF33/BT10/WLANC10/PKGTLS11 related to the examination of the information contained in the TSS.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted

in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the MDF33/BT10/WLANC10/PKGTLS11 and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The Evaluation team searched the (National Vulnerability Database (https://web.nvd.nist.gov/vuln/search, ref NVD), MITRE CVE Database, National Vulnerability Database, and CVE details (https://www.cve.org/, https://web.nvd.nist.gov/vuln/search, and https://www.cvedetails.com/vulnerability-search.php, ref CVE), Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog, ref KEV) Vulnerability Notes Database (http://www.kb.cert.org/vuls/, ref VND), on 10/07/2025 (from 7/1/2024 as the TOEs have all gone through a CC evaluation since this date) with the following search terms: "Android", "Android 14", "BoringSSL", "Android Locksettings service KBKDF", "QTI Crypto Engine Core", "QTI Inline Crypto Engine", "QTI Random Number Generator", "Zebra Technologies Corporation", "Zebra", "QCM4490", "SD660", "SDM6375", "QCM5430", "QCM6490", "QCM4490", "WCN3990", "WCN3980", "BCM43752", "WCN3988", "WCN6856", "PS30", "TC53e", "TC58e", "MC9400", "MC9450", "MC3400", "MC3450", "WT5400", "WT6400", "FR55", "FR55S ", "CC600", "CC6000", "ET51", "ET56", "L10A", "MC20", "MC9300", "PS20", "TC21", "TC21-HC", "TC26", "TC26-HC", "TC52", "TC52ax", "TC52-HC", "TC52x", "TC52x-HC", "TC57", "TC57x", "TC72", "TC77", "TC83", "VC83", "WT6300", "EC30", "EC50", "EC55", "MC2200", "MC2700", "MC3300x", "MC33ax", "MC33xR", "ET60", "ET65", "TC53", "TC58", "TC73", "TC78", "HC20", "HC50", "TC22",

"TC27", "TC22R ", "TC27R", "EM45", "TC78-5430", "KC50S ", "KC50L", "HC25 ", "HC55", "ZEC500", "ET40", "ET40HC", "ET45", "ET45HC", "TC15", "TN28".

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Android 14 Common Criteria Administrator Guidance for Zebra Devices (SD660/SM6375/ QCM6490/QCM5430/ QCM4490/)*, Version 0.3, October 7, 2025. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the MDF33/BT10/WLANC10/PKGTLS11 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Zebra Devices on Android 14 Security Target*, Version 0.5, October 7, 2025.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

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

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.

[4] *Mobile Device Fundamentals*, Version 3.3, 12 September 2022 (MDF33).

[5] *PP-Module for Bluetooth*, Version 1.0, 15 April 2021 (BT10).

[6] *PP-Module for WLAN Clients*, Version 1.0, 31 March 2022 (WLANC10).

[7] *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 1 March 2019 (PKGTLS11).

[8] *Zebra Devices on Android 14 Security Target*, Version 0.5, October 7, 2025 (ST).

[9] *Assurance Activity Report for Zebra Devices on Android 14*, Version 0.3, October 7, 2025 (AAR).

[10] *Detailed Test Report for Zebra Devices on Android 14*, Version 0.3, October 7, 2025 (DTR).

[11] *Evaluation Technical Report for Zebra Devices on Android 14*, Version 0.3, October 7, 2025 (ETR).

[12] *Android 14 Common Criteria Administrator Guidance for Zebra Devices (SD660/SM6375/ QCM6490/QCM5430/ QCM4490/)*, Version 0.3, October 7, 2025 (AGD).

[13] *Zebra Devices on Android 14 Key Management Description*, Version 0.5, October 7, 2025 (KMD).