



Zebra Android™ 13 Mobile Devices are Common Criteria Certified

Mobile devices are indispensable tools for frontline workers who need access to critical information wherever they are located, with the level of security and performance required to achieve focused initiatives. Yet, at every organization, an unprecedented amount of sensitive data is stored on mobile devices and changes hands every day—in data connections, text messages, email app alerts, device handoffs and more. While mobility heightens workforce performance, it also presents unique challenges that must be addressed to safeguard and protect both the device and data. This need has never been more urgent.

With cybersecurity threats increasing every day, private and public organizations must ensure their devices are secure and adhere to the highest industry standards to reduce risks. For example, U.S. national policy governing the acquisition of information assurance (IA) and IA-enabled information technology products, federal agencies must prevent access by unauthorized users, use secure networks and set strict device parameters for workers seeking to access sensitive data on those networks.

Organizations across the board are repeatedly targeted based on security vulnerabilities that, in most cases, could be avoided. In today's environment, no one is immune to cyber-attacks. It is critical to have effective security policies in place and implement devices that help protect your organization from these threats.

High Security Clearance for Today's Mobile Devices

Common Criteria (CC) is an international framework developed for the evaluation of software and hardware information technology products to ensure that they meet an agreed-upon security standard. Standardized as ISO 15408, it is a vital criterion for mobile solutions used by frontline workers. Common Criteria certification provides assurance that a device meets a high standard of security and that the evaluation of the device was conducted in a comprehensive and standardized manner.

Today, over 25 Zebra mobile devices that employ the Android 13 operating system are validated for Common Criteria certification under the U.S. schema administered by the National Information Assurance Partnership (NIAP). This certification enables organizations to purchase Zebra devices with the security and assurance your frontline workers need to meet globally recognized security standards.



Taking Mobile Security to New Levels

Zebra's best-in-class mobile technology solutions enable organizations to fulfill their initiatives effectively and efficiently. Our enterprise-grade devices empower mobile workforces with 24/7 access to critical networks, while helping ensure endpoint security and contain costs. Because we understand that security is critical for enterprise operations, we proactively guard against vulnerabilities by integrating multiple layers of protection into our mobile devices, solutions and services.

Fortifying the Android System

Only Zebra Android devices feature built-in Zebra DNA™ and Mobility Extensions (Mx) technology, that delivers enterprise-class security and manageability features not available on the standard, consumer-grade Android operating system. Mx security fortifies the Android operating system so that your agency can select the data you want to encrypt and uses a government-grade AES-256 encryption that does not slow down performance.

Operating Up to Government Standards for Public and Private Organizations

At Zebra, we work with government agencies, as well as private companies to connect their assets, people and data to enable informed decision making and efficient workflows. We continue to ensure that our growing portfolio of mobile devices adhere to the most relevant security standards. Our mobile devices incorporate leading security features, and many are validated to comply with FIPS.

In addition to compliance with vital security features, many Zebra products adhere to the Department of Defense's MIL-STD-810G or MIL-STD-810H durability standards for drops, vibration, moisture and dust. Zebra's Android mobile computers and mobile printers have also earned many IP ratings for ruggedness, dust and water resistance.

Zebra is committed to ensuring our products are rugged and secure. We will continue to test future devices and new versions of the Android operating system to meet these high standards.

Zebra Common Criteria Certified Devices

Zebra has a broad portfolio of enterprise-optimized Android devices. More than 25 Zebra devices, including mobile computers, tablets and wearables, running the Android 13 operating system are certified for Common Criteria compliance with a commitment from Zebra to validate future devices and Android OS software releases.

Zebra Common Criteria Certified Devices

TCX Series Mobile Computers



TC21/TC26



TC22/TC27



TC52/TC52x/TC57/
TC57x/TC52ax



TC53/TC58



TC72/TC77



TC73/TC78



TC8300

Healthcare Mobile Computers



TC21-HC/TC26-HC



HC20



TC52-HC/TC52x-HC/
TC52ax-HC



HC50

ECx Series Mobile Computers



EC50/EC55

To learn more about Zebra's Common Criteria certification, visit zebra.com/commoncriteria

MCx Series Mobile Computers



MC2200/MC2700



MC3300x/MC3300ax



MC9300

Wearable Computers



WT6300

Personal Shoppers



PS20

Tablets



ET40/ET45



ET60/ET65

Vehicle Mounted Computers



VC8300

Customer Concierge/Kiosks



CC600/CC6000

To learn more about Zebra's commitment to IT security, visit zebra.com/product-security



NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

EMEA Headquarters
zebra.com/locations
contact.emea@zebra.com

Latin America Headquarters
zebra.com/locations
la.contactme@zebra.com

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corp., registered in many jurisdictions worldwide. Android is a trademark of Google LLC. All other trademarks are the property of their respective owners. ©2024 Zebra Technologies Corp. and/or its affiliates. 08/08/2024