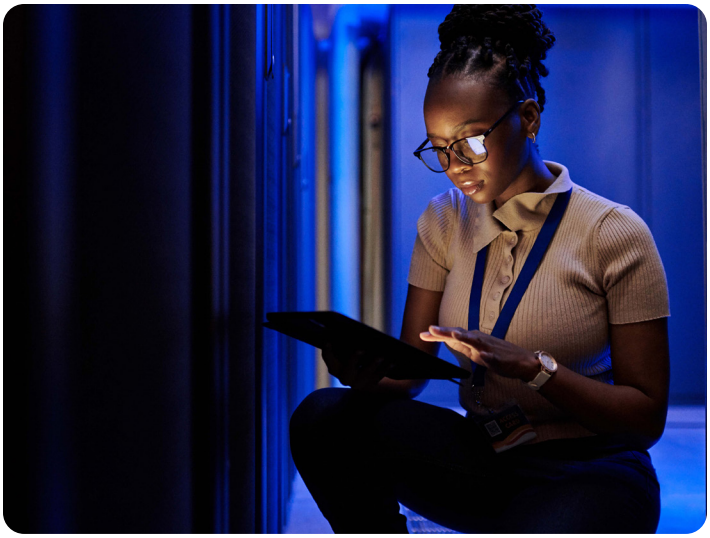
Zebra Android™ products security certifications



Frequently Asked Questions

Table of contents

What is FIPS 140-2? (ISO/IEC 19790:2012)

The Federal Information Processing Standard (FIPS) 140-2 is a U.S. and Canadian government standard that sets the benchmark for validating the effectiveness of cryptographic hardware. If a product has a FIPS 140-2 certificate, it means it has been tested and formally validated by the U.S. and Canadian governments. The standard specifies the security requirements for cryptographic modules, which are the hardware, software, and/or firmware that implement cryptographic functions like encryption.

FIPS 140-2 defines four increasing, qualitative levels of security:

- **Level 1:** Requires production-grade equipment and externally tested algorithms.
- **Level 2:** Adds requirements for physical tamper-evidence and role-based authentication.
- **Level 3:** Adds requirements for physical tamper-resistance and identity-based authentication.
- **Level 4:** This level makes the physical security requirements more stringent, requiring the ability to be tamper-active, erasing the contents of the device if it detects various forms of environmental attack.

Zebra products running A13 and below achieve Level 1 to meet market requirements. Certificate #3866 is now on the historical list with the introduction of the -3 version of the FIPS 140 standard.

What is FIPS 140-3? (ISO/IEC 24759)

FIPS 140-3 is the current and third version of the U.S. government standard for validating cryptographic modules used to protect sensitive information. It replaces FIPS 140-2 and aligns with international encryption standards, specifically ISO/IEC 19790:2012 and ISO/IEC 24759. The standard defines how encryption modules must operate to ensure strong, tamper-resistant protections for sensitive data. FIPS 140-3 is applicable to federal agencies, defense contractors, healthcare providers, financial institutions, and cloud platforms.

Key differences and enhancements in FIPS 140-3 compared to FIPS 140-2 include:

- **Stricter Integrity Test Requirements:** More rigorous testing
- **Module Identification:** Output the module name/identifier and version.
- **Key Zeroization:** Required for all unprotected “Sensitive Security Parameters” (SSP)

Zebra products running A14 and beyond will be evaluated under the -3 version of the FIPS 140 standard.

What is Common Criteria (CC)? (ISO/IEC 15408)

Common Criteria (CC), also known as ISO/IEC 15408, is an international standard for computer security certification. It provides a framework for users to specify their security requirements in a Security Target (ST) and for vendors to make claims about the security attributes of their products, which are known as the Target of Evaluation (TOE). Common Criteria is used by governments and organizations to evaluate and certify that IT products meet specified security standards for use in secure environments. The goal of the Common Criteria framework is to build confidence and trust in the security characteristics of an IT product.

What is NIAP Common Criteria Certification?

Key differences and enhancements in FIPS 140-3 compared to FIPS 140-2 include:

- **Platforms & Products:** 66 of Zebra's enterprise mobile computers, tablets, and wearables running the Android 14 operating system are Common Criteria certified. The certification covers the device's hardware and software, including permissions, access control, and data encryption. Zebra's portfolio of Android 10, 11 and 13 mobile devices has also previously received this internationally recognized certification. Android 15 is currently in process.

What is CSfC Component Listing?

The NSA's Commercial Solutions for Classified (CSfC) program approves commercial products for use in layered solutions to protect classified government data.

- **Platforms & Products:** As of August 2024, Zebra Devices on Android 13 are officially included on the CSfC Components List under the "End User Device / Mobile Platform" category.

What is STIG Validation?

The Security Technical Implementation Guide (STIG) is a cybersecurity standard from the Defense Information Systems Agency (DISA) required for products used on Department of Defense (DoD) networks.

- **Platforms & Products:** Zebra has the broadest portfolio of enterprise-grade rugged mobile devices with STIG validation. This includes a wide range of devices running Android 10, 11, 13 and 14. The validation covers Corporate Owned Business Only (COBO) for Android 11 and below and Corporate Owned Personally Enabled (COPE) use cases for Android 13 and 14.

What is DoD IN APL? (Department of Defense Information Network Approved Products List)

Achieving STIG validation allows products to be placed on the DoDIN APL, which is the master list of products certified for use on DoD networks.

- **Platforms & Products:** Zebra offers the largest number of rugged, enterprise-grade mobile devices on the DoDIN Approved Products List. This includes the extensive portfolio of Android devices. These STIG-validated devices are approved for deployment across all branches of the U.S. military and other federal agencies. Note: DoDIN APL program will be officially sunset on 30 September 2025. The APL process will undergo a renewal cycle.

Who is NIAP?

The National Information Assurance Partnership (NIAP) is a United States government initiative operated by the National Security Agency (NSA) that is responsible for the U.S. implementation of the Common Criteria. It was originally a joint effort between the NSA and the National Institute of Standards and Technology (NIST). NIAP's main goal is to improve the security of information technology products and systems by promoting the use of the Common Criteria (CC) evaluation and validation. The organization oversees a program to evaluate Commercial Off-The-Shelf (COTS) IT products to ensure they conform to the international Common Criteria standard. Products that are successfully evaluated are listed on the U.S. NIAP Product Compliant List and the international CCRA Certified Products List.

Who is NIST?

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce. Founded in 1901, it is one of the nation's oldest physical science laboratories. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. The agency develops and promotes measurement standards, calibration services, and quality assurance programs. In the realm of cybersecurity, NIST creates fundamental security frameworks that help organizations manage risk, detect threats, and respond to incidents.

What is Mobile Device Fundamentals Protection Profile?

The Mobile Device Fundamentals Protection Profile (PP) specifies information security requirements for mobile devices, such as smartphones and tablets, for use in an enterprise. This assurance standard describes the essential security services a mobile device should provide to serve as a foundation for a secure mobile architecture. The Protection Profile was developed by a "Mobility Technical Community" with representatives from industry, U.S. Government agencies, Common Criteria Test Laboratories, and international Common Criteria schemes. It covers security features like cryptographic services, data-at-rest protection, key storage, security policy enforcement, application mandatory access control, anti-exploitation features, user authentication, and software integrity protection.

What is a STIG?

A Security Technical Implementation Guide (STIG) is a cybersecurity configuration standard for United States Department of Defense (DoD) information systems and software. Developed and maintained by the Defense Information Systems Agency (DISA), STIGs provide detailed guidance on how to implement security policies and procedures to harden systems and reduce their vulnerability to cyberattacks. They specify configuration settings and security requirements for a wide range of technologies, including operating systems, applications, and network devices, to ensure a consistent and secure baseline.

What is CSfC Component Listing?

The Commercial Solutions for Classified (CSfC) Component List is a list of commercial hardware and software products that have been approved by the National Security Agency (NSA) to be used in layered solutions to protect classified National Security Systems (NSS) data. The CSfC program allows for the use of commercial off-the-shelf (COTS) products that have met specific IT security evaluation criteria, including Common Criteria and FIPS validations, to build secure solutions. Customers can select products from this list to create solutions based on published Capability Packages that provide reference architectures and configuration information.

What is a DoD IN APL?

The Department of Defense Information Network (DoDIN) Approved Products List (APL) is a single, consolidated list of products that have successfully completed Cybersecurity (CS) and Interoperability (IO) certification. The DoDIN APL serves as an acquisition decision support tool for DoD organizations to purchase and operate systems across all DoD network infrastructures. To be listed, products undergo rigorous testing at a DISA Testing Center against standards like Security Technical Implementation Guides (STIGs).

What is a Consumer Mobile Device Protection Profile?

The ETSI Consumer Mobile Device Protection Profile (ETSI TS 103 732 series) is a standard that outlines security requirements for consumer mobile devices. This profile is the basis for the GSMA's Mobile Device Security Certification (MDSCert) scheme. It focuses on ensuring a baseline of security for consumer smartphones and other mobile devices.

Who is TrustCB with respect to MDSCert?

TrustCB is a commercial Certification Body that operates the GSMA Mobile Device Security Certification (MDSCert) scheme. GSMA designed the requirements for the MDSCert scheme, which evaluates mobile devices against the ETSI Consumer Mobile Device Protection Profile. As the scheme owner and operator, TrustCB is responsible for implementing this certification. After a device is evaluated by an authorized lab, TrustCB reviews the results, and upon approval, prepares a Certification Report and delivers it to the manufacturer and the lab.

What is Mobile Device Security Certification GSMA?

The GSMA Mobile Device Security Certification (MDSCert) is a scheme that provides a framework for assessing and certifying the security capabilities of consumer mobile devices like smartphones and tablets. The scheme aims to increase the transparency of security in mobile devices and improve security levels across the mobile ecosystem. The certification is based on the ETSI Consumer Mobile Device Protection Profile (ETSI TS 103 732 series / EN18031). Mobile device manufacturers can have their products evaluated by an authorized lab to demonstrate their commitment to protecting users against cyber threats.

What is EU RED?

The EU's Radio Equipment Directive (RED) (2014/53/EU) establishes a regulatory framework for placing radio equipment on the market in the European Union. It aims to create a uniform regulatory framework for radio equipment within the internal market. The directive sets essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It applies to any equipment that uses radio technology to communicate, such as Wi-Fi™ printers, scanners, mobile computers, and IoT equipment.

What is EU CRA?

The EU Cyber Resilience Act (CRA) is a regulation that aims to improve the cybersecurity of products with digital elements that are placed on the market in the European Union. The CRA will require manufacturers to ensure their products are secure by design and by default, and to provide security support and software updates for a reasonable period. The Act will also introduce a CE marking for products that comply with its requirements, making it easier for consumers and businesses to identify secure products. The CRA is expected to apply to a wide range of products, including both hardware and software.

For more information, visit zebra.com/security