SAMSUNG

Samsung Secure Devices

Common Criteria and FIPS-validated devices for the security conscious.

In today's increasingly BYOD environment, security is paramount. Samsung is on the leading edge of defense-grade security, and we design our products to meet the most stringent security standards. Two of the most demanding sets of standards are Common Criteria and FIPS 140-2, used as the basis for government security up to Top Secret through the Commercial Solutions for Classified (CSfC) program. Samsung has achieved validation with many of its devices through each of these certification programs.

Samsung's concern for security encompasses both the hardware and the software. Our mobile devices incorporate leading security features from on-device encryption and secure data connectivity to protection by Samsung Knox. Trusted by governments around the world and voted "most strong" by Gartner[1], Knox delivers a holistic array of security enhancements from the hardware layer all the way to the application layer. With Samsung, you're protected from the moment you power on your device.

The Samsung Difference

Our intention is to have a growing portfolio of mobile devices that adhere to the most relevant security standards recognized by customers worldwide, including Common Criteria and FIPS 140-2, and to make our devices available for programs such as CSfC. To ensure Samsung Mobile devices remain the ideal choice for security-conscious customers, Samsung continually pursues validation against the most stringent certifications available. It's important to note that certifications awarded to Samsung are based on Samsung-specific enhancements; they are not obtained based on generic Android devices.

Samsung has been investing in our world-class security platform, Samsung Knox, and in our market-leading portfolio of mobile devices since the Samsung Galaxy S3. The result is our customers enjoy Samsung performance, reliability and ease of use along with advanced, defense-grade security. We're continually rethinking security, so that Samsung will remain the choice of enterprise for countless years and innovative products to come.

Contact Us: samsung.com/government

Knox

Common Criteria

The Common Criteria for Information Technology Security Evaluation, commonly referred to as Common Criteria, is an internationally recognized standard for defining security objectives of information technology products and for evaluating vendor compliance with these objectives.

The evaluation looks holistically at the entire product, from development/creation to physical delivery to end use by the customer, in order to establish the chain of trust for the mobile device.

Today, almost all evaluations are performed against a set of requirements laid out in a document called a Protection Profile (PP). The PP states exactly what the security services/features must be provided, such as requiring the user to log in with a password and enforcing parameters and consequences should the login fail (i.e., password requirements, failure scenarios, etc.).

Samsung targets three PPs: the Mobile Device Fundamentals Protection Profile (MDFPP) for the whole mobile device, the PP-Module for Virtual Private Network (VPN) Clients for secure data in transit, and the PP-Module for File Encryption and PP for Application Software combination for file encryption. These PPs have been created by the National Information Assurance Partnership (NIAP) to address the security requirements of mobile device use and data security within the enterprise.

Select Galaxy devices with Knox embedded have received Common Criteria (CC) certification. Samsung Knox is approved by the United States government as the first NIAP-validated consumer mobile devices to handle the full range of classified information. Additionally, all validated Samsung devices support using fingerprints as an approved authentication mechanism.

Knox File Encryption is designed to provide a second, independent layer of encryption for files inside the Knox Work Profile. This second layer of encryption is designed to meet the requirements of the NSA Data at Rest Capability Package as part of the CSfC program, allowing Top Secret data to be stored on a mobile device.

FIPS

Issued by the National Institute of Standards and Technology (NIST), the Federal Information Processing Standard (FIPS) is a US security standard that helps ensure companies that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information and controlled unclassified information (CUI) can make informed purchasing decisions when choosing devices to use in their workplace.

FIPS 140-2 (the current version) is a standard that specifies requirements for cryptographic modules. In other words, it validates that a mobile device uses and implements encryption algorithms correctly.

Samsung cryptographic modules are certified to the requirements for FIPS 140-2 Level 1.

To provide the basis for a broad set of functionality, including TLS, VPN, S/MIME and On-Device/File/SD Card Encryption, Samsung provides these certified modules as common low-level cryptographic libraries that can be used and reused by many different applications and services. All Samsung Knox services utilize these certified libraries.

In addition, Samsung utilizes the same module in multiple platforms without modification, allowing the devices to be FIPS-compliant without revalidating for each individual device.

Samsung Certified Devices

Listed devices also validated for the VPN Client and FIPS 140-2.

Common Criteria-Certified Devices, MDFPP v3

Supported on Android 10

- Samsung Galaxy S20 | S20+ | S20 Ultra
- Samsung Galaxy Z Flip
- Samsung Galaxy XCover Pro
- Samsung Galaxy XCover FieldPro
- Samsung Galaxy A51
- Samsung Galaxy S10e | S10 | S10+ | S10 5G
- Samsung Galaxy Note10 | Note10+ | Note10+ 5G
- Samsung Galaxy Fold | Fold 5G
- Samsung Galaxy S9 | S9+
- Samsung Galaxy Note9
- Samsung Galaxy Tab S6 | Tab S6 5G

Supported on Android 9

- Samsung Galaxy S9 Tactical Edition
- Samsung Galaxy S8 | S8+ | S8 Active
- Samsung Galaxy Note8
- Samsung Galaxy Tab S4
- Samsung Galaxy Tab S3
- Samsung Galaxy Tab Active2

Supported on Android 8

- Samsung Galaxy S7 | S7 edge | S7 active

Common Criteria-Certified Devices, File Encryption

- Samsung Galaxy S20 | S20+ | S20 Ultra
- Samsung Galaxy S10e | S10 | S10+ | S10 5G
- Samsung Galaxy Note10 | Note10+ | Note10+ 5G

For more information or to view the latest documentation on device software updates, please visit **samsung.com/us/knox** or contact a Samsung representative.

Samsung Galaxy Tab S6

Samsung Galaxy XCover Pro

Samsung Galaxy Note10

Samsung Galaxy S20 Ultra

Samsung Galaxy Z Flip

Learn More samsung.com/business insights.samsung.com samsung.com/government

Product Support 1-866-SAM4BIZ

Follow Us youtube.com/samsungbizusa @SamsungBizUSA

SAMSUNG | Knox

[1] Hevesi, P. "Mobile Device Security: A Comparison of Platforms." Gartner, Inc. https://www.gartner.com/doc/3276422/mobile-device-security-comparison-platforms.