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, and 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 29 governments 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. 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.

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 mobile device must provide, 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.).

The current CC certification targets the new Mobile Device Fundamentals Protection Profile (MDFPP) of the National Information Assurance Partnership (NIAP), which addresses the security requirements of mobile devices for use in 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 newly validated Samsung devices support fingerprint as an approved authentication mechanism.

In addition to the MDFPP validation, Samsung Mobile devices have also been validated against the Protection Profile for IPsec Virtual Private Network (VPN) Clients. Similarly developed by NIAP, this PP specifies the requirements for any IPsec VPN client, including FIPS 140-2 cryptography and enterprise-grade connectivity. This VPN client is available built-in on all MDFPP-validated devices with nothing else to install.

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

Samsung Knox meets the requirements for FIPS 140-2 Level 1 certification for both data-at-rest (DAR) and data-in-transit (DIT).

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

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 PP v1.4 and FIPS 140-2.

Common Criteria-Certified Devices, MDFPP v3

- Samsung Galaxy S8/S8+
- Samsung Galaxy S7/S7 edge/S7 active
- Samsung Galaxy S6/S6 edge/S6 edge+/S6 active
- Samsung Galaxy Tab S3
- Samsung Galaxy Note 5

MDFPP v3 is supported on Android 7

Common Criteria-Certified Devices, MDFPP v2

- Samsung Galaxy Note 4/Note edge
- Samsung Galaxy Tab S2 8" and 9.7"

MDFPP v2 is supported on Android 5 and Android 6

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 S3

Samsung Galaxy S8+

Samsung Galaxy S8

Samsung Galaxy S7 Active

Samsung Galaxy Note 5

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.