SAMSUNG

Samsung Devices

Validated through Common Criteria and FIPS

In today's mobile ecosystem, there are many types of certifications currently in the market. Of these, some of the most important are Common Criteria and FIPS. Samsung has vigorously pursued and achieved validation through each of these certification programs.

Samsung devices are also equipped with leading security features, including on-device encryption and secure data connectivity. Additionally, each device is protected by Samsung KNOX—a holistic array of security enhancements from the hardware layer all the way to the application layer.

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. A number of Governments use Common Criteria as the basis for their own certification schemes.

Instead of focusing just on the cryptography, 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 mobile device must accomplish, 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 overall evaluation ensures compliance against both the mobile device documentation as well as the mobile device itself to verify that stated requirements are met.

Select Galaxy devices with KNOX embedded received Common Criteria (CC) certification. 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 enterprise. 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.

The MDFPP is continually updated to both take advantage of the latest technology and meet the needs of government users. Samsung actively participates in the communities related to mobility to drive this change and ensure our products are matched to the government's needs.

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.

Common Criteria evaluates not only encryption capabilities but also other components within the device, ensuring that it meets stated regulatory requirements and is secure as a whole.

Current Samsung Certified Devices

MDFPP v2
Common Criteria-Certified Devices

- Samsung Galaxy S7
- Samsung Galaxy S7 Edge
- Samsung Galaxy S6
- Samsung Galaxy S6 Edge
- Samsung Galaxy S6 Edge+
- Samsung Galaxy Note5
- Samsung Galaxy Note Edge
- Samsung Galaxy Note 4
- Samsung Galaxy Tab S2 8" and 9.7"

Devices listed are the most current, and are also validated to the VPN PP v1.4.

Common Criteria is supported from Marshmallow (Android OS 6) to KitKat (Android OS 4.4).*

*In order to confirm the device contains the version that supports Common Criteria, please go to Settings > About phone > "Security software version." For more information or to view the latest documentation on device software updates, please visit samsung.com/us/knox or contact a Samsung representative.

Contact us
1-866-SAM4BIZ
samsung.com/us/business

Follow us
youtube.com/samsungbizusa
@SamsungBizUSA

SAMSUNG Knox

Samsung Devices

Validated through common criteria and FIPS

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

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.

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. In this particular case, as the operating system evolves, these modules are not modified, and the mobile device still keeps the certification valid.

The Samsung difference

In order to make sure that the extensive security enhancements made to Samsung Mobile devices are suitable for security-conscious customers, Samsung will continue to pursue validation against the most stringent certifications available in the market today. Our intention is to have a continually growing portfolio of mobile devices that adhere to the most relevant security standards recognized by customers worldwide, including Common Criteria and FIPS.

It's very 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. And we will continue to do so for countless years and innovative products come. Our customers will enjoy the ease of use they have come to expect on Samsung devices without having to compromise security.

FIPS-compliant devices

- Samsung Galaxy S7
- Samsung Galaxy S7 Edge
- Samsung Galaxy S6
- Samsung Galaxy S6 Edge
- Samsung Galaxy S6 Edge+
- Samsung Galaxy Note5
- Samsung Galaxy Note Edge
- Samsung Galaxy Note 4
- Samsung Galaxy Tab S2 8" and 9.7"

FIPS is supported from Marshmallow (Android OS 6) to KitKat (Android OS 4.4).

Samsung Galaxy Tab S2 8"

Samsung Galaxy Tab S2 9.7"

Samsung Galaxy Note Edge

Samsung Galaxy Note5

Samsung Galaxy S7

Samsung Galaxy S7 edge

Learn more samsung.com/us/business
Product support 1-800-SAMSUNG 1-866-SAM4BIZ
Follow us youtube.com/samsungbizusa @SamsungBizUSA

SAMSUNG Knox | SAMSUNG