SAMSUNG

Samsung Devices—Now 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 certification evaluates a mobile device from the outside in, looking at where and how it will be used and then measuring it to see that it provides an adequate level of security for the stated purpose.

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.

In the case of Samsung Mobile devices, Common Criteria validation was performed against the Mobile Device Fundamentals Protection Profile (MDFPP). The MDFPP was developed by the National Information Assurance Partnership (NIAP). Under this baseline security definition for mobility, part of the FIPS 140-2 validations is also integrated, as per international specifications.

The MDFPP is continually evolving, with updates being driven in large part through Samsung efforts, to better meet the needs of government users.

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 an 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.

Common Criteria-Certified Devices:

- Samsung Galaxy S® 4
- Samsung Galaxy Note® 3
- Samsung Galaxy Note® Pro 12.2
- Samsung Galaxy S® 5
- Samsung Galaxy Note® 10.1 2014 Edition

Common Criteria is available in the second release of KitKat (Android™ OS 4.4).[1]

[1]In order to confirm if the device contains the version that supports Common Criteria, please go to: Settings > About phone > "Security software version." The version listed needs to state "MDF v1.0 Release 3." For more information, please visit www.samsung.com/us/knox or contact a Samsung representative.

Galaxy S 4

Galaxy S 5

Galaxy Note 3

Galaxy Note 10.1 2014 Edition

Galaxy Note Pro 12.2

FIPS

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.

FIPS-Compliant Devices:

- Samsung Galaxy S® 4
- Samsung Galaxy S 4 Active®
- Samsung Galaxy S® 5
- Samsung Galaxy Note® 3
- Samsung Galaxy Note® Pro 12.2
- Samsung Galaxy Note® 10.1 2014 Edition

FIPS is supported with the KitKat update (Android OS 4.4).

The Samsung Promise

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 will continue to invest in our world-class security platform, Samsung Knox, and in our market-leading portfolio of mobile devices for years to come. Our customers will enjoy the ease of use they have come to expect on Samsung devices without having to compromise security.

Samsung Knox

SAFE SAMSUNG FOR ENTERPRISE

SAMSUNG