STANDARDS AND CERTIFICATIONS FOR HSM DEVICES

CC, FIPS or something else…?

There is no simple way to determine which certified product is the absolute best, which one you need for your organization and its processes. Different solutions are required in different regions and different use cases. However, understanding the background and the details of the most common standards and certifications can make the choice easier.

What are certifications and why they are necessary?

In the IT world, certifications demonstrate that a product is compliant with specific, strict requirements compiled by trusted organizations. The solutions are examined and tested in accredited laboratories with several methods, including independently validated quality and performance tests. These have to be done by experts thoroughly independent from the developer of the tested product. After these tests, appropriate government agencies also examine the results of the evaluation before the certification is achieved.

This method ensures that the product works exactly as the vendor claims it does while meeting strict criteria. The gained certification is to assure customers of it, removing the burden of comprehensive product evaluations from the shoulders of project managers or decision makers in charge of purchases.

Where are certifications required?

Government agencies in many countries are obliged to purchase and use IT products that earned specific certifications. For example, FIPS 140-2 is mandated in the US for many federal agencies using cryptographic-based security systems to protect sensitive information in computer and telecommunication systems, while in many European countries, Common Criteria certifications are required in such cases.

A great number of public organizations also choose to buy solutions with such certifications in order to ensure the security and reliability of the purchased product.

How can a product be certified?

Achieving a certification is a complicated, expensive, and time-consuming process for the manufacturer of the product, and it requires strict documentation, testing, and consultation efforts.

First, the company needs to develop a product that can perform the tasks and functions listed in the requirements of the certification. Then a detailed documentation is prepared, which describes the features and operations the product can run, while confirming that it meets the necessary criteria for them. A developer may choose to use third party services to help preparing for the validation processes, which might save costs and efforts in the long run.

As mentioned before, the solution then needs to be tested by several engineers in an independent, accredited laboratory. After the successful evaluation of the laboratory, the results of the evaluation have to be examined and validated by the appropriate government agency as well.

After successfully completing these steps, the product receives the certificate and it is added to the official list of certified solutions (e.g. the list of FIPS validated modules[1] and the list of CC certified products[2]).

Many organizations choose to purchase a product that has one of the most common certifications to make sure the solution is secure, but then use them with the latest software version that has not yet been certified. This option is only available for organizations that are not obliged to use products with specific certificates, otherwise this means an actual violation of the law.

An important note: A certification is only valid for the exact same version of the solution that has been evaluated and certified. In case the vendor issues any updates or bug fixes for the product, those changes also need to be evaluated to maintain the certified status of the upgraded product. This process is usually shorter than the evaluation of the entire product, however, it might still take several months.

The most common certifications for cryptographic modules

In case of cryptographic modules, companies can rely on two certificates: FIPS 140 and Common Criteria (in some cases, financial institutions have to comply with PCI DSS as well).

FIPS 140-2 and 140-3

The Federal Information Processing Standard Publication 140-2 (FIPS 140-2)[3], is a US government computer security standard used to approve cryptographic modules. It was first published on May 25, 2001 by the National Institute of Standards and Technology. On March 22, 2019, FIPS 140-3[4] was approved to succeed FIPS 140-2. Validated through the Cryptographic Module Validation Program (CMVP), FIPS 140-3 testing will begin on September 22, 2020. After FIPS 140-3 testing begins, FIPS 140-2 testing will continue for at least a year, making the two standards to coexist for some time.

The FIPS 140 standard coordinates and determines the requirements for cryptography modules that include both hardware and software components. The standard defines four levels of different security aspects (see box for physical security) to cover a wide range of potential applications and environments. Although it is a federal standard used in the US and Canada, FIPS 140 compliance has been widely adopted around the world in both governmental and non-governmental sectors.

Requirements for FIPS 140 levels:

Level 1: production-grade equipment

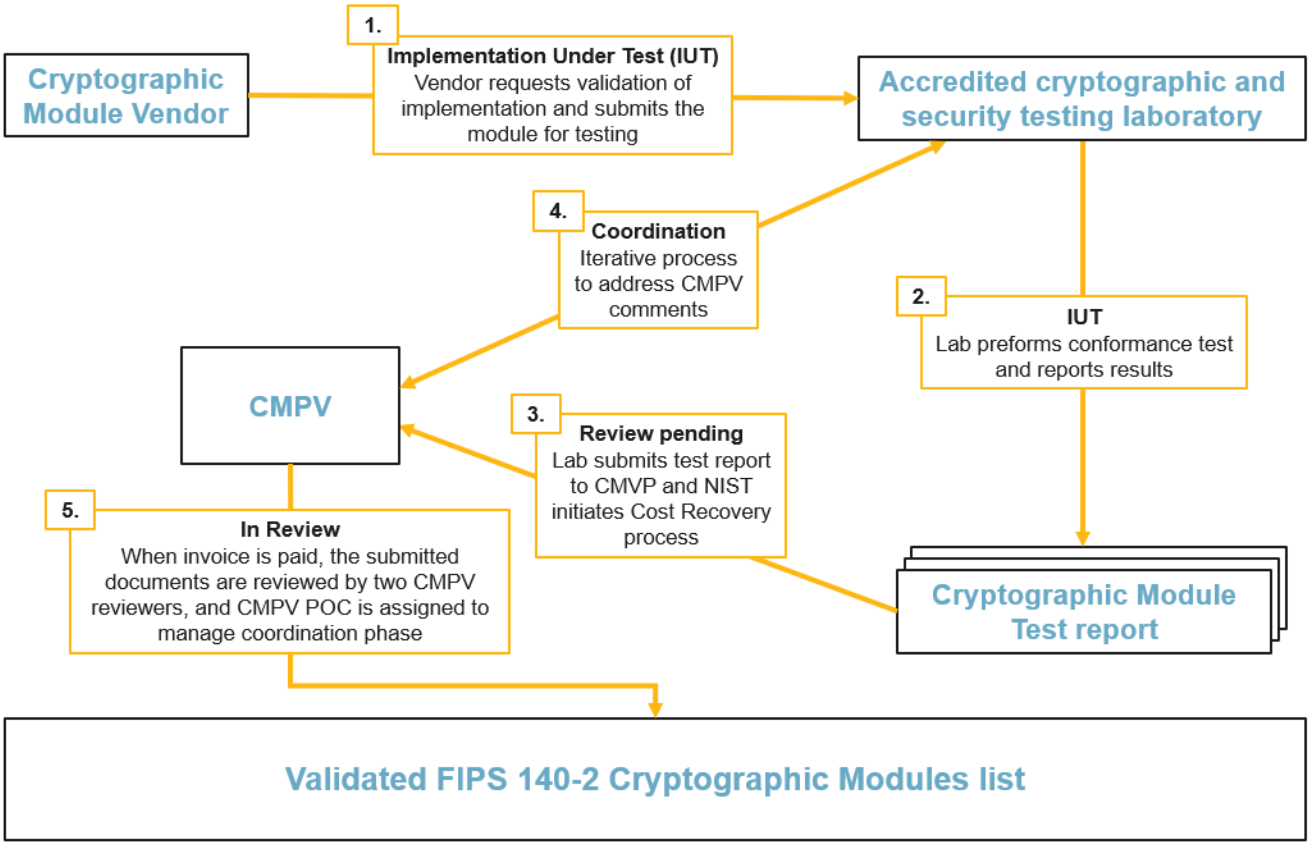
Level 2: Level 1 + physical tamper-evidence

Level 3: Level 2 + Tamper detection and response for covers and doors

Level 4: Level 3 + Tamper detection and

[1] see: https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules
[2] see: https://www.commoncriteriaportal.org/products/
[3] see: https://csrc.nist.gov/publications/detail/fips/140/2/final
[4] see: https://csrc.nist.gov/publications/detail/fips/140/3/final

Evaluation processes for FIPS 140-2 certifications


Cryptographic Module Vendor
1.
Implementation Under Test (IUT)
Vendor requests validation of implementation and submits the module for testing
Accredited cryptographic and security testing laboratory
4.
Coordination
Iterative process to address CMPV comments
2.
IUT
Lab preforms conformance test and reports results
CMPV
3.
Review pending
Lab submits test report to CMVP and NIST initiates Cost Recovery process
5.
In Review
When invoice is paid, the submitted documents are reviewed by two CMPV reviewers, and CMPV POC is assigned to manage coordination phase
Cryptographic Module Test report
Validated FIPS 140-2 Cryptographic Modules list

[5]

[5] source: https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing

Common Criteria

The Common Criteria for Information Technology Security Evaluation (Common Criteria or CC in short)[6] is an international standard (ISO/IEC 15408) for computer security certification. It provides a framework in which computer system users can specify their security requirements through different Protection Profiles (PP) for different products, using different documents and assurance and functional requirements[7]. This way, vendors can implement the determined security features in their products, and accredited testing laboratories can evaluate the products to ensure their performance at the required levels.

While FIPS 140 is a standard for cryptographic modules, CC covers a wide range of IT security solutions from smart cards to digital signature related devices. User communities create Protection Profiles for each of these areas, detailing their security needs for the variety of solutions. Product vendors can certify their solutions against one or several PPs, making selection process easier for customers, as they can purposefully look up certain types of products by their compliance to the PPs in question.

The solutions can be evaluated in different levels of depth and rigor and this is described by the Evaluation Assurance Levels (EAL) ranging from 1 to 7 (see box[8]). Each EAL corresponds to a package of security assurance requirements, which covers the complete development of a product with a given level of strictness. In this case, the level refers to the expected thoroughness of the laboratory's work during the evaluation – as opposed to FIPS 140-2 where the level describes the strength of security. A + mark after the EAL level indicates that the certified product not only fulfils the requirements specified at the level but meets requirements from higher packages.

Evaluation Assurance Levels:

EAL1 (Functionally Tested): Applicable when there is some need of assurance in the correct operation, but security threats are not viewed as serious

EAL2 (Structurally Tested): Applicable when a low to moderate level of independently assured security is required, while lacking availability of the complete development record. An example can be when securing legacy systems

EAL3 (Methodically Tested and Checked): Applicable when a moderate level of independently assured security is required along with a thorough investigation of the TOE and its development without massive re-engineering.

EAL4 (Methodically Designed, Tested and Reviewed): This level enables the maximum assurance from positive security engineering which are rigorous, but do not require substantial specialist knowledge or resources. It is applicable when a moderate to high level of independently assured security is required in conventional commodity TOEs and additional security-specific engineering costs might be incurred.

EAL5 (Semi-formally Designed and Tested): Applicable when a high level of independently assured security is required in a planned development and a rigorous development approach is needed without incurring unreasonable costs attributable to specialist security engineering techniques.

EAL6 (Semi-formally Verified Design and Tested): Applicable in high risk situations where the value of the protected assets justifies the additional costs.

EAL7 (Formally Verified Design and Tested): Applicable in extremely high-risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

[6] see: https://www.commoncriteriaportal.org/
[7] source: https://en.wikipedia.org/wiki/Common_Criteria#Key_concepts
[8] source: https://en.wikipedia.org/wiki/Evaluation_Assurance_Level

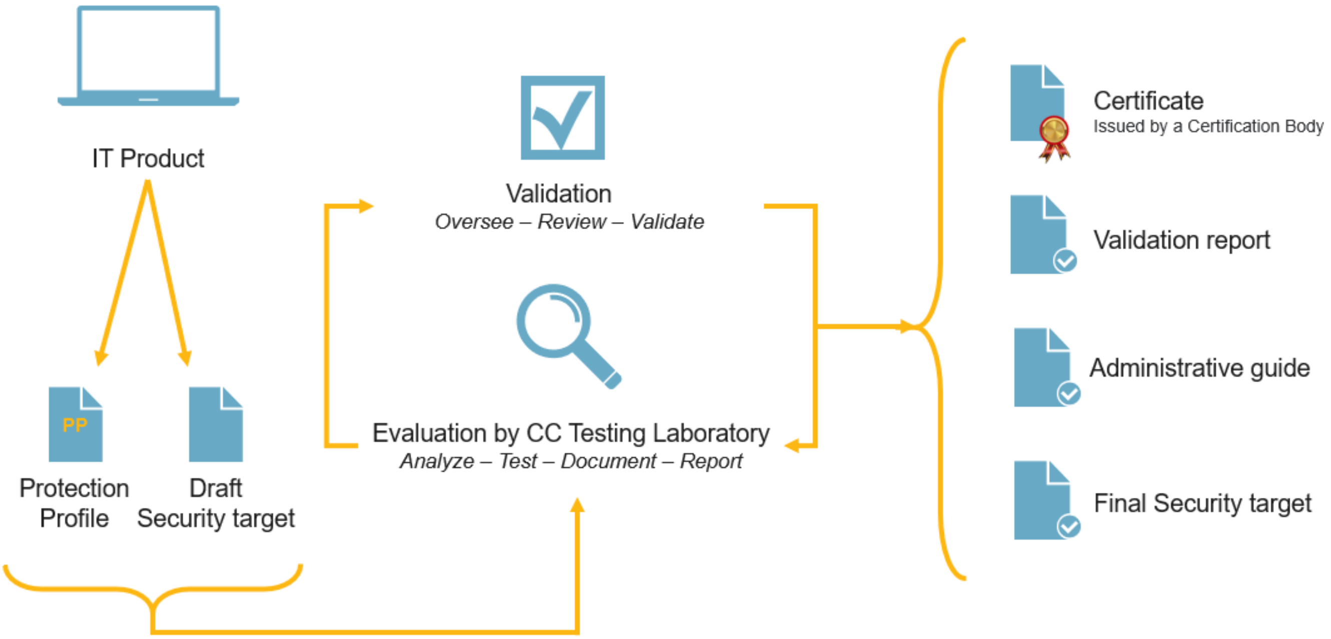
Some national evaluation schemes only accept products for evaluation which claim a strict conformance with an approved PP.

When an organization is assessing a product and its certifications' value, they should consider the PP, the EAL and in some cases the strict conformance as well.

For example, TRIDENT HSM and SAM, developed by i4p has achieved Common Criteria EAL 4+ certification (EAL4 augmented by AVA_VAN.5 and ALC_FLR.3) meeting both the Protection Profile for Cryptographic Module for Trust Services[9] and the Protection Profile for QSCD for Server Signing[10] with strict conformance.

This counts as a highly valuable certificate and only a handful of products own it on the market.

Evaluation processes for Common Criteria certifications



Documents:

- **Protection Profile:** An implementation independent set of security requirements for a category of IT products that meet specific consumer needs.
- **Security target:** Specification of the security functions against which the IT product, i.e., the target of evaluation (TOE), will be evaluated and as a description relating the product to the environment in which it will operate.
- **Administrative Guidance:** Instructions to users on how to configure the product so that it is consistent with the evaluated configuration.
- **Assurance Activity Report:** Summarized assurance activities of the product evaluation.

[9] EN 419221-5:2018

[10] EN 419241-2:2019

Which certification is better?

In most aspects, the two certificates require the same security features and assurances. Basically, if a product has a CC EAL 4+ certificate for the PP for Cryptographic Module for Trust Services, it provides around the same functionality as a product with a FIPS 140-2 Level 3 certificate.

However, organizations need different specifications and certificates for different use cases. For example, to create qualified electronic signatures, one needs a qualified signature creation device (QSCD) and is required to use a device that is on the eIDAS Futurium list[11]. The process for getting the required certification is currently the following: the device should be assessed by a conformity assessment body[12] who are using similar, but independent, so called alternative processes[13]. These alternative processes may also require Common Criteria certificates, more precisely the product should claim conformance to a specific Protection Profile.

If an organization wants to create qualified electronic signatures remotely, they are obliged to use a QSCD that can prove conformance to two Common Criteria Protection Profiles (EN 419221-5: Protection Profile for Cryptographic Module for Trust Services and EN 419241-2: Protection Profile for QSCD for Server Signing).

In case an organization needs electronic signatures to assure the integrity of their data, they are required to use a general purpose HSM that has one of the related security certifications: CC EAL4+ (PP: EN 419221-5:2018) or FIPS 140-2 Level 3. Such a device is required if the organization uses encryption to protect sensitive data.

Since Trident HSM has a Common Criteria EAL 4+ certification meeting both the Protection Profile for Cryptographic Module for Trust Services and the Protection Profile for QSCD for Server Signing, it can be used for all the purposes above.

Financial institutions need special payment HSMs to protect payment systems from breaches and theft of cardholder data that has a PCI DSS certification.

[11] see: https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
[12] see: https://ec.europa.eu/futurium/en/system/files/ged/list_of_eidas_accredited_cabs-2019-11-28.pdf
[13] see: https://ec.europa.eu/futurium/en/system/files/ged/list_of_alternative_processes_27032020_0.pdf