The most widely recognized security validation for Cryptographic Modules

What is the FIPS 140-3?

FIPS (Federal Information Processing Standard) 140-3 is the standard for validating the effectiveness of cryptographic modules.

Although FIPS 140-3 is a U.S./Canadian Federal standard, FIPS 140-3 compliance has been widely adopted around the world in both governmental and non-governmental sectors as a practical security benchmark and realistic best practice.

FIPS 140-3 is based on ISO/IEC 19790, an international standard. Several countries also issue certificates according to ISO/IEC 19790.

Organizations use the FIPS 140-3 standard to ensure that the hardware, software or firmware they select meets specific security functional requirements and approved algorithms.

How does it work?

The FIPS 140-3 certification standard defines four increasing, qualitative levels of security:

Level 1: Validation of at least one approved algorithm or security function. Requires explicit or implicit authentication, production-grade components and functional testing.

Level 2: Requires role-based authentication and physical security requirements for tamper evidence.

Level 3: Requires identity-based authentication.

Adds requirements for physical tamper-resistance and environmental conditions for temperature and voltage. Trusted channel for the transmission of unprotected key material.

Level 4: Requires multifactor-based authentication. Adds requirements for tamper detection and response envelope, EFP and fault injection mitigation.

What is tested in FIPS 140-3?

Each one of the FIPS 140-3 levels focuses on eleven functional areas of product security related to secure design and implementation.

At each level, greater amount of evidence and engineering is required from the product manufacturer in order to show compliance with the standard.

The functional areas that must be addressed are:

1. Cryptographic module specification
2. Cryptographic module interfaces
3. Roles, services, and authentication
4. Software/Firmware security
5. Operational environment
6. Physical security
7. Non-invasive security
8. Sensitive security parameter management
9. Self-tests
10. Life-cycle assurance
11. Mitigation of other attacks

Certifying your Cryptographic Module with DEKRA

We understand that achieving FIPS 140-3 Certification represents a significant investment by our customers.

We help our clients to gain a FIPS 140-3 certificate as quickly as possible (on time and on budget).

Our validation procedures are fully optimized to minimize the impact on our customers' resources.

We run fast and smooth testing processes.

Why DEKRA

DEKRA Security Lab is one of the few security laboratories accredited by the NIST to perform validation of cryptographic modules under FIPS 140-3. (Twenty laboratories worldwide, at the time of writing).

DEKRA Security lab performs FIPS 140-3 evaluations and supporting services, for the NIST Certification Scheme in the US.

DEKRA Testing & Certification S.A.U.
Parque Tecnológico de Andalucía
C/ Severo Ochoa, 2 & 6
29590 Málaga - Spain
Tel: + 34 952 61 98 20

wireless.global.es@dekra.com
https://www.dekra-product-safety.com/en/programs/cyber-security