unbound security

FIPS 140-2 Certification Levels

Security and Compliance Considerations

March 2021

FIPS 140-2 Certification Levels – Background

The FIPS (Federal Information Processing Standard) 140-2 standard was originally published in 2001 by the US NIST (National Institute of Standards and Technology), with the purpose of assessing the security level of cryptographic modules, namely their ability to protect the confidentiality and integrity of cryptographic keys. Since then, it has been widely adopted around the world as a practical security benchmark and realistic best practice, by various governmental and private sector organizations.

There are 4 levels within FIPS 140-2; each increase in level represents an increasing level of rigor and qualitative security. FIPS 140-2 levels 2, 3, 4 require physical security. This entails tamper detection and tamper response in case an attacker obtains physical access to the cryptographic module.

The FIPS 140-2 certification criteria are based on the IT environment and technologies available at the time it was conceived, nearly twenty years ago. The digital IT transformation has greatly impacted the security threat environment across all networks and devices, with implications for cryptographic modules as well.

Changes in the Cyber Threat Landscape

The advancement of data center, networking, cloud, and mobility infrastructures has completely changed the cyber threat landscape in the 21st century.

Modern cloud and data center environments typically employ meticulous access control and strong physical security while compute and storage resources are shared over the network, particularly the over the Internet. Thus, the risk of physical access to servers and physical tampering by attackers is low. The risk of software attack or compromise, on the other hand, is of much greater concern. Remote software attacks have become the principal attack vector, with attackers adopting increasingly sophisticated tactics and technologies.

The risk of physical attacks is more of a concern today mainly for endpoint devices because they are mobile and dispersed by design.

Unbound CORE: FIPS Certified Solution Addressing Modern IT Needs

Unbound CORE has received FIPS 140-2 Level 1 & 2 certification by the US National Institute for Standards and Technology (NIST).

CORE is a combined key protection, key management, and cryptographic mesh solution, the first to offer physical HSM-level security and beyond purely in software, as well as unified lifecycle management of keys across any on-premises or cloud infrastructure.

Unbound solutions offer a security guarantee on par with FIPS 140-2 Level 3 certified modules, with added security benefits that were designed for the modern digital IT environment.

Compliance Comparison: Unbound CORE and FIPS 140-2 Level 3 Certified HSM

In order to become certified according to FIPS 140-2, the cryptographic module under test must satisfy 11 requirements sections (see table below for detail). The security requirements cover areas related to the secure design and implementation of the cryptographic module. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules' compliance with FIPS 140-2, while the final certification level is the minimal level of accreditation achieved in each of the 11 requirement sections (i.e., if a certain cryptographic module passed 10 requirement sections as Level 3 and one as Level 2, the overall certified level would be Level 2).

CORE practically meets all FIPS 140-2 Level 3 security requirements, however officially it cannot be certified Level 3 as these requirements cannot be fulfilled without hardware-based tamper response mechanisms.

The following table summarizes FIPS 140-2 requirements and Unbound Key Control compliance compared with a FIPS 140-2 Level 3 HSM.

FIPS 140-2 Requirement	FIPS 140-2 Level 3 HSM	Unbound CORE
Cryptographic Module Specification - Specification of cryptographic module and boundary, approved algorithms, and modes of operation. Description of cryptographic module (HW, SW and firmware). Statement of module security policy.	Level 3	Level 3
Finite State Model - Specification of the various operational states of the cryptographic modules and transitions between states.	Level 3	Level 3
Self-Tests – Power-up self-tests are performed when the cryptographic module is powered up (power-up test, cryptographic algorithm test, software/firmware integrity test, critical functions test). Conditional self-tests are performed when an applicable security function or operation is invoked.	Level 3	Level 3
Mitigation of Other Attacks - Specification of mitigation of attacks for which no testable requirements are currently available.	Level 3	Level 3
Cryptographic Key Management - Security requirements encompassing the entire lifecycle of cryptographic keys and key components employed by the cryptographic module. Key management includes random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization. Level 1 & 2 - Secret and private keys established using manual methods may be entered or output in plaintext form; Level 3 & 4 - Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	Level 3	Level 3

Cryptographic Module Ports and Interfaces - Requires restriction of all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module. Level 1 & 2 - required and optional interfaces, specification of all interfaces and of all input and output data paths; Level 3 & 4 - data ports for unprotected critical security parameters logically or physically separated from other data ports.	Level 3	Level 3
Roles, Services and Authentication - Support for authorized roles for operators and corresponding services within each role. Level 1 - logical separation of required and optional roles and services; Level 2 - role-based or identity-based operator authentication; Level 3 & 4 - identity-based operator authentication.	Level 3	Level 3
Design Assurance - Use of best practices by the vendor during the design, deployment, and operation of a cryptographic module, providing assurance that the module is properly tested, configured, delivered, installed, and developed, and that the proper operator guidance documentation is provided.	Level 3	Level 3
Physical Security -- Use of physical security mechanisms to restrict unauthorized physical access to the module's contents and to deter unauthorized use or modification of the module when installed. Level 1 - production grade equipment; Level 2 - locks or tamper evidence; Level 3 - tamper detection and response for covers and doors; Level 4 - tamper detection and response envelope, Environmental Failure Protection or Environmental Failure Testing.	Level 3	Level 2
EMI/EMC - Specification of EMI/EMC requirements. Level 1 & 2 - 47 CFR FCC Part 15, Subpart B, Class A (Business use). Applicable FCC requirements (for radio); Level 3 & 4 - 47 CFR FCC Part 15, Subpart B, Class B (Home use).	Level 3	Level 2
Operational Environment - Requirements related to the management of the software, firmware, and/or hardware components required for the module to operate. Level 1 - single operator, executable code, approved integrity technique; Level 2 -- referenced protection profiles evaluated at Common Criteria EAL2 with specified discretionary access control mechanisms and auditing; Level 3 - referenced protection profiles plus trusted path evaluated at EAL3 plus security policy modelling, Level 4 - referenced protection profiles plus trusted path evaluated at EAL4.	N/A (see below)	N/A (see below)

The following requirements sections are met with **CORE via the implementation topology and underlying server hardware**:

- *Physical security* -- Tamper detection and response for covers and doors -- not applicable for software. The UKC security guarantee comes from the use of secure multiparty

computation (MPC) on multiple highly segregated machines holding random key shares, rather than physical security on a single machine where key material exists in full.
- *EMI/EMC* – An environmental, non-security related (i.e., TEMPEST) requirement related to electromagnetic radiation – not applicable for software.
- *Operational environment* – Relevant to modifiable operating system (OS) only – Unbound provides CORE with a non-modifiable hardened OS (hardening guidelines available for other OSs if needed.)

FIPS 140-2 Level 3 Security and Beyond

Unbound CORE also offers unique security benefits that no other FIPS level 3 or higher certified module delivers.

Eliminating the Single Point of Failure

With CORE, physical tampering on one machine gives no information on keys. Physical key theft or misuse would require physical access to all CORE nodes simultaneously. When CORE is deployed with a high level of segregation between nodes placed in physically secured environments, physical security is even higher than FIPS 140-2 level 3. In a similar fashion, a software-based attack would require simultaneous failure of all CORE nodes, which is extremely difficult when a high level of segregation is implemented.

Key Control and Protection in External IT Environments

The transition from on-premises to external infrastructure has resulted in another source of risk: a third party can gain access to an organization's cryptographic keys (i.e., following subpoena/warrant or a rogue employee). Splitting CORE nodes between multiple external infrastructure vendors (e.g., multiple cloud IaaS providers) or between external and on-premises guarantees that third-party vendors never have access to keys and thus cannot expose them.

Crypto-agility

A benefit of Unbound solutions vs. hardware cryptographic modules is the ability to quickly add support for new cryptographic algorithms and fix discovered vulnerabilities via software upgrade.

Key Usage Monitoring, Validation and Enforcement

In addition to protecting the cryptographic keys at rest, there is a strong need to monitor and enforce policies on the keys' usage through the key lifecycle (generation, distribution, usage, storage, rotation, backup and destruction), to prevent key compromise. Addressing this risk requires detection and response mechanisms that are not typically considered in the design of hardware cryptography solutions. This is detrimental for cryptography use case where even a single malicious key usage can lead to significant negative ramifications, e.g., with code signing, root CA or cryptocurrency.

Unbound enables advanced real-time monitoring by utilizing a module that can correlate and control the usage of keys within CORE, according to certain parameters such as threshold, low & slow, gradual change over time, crypto-commands analysis, users' commands, etc., and alert accordingly. Such functionality allows detection and prevention of malicious usage, or breach attempts of attackers, rogue insiders or well-meaning employees that make honest mistakes.

Summary

The FIPS 140-2 certification provides vital assurance that cryptographic modules meet industry-accepted standards for protecting keys. Alongside with compliance with FIPS requirements, organizations deploying cryptographic products should evaluate their practical security capabilities and alignment with a modern IT architecture.

The IT revolution has greatly impacted the threat landscape across all networks and devices, and mandates a new approach to security, with implications for cryptographic modules as well. Protection of keys in untrusted environments, crypto-agility, and real-time detection and response to potential key misuse are examples of emerging security needs that require consideration.

Leveraging secure multiparty computation (MPC) technology, Unbound CORE serves as a first-ever pure-software cryptographic module that delivers security on par with FIPS 140-2 level 3, as well as additional unique security benefits.

unbound security

In a world moving towards everything encrypted, signed, and authenticated — secure and operationally efficient cryptographic infrastructure is an absolute must for enterprises. Our vision at Unbound is to be the global cryptographic orchestration platform of choice for the enterprise. By leveraging the latest advancements in multi-party computations, our platform is the industry choice to secure the world's largest banks and Fortune 500 companies. With a headquarters in New York, and an EMEA office in Tel Aviv, Unbound provides the cryptographic orchestration platform that enables enterprises worldwide to easily secure and manage all their information and crypto assets.