Security Requirements for Crypto Devices

Version 2.2

28 Nov 2024

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	Security Requirements for Crypto devices
Status	Release
Version	2.2
Last update	28.11.2024
Document Owner	Controller of Certifying Authorities, India

Contents

1   Introduction

The X.509 Certificate Policy for India PKI mandates that the private key of a subscriber should be stored within a Hardware Cryptographic Module which has been validated to FIPS 140-2/3 Level 2 or higher for class 2 and class 3 DSCs.

This document defines the security requirements for crypto devices used by the end users in performing digital signature functions. In this document, a crypto device is referred to as a PKI Smart card or a PKI crypto token.

Purpose

The purpose of this document is to specify the requirements for crypto devices to be used in carrying out digital signatures in India.

Scope

The scope of this effort is limited to crypto devices and includes all hardware, firmware and software embedded in the Cryptographic boundary. The scope of this effort also includes conditional requirements, i.e., requirements that must be met if certain conditions hold true.

Terminologies and definitions

Cryptographic boundary: A defined perimeter that establishes the boundary of all hardware, software, or firmware components that collectively implement the cryptographic functions within a cryptographic module.

Cryptographic module: A cryptographic module comprises hardware, software, and/or firmware that implements approved security functions, including cryptographic algorithms and key generation.

Software: the programs and data components within the cryptographic boundary, usually stored on erasable media, that can be dynamically written and modified during execution.

Firmware: the programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

Operating system: The operating system controls or allows the execution of software or firmware on the computing platform, including any virtual machines or runtime environments (e.g., Java Runtime Environment - JRE) within the cryptographic boundary

A limited operational environment is a static, non-modifiable virtual environment (e.g., a JAVA virtual machine on a non-programmable PC card) with no underlying general-purpose operating system.

CSP(critical security parameter): security-related information whose disclosure or modification can compromise the security of a cryptographic module. e.g. Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors

Hardware: physical equipment/components within the cryptographic boundary used to process programs and data

Crypto Device: The term "Crypto device" in this document refers to a complete crypto device or a device that utilizes only a validated crypto module as sub-component to perform its cryptographic functions.

2   Crypto device requirements

This section contains the mandatory requirements for cryptographic devices and ways to test each of the requirements.

For a device that utilizes only a validated sub-component to perform its cryptographic functions, the scope will be limited to the validated sub-component.

2.1   Functions Prior to User Authentication:

The functions that can be performed before user authentication shall:
   a) be limited to access and use of public information such as examination of public key certificates; and

   b) Shall not include any access or operation involving private or secret key operations.

> **Compliance requirements**
>
> FIPS 140-2/3 does not contain the notion of functions that can be performed prior to authentication explicitly.
>
> An analysis must be conducted of functions that can be performed prior to authentication to ensure that they meet the requirements stated above.
>
> Functional security testing must be conducted using the functional specification to confirm that no other functions can be performed prior to authentication other than those listed in the documents.

2.2   User Authentication:

User Authentication mechanism shall meet the following requirements:
   a) Authentication mechanism shall be such that a random guess has less than 1 in 1,000,000 probability of success.

b) Authentication mechanism shall be such that multiple random guesses in any one-minute interval shall have less than 1 in 100,000 probability of success.

c) Authentication information stored on the crypto device in any form (e.g., plaintext, cryptographic hash, encrypted) shall be protected from unauthorized access or modification in order to protect from offline dictionary attacks.

d) In order to prevent unauthorized access, the mechanism should also have a provision to disable access to the file system of PKI Crypto device / Crypto token after a pre-defined unsuccessful attempt of user authentication. The maximum number of such attempts shall not be more than 10.

Compliance requirements

Requirements are fully addressed by FIPS 140-2/3. Thus, no additional analysis is required for FIPS 140-2/3 Level 2 or higher validated products for a, b & c. The implementation of d should be verified

---

2.3 Physical Security:

The cryptographic devices shall be designed to either detect physical tampering or to zeroize upon physical tampering. Physical tamper detection can be implemented on the cryptographic device or the cryptographic module.

The cryptographic devices shall successfully undergo the process of the Cryptographic Module Validation Program (CMVP) of FIPS 140-2/3, Security Requirements for Cryptographic Modules. These Security requirements cover different areas related to the design and implementation of a cryptographic module. A copy of such validation certificate shall be submitted by the crypto device vendor.

Compliance requirements

Requirements are fully addressed by FIPS 140-2/3. Thus, no additional analysis is required for FIPS 140-2/3 Level 2 or higher validated products.

2.4 Cryptographic Algorithms:

The cryptographic device shall successfully undergo the FIPS Cryptographic Algorithm Validation Program (CAVP) for each FIPS algorithm claimed to be implemented. If the cryptographic module

generates keys for a FIPS algorithm, the crypto device shall also successfully undergo FIPS CAVP for key generation for that algorithm.

> **Compliance requirements**
>
> This requirement must be satisfied using the CAVP algorithm certificate. However, The cryptographic device shall support either ECC or RSA or both as per the key length specified in the IOG issued by CCA.

2.5 Key Entry:

The cryptographic module shall only import keys into the crypto device in encrypted form. The encryption mechanism and key encrypting keys shall be at least as strong as the key being imported.

> **Compliance requirements**
>
> FIPS 140-2/3 addresses the key entry requirement but does not address the security strength of the keys.   For the FIPS 140-2/3 validated products, it would be sufficient to examine if the cryptographic algorithms and key size used for encrypting the keys are commensurate with the key being entered.

2.6 Key Output:

The cryptographic device shall be pre-configured to make private keys non-exportable in any form.

> **Compliance requirements**
>
> FIPS 140-2/3 addresses the key output requirement but does not address disabling the option of exporting the keys. This functionality should be verified.

2.7 Key Zeroization:

The crypto device shall provide a mechanism to zeroize the card by zeroizing all keys, passwords, PINs, seeds, etc., held on the crypto device.

> **Compliance requirements**
>
> FIPS 140-2/3 addresses this requirement.

2.8   Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC):

The cryptographic device shall conform to the EMI/EMC requirements specified by the United States 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use)

> **Compliance requirements**
>
> FIPS 140-2/3 addresses this requirement.

2.9   Power Up Self-Tests:

The cryptographic device shall undergo self-tests during power-up to ensure that the underlying hardware is operating correctly.

> **Compliance requirements**
>
> FIPS 140-2/3 addresses this requirement indirectly by specifying a list of tests for cryptographic operations.

2.10   Interface Specification:

The product documentation shall describe all interfaces to the cryptographic module, including Application Programming Interfaces (APIs). The API shall describe each interface in full detail including, function call, description of the function, inputs, outputs, errors and exceptions, and side effects.

> **Compliance requirements**
>
> For FIPS 140-2/3 validated products that do not have ADV_FSP.4 or higher security assurance requirements, the vendor should be required to provide a complete functional specification.

2.11   Key Management Document:

 The documentation shall describe types of internal and user keys and their life-cycle and states in terms of the following:

a)   Algorithm and mode for the key and the key size

b)   Whether the key is generated onboard on the crypto device or imported

c)   Whether the key can be output

d)   How the key can be destroyed/zeroized

e) The functions/purposes key is used for

Compliance requirements

This document is not required by FIPS 140-2/3 explicitly. The information from this document should be used to perform the analysis of the keys and their security. The information from this document should also be used for cross-checking consistency with the Functional Specification and the completeness and accuracy of the functional specification.

2.12 Mitigation of Other Attacks:

The documentation shall describe which if any, side channels are mitigated by the crypto device design. Examples of side-channel attacks are Simple Power Analysis (SPA), Differential Power Analysis (DPA), Timing Analysis, and Fault Injection. The documentation shall describe how each attack is mitigated and what testing has been conducted to prove the effectiveness of mitigation.

It is always desirable to have mitigation against attacks listed herein. Whether to mandate protection against these attacks or not is dependent on the crypto device functionality and environment the card will be used. For example, if the card has some stored value where the user of the crypto device has a vested interest in compromising its security, protection against these attacks is a must. The protection against timing analysis is very critical if the end system used to invoke the crypto device is not sufficiently trustworthy and may have Trojan Horses.

Compliance requirements

FIPS 140-2/3 validated products have this as an optional requirement. Thus, examination of the FIPS 140-2/3 validation certificate and security policy document (both publically accessible) will reveal which, if any, attacks are mitigated.

2.13 Operating System Security:

If application software such as applets can be loaded on the crypto device, the operating system must provide robust security features. The following requirements shall be met:

a) **Self-Protection:** The operating system shall be designed to protect itself from external interference and tampering, including attacks from applications.

b) **Non-By passable:** The security-enforcing functions of the operating system shall not be by-passable.

c) **Domain Isolation:** The operating system shall provide each application with an execution domain that cannot be interfered with.

d) **Identification & Authentication:** The operating system shall provide a mechanism for users and applications to authenticate to the operating system for access control purposes. The operating system shall protect the authentication mechanism and authentication databases (e.g., plaintext or encrypted forms of passwords and PINs) as part of self-protection.

e) **Access Control:** The operating system shall enforce an access control policy in terms of applications being able to access data and other applications.

f) **Residual Information Protection:** The operating system shall ensure that the previous information contents are unavailable when a resource (e.g., memory) is allocated.

Compliance requirements

FIPS 140-2/3 addresses these requirements by requiring a trusted operating system at EAL 2 or higher for 13 a-c. No additional verification is required for FIPS 140-2/3 Level 2 or Higher validated crypto devices for 13 d-f

---

2.14 Key Storage:

The cryptographic device should store private and secret keys in encrypted form. Decryption shall require the entry of a password or PIN. In other words, a password or PIN shall be used to derive the key encrypting key.

The cryptographic device does not have information stored in the cryptographic device that can be used to decrypt the key; it should require some user-entered information to reconstitute the key decrypting key. This approach provides added protection against physically hacking the crypto device.

Compliance requirements

This is not a requirement for FIPS 140-2/3. Thus, this will require additional testing

---

2.15 Specific Key Zeroization:

The crypto device should provide a mechanism to zeroize a specific key.

FIPS

This is not a requirement for FIPS 140-2. Thus, in order to meet this requirement Functional Specification and Key Management document should be examined and analyzed to determine which keys or types of keys can be zeroized individually.

2.16 Application Integrity:

For the software (e.g., Applet) being loaded, the operating system should verify integrity, source, and source authorization using cryptographic means such as digital signature verification or HMAC verification.

> **Compliance requirements**
>
> FIP 140-2/3 addresses this requirement.

2.17 Admin Password feature for USB-based crypto device

Generally, crypto devices have a User Module & Admin Module. The commonly used functions are below

- User Module: Change User PIN, Token Name, Delete Keys, Access to keys for signing / Encryption
- Admin Module: Reset User PIN, Initialize token, Key Zeroization

The crypto device should meet the following criteria:

a) The OEM or authorized representative of the crypto device shall offer crypto devices for issuance of DSC by CAs without having a user PIN reset option by any means. Such crypto devices shall have a new unique Serial Number series. The serial number should start with the first two letters representing OEM.

b) From 01.04.2023 onwards, CAs shall allow only the download of DSC on the crypto tokens holding the new unique serial number and having no user PIN reset option by any means.

c) The resetting PIN of the crypto token holding a valid encryption certificate issued before 01.01.2022 shall be carried only after the authentication of the subscriber by CA. The resetting password of the crypto device having an encryption certificate shall be carried out only by the Token Manufacturer or authorized representative organization(in the absence of the OEM office in India).

The Admin Password should be maintained in a controlled manner wherein it should be used only for specific administrative purposes and should not be exposed in any manner which can lead to compromising the security of the device or misuse.

2.18 General Requirements for USB-based Crypto Devices.

a) A unique Serial Number shall be generated by the Cryptographic Hardware manufacturer for each Token. Such Unique Serial Numbers should be stored inside the token file system and also engraved on the token shell. The Cryptographic Hardware manufacturer shall provide necessary libraries to the CAs to read the make, model & Unique Serial Number from the token file system and record the same while generating a key pair or while downloading the DSC into the token.

b) The Crypto Devices should have product-specific interface software and should be made available for various versions of Windows, Mac, iOS, Linux, and Android by Manufacturers and Suppliers. The crypto device interface software shall be made available by the OEM of the crypto device within three months, from the date of release of the latest version of the Operating system.

c) The crypto device vendors should make available a single page containing all the details of the Crypto Device and the same shall be shared with CAs. The details should be downloadable from the same site where the page is hosted.

d) To ensure transparency on the certification &security aspects, the brand name of the Token should bear the name of the OEM as mentioned in its module validation report (FIPS). The firmware name & version should match its module validation report (FIPS). The software embedded in the crypto devices should be of the same OEM. The certified product should be verifiable physically as well as electronically using software tools.

e) Other than OEM offering, the customization of tokens and custom branding is not allowed. The OEM interface software should allow the co-existence of other crypto OEM interfaces in the user's system.

f) CA shall remove Cryptographic Device products from their empanelled list upon the revocation of the FIPS validation certificate which was referenced in this document to demonstrate compliance with crypto device requirements.

g) Crypto Devices having Historical FIPS certificate status, relying on this document, are to be discontinued by CAs from January 01, 2026, onwards or their sunset whichever is earlier.

3 Audit Requirements

a) For the compliance audit, the security requirements mentioned in this document refer to the underlying certification (FIPS) of the crypto device, for cross-verification. The

overall security requirements mentioned in this document should refer to where the certification of both hardware and firmware is covered under the same OEM &version.

b) Token Manufacturers (OEM) or representative organizations (in the absence of the OEM office in India) should engage a Cert-in empanelled auditor to carry out Smartcard Security Assessment. If the representative organization engages an auditor, then an authorization certificate from the OEM for appointing an auditor should be submitted to CA along with the audit report.

c) CA should empanel the Cryptographic Device product with Module Name, OEM Name &Version (HW, FW & SW)Information, based on audited report and certificate.

d) If the product version undergoes any change to the auditable parameters, a fresh audit needs to be carried out.

e) For each version of the product, the CA shall list the Crypto devices only after the successful completion of the audit.

f) For cryptographic devices with FIPS 140-2/3 validated sub-module integration, all additional hardware & software components acting as interfaces to the validated cryptographic module must undergo a security audit in compliance with CCA-LIC Annexure VI, conducted by CERT-In empanelled agencies. The audit must verify that the software does not contain any functionality that could compromise the certification.

4 Action on Token suppliers /OEM

In the case of non-compliance to the CCA-CRPTO version 2.2, CCA may consider black-listing/de-empanelling the crypto device product at the discretion of CCA.

Audit Checklist

SN	Criteria under	Compliance

1	2.1 Functions Before User Authentication	
2	2.1 User Authentication	
3	2.2 User Authentication	
4	2.3 Physical Security (CMVP)	
5	2.4 Cryptographic Algorithms (CAVP Certificate)	
6	2.5 Key Entry	
7	2.6 Key Output	
8	2.7 Key Zeroization	
9	2.8 EMI/EMC	
10	2.9 Power Up Self-Tests	
11	2.10 Interface Specification	
12	2.12 Mitigation of Other Attacks	
13	2.13 Operating System Security	
14	2.14 Key Storage	
15	2.15 Key Zeroization	
16	2.16 Application Integrity	
17	2.17 Admin Password feature	
18	2.18 General requirements	

List of Acronyms

API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCA	Controller of Certifying Authorities
DES	Data Encryption Standard
DEMA	Differential Electromagnetic Analysis
DPA	Differential Power Analysis
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard (United States Standards)
PP	Protection Profile
SCP	Secure Channel Protocol
SPA	Simple Power Analysis
ST	Security Target
US	United States

Change History

SL	DATE	SECTION	MODIFICATION
1.	20.06.2018	2.17(a)	substituted the word "subscriber" in place of "user"
2.	14.11.2022	2(17), 2(18),3 & 4	Removed PIN reset, unique OEM brand name, software, historical, revocation , de-empanelment options.
3.	23.02.2024	2(18) (g)	Modification in the cut-off date of historical tokens
4.	27.11.2024	(1), (2) & (3.f)	Terminologies and Definitions , Crypto Device Requirements , Audit