Security Requirements for Crypto Devices

Version 1.0

02 May 2018

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	Security Requirements for Crypto devices
Status	Release
Version	1.0
Last update	20.06. 2018
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 in a Hardware Cryptographic Module /token which has been validated to FIPS 140-1/2 Level 2 for class 2 and class 3 DSCs.

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

Purpose

The purpose of this document is to specify the requirements for crypto device 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 crypto devices. The scope of this effort also includes conditional requirements, i.e., requirements that must be met if certain conditions hold true.

2 Crypto device Requirements

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

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.

FIPS 140-2 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 requirement 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 attack.

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

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

2.3 Physical Security:

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

The crypto device shall successfully undergo the process of Cryptographic Module Validation Program (CMVP) of FIPS 140-2, 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 for each device.

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

2.4 Cryptographic Algorithms:

The crypto device shall successfully undergo FIPS Cryptographic Algorithm Validation Program (CAVP) for each FIPS algorithm claimed to be implemented. If the crypto device generates keys for a FIPS algorithm, the crypto device shall also successfully undergo FIPS CAVP for key generation for that algorithm.

This requirement must be satisfied using CAVP algorithm certificate. However The crypto 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 crypto device shall only import keys into crypto device in encrypted form. The encryption mechanism and key encrypting keys shall be at least as strong as the key being imported.

FIPS 140-2 addresses the key entry requirement, but does not address the security strength of the keys. For the FIPS 140-2 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 crypto device shall be pre-configured to make private keys to be non-exportable in any form.

FIPS 140-2 addresses the key output requirement, but does not address the 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.

FIPS 140-2 address this requirement

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

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

FIPS 140-2 addresses this requirement.

2.9 Power Up Self-Tests:

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

FIPS 140-2 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.

For FIPS 140-2 evaluated products, it is possible that a well-written and complete security policy covers the functional specification under the services and functions available to each role.

For FIPS 140-2 validated products that are not have ADV_FSP.4 or higher security assurance requirement, 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) Functions/purposes key is used for

This document is not required by FIPS 140-2 explicitly. It is possible that the other required documents contain the information sought here. But, it is better to have this information properly organized in a single document. 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 in. For example, if the card has some stored value where the user of the crypto device has 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. FIPS 140-2 validated products have this as optional requirement. Thus, examination of FIPS 140-2 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 following requirements shall be met:

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

b) **Non-Bypassable:** The security enforcing functions of the operating system shall not be bypassable.

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

d) **Identification & Authentication:** The operating system shall provide 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.

FIPS 140-2 addresses these requirements by requiring a trusted operating system at EAL 2 or higher. Thus, no additional verification is required for FIPS 140-2 Level 2 or Higher' validated crypto devices

2.14 Key Storage:

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

This is not a requirement for FIPS 140-2. Thus, this will require additional testing. Note that it is critical that the crypto device does not have information stored in the crypto 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.

2.15 Key Zeroization:

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

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.

FIP 140-2 addresses this requirement.

2.17 Admin Password feature:

The crypto device should have an Admin Password feature for certain operational reasons. But should meet the following criteria:

a) Admin password can be used to perform certain administrative activities such as resetting the device or resetting password of subscriber. The resetting password of subscriber for access to the file system of PKI Crypto device / Crypto token by Admin shall be carried out only by Token Manufacturer or authorised representative organization(in the absence of OEM office in India). Such resetting of the password of the subscriber shall be carried out only after authentication of subscriber.

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

2.18 General Requirements

a) Unique Serial Number shall be generated by the Cryptographic Hardware manufacturer for each Token. Such Unique Serial Number 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 key pair or while downloading the DSC into the token.

b) The token drivers shall be available for various popular Operating Systems including various versions of Windows, Mac and Linux by Manufacturers and Supplier.

3 Audit Requirements

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

b) CA should empanel the Cryptographic Device products with product series on the basis of audited report and certificate.

c) If the product / series undergo any change to the auditable parameters, a fresh audit needs to be carried out.

d) For each product series, CA shall list the Crypto Token devices only after the successful completion of audit.

Audit Checklist

SN	Criteria under	Compliance
1	2.1 Functions Prior to 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	

19 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"