What is FIPS 140-2?

National Institute of Standards and Technology (NIST) issued the Federal Information Processing Standards Publications (FIPS PUBS) 140-2 in May 2001 (Lately updated in December 2002) as a Security Requirements for Cryptographic Modules (FIPS PUB 140-2) standard. *"This is a Computer Security Standard for Cryptography, and identifies the safety measures which are needed to be satisfied by a cryptographic module at any software or hardware level, which is used in any security system to protect the sensitive but unclassified data"*. This standard endow with four growing, qualitative levels of security (from Level 1 (lowest) to Level 4 (highest)), and these levels are anticipated to cover almost all those applications and environments wherever these cryptographic modules can be deployed.

FIPS 140-2 has also established a Cryptographic Module Validation Program (CMVP) which is basically a joint effort of NIST and the Communications Security Establishment (CSE) for the Canadian government. The FIPS 140-2 standard security accreditation program is helpful for the vendors who want to get their products certified which holds cryptographic modules. The goal of the CMVP is to endorse the use of validated cryptographic modules. Third party laboratories which are accredited as Cryptographic Module Testing Laboratories (CMTL) handle the tests and the vendors which are interested to get their devices certified may select any of the accredited lab for this purpose.

What are the functional security objectives?

The standard provides all those security requirements which are required for the designing and implementation of a cryptographic module. Following mentioned are the functional security objectives from which the requirements have been derived;

- Approved security functions which are made to protect sensitive information can be implemented correctly.
- Unauthorized operation or use of the cryptographic module could be blocked.
- So that the content of cryptographic module can be prevented from the unauthorized disclosure.
- To maintain the safety and security of cryptographic module itself from the unauthorized modification of cryptographic keys and CSPs.
- The operational state of the cryptographic module can be indicated.
- The working of cryptographic module can be ensured in the way that is performing and operating is approved mode of operation.
- To identify if there are some errors in the operation of cryptographic module so that sensitive data do not get compromised due to the errors.

What have been defined in its security requirements?

In the security requirements of a cryptographic module the following matters have been defined under the standard FIPS 140-2;

1. **Cryptographic Module Specification:**

It has been defined that it will be a set of hardware, software, firmware or a combination of these which will help to implement the cryptographic functions or processes including algorithm and within the pre-defined cryptographic boundaries.

2. **Cryptographic Module Ports and Interfaces:**
   It will be able to restrict the information flow and access points to all physical and logical ports and pre-define the entry and exit points.
3. **Roles, Services, and Authentication:**
   It must support some authorized roles of operators there must be corresponding services against those roles.
4. **Finite State Model:**
   Its operation will be specified using finite stated model and will also be represented using some state transition diagram or a state transition table.
5. **Physical Security:**
   This module will also implement physical security mechanism in order to avoid unauthorized access, use and modification.
6. **Operational Environment:**
   A non modifiable and pre-defined operational environment for the management of this module will be defined.
7. **Cryptographic Key Management:**
   The entire lifecycle of cryptographic keys and key components CSPs need to be properly defined. Key management includes random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.
8. **Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC):**
   Documentation of security levels 1, 2, 3 and 4 shall include the proof of EMI and EMC.
9. **Self-Tests:**
   The module will be able to perform self tests on power up or in any conditional situation.
10. **Design Assurance:**
    The best practices during the design, deployment and operation of the module will be followed and proper testing, configuration, delivery, installation and development along with the guidance will be provided.
11. **Mitigation of Other Attacks:**
    All known attacks and their types will be studied and the device must have the capability to mitigate from these attacks.

If there is a cryptographic module which match this standard will have to employ approved security functions such as cryptographic algorithms, cryptographic key management techniques, and authentication techniques that have been approved for protecting Federal government sensitive information.