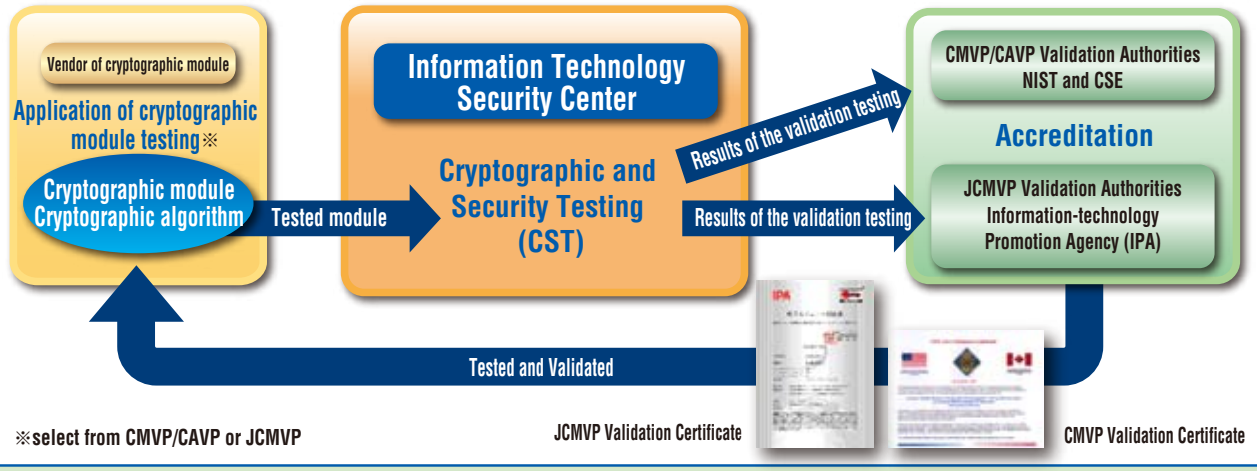
ITSC

Cryptographic Modules / Cryptographic Algorithms Testing

●To provide testing services of Cryptographic Modules and Cryptographic Algorithms of CMVP/CAVP(USA and Canada) and/or JCMVP(Japan)

Cryptographic Modules and Cryptographic Algorithms Validation Program

ITSC is accredited by National Voluntary Laboratory Accreditation Program (NVLAP) (LAB CODE: 200822-0) for Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP), and by Informationtechnology Promotion Agency(IPA) for Japan Cryptographic Module Validation Program (JCMVP).



Cryptographic Testing

Examples of Cryptographic Module

Smart card　USB token　PCI card　Gateway　Software cryptographic library
File encryption software　Hardware/Software that use encryption

Approved Security Functions

The categories of Security functions include Symmetric Key, Asymmetric Key, Secure Hash Standard, Random Number Generators, Message Authentication, and Key Management.
In CMVP/CAVP, security functions will be verified based on FIPS PUB 140.
In JCMVP, security functions will be verified based on JIS X 19790 especially in e-Government recommended cipher list.

Vendor Provided Materials (Differ depending on the tested cryptographic module)

Tested Cryptographic Module:
The testing requirement concerning physical security is performed to the hardware Cryptographic Module.

Security Policy(SP):
Block diagram and if necessary, photograph of the cryptographic module
《After the completion of validation, the non-proprietary Security Policy is open to the public.》

Vendor Evidence:
Development documents(design documents, schematic diagram, and source code), User document (manuals)
State transition diagram and specification of state transitions

Information Technology Security Center(IT Security Center)　URL : http://www.itsc.or.jp/

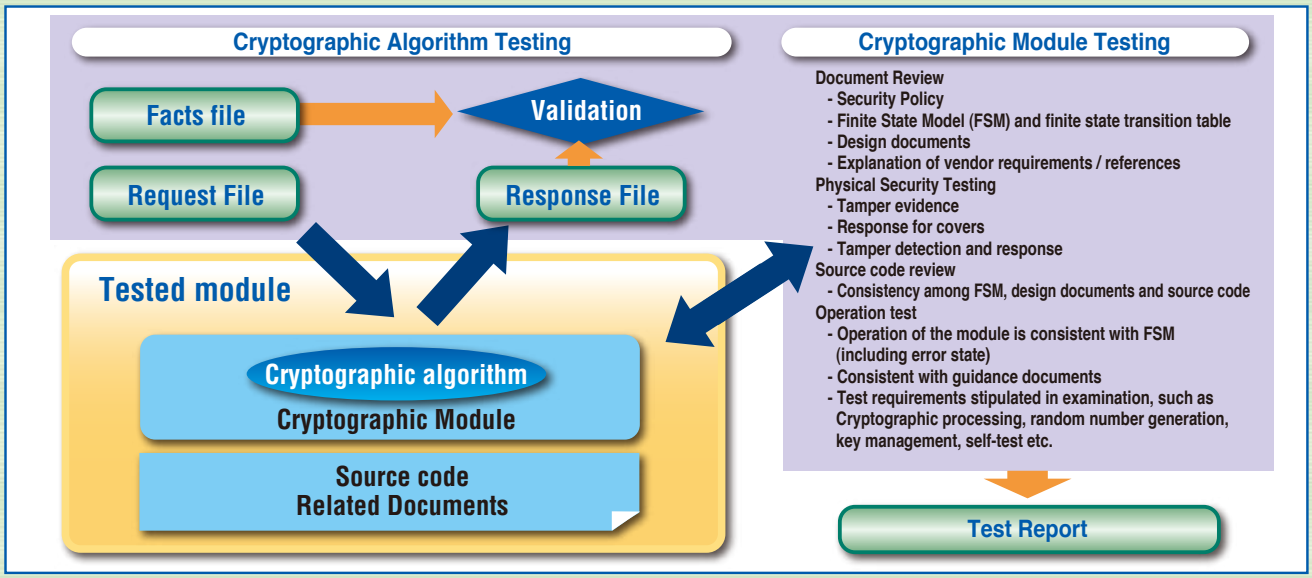
ITSC

Cryptographic Testing Process

Cryptographic module testing / Cryptographic algorithms testing make sure the following security objectives.

- To employ and correctly implement the Approved security functions for the protection of sensitive information
- To protect a cryptographic module from unauthorized operation or use
- To prevent the unauthorized disclosure of the contents of the cryptographic module, including plaintext cryptographic keys and CSPs (Critical Security Parameters)
- To prevent the unauthorized and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorized modification, substitution, insertion, and deletion of cryptographic keys and CSPs
- To provide indications of the operational state of the cryptographic module
- To ensure that the cryptographic module performs properly when operating in an Approved mode of operation
- To detect errors in the operation of the cryptographic module and to prevent the compromise of sensitive data and CSPs resulting from these errors

quoted from FIPS PUB 140



Security Requirements for a Cryptographic Module

Security Requirements	Contents	Security level			
		1	2	3	4
Cryptographic Module Specification	Cryptographic boundary, Interface specification, Security policy	●	●	●	●
Cryptographic Module Ports and Interfaces	Specification of all interfaces and of all input and output data paths	●	●		
	Data ports logically or physically separated from other data ports			●	●
Roles, Services, and Authentication	Logical separation of required and optional roles and services	●			
	Role-based or identity-based operator authentication		●		
	Identity-based operator authentication			●	●
Finite State Model	State transition diagram and specification of state transitions	●	●	●	●
Physical Security	Production grade equipment	●	●	●	●
	Locks or tamper evidence		●	●	●
	Tamper detection and response for covers and doors			●	●
	Tamper detection and response envelope, EFP or EFT				●
Operational Environment	Single operator, Executable code, Approved integrity technique	●	●	●	●
	Referenced PPs evaluated at EAL2 with specified discretionary access		●	●	●
	Trusted path evaluated at EAL3 plus security policy modeling			●	●
	Trusted path evaluated at EAL4				●
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization	●	●	●	●
	Secret and private keys established using manual methods may be entered or output in plaintext form	●	●		
	Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures			●	●
EMI/EMC	Class A (Business use)	●	●		
	Class B (Home use)			●	●
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical function tests, Conditional tests	●	●	●	●
Design Assurance	Configuration management (CM), Secure installation and generation, Design and policy	●	●	●	●
	Source code	●	●	●	●
	CM system, Secure distribution, Functional specification		●	●	●
	High-level language implementation			●	●
	Formal model				●