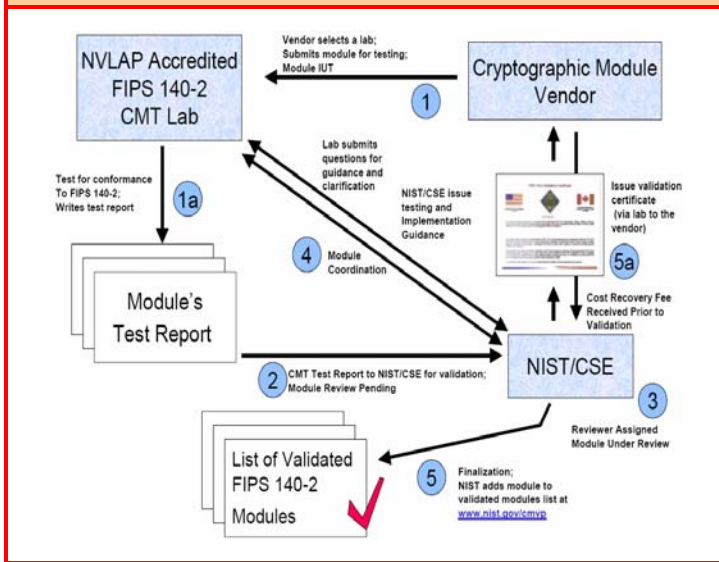


### FIPS 140-2 Validation Process\*



### FIPS 140-2 Sections and Security Levels

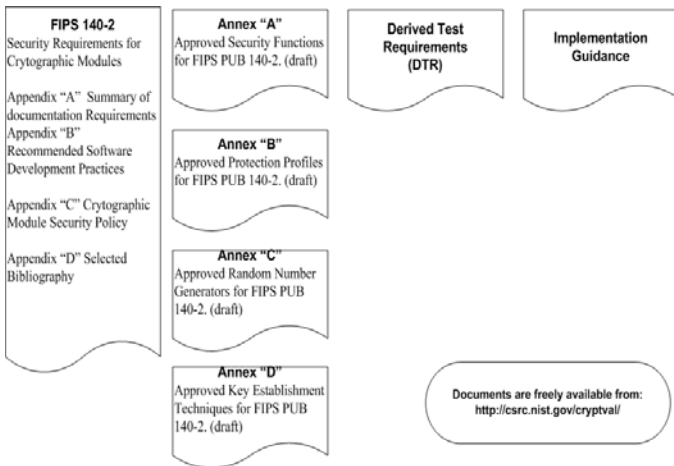
Sections	Security Levels			
	1	2	3	4
1. Cryptographic Module Specification				
2. Cryptographic Module Ports and Interfaces				
3. Roles, Services and Authentication				
4. Finite State Model				
5. Physical Security				
6. Operational Environment				
7. Cryptographic Key Management				
8. EMI/EMC				
9. Self-Tests				
10. Design Assurance				
11. Mitigation of Other Attacks				

\* source: Frequently Asked Questions for the Cryptographic Module Validation Program, (NIST, 12/4/2007)

### Summary of Security Requirements for FIPS 140-2

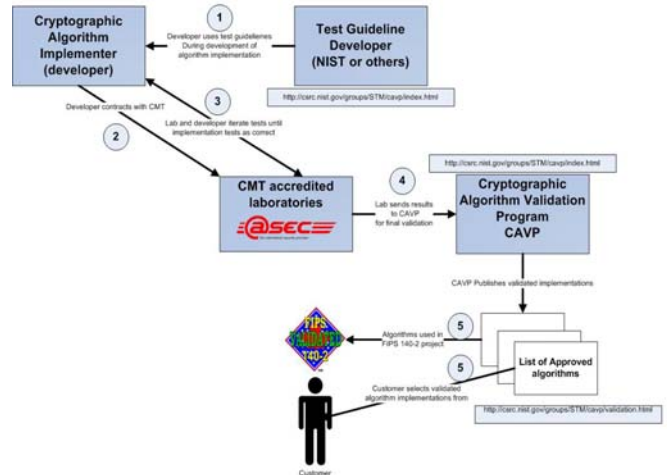
	Security level 1	Security level 2	Security level 3	Security level 4
<b>Cryptographic Module Specification</b>	Specification of cryptographic module, cryptographic boundary, approved algorithms and approved modes of operation. Description of cryptographic module including all hardware, software and firmware components. Statement of module security policy.			
<b>Cryptographic Module Ports and Interfaces</b>	Required and optional interfaces. Specification of all interfaces and of all input and output paths.		Data ports for unprotected CSPs, logically or physical separated from all other data ports.	
<b>Roles, Services and Authentication</b>	Logical separation for required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
<b>Finite State Model</b>	Specification of finite state model. Required states and operational states. State transition diagram and specification of state transitions.			
<b>Physical Security</b>	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for doors and covers.	Tamper detection and response envelope. EFP or EFT.
<b>Operational Environment</b>	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
<b>Cryptographic Key Management</b>	Key management mechanisms: random number and key generation, key establishment, key distribution, key input/output, key storage and key zeroization.			
<b>EMI/EMC</b>	47 CFR FCC Part 15, Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15, Subpart B, Class B (Home use).	
<b>Self-Tests</b>	Power-up tests, cryptographic algorithm tests, software/firmware integrity tests, critical functions tests, conditional tests.			
<b>Design Assurance</b>	Configuration management (CM). Secure installation and generation, design and policy correspondence. Guidance documentation.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations. (informal proofs). Pre-conditions and post-conditions.
<b>Mitigation of Other Attacks</b>	Specification of mitigation of other attacks for which no testable requirements are currently available.			

## FIPS 140-2 Specification and Documents



## Cryptographic Algorithm Validation Process

### Cryptographic Algorithm Validation Process



## FIPS Approved/NIST Recommended Cryptographic Algorithms

### Symmetric key

- Triple DES (TDEA) (SP 800-67)
- AES (FIPS 197)
- EES - Skipjack (FIPS 185)

### Asymmetric key

- DSA2  RSA2  ECDSA2 (FIPS 186-3)
- Digital Signature Standard (DSS) (FIPS 186-2)

### Message Authentication

- CMAC (SP 800-38B)
- CCM (SP 800-38C)
- HMAC (FIPS 198)
- GCM and GMAC (SP 800-38D)

### Hash

- SHA-1,224,256,384,512 (FIPS 180-3)

### Random Number Generators

- Random Number Generation for DSA (FIPS 186-2)
- RNG for ECDSA (ANSI X9.62)
- RNG for RSA (ANSI X9.31)
- DRBG deterministic random bit generator (SP 800-90)

### Key Management

- KAS FFC  KAS ECC (SP 800-56A)

## Useful FIPS 140-2 and Cryptographic Algorithm Validation Web Addresses

NIST Cryptographic Module Validation Program	<a href="http://csrc.nist.gov/groups/STM/cmvp/">csrc.nist.gov/groups/STM/cmvp/</a>
NIST Cryptographic Algorithm Validation Program	<a href="http://csrc.nist.gov/groups/STM/cavp/">csrc.nist.gov/groups/STM/cavp/</a>
NIST Cryptographic Module Validation List	<a href="http://csrc.nist.gov/groups/STM/cmvp/validation.html">csrc.nist.gov/groups/STM/cmvp/validation.html</a>
NIST Cryptographic Algorithm Validation List	<a href="http://csrc.nist.gov/groups/STM/cavp/validation.html">csrc.nist.gov/groups/STM/cavp/validation.html</a>
atsec Cryptographic Module Test Lab	<a href="http://www.atsec.com/fips-140-2-testing.html">www.atsec.com/fips-140-2-testing.html</a>