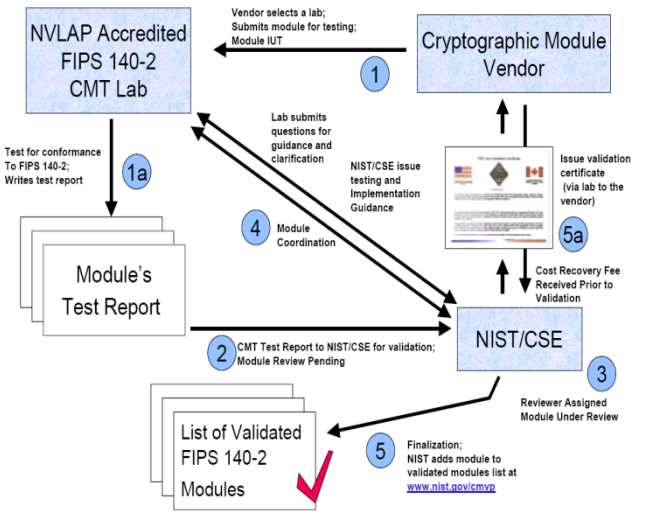
FIPS 140-2 Validation Process*



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				
Overall Security Level	**Lowest of above**			

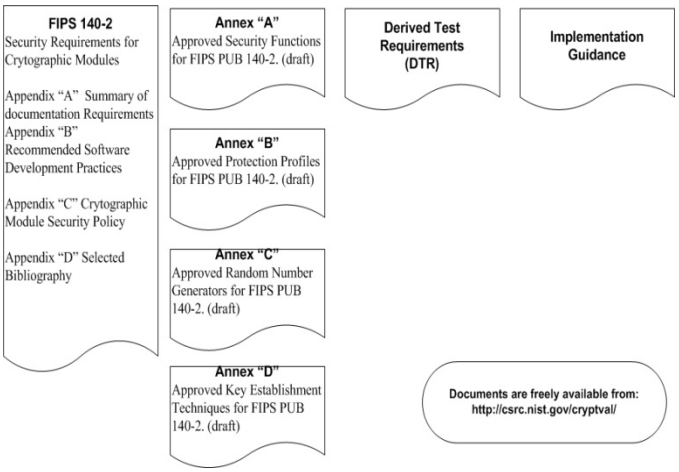
* source: Frequently Asked Questions for the Cryptographic Module Validation Program, (NIST, June 05, 2014)

Summary of Security Requirements for FIPS 140-2

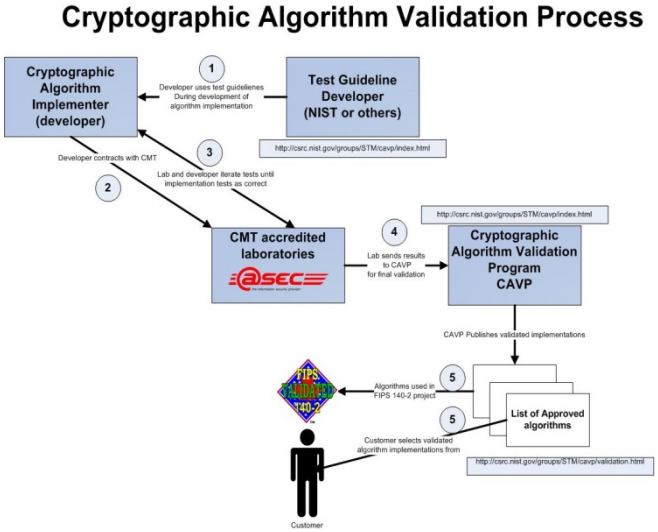
	Security level 1	Security level 2	Security level 3	Security level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved algorithms and approved modes of operation. Description of cryptographic module including all hardware, software and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	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.	
Roles, Services and Authentication	Logical separation for required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and operational states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for doors and covers.	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 control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key input/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	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).	
Self-Tests	Power-up tests, cryptographic algorithm tests, software/firmware integrity tests, critical functions tests, conditional tests.			
Design Assurance	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.
Mitigation of Other Attacks	Specification of mitigation of other attacks for which no testable requirements are currently available.			

9130 Jollyville Road, Suite 260, Austin, TX 78759, 512-615-7300: www.atsec.com

FIPS 140-2 Specification and Documents



Cryptographic Algorithm Validation Process



FIPS Approved/NIST Recommended Cryptographic Algorithms

Symmetric key
☐ Triple DES (TDEA) *(SP 800-67)*
☐ AES *(FIPS 197)*
Asymmetric key
☐ DSA ☐ RSA ☐ ECDSA *(FIPS 186-4)*
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 180-4*)
Random Number Generators
☐ DRBG deterministic random bit generator *(SP 800-90A)*
Key Management
☐ KAS FFC ☐ KAS ECC *(SP 800-56A)*
☐ KDF *(SP 800-135)*

Useful FIPS 140-2 and Cryptographic Algorithm Validation Web Addresses

NIST Cryptographic Module Validation Program	csrc.nist.gov/groups/STM/cmvp/
NIST Cryptographic Algorithm Validation Program	csrc.nist.gov/groups/STM/cavp/
NIST Cryptographic Module Validation List	csrc.nist.gov/groups/STM/cmvp/validation.html
NIST Cryptographic Algorithm Validation List	csrc.nist.gov/groups/STM/cavp/validation.html
atsec Cryptographic Security Test Lab	http://www.atsec.com/us/fips-140-2-testing-and-consulting.html

9130 Jollyville Road, Suite 260, Austin, TX 78759, 512-615-7300: www.atsec.com