Modifying an Existing Commercial Product for Cryptographic Module Evaluation

ICMC16 Ottawa, Canada

18-20 May 2016

Presented by Alan Gornall

Introduction

- I provide certification support to my clients: compliance audit, design, implementation, testing, documentation, project management
- I have over 25 years of certification experience and have completed over 50 certifications
- Issue addressed by this presentation: How to modify an existing commercial product to achieve FIPS 140-2 certification.
- ISO 19790/FIPS 140-3 is also discussed.

What is a Module?

- Contains at least one approved function
- Meets the requirements of FIPS 140-2 standard at chosen level

11 Sections

There are 11 sections of the FIPS 140-2 requirements, each one relating to a different aspect of a cryptographic module:

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

	Level 1	Level 2	Level 3	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 data paths.		Data ports for unprotected critical security parameters 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	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			

	Level 1	Level 2	Level 3	Level 4
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 control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modelling.	Referenced PPs plus 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.	

	Level 1	Level 2	Level 3	Level 4
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 documents.	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 attacks for which no testable requirements are currently available.			

What level do you need?

- FIPS 140-2 is a market enabler.
- There are very few occasions when you will need more than level 1.
- Any certification needs to be cost justified.
- I am going to concern myself with level 1 as that can usually be “retrofitted”, however I will also discuss the possibilities of grafting on compliance to higher levels

How much work do you want to do?

- Do a compliance audit on what you have already
- Define your cryptographic boundary
- Identify the gaps
- Investigate what the implementation options are
- Use this as a learning opportunity so that if you get the chance later to do a development from scratch, you will be prepared.

What will need to change?

- Almost guaranteed: Self-tests and key zeroization
- Other areas that may/will need attention:
  - Algorithms
  - Entropy
  - Key Management

Algorithms

- Approved algorithms have to have CAVP test certificates.
- Algorithm testing is a prerequisite for module functional testing.
- CAVP testing is free. Labs will charge for administering issuing test vectors and check results and submissions.
- Test early. CAVP testing is quick and the results are listed publicly on the NIST website.

Self-tests - 1

- Power-up self-tests:
  - Cryptographic algorithm test for all cryptographic functions of each approved algorithm implemented by the module
  - Software/firmware integrity test for all validated components (must use an approved authentication technique if Operating System requirements are applicable)

Self-tests - 2

- Plus conditional tests as applicable.
- ISO 19790 treats self-tests slightly differently, but if you are starting with a FIPS 140-2 module, then the integrity test is synonymous with the pre-operational software/firmware integrity test of ISO 19790 and the algorithm tests can be used to map onto the conditional cryptographic algorithm self-test of ISO 19790.

Entropy

- The strength of keys in a module depends on the quality of the DRBG and also on the quality of the entropy used to seed that DRBG. (AS7.13)
- The strength of the key is the weaker of these two factors.
- If you have no entropy, you have no key strength.
- IGs have been introduced in recent years that have added to the scrutiny that entropy sources are under. Need to demonstrate the quality of entropy sources through design evidence and statistical testing.

Key Management - 1

- Amount of work depends on the scope of the module.
- The wider the scope of the key management within the module (e.g. key distribution, transport, or derivation) the more standards need to be complied with and so the more work there is to do.
- If you do not generate keys/CSPs, then there is less work that if you do.
- In most cases, the key zeroization requirement can be met procedurally.

Key Management - 2

- Key management standards are listed in Annex D:
  - IG D.2.
  - FIPS 186-4
  - SP 800-56A Rev 2
  - SP 800-56B Rev. 1
  - SP 800-108
  - SP 800-132
  - SP 800-135rev1
  - SP 800-56C
  - SP 800-38F
  - SP 800-133

Level 2/3/4

- It may be possible to bolt-on level 2 compliance. Added to level 1:
  - Tamper evident physical security
  - Role-based authentication
- It is unlikely that level 3 can be bolted-on:
  - Port separation
  - Manual key transport security
  - Tamper detection and response physical security
  - Identity based authentication
  - Class B EMI/EMC
- Level 4 needs to be built-in due to the requirements for formal model and informal proofs for design.

Module, Product, Solution

- A certified module needs to be part of a compliant solution. A module need not provide all of the security necessary to protect assets, but it does need to be part of a compliant solution.
- If you have control over where the cryptographic boundary is drawn, it can reduce the work required to provide a compliant module.
- This is usually only practicable with software modules.
- Excluding as much key management as possible from a module makes it easier to certify, but you need to bear in mind the context of the security of the whole solution.

Conclusion/The Future

- FIPS 140-2 and ISO 19790 embody standards-based cryptography and this embodiment increases over time
  - It is getting harder to adapt proprietary solutions to meet the requirements of the CMVP.
- Certification is always an exercise in cost justification.
- Planning in conformance is usually cheaper than bolting it on afterwards.

Contact Details

Alan Gornall

Rycombe Consulting Limited

alan.gornall@rycombe.com

+44 1273 476366

RYCOMBE CONSULTING