Overcoming the Self-Test Hurdle

ICMC17 Westin Arlington Gateway

16-19 May 2017

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 implement self-tests required by FIPS 140-2, ISO 19790/FIPS 140-3 and Common Criteria.

What are self-tests?

- Tests performed at start-up/pre-operationally or when specific conditions occur in order to ensure the correct operation of the cryptographic module/device
- FIPS 140-2 has power-up and conditional tests
- ISO 19790 has pre-operational and conditional tests
- Common Criteria self-tests are ST/cPP specific but are usually a subset of FIPS 140-2/ISO 19790 self-tests

Why talk about self-tests?

- If you have implemented a product that uses cryptography and you now need to certify it against FIPS 140-2/ISO 19790/a CC cPP you will probably have to implement self-tests
- It's easy to miss some required self-tests
- It's easy to implement them inefficiently
- It's easy to be non-compliant

Self-tests – FIPS 140-2

- 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)
- Plus conditional tests as applicable.

Self-tests - 2

- ISO 19790 treats self-tests slightly differently, but comparing with a FIPS 140-2 module, 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.

Algorithm Tests

- Typically an algorithm test takes the form of a known answer test

Exceptions

- Algorithms where the output may vary for a given set of inputs cannot use a known answer test.
- For example RSA Probabilistic Signature Scheme (PSS). This can be tested by a pairwise consistency test.
- However, if the module implements at least one other approved RSA scheme whose output does not vary for a given input, then an RSA KAT using the pre-computed values can/must be performed instead.

Don’t miss anything

- Separate tests for each mode for both encrypt and decrypt (if both are implemented)
  - For example if you have AES-128 and AES-256 for CBC and CFB128 modes, you will need the following KATs: AES-128-CBC encrypt, AES-128-CBC decrypt, AES-256-CBC encrypt, AES-256-CBC decrypt, AES-128-CFB128 encrypt, AES-128-CFB128 decrypt, AES-256-CFB128 encrypt, AES-256-CFB128 decrypt
- All RNGs require a continuous RNG test, not just approved ones

Don’t miss anything - 2

- Also there are less obvious algorithm self-test requirements:
  - SP 800-90A Section 11 health tests
  - KAS Primitive Z computation KAT
  - RSA SP 800-56B self-tests
- Approved functionality not requiring self-tests
  - KDFs (e.g. IKE, TLS)
  - Approved AES key wrapping

Efficiency

- For SHS, If SHA-512 KAT is implemented, SHA-384 KAT is not required. Similarly, SHA-224 KAT not required if have SHA-256 KAT
- For HMAC, only need KAT with one underlying SHS algorithm, not all that are supported
- For public key algorithms, you only need a KAT for one approved scheme, not all of the schemes that you support.
- HMAC is faster than RSA for software module integrity checking

Compliance - 1

- Implementing the self-tests is not the end of the story
  - AS09.08: Power-up tests shall be performed by a cryptographic module when the module is powered up (after being powered off, reset, rebooted, etc.)
  - AS09.09: The power-up tests shall be initiated automatically and shall not require operator intervention.

Compliance - 2

- The module must not output any data until power-up self-tests have completed successfully
- AS09.10: When the power-up tests are completed, the results … shall be output via the “status output” interface.
- AS09.05: The cryptographic module shall not perform any cryptographic operations while in an error state.

Conclusion

- During transition for FIPS 140-2 to FIPS 140-3 remember that FIPS 140-2 modules are probably FIPS 140-3 compliant wrt self-tests
- The self-test requirements are complex but with one or two exceptions are not complicated
- Preparation and attention to detail will make your life easier

Contact Details

Alan Gornall

Rycombe Consulting Limited

alan.gornall@rycombe.com

+44 1273 476366

RYCOMBE

CONSULTING