ISO's Cryptographic Module Work

Fiona Pattinson

October 17th, 2012

Version 1.0

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301
www.atsec.com

Table of contents

1 ISO's Cryptographic Module work

atsec customers who have projects for testing, validating, and certifying cryptographic modules for the US government market are intimately familiar with the FIPS 140-2 standard. This standard and its associated supporting documents are produced and published by NIST. Together, the suite of documents define the specification and testing requirements for a cryptographic module that is used by the US Federal government to meet their requirements under the Federal Information Security Management Act (FISMA) of 2002.

For several years the value of conformance testing against the FIPS 140-2 specification has been well accepted, and the assurance gained through validated conformance has been specified (with varying degrees of rigor) in several other markets. For example:

- Other governments that recognize the assurance provided. Most noteworthy is Canada, who partners with NIST in operating the CMVP as a joint endeavor between NIST and the Communications Security Establishment of Canada (CSEC). There are examples of others, such as the Japan CMVP which is part of the Information-technology Promotion Agency (IPA). They developed and operate a validation program (similar to that used in the US and Canada) in support of procurement in compliance with the Japanese Standards for Information Security Measures for the Central Government Computer Systems.
- The UK's information commissioner's office and Treasury Solicitor's Department, both of which recommend using FIPS 140-2 validated encryption products.
- The Health industry. For example, the HITECH act provides for "safe harbor" from the costs of patient notification as well as the reputational risk if the data was protected from using encryption. The approved encryption processes to claim safe harbor are those that comply with the requirements of the Federal Information Processing Standards (FIPS) 140-2.
- The Financial industry. This industry has long referenced use of FIPS 140-2 and its predecessors as a best practice. More recently, the Payment Card Industry has drawn heavily from FIPS 140-2 in their endeavors to obtain cryptography assurance within PCI environments and systems in several of their standards.
- Voting Systems. The Electoral Assistance Commission's Voluntary Voting System Guidelines recommend the use of FIPS 140-2 for cryptography in voting systems.
- Digital Cinema. FIPS 140-2 is specified in the digital cinema specification, V1.2.

Despite the obvious usefulness of the standard and the assurance that is gained from programmatic testing and validation of the results, it has been long recognized that a US government-produced standard (and US government validations) may not be appropriate for scenarios beyond the US Government regulations.

So, in 2003, a project was initiated by ISO/IEC JTC 1 sub-committee 27 which focuses on IT security techniques. The project was allocated to Working Group 3, and the assigned editors and experts from the US, France and Japan led the international co-ordination to produce the first edition of **ISO/IEC 19790** which was published in 2006 (and was very familiar to those with knowledge of FIPS 140-2).

Abstract

ISO/IEC 19790:2006 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems.

ISO/IEC 19790:2006 specifies the following.

- Four levels of increasing security for cryptographic modules. Each level offers an increase in security over the preceding level.
- The following functional security objectives:
  - module specification;
  - ports and interfaces;
  - roles, services and authentication;
  - finite state model;
  - physical security;
  - operational environment;
  - cryptographic key management;
  - self-tests;
  - design assurance;
  - mitigation of other attacks.

ISO/IEC 19790:2006 will be complemented by a future International Standard defining the associated evaluation and test methods.

ISO/IEC 19790:2006 is derived from NIST Federal Information Processing Standard PUB 140-2 May 25, 2001.

Most of the differences between the ISO version and the FIPS version of the cryptographic module specification were those of internationalization. References to US legislation were removed and reliance on the US algorithm suite was modified (so that an authority could specify their own preferred set of algorithms, protection profiles, random number generators, and key establishment techniques). Terms referencing the CMVP were replaced by “approval authority,” and the terminology was updated to include “Sensitive Security Parameters” (SSP), “Critical Security Parameters” (CSP), etc. Technically, the specification was very similar to FIPS 140-2.

Abstract

ISO/IEC 24759:2008 specifies the methods to be used by testing laboratories to test whether a cryptographic module conforms to the requirements specified in ISO/IEC 19790:2006. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories. Within each subclause of the security requirements clause of ISO/IEC 24759:2008, the corresponding security requirements from ISO/IEC 19790:2006 are divided into a set of assertions (i.e. statements that have to be true for the module to satisfy the requirement of a given area at a given level). All of the assertions are direct quotations from ISO/IEC 19790:2006.

Following each assertion is a set of requirements levied on the vendor. These specify the types of documentation or explicit information that the vendor is required to provide in order for the tester to verify conformance to the given assertion.

Also following each assertion and the requirements levied on the vendor is a set of requirements levied on the tester of the cryptographic module. These specify what the tester needs to do in order to test the cryptographic module with respect to the given assertion.

Vendors can use ISO/IEC 24759:2008 as guidance in trying to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2006 before they apply to the testing laboratory for testing.

In 2008 a companion document, equivalent to the NISTs "Derived Test Requirements" for FIPS 140-2, was published. **ISO/IEC 24759:2008**: Information technology -- Security techniques -- Test requirements for cryptographic modules.

This document pair provided the basic requirements for forming an approval authority independent of the CMVP.

In 2008, with drafts of FIPS 140-3 from NIST becoming publicly available, ISO decided to also revise their standard with the intention of publishing a revision of **ISO/IEC 19790** as close as possible to the final release of FIPS 140-3. ISO communicated with NIST for status as NIST wrestled with the high volume of comments they received regarding FIPS 140-2, but finally, ISO took the lead in moving their specification forward to cope with evolving technologies and enthusiastic input from the many experts and nations represented in ISO. This second revision of ISO/IEC 19790 was published in August of 2012. (It is available for purchase from ISO's online store or from your favorite purveyor of standards.)

The companion test requirements document, **ISO/IEC 24759**, is currently undergoing revision and will be published when the final draft is approved by the ISO voting members.

Also in the works is a project to specify the necessary standards to enable implementation testing for cryptographic algorithms and other security functions. This project aims to enable an authority to develop a program along the lines of NIST's cryptographic algorithm validation program (CAVP) that provides the pre-requisite assurances for the fundamental functions employed in cryptographic modules.

1.1 Testing and validation of conformance to ISO/IEC 19790

Now that there is an internationally recognized set of standards for the specification and testing of cryptographic modules, a base set of cryptographic standards and fundamentals, as well as a means of testing their implementation correctness, all the needed tools are in place for various authorities to develop validation programs - and use of the tools provide for consistent testing, validation, and certification of

conformance to the ISO standard.

This is already happening.

- In Japan, IPA operates a cryptographic module validation program with ISO/IEC 19790 as a basis. and
- in Korea, the Korean Cryptographic Module Validation Program (KCMVP) was established in 2005 and uses ISO/IEC 19790 as a basis for their program specifying the Korean approved set of cryptographic algorithms and security functions.

With the development of validation programs using the standards -- and perhaps even one day mutual recognition by different programs -- the needs of the commercial sector around the world can be addressed. This would help developers and vendors of cryptographic modules to address markets on a multi-national basis (and may even help address some of the issues apparent in the critical infrastructures and the international supply chain).

To successfully offer such a service, a validation program must define the operational activities that are the vital to a successful program. These activities include:

- accrediting test laboratories
- making program policies
- defining the approved cryptographic functions,
- establishing algorithm implementation testing and validation
- establishing a management system for validating and certifying the testing results
- providing any necessary interpretations of the standards
- dealing with comments, requests, and issues from labs and vendors
- policing the certificate and logo usage

2 What changed in the 2012 revision of ISO/IEC 19790?

The following gives some of the highlights of ISO/IEC 19790:2012 and those familiar with FIPS 140-2 will notice some differences. Of course, for the full specification the ISO standard must be consulted. The following is not intended to be a complete analysis, but rather highlights some of the key points that affect developers of complex cryptographic modules. These include:

- A Degraded mode of operation is introduced, which allows modules to provide cryptographic services in the event that some part is not behaving, but the other parts are acting as expected. In the 2008 standard, if one part is "sick" the entire module must refuse any services. This requirement has been quite restrictive but is now relaxed.
- The dependency on Common Criteria for the Operating Environment for modules aiming for Validation Level 2 or higher is removed. Instead, the new ISO version introduces some specific security requirements on the Operating Environment that must be tested and configured independently by the laboratory. This allows independent validation of Software Modules at level 2, which right now is practically not feasible.
- New requirements for developer testing on the module have been introduced to complement the lab's testing. In this sense, the testing requirements become more aligned with what Common Criteria considers "developer" vs."independent" testing. This means that with the new revision, developers of cryptographic modules will have to spend time and effort to document their own security testing of the services the module provides, which is something they do not need to care about right now. Generally speaking, this is targeted towards increasing the assurance provided by the modules, but any assurance gained will heavily depend on how the different national programs develop their specific requirements and metrics for this activity.

The new revision continues to specify four security levels. Below is a summary of the levels and the basic requirements of each:

2.1 Security Level 1

- At least one approved security function or approved sensitive security parameter establishment method
- Operation in a non-modifiable, limited, or modifiable operating environment
- No physical security mechanisms are required above production-grade components
- Any Non-invasive mitigation methods or mitigation of other attacks which are implemented are documented

2.2 Security Level 2

- Adds the requirement for tamper evidence, which includes the use of tamper-evident coatings or seals or pick-resistant locks on removable covers or doors
- Role-based authentication
- Software cryptographic module to be executed in a modifiable environment that implements role-based access controls or, at the minimum, a discretionary access control with a robust mechanism of defining new groups and assigning restrictive permissions through access control lists (ACLs), and with the capability of assigning each user to more than one group, and that protects against unauthorized execution, modification, and reading of cryptographic software

Security level 2 continues to be the highest security level attainable by a pure software module.

2.3 Security Level 3

- Additional requirements to mitigate the unauthorized access to SSPs held within the cryptographic module
- Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at direct physical access, use or modification of the cryptographic module and probing through ventilation holes or slits
- Identity-based authentication mechanisms
- Manually established plaintext CSPs must be encrypted, utilize a trusted channel or use a split knowledge procedure for entry or output
- Mechanisms to protect a cryptographic module against a security compromise due to environmental conditions outside of the module's normal operating ranges for voltage and temperature
- Any Non-invasive mitigation methods that are implemented in the module must be tested against metrics for security level 3 that are defined in the standard
- Additional life-cycle assurances, such as automated configuration management, detailed design, low-level testing, and operator authentication using vendor-provided authentication information

2.4 Security Level 4

- Multi-factor authentication for operator
- The module includes special environmental protection features designed to detect voltage and temperature boundaries and zeroize CSPs
- Any Non-invasive mitigation methods that are implemented in the module must be tested against metrics for security level 4 that are defined in the standard
- Design verification by the correspondence between both pre- and post-state conditions and the functional specification

2.5 Requirements areas

The security requirements are organized into 11 requirement areas; many of these areas have changes from those specified in FIPS 140-2:

1. **Cryptographic module specification:** This area includes the cryptographic module specification general requirements, the types of cryptographic modules, the cryptographic boundary and the modes of operations
2. **Cryptographic module interfaces:** This area includes the cryptographic module interfaces general requirements, the types of interfaces, the definition of interfaces and trusted channel requirements
3. **Roles, services, and authentication:** This area includes the general requirements for roles, services, and authentication
4. **Software/Firmware security:**
5. **Operational environment:** This area includes general requirements for the operational environment, Operating system requirements for limited or non-modifiable operational environments, and Operating system requirements for modifiable operational environments
6. **Physical security**: This area includes requirements for embodiments, general requirements, requirements for each physical security embodiment and Environmental failure protection/testing requirements
7. **Non-invasive security**
8. **Sensitive security parameter management :** This area includes general requirements, Random bit generators , Sensitive security parameter generation , Sensitive security parameter establishment , Sensitive security parameter entry and output , Sensitive security parameter storage, and Sensitive security parameter zeroization

9. **Self-tests:** general requirements for self tests, pre-operational self-tests, and conditional self-tests
10. **Life-cycle assurance:** This area includes the life-cycle general requirements, Configuration management , Design ,Finite state model , Development ,Vendor testing, Delivery and operation, End of life and Guidance documents
11. **Mitigation of other attacks**

2.6 Summary of the security requirements by area and Security Level

Requirement Area	Security Level 1	2	3	4
❶ Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function or process in an approved manner.			
❷ Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel.	
❸ Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	Multi-factor authentication.
❹ Software / Firmware Security	Approved integrity technique, defined SFMI, HFMI and HSMI. Executable code.	Approved digital signature or keyed message authentication code- based integrity test.	Approved digital signature based integrity test.	
❺ Operational Environment	Non-Modifiable, Limited or Modifiable. Control of SSPs.	Modifiable. Role-based or discretionary access control. Audit mechanism		
❻ Physical Security	Production-grade components.	Tamper evidence. Opaque covering or enclosure.	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing. EFP or EFT.	Tamper detection and response envelope. EFP. Fault injection mitigation.
❼ Non-Invasive Security	Module is designed to mitigate against non-invasive attacks specified in Annex F.			
	Documentation and effectiveness of mitigation techniques specified in Annex F.		Mitigation Testing. (level 3)	Mitigation Testing. (level 4)
❽ Security Parameter Management	Random bit generators, SSP generation, establishment, entry and output, storage and zeroisation			
	Automated SSP transport or SSP agreement using approved methods.			
	Manually established SSPs may be entered or output in plaintext form.		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures.	
❾ Self-Tests	Pre-operational: software/firmware integrity, bypass, and critical functions test.			
	Conditional: cryptographic algorithm, pair-wise consistency, software/firmware loading, manual entry, conditional bypass and critical functions test.			
❿ Life-Cycle Assurance				
Configuration Management	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system.	
Design	Module designed to allow testing of all provided security related services.			
Finite State Model	Finite state model.			
Development	Annotated source code, schematics or HDL.	Software high-level language. Hardware high-level descriptive language.		Documentation annotated with pre- conditions upon entry into module components and postconditions expected to be true when components is completed.
Testing	Functional Testing.		Low-level Testing.	
Delivery and Operation	Initialisation procedures.	Delivery Procedures.		Operator authentication using vendor provided authentication information.
Guidance	Administrator and non-administrator guidance.			
⓫ Mitigation of other attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			Specification of mitigation of attacks with testable requirements.

2.7 The Annexes of ISO/IEC 19790:2012

A. Documentation requirements for each of the eleven requirement areas.

B. Details of the requirements for the contents of the non-proprietary security policy and the order of the contents. This aims to make the security policy document more consistent between vendors.

C. A default set of Approved security functions, referring to various ISO standards for block ciphers, stream ciphers, asymmetric algorithms and techniques, message authentication codes, hash functions, entity authentication, key management and random bit generation. As mentioned above, it is possible for an approval authority to supplement or supersede this Annex with their specific approved set of algorithms.

D. A list of the ISO/IEC approved sensitive security parameter generation and establishment methods. As mentioned above, it is possible for an approval authority to supplement or supersede this Annex with their specific requirements.

E. An empty list of the ISO/IEC approved authentication mechanisms. Since there are no ISO/IEC approved authentication mechanisms, it would be necessary for an approval authority to supersede this Annex with their own requirements.

F. An empty list of the ISO/IEC approved non-invasive attack mitigation test metrics. Since there are no ISO/IEC approved test metrics, it would be necessary for an approval authority to supersede this Annex with their own requirements.

3 But wait! There's more. Supporting work from ISO

The work in ISO is not restricted to the specification and the associated Dervied Test Requirements. There are several other work items that have been published or are currently being developed in WG 3. These include:

3.1 IS 17825: Testing methods for the mitigation of non-invasive attack classes against cryptographic modules (draft):

This draft International Standard specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for Security Levels 3 and 4. The test metrics are associated with the security functions specified in ISO/IEC 19790:2012.
The test methods used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012 and the test metrics specified in this International Standard for each of the associated security functions specified in ISO/IEC 19790:2012 are specified in ISO/IEC 24759.

3.2 IS 29128: Verification of cryptographic protocols (Published in 2011):

The goal of this International Standard is to establish means for verification of cryptographic protocol specifications to provide defined levels
of confidence concerning the security of the specification of cryptographic protocols

3.3 TR 30104: Physical Security Attacks, Mitigation Techniques and Security Requirements (draft):

This technical report will provide guidance and addresses the following topics:

- a survey of physical security attacks directed against different types of hardware embodiments including a description of known physical attacks, ranging from simple attacks that require little skill or resource, to complex attacks that require trained, technical people and considerable resources;
- guidance on the principles, best practices and techniques for the design of tamper protection mechanisms and methods for the mitigation of those attacks; and
- guidance on the evaluation or testing of hardware tamper protection mechanisms and references to current standards and test programs that address hardware tamper evaluation and testing.

3.4 IS 18367: Cryptographic algorithms and security mechanisms conformance testing (draft):

This draft document is in the early stages of development and is intended to provide the basis for testing the implementation correctness of cryptographic algorithms published by ISO.
Conformance testing assures that an implementation of a cryptographic algorithm or security mechanism implementation is correct whether implemented in hardware, software or firmware or in a specific operating environment. Testing may consist of known-answer or
Monte Carlo testing, or a combination of test methods. Testing may be performed on the actual implementation or modeled in a simulation environment.

--- With thanks to the editors of ISO/IEC 19790 including Randall Easter, Jean-Pierre Quémard and Junichi Kondo and also the convener of SC 27's working group 3, Miguel Bañón, for their review of this text and for suggesting corrections and improvements.

