TIPS for FIPS 140

Selling Applications with Cryptography to Federal Agencies

For applications or devices that include cryptography, U.S. and Canadian federal government agencies are required to use a cryptographic product that has been FIPS 140 validated or Common Criteria (CC) validated. Most CC Protection Profiles rely on FIPS validation for cryptographic security, and we will focus on this easier path (more details about the differences between CC and FIPS validations is included in the FAQ section at the end of this document). We have created this document to help you understand the FIPS 140 requirements and your compliance options, to help you find the best, cost-effective solution to allow you to meet your product launch dates.

RSA SECURITY®

Contents

I. The Requirement for FIPS

The requirement is: **"FIPS 140-1 has been made mandatory and binding by the Secretary of Commerce and is applicable to all U.S. Government departments and agencies which use cryptographic-based security systems to protect unclassified information** within computer and telecommunication systems (including voice systems) that are not national security systems...." (bold emphasis added)*

The National Security Telecommunications and Information Systems Security Policy No. 11 requires that effective July 1, 2002, such **systems use only approved information assurance products**, said Diana Maurer, a National Security Agency official who worked on the policy.

According to the rule, systems that enter, process, store, display or transmit national security information must include information assurance products validated against the International Common Criteria for Information Security Technology or Federal Information Processing Standard (FIPS) 140-2.

RSA Security offers you many solutions to help solve some aspects of your FIPS requirements. RSA BSAFE® FIPS validated products are designed to provide you with these great benefits:

- **Saving time and expense** — Save months of development work from reduced or eliminated FIPS preparation and validation work for your team.
- **Increasing revenue** — Since the application may take less time to both develop and test, you can launch your application to market faster so you can generate more revenue.
- **Reducing risk** — Outsourcing complex security needs to the security experts at RSA Security reduces your risk of introducing vulnerabilities into your product.

II. The FIPS 140 Validation Process

FIPS 140 is the standard to be used by Federal organizations when specifying cryptographic-based security systems to provide protection for sensitive or valuable data (maintaining the confidentiality and integrity of information). The FIPS 140 standard specifies the security requirements to be satisfied by a cryptographic module in four increasing, qualitative levels of security (Level 1 to 4, from low to high).

Since this standard is intended to cover a wide range of potential applications and environments, and the process of implementing cryptographic security is so complicated, NIST developed Special Publication 800-21, *Guideline for Implementing Cryptography in the Federal Government* (see the URL http://csrc.nist.gov/cryptval/, and click on the "Helpful Documents" link) with **138 pages of guidance** to clarify this involved process. This RSA Security document provides only an overview of the FIPS 140 validation process.

FIPS 140 covers 11 areas related to the design and implementation, as well as self-tests, of cryptographic modules as summarized in the table on the following page. Within most areas, a cryptographic module receives a security level rating from 1 to 4, depending on the requirements met. For areas that do not provide for different levels of security, a cryptographic module receives a rating that reflects fulfillment of *all* of the requirements for that area.

Once you create your cryptographic module, you must then select a laboratory NIST has accredited for FIPS validation testing and pay a testing fee. The lab will test your cryptographic algorithms and then your cryptographic module for conformance to the FIPS standard. The lab then writes a test report and sends this report to NIST/CSE for validation. A NIST/CSE representative reviews the report and, if everything is correct, issues a validation certificate and publishes the module on the list of FIPS 140 validated modules. Given the complexity of this process, you can understand why so many months elapse between the time of creating/documenting cryptographic algorithms and modules, and receiving a FIPS 140 validation certificate.

This complex process also means that excellence in creating solid cryptographic algorithms and modules is difficult to achieve. NIST surveyed the accredited laboratories to receive the data for these statistics:

Of the 162 cryptographic modules surveyed, during testing the labs found:

- **48.8%** (80) included **security flaws**
- **96.3%** (158) included **FIPS interpretation and documentation errors**

Of the 332 DES, 3DES, DSA and SHA-1 algorithm validations surveyed, during testing the labs found:

- **26.5%** (88) included **security flaws**
- **65.1%** (216) included **FIPS interpretation and documentation errors**

The areas of greatest difficulty were:

- Physical Security
- Self-Tests
- Random Number Generation
- Key Management**

*Source: NSTISSAM INFOSEC/1-00, Advisory Memorandum for the use of the Federal Information Processing Standards (FIPS) 140-1 Validated Cryptographic Modules in Protecting Unclassified National Security Systems.

**Source: Annabelle Lee, NIST

FIPS 140 Requirements

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module	Specification of crypto module and boundary. Description of module including all hardware, software and firmware. Statement of module's security policy.	Same as Level 1.	Same as Level 1.	Same as Level 1.
Module Interfaces	Required and optional interfaces. Specification of all interfaces and all internal data paths.	Same as Level 1.	Data ports for critical security parameters physically separated from other data ports.	Same as Level 3.
Roles & Services	Logical separation of required and optional roles and services.	Role-based operator authentication.	Identity-based operator authentication.	Same as Level 3.
Finite State Machine	Specification of the finite state machine model. Required states and optional states. State transition diagram and specification of state transitions.	Same as Level 1.	Same as Level 1.	Same as Level 1.
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope.
EFP/EFT*	No requirements.	No requirements.	No requirements.	Temperature and voltage.
Software Security	Specification of software design. Relate software to finite machine model.	Same as Level 1.	High-level language implementation.	Formal model. Pre- and post-conditions.
Operating System Security	Executable code. Authenticated. Single user, single process.	Controlled access protection (C2 or equivalent).	Labeled protection (B1 or equivalent). Trusted communications path.	Structured protection (B2 or equivalent).
Key Management	FIPS approved generation/distribution techniques.	Same as Level 1.	Entry/exit of keys in encrypted form or direct entry/exit with split knowledge procedures.	Same as Level 3.
Crypto Algorithms	FIPS approved cryptographic algorithms for protecting unclassified information.	Same as Level 1.	Same as Level 1.	Same as Level 1.
EMI/EMC**	FCC Part 15, Subpart B, Class A (Business use). Applicable FCC requirements (for voice).	Same as Level 1.	FCC Part 15, Subpart B, Class B (Home use).	Same as Level 3.
Self-Tests	Power-up and conditional tests.	Same as Level 1.	Same as Level 1.	Same as Level 1.

*Environmental Failure Protection / Environmental Failure Testing
**Electromagnetic Interference / Electromagnetic Compatibility
Source: NIST Special Publication 800-21, "*Guideline for Implementing Cryptography in the Federal Government*", Page 59.

III. Implementation Strategies for FIPS 140

RSA Security understands the complexities of the FIPS validation process. No matter which of the two implementation strategies you choose, RSA Security can help in your FIPS validation work.

You have the choice of following implementation strategies:

- Using a FIPS 140 validated cryptographic module
- Submitting your entire application for validation

3.1 Using a FIPS Validated Cryptographic Module

By your application using a FIPS 140 validated module, you can claim your application uses FIPS 140 validated cryptography and so is FIPS 140 compliant. NIST suggests using the phrase "FIPS 140-2 Inside" to note the use of FIPS 140 validated cryptography in your application.

Using a FIPS 140 validated module has the advantages of:

- **Saving time and expense** — You can save months of work from your development team by reducing or eliminating FIPS effort for the tasks outlined above. In addition to making modifications to your product and creating test routines to demonstrate how your application works, the FIPS validation process requires you to create detailed documentation describing the 11 areas of security policy, application design and test requirements. Also, a product being considered for FIPS validation must be submitted to a National Voluntary Laboratory Accreditation Program (NVLAP) for conformance testing, and you can avoid undertaking this lengthy, expensive procedure by using a FIPS 140 validated cryptographic module.
- **Increasing revenue** — Since your application may take less time to both develop and test by including our validated cryptographic module, you can launch your application to market faster so you can generate more revenue. Our award-winning documentation, developer support and technical training make it easy for your staff to use RSA BSAFE products quickly and confidently. Launching to the market quickly may allow you more time to capture the increasing federal government budget for IT spending ($52.6 billion in FY 2003).
- **Reducing risk** — Outsourcing the complex security needs to security experts at RSA Security reduces your risk of introducing inadvertent vulnerabilities into your product that can damage your company's reputation and even lead to legal liabilities. By leveraging the work of RSA Security's experts, your team can concentrate their limited development time on their core competencies, creating more competitive products. Rather than submit an application with security flaws or other errors — a large group as noted in the laboratory statistics in the previous section — you can avoid the risk of the expensive, time-consuming process of submitting (and resubmitting) your application for review.

When choosing this strategy, following are your options for RSA BSAFE products:

- **RSA BSAFE Crypto-C 5.2.1** — Validated FIPS 140-1 Cryptographic Module — Certificate # 163 http://csrc.nist.gov/cryptval/140-1/140crt/140crt163.pdf
- **RSA BSAFE Crypto-J 3.3.4** — Validated FIPS 140-1 Cryptographic Module — Certificate # 289 http://csrc.nist.gov/cryptval/140-1/140crt/140crt289.pdf
- **RSA BSAFE Crypto-C Micro Edition 1.7** — Validated FIPS 140-2 Cryptographic Module — Certificate # 309 http://csrc.nist.gov/cryptval/140-1/140crt/140crt309.pdf

Applications for Operating Systems other than Microsoft® Windows® or Java™ Operating Systems

When we port our FIPS validated DLL to other platforms without modifying the functionality of the DLL (for example, changing from a DLL to a UNIX shared library), RSA Security customers can claim their application is built on a FIPS validated module.*

If you are interested in a FIPS validated module on an operating system other than Microsoft Windows or Java operating system, please contact your RSA Security Account Manager to make these arrangements.

3.2 Submitting Your Entire Application for Validation

There are situations when product architecture will not allow for a FIPS validated cryptographic module to be used, so the alternative is to submit your application for FIPS validation. RSA Security can offer the ability to save time and expense by providing validated algorithms as the foundation for your work. By starting with validated algorithms, you eliminate the development and testing needed at the algorithm level and can begin your application's validation at the cryptographic module level.

The list below describes all the validated algorithms included in the RSA BSAFE cryptographic products. Since you are starting with validated algorithms, you save the time and expense needed for this validation effort and begin at a later stage in the process.

*Source: http://csrc.nist.gov/cryptval/140-1/FIPS1401IG.pdf, Implementation Guidance, Section G.5.

The FIPS validation process involves substantial resource investment, especially for the initial validation. There are many security-consulting companies that can help you plan and navigate this complex process to help ensure your products can be validated quickly and cost-effectively.

Validated Algorithms in RSA BSAFE Cryptographic Products

RSA BSAFE Crypto-C 5.2.1

1. Triple DES validated algorithm — Certificate # 70 http://csrc.nist.gov/cryptval/des/tripledesval.htm
2. DES validated algorithm — Certificate # 131 http://csrc.nist.gov/cryptval/des/desval.htm
3. DSA validated algorithm — Certificate # 49 http://csrc.nist.gov/cryptval/dss/dsaval.htm
4. SHA-1 validated algorithm — Certificate # 59 http://csrc.nist.gov/cryptval/shs/shaval.htm
5. RSA (ANSI X9.31 and PKCS #1 for signature) — vendor affirmed http://csrc.nist.gov/cryptval/140-1/1401val2001.htm
6. ECDSA — vendor affirmed http://csrc.nist.gov/cryptval/140-1/1401val2001.htm

RSA BSAFE Crypto-J 3.3.4

1. AES validated algorithm — Certificate # 45 http://csrc.nist.gov/cryptval/aes/aesval.htm
2. Triple DES validated algorithm — Certificate # 112 http://csrc.nist.gov/cryptval/des/tripledesval.htm
3. DES validated algorithm — Certificate # 168 http://csrc.nist.gov/cryptval/des/desval.htm
4. DSA validated algorithm — Certificate # 63 http://csrc.nist.gov/cryptval/dss/dsaval.htm
5. SHA-1 validated algorithm — Certificate # 97 http://csrc.nist.gov/cryptval/shs/shaval.htm
6. RSA (ANSI X9.31 and PKCS #1 for signature) — vendor affirmed http://csrc.nist.gov/cryptval/140-1/1401val2002.htm

RSA BSAFE Crypto-C Micro Edition 1.7

1. AES validated algorithm — Certificate # 26 http://csrc.nist.gov/cryptval/aes/aesval.htm
2. Triple DES validated algorithm — Certificate # 135 http://csrc.nist.gov/cryptval/des/tripledesval.htm
3. DES validated algorithm — Certificate # 186 http://csrc.nist.gov/cryptval/des/desval.html
4. DSA validated algorithm — Certificate # 72 http://csrc.nist.gov/cryptval/dss/dsaval.htm
5. SHA-1 validated algorithm — Certificate # 121 http://csrc.nist.gov/cryptval/shs/shaval.htm
6. HMAC SHA-1 validated algorithm — vendor affirmed
7. RSA (ANSI X9.31 and PKCS #1 for signature) — vendor affirmed

3.3 FIPS Planning Resources

A great resource for planning a FIPS submission is the NIST Web site. Visit the URL www.nist.gov/cmvp for information on the FIPS 140-2 Security Requirements for Cryptographic Modules and Derived Test Requirements. Special Publication 800-21 "*Guideline for Implementing Cryptography In the Federal Government*" provides important guidance and the FAQ document at http://csrc.nist.gov/cryptval/140-1/CMVPFAQ.pdf answers frequently asked questions about implementation issues. Other good resources are representatives of a National Voluntary Laboratory Accreditation Program (NVLAP) — names and contact information are listed on the NIST Web site under the "Testing Laboratories" link.

IV. Frequently Asked Questions

What is NIST?

NIST is the abbreviation for the National Institute of Standards and Technology. NIST laboratories provide measurements and standards for U.S. industries.

What is CSE?

CSE is the Communications Security Establishment, the Canadian Federal Government lead agency that delivers information technology solutions to the government of Canada.

What is NVLAP?

The National Voluntary Laboratory Accreditation Program (NVLAP) provides third-party accreditation to testing and calibration laboratories. NVLAP's accreditation programs are established in response to Congressional mandates or administrative actions by the Federal Government or from requests by private-sector organizations. The directory of accredited laboratories for cryptographic module testing is online at http://ts.nist.gov/ts/htdocs/210/214/scopes/crypt.htm

What is FIPS?

FIPS is the abbreviation for the Federal Information Processing Standards, a set of standards that describe document processing, provide standard algorithms for searching and provide other information processing standards for use within government agencies.

How is FIPS 140 validation used?

A FIPS 140 validation is required on products to be sold to U.S. and Canadian government agencies. When the FIPS 140 regulation was introduced, this requirement was often waived since there were a limited number of validated cryptographic modules. The waiver must be granted by the agency doing the procurement (not NIST) and we are unaware of any waiver being granted in 2002 or 2003.

What is FIPS 140-1?

This standard specifies the security requirements to be satisfied by a cryptographic module used within a security system protecting unclassified information within computer and telecommunications systems (including voice systems).

What is FIPS 140-2?

This is the second version (denoted by the -2) of the standard that describes the Security Requirements for Cryptographic Modules. The FIPS 140 standard is reexamined and reaffirmed every five years. A document posted on the NIST Web site at http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf gives an overview of the differences between the FIPS 140-1 and FIPS 140-2.

Since there is a FIPS 140-2 standard, what does this mean for a FIPS 140-1 validated product?

A FIPS 140-1 validation carries all the effects, rights and privileges of a FIPS 140-1 validation, and the FIPS 140-1 validation does not expire. All agencies may continue to purchase, retain and use FIPS 140-1 validated products.

What is the Cryptographic Module Validation Program?

The Computer Security Division at NIST maintains a number of cryptographic standards and coordinates validation programs for many of those standards. The Cryptographic Module Validation (CMV) Program encompasses validation testing for cryptographic modules and algorithms. More details are on the Web page http://csrc.nist.gov/cryptval/.

What is the difference between a FIPS 140-2 certification and a FIPS 140-2 validation?

The correct term to use is *validation*. NIST and CSE validate products that have been tested by a NVLAP approved laboratory. Once a testing laboratory has evaluated a product and found it meets the FIPS 140-2 requirements, they present a report to NIST and CSE to this effect. After a quality review, NIST and CSE can then issue a validation noting that the product conforms to the standard.

For this reason, the CMVP is named the Cryptographic Module *Validation* Program and not the Cryptographic Module *Certification* Program.

To add to the confusion over terminology, when a cryptographic module receives FIPS 140-2 validation, NIST issues a certificate (though not a certification) to note this achievement. The certificates are listed online on the Cryptographic Modules Validation List at: http://csrc.nist.gov/cryptval/140-1/1401val.htm.

Within FIPS 140-2, there are different security levels. What are the differences among the Security Level designations (Security Level 1, 2, 3 and 4)?

The Security Level designation can be confusing (Note: The -2 at the end of FIPS 140-2 designates the second revision of the FIPS 140 standard and has no relation to the Security Level). Within the FIPS 140-2 (or 140-1) validations, there are four possible Security Levels for which a product may receive validation.

Security Level 1 provides the lowest level of security. It specifies basic security requirements for a cryptographic module. This is the level for which our RSA BSAFE products receive FIPS validation since our RSA BSAFE products are software only.

Security Level 2 improves the physical security of a Security Level 1 cryptographic module by adding the requirement for tamper evident coatings or seals, or for pick-resistant locks.

Security Level 3 requires enhanced physical security, attempting to prevent the intruder from gaining access to critical security parameters held within the module.

Security Level 4 provides the highest level of security. Level 4 physical security provides an envelope of protection around the cryptographic module to detect a penetration of the device from any direction.

There is more information about the Security Levels beginning on page 1 of the FIPS PUB 140-2, "*Security Requirements for Cryptographic Modules,*" posted on the NIST Web site http://csrc.nist.gov/cryptval/.

What are the differences between the Common Criteria (CC) and FIPS 140-2 validations?

The Common Criteria (CC) and FIPS 140-2 differ in the abstractness and focus of tests.

FIPS 140-2 testing is against a defined cryptographic module and provides a suite of conformance tests to four security levels. FIPS 140-2 describes the requirements for cryptographic modules and includes such areas as physical security, key management, self tests, roles and services, etc.

CC is an evaluation against a created protection profile (PP) or security target (ST). The Protection Profile (PP) construct allows prospective consumers or developers to create standardized sets of security requirements that will meet their needs, and

typically a PP covers a broad range of products. The CC is a voluntary standard used to describe the security properties (functional and assurance) of IT products (or classes of products) and systems. Products with security properties specified using the CC may then be validated (tested) for conformance to their CC specifications. Such a validation, when performed by an accredited testing laboratory, confirms the product meets its security specification(s).

A CC evaluation does not supersede or substitute for a FIPS 140-2 validation. The four security levels in FIPS 140-2 are not intended to map directly to specific CC EALs or to CC functional requirements. FIPS 140-2 is the current *de facto* standard for cryptography and we are unaware of any other standard worldwide that is comparable. Also, there is no document that correlates CC functionality to FIPS 140-2 functionality, so a CC certificate cannot be a substitute for a FIPS 140-2 certificate. FIPS 140-2 test data may be submitted as part of a CC evaluation, with the hope that the tests will not need to be repeated.

For a validated software cryptographic module, may the module be used with an operating system other than the one noted on the FIPS validation certificate?

A software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any general purpose computer (GPC) provided that:

a. the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and

b. the software of the cryptographic module does not require modification when ported (platform specific configuration modifications are excluded).*

To make this easy for customers, we have ported our FIPS validated cryptographic modules from Microsoft Windows operating system to become shared libraries on other platforms.

May Level 1 software modules be used by a server?

Because the cryptographic module is not an application and is required to execute on an OS configured in single user mode, only one instance of the crypto module may be executed at any given time. When a crypto module is implemented in a server environment, the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. **Therefore, the server application is the single user of the cryptographic module, even when the server application is serving multiple clients**. The OS enforces the requirement that only a single cryptographic process may be executed at a given time.**

Will using FIPS validated algorithms only (not a validated module) satisfy NIST requirements?

No, one must use a validated cryptographic module to satisfy NIST requirements. Validating algorithms is the first step of a module's validation process. For an algorithm to be listed on a validation certificate as FIPS Approved, the algorithm implementation must meet all the requirements of FIPS 140-2 and must have received an algorithm validation certificate. A FIPS 140-2 validation certificate will not be issued unless the underlying FIPS Approved algorithm certificates have been completed.

*Source: 140-2 Implementation Guidance G.5 (page 11 of the document posted at http://csrc.nist.gov/cryptval/140-1/FIPS1402IG.pdf) discusses "Maintaining Validation Compliance of Software Cryptographic Modules."

**Source: "Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program", Section 6.1, page 22. http://csrc.nist.gov/cryptval/140-1/FIPS1402IG.pdf

V. Partnering with RSA Security

With more than 11,000 customers around the globe, RSA Security provides interoperable solutions for establishing online identities, access rights and privileges for people, applications and devices. Built to work seamlessly and transparently in complex environments, the Company's comprehensive portfolio of identity and access management solutions — including authentication, Web access management and developer solutions — is designed to allow customers to confidently exploit new technologies for competitive advantage. RSA Security's strong reputation is built on its history of ingenuity and leadership, proven technologies and long-standing relationships with more than 1,000 technology partners.

Market Leader — For nearly 20 years, RSA Security has been a market leader in providing cryptographic toolkits of the highest quality to developers. With more than one billion RSA BSAFE-enabled applications in use worldwide, RSA Security has the proven leadership and innovative technology to address the changing security needs of e-business and bring trust to the online economy.

Broad Platform Support — RSA Security's products support many operating systems to provide our customers with a wide variety of platforms out of the box.

Interoperability — RSA Security's offerings are a set of open, standards-based products and technologies, helping ensure the interoperability you need to be successful in your e-business endeavors. RSA Security keeps current on industry developments so you don't have to. And RSA Security plays active, leadership roles in standards development initiatives to help ensure interoperability of our solutions.

Support — RSA Security's technical support organization is known for resolving requests quickly, gaining customers' confidence and exceeding expectations. Also, our RSA BSAFE products include award-winning documentation and easy-to-use sample code to help get you on the road to development quickly.

Maintenance — RSA Security maintenance includes product upgrades while some of our competitors charge for each upgrade — a hidden, future cost to consider in your decision process.

Educational Services — RSA Security can provide security assessments and implementation consulting to guide you in your development plans. We also offer education and training services to help your team quickly understand how to use our products to solve your security problems.

Research and Development — RSA Security continues to make major investments in improving our technical superiority, as in developing cryptographic performance enhancements and solving difficult issues like key management with our Nightingale offering. By reinvesting in our products, we continue to provide innovative offerings to our customers.

Custom Development — If your requirements are unsatisfied by RSA Security's standard offerings, we can provide custom development services to meet your needs, like small code size implementations, ports to unusual operating systems and special service providers for certificate management.

Notes

Notes

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

FIPS WP 0603