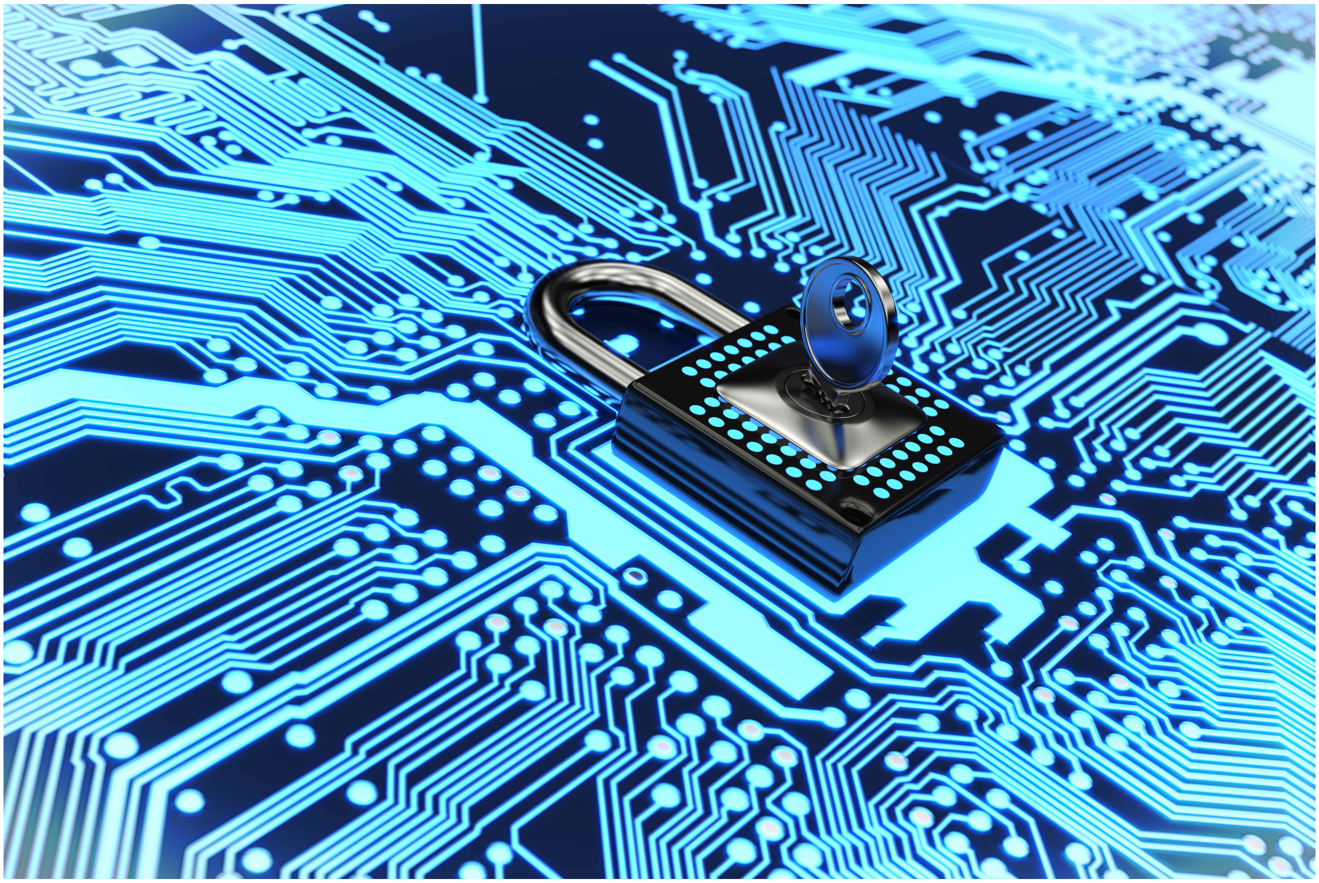
FIPS 140-2 Inside



A strategy for your FIPS 140-2 project

Version 1.1

This report may be freely shared

KeyPair CONSULTING

Introduction

A product may satisfy FIPS 140-2 requirements by incorporating a validated cryptographic module, a strategy called "FIPS 140-2 Inside." How do vendors responsibly integrate cryptographic functionality into their product to achieve the intent of "FIPS 140-2 Inside"?

About KeyPair Consulting Inc

Mark Minnoch and Steve Weymann are Co-Founders of KeyPair Consulting Inc. and creators of this paper.

With over two decades of combined experience and hundreds of successful FIPS validations, KeyPair Consulting Inc. expertly guides technology companies in achieving their FIPS goals.

Mark Minnoch

Steve Weymann

Get In Touch

Please contact KeyPair Consulting Inc. at +1 (805) 316-5024 or info@KeyPair.us

Our dramatically superior service will squash your FIPS pains.

Under the Hood

What is FIPS 140-2 Inside?

When a cryptographic module is validated by the Cryptographic Module Validation Program (CMVP)[1] as complying with FIPS 140-2, Security Requirements for Cryptographic Modules, then a technology vendor may use the phrase *FIPS 140-2 Validated*.

A **cryptographic module** may be a standalone product or a component of a product. This paper details the strategy of using cryptographic modules as components of a product. This approach is known as "FIPS 140-2 Inside."

Examples of cryptographic modules often used as FIPS validated components in products include embedded cards, single-chip modules, and software libraries.

Let us assume that ZZZ Security Inc. (pronounced "Snore Security" - a fictitious company) develops a network security device for commercial and federal customers. The name of ZZZ Security's product is the ZZZ Information Protection for IT ("ZZZipit!" for short). ZZZipit performs cryptographic services using a cryptographic engine software library on a high throughput CPU in software contained within the ZZZipit enclosure.

The ZZZ Sales Team needs a FIPS 140-2 certificate for the ZZZipit so that they can satisfy procurement requirements from their federal prospects. To meet company revenue goals for the year, the ZZZ Product Team must deliver a FIPS 140-2 certificate for ZZZipit - quickly.

With limited budget, resources, and time, the ZZZ Product Team researches strategies other than performing a traditional FIPS 140-2 validation of a standalone cryptographic module. A team member notices the CMVP FAQ discussion of "FIPS 140-2 Inside," and observes that the solid-state drive (SSD) embedded in ZZZipit is on the FIPS 140-2 validation list.

So - has ZZZipit met the expectation for "FIPS 140-2 Inside" ... is that all there is to it?

[1] The CMVP is joint effort between National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of Canada

The CMVP Position on *FIPS 140-2 Inside*

From the CMVP Validated Modules page:

> *It is important to note that validation certificates are issued for cryptographic modules. A module may either be an embedded* ***component*** *of a product or application, or a complete* ***product*** *in and of itself. If the cryptographic module is a component of a larger product or application, one should contact the product or application vendor in order to determine what products utilize an embedded validated cryptographic module.*
>
> *Ask the vendor to supply a signed letter stating their application, product or module is a validated module or incorporates a validated module, the module provides all the cryptographic services in the solution, and reference the modules validation certificate number. The information on the CMVP validation entry can be checked against the information provided by the vendor and verified that they agree. If they do not agree, the vendor is not offering a validated solution.*

Although the FIPS validated SSD is present, it clearly does not "... provide all the cryptographic services in the solution." However, the ZZZ Product Team analysis concludes that an update of the current software library version with a FIPS 140-2 validated variant is reasonable. The Product Team adopts a "*FIPS 140-2 Inside*" strategy — *leveraging the FIPS validated SSD* ***and*** *replacing their software crypto library with a FIPS validated crypto module* — to quickly provide validated cryptography for the ZZZipit.

Following the integration effort, ZZZ Security Inc. moves forward with the claim that the ZZZipit includes FIPS 140-2 validated cryptographic modules for the protection of sensitive information. Federal agencies can easily verify the FIPS 140-2 certificate numbers for the embedded SSD (FIPS 140-2 Cert. #9998)[2] and software crypto library (FIPS 140-2 Cert. #9999) during the procurement process. Everyone is happy.

[2] FIPS Certificates #9998 and #9999 do not exist and are for example purposes only

Behind the Curtain

Benefits of FIPS 140-2 Inside - Real or Perceived?

Using the *FIPS 140-2 Inside* approach, a product may be sold to federal agencies as soon as the validated cryptographic modules have been integrated properly. Since the timeline to complete a first-time FIPS 140-2 validation of a standalone cryptographic module can exceed a year, the *FIPS 140-2 Inside* approach is compelling and popular.

The benefits to using a *FIPS 140-2 Inside* strategy can be significant:

- Leverage existing FIPS 140-2 validated crypto modules (avoid or reduce the FIPS validation process)
- Well defined cryptographic boundary (or boundaries) allows for easier product updates
- Offload the FIPS maintenance to the crypto module vendors
- Project and schedule risk are reduced
- "Everyone is happy"

Procurement Check-Box

Most technology vendors rely on the assumption that FIPS 140-2 requirements simplify down to a *procurement check-box*.

> **The Procurement Check-Box Assumption**
>
> *If the federal agency is able to verify a FIPS 140-2 certificate is associated with a desirable product, then the procurement requirements are met.*

In the example in Section 1 of this paper, ZZZ Security Inc. has met the so called *procurement check-box* criteria with their ZZZipit product. At this point, the ZZZ Sales Team may have some initial success selling their ZZZipit product to federal agencies.

If this seems like a low-bar to you, then you are in the majority of those that agree this is less than ideal. Satisfying the *procurement check-box* is the starting line, not the finish line. Your federal customers deserve more.

What Federal Agencies Need

Federal agencies need to protect sensitive data using FIPS 140-2 validated cryptography. These agencies want to acquire products that satisfy the intent of the FIPS 140-2 requirements. Diligent agencies will ask the following questions:

1. Is the product using FIPS validated functionality to fulfill all cryptographic needs and to protect all sensitive data?
2. Does the product utilize cryptography that is not FIPS validated or has been deprecated or disallowed? If so, can the product be configured to use cryptography other than FIPS approved algorithms? How is configuration controlled?
3. Are the security protocols (TLS, SSH, …) included in the FIPS validated modules? What cipher suites or protocol parameters may be used within FIPS constraints, and how are those controlled or enforced?
4. How are appropriately strong, valid keys established (generated, derived, transported) into the module, and how are the keys and other sensitive parameters protected?
5. Are the key strengths used for key transport and/or key agreement sufficient for the symmetric keys used to protect sensitive data?

What are " … all the cryptographic services in the solution … "?

The CMVP statement recommends assurance that the cryptographic module inside the product provides " … all the cryptographic services in the solution." What functions use cryptographic functionality?

Many solutions incorporate the following:

- Application layer secure communication protocols, like TLS, https, and TLS VPNs
- Network layer secure communication protocols, like IPsec and IPsec VPNs
- Administrative and monitoring protocols, like SSH and SNMP
- Authentication of:
    - Operators
    - Firmware or software
    - Certificates and chain of trust
    - Namespace and domain parameters, like DNSSEC
- Media encryption (e.g. dm-crypt and associated utilities like cryptsetup)
- Protection of secrets (e.g. encrypted storage or file formats)

A Better Approach

Assuring FIPS 140-2 Inside

How can you provide your federal customers with the assurance that you have implemented FIPS validated modules properly without going through the entire FIPS validation process?

Often times, the federal agencies planning to acquire your product do not provide specific guidance for the type of FIPS 140-2 validation that you should pursue. As you determine your FIPS strategy, communicate your plans to your prospective federal customers to solicit feedback.

In the absence of customer requirements, a *FIPS 140-2 Inside* strategy may be the clearest path to reaching federal customers. At a minimum, using FIPS validated modules should speed up and simplify a larger FIPS validation effort if that becomes a future requirement.

A Good Approach

If you currently leverage the *FIPS 140-2 Inside* strategy at your company, then ask your Product or Certification Team — "Can we credibly supply a signed letter stating (a) our product incorporates a validated module, (b) the module provides all the cryptographic services in the solution, and (c) the module's validation certificate number?"

Very few companies create this signed letter for their federal customers even though the CMVP recommends agencies should obtain such a letter before acquiring a product. Would this type of letter save your company time by reducing "FIPS" technical calls? Would this type of letter differentiate your company as one that is proactive in bringing value?

At a minimum, your federal customers deserve this signed self-assessment letter.

A Better Approach - Be the 10%

An even better approach is to provide an independent report as assurance to your customers that your product meets the intent of the FIPS 140-2 requirements.

Joining the top 10% of companies providing critical information about their FIPS 140-2 Inside implementation is straightforward. Following the suggestions in this section is a win for your company and for your federal customers. Offering assurance of proper *FIPS 140-2 Inside* implementations will place you ahead of your competitors that continue to believe the *procurement check-box* is all that federal agencies want.

The ZZZ Product Team decided to join the 10% by executing these *FIPS 140-2 Inside* best practices.

FIPS 140-2 Inside Best Practices

Consider these best practices for properly implementing a *FIPS 140-2 Inside* strategy.

1. **Select FIPS validated modules with a strong shelf life**
   Some examples include the following. If you need to generate RSA keys, then make sure the FIPS module has an associated CAVP certificate for FIPS 186-4 RSA Key Gen. In the 2018 timeframe, we expect ECDH implementations will need to be compliant to SP 800-56A (a revision to SP 800-56A is currently in the works at NIST).

2. **Follow the intent of the FIPS 140-2 requirements in your implementation**
   Approach your implementation of FIPS validated modules in the same way that you would if you were validating a larger FIPS cryptographic boundary. Document the entropy sources if keying material comes from outside of the FIPS validated modules. Document the management of keys that exist outside of the FIPS validated modules. Document other cryptographic libraries that are not included in the FIPS validated modules. Provide instructions for configuring your product for proper use by customers that require FIPS. Include a method to verify that your product is configured for "FIPS mode."

3. **Know how keys are generated and the source of randomness**
   Document the methods of key generation, and assure that these methods use appropriately strong sources of randomness for keying material. Be especially cautious about sources of entropy that are outside of the FIPS validated modules.

   Is randomness really an issue? See what these researchers found: https://factorable.net

4. **For software modules, make a decision on "Tested Configuration" or "Vendor Affirmation"**
   During the FIPS validation process, software modules are tested on a specific operating system and hardware device. These "Tested Configuration(s)" are listed as part of the FIPS 140-2 certificate that is posted on the NIST website. To have your specific operating system and hardware listed as a "Tested Configuration," you will need to work with your FIPS consultant or FIPS module vendor to execute the proper FIPS testing with an accredited FIPS Lab. If you are using an open source FIPS module, then you will need to work with your FIPS consultant or your FIPS Lab to perform the proper testing.

   Another option exists to "Vendor Affirm" the operating system you are using with the FIPS module. An overview of this process is available at the KeyPair Consulting Inc.'s News link or you may reference the requirements in FIPS 140-2 Implementation Guidance G.5. Please note that the vendor listed on the FIPS 140-2 certificate is responsible for adding "Vendor Affirmed" operating systems to the FIPS 140-2 Security Policy. Your FIPS consultant or your FIPS module vendor are able to assist with "Vendor

Affirmations" of operating systems.

5. **Perform an independent review**
   Contact KeyPair Consulting to perform an independent assessment of your *FIPS 140-2 Inside* implementation. We will prepare the documentation and perform a code review to confirm that your integration and use of FIPS validated modules are consistent with the intent of the FIPS 140-2 requirements.

   In the CMVP document *Frequently Asked Questions for the Cryptographic Module Validation Program,* the following statement cautions end users of products leveraging *FIPS 140-2 Inside* (embedded modules):

   > *There is no assurance that a product is correctly utilizing an embedded validated cryptographic module – this is outside the scope of the FIPS 140-1 or FIPS 140-2 validation.*

   By performing an independent review, you are providing assurance to your customers that your product is correctly utilizing an embedded validated cryptographic module.

Zipping It All Up

After the ZZZ Product Team completed these best practices, they observed the following results:

- By presenting an assurance letter from an independent review, the ZZZ Sales Team proactively communicates to their prospects that ZZZ Security's *FIPS 140-2 Inside* strategy was executed properly
- The ZZZ Product Team and ZZZ Engineering Team have fewer FIPS-related conference calls with prospective customers
- By leveraging an effective *FIPS 140-2 Inside* strategy, the ZZZ Engineering Team avoided FIPS validation testing tasks which allowed them to meet their product feature development deadlines

Take Action

If you are the TL;DR[3] type, here is the quick take on your next steps to crossing the *FIPS 140-2 Inside* finish line:

1. GOOD: Have your organization assess the solution and create a signed self-assertion letter that includes the information in **A Good Approach** section above
2. BETTER: Complete an independent review of your *FIPS 140-2 Inside* integration as described in **A Better Approach - Be the 10%** section above.

> *It is easy to sit up and take notice, what is difficult is getting up and taking action.*
>
> Honore de Balzac

The latest version of this paper may be downloaded at:

https://keypair.us/2017/10/fips-140-2-inside-paper/

[3] TL;DR is short for "too long; didn't read"