FIPS vs “FIPS Inside”

Corsec Explains the Differences Between FIPS 140-2 and “FIPS Inside”

Cryptography and FIPS Validations:

Early on in the pursuit of validations for cryptography-enabled products, the roadmap was clear: a crypto device meant for federal networks processing SBU information needed to undergo a FIPS validation. These products were hardware-based, and the standards written against which they'd be evaluated were written with hardware-based solutions in mind. Initial products had one subcomponent that's sole responsibility was to encrypt data and deliver it securely. This function was well defined and the rest of the product operated independently of that function. An original link encryptor is a perfect example of a function within a product that focused entirely on encryption. The only piece of the product that needed to address security for encryption was fully validated and protected, resulting in a completely secured product.

Fast-forward to today. Continuing improvements in cryptography have resulted in solutions that come in many forms, including software, hardware, firmware, and combinations thereof. To address the changing landscape of cryptographic enablement, the FIPS standard also had to change.

For more on FIPS 140-2, click here.

What is "FIPS Inside":

"FIPS Inside" is a term used to reference a device or appliance that employs a FIPS-validated subcomponent to provide its cryptographic services. The option of validating a software-based "FIPS Inside" solution opened the door for third party vendors to develop, validate, and market their own cryptographic solutions. Open-source libraries have been heavily leveraged over the past few years because they offer a "plug and play" validation solution. Vendors needing to make the claim of using FIPS-validated cryptography would simply integrate these third-party libraries into their proprietary code.

Although the original intent of the standard was to validate all of the encryption within a product, the ability to validate a subcomponent still exists. FIPS validations can still be performed on sub-components such as server blades, embedded cards, crypto chips, and even software libraries. This became an attractive validation alternative, particularly

Corsec Security Inc.
13921 Park Center Rd., Suite 420, Herndon, VA 20171

for vendors that only developed software, or for those that wanted to insulate their validation status from non-security-related product changes.

In reality, most products contain multiple sources of encryption and require higher levels of security product wide. Take a cryptographic library for example; multiple components within a product access and communicate with the library, leaving multiple points of entry and sources of vulnerability. To conform with the intent and spirit of the standard, all components of the product should now be validated. Although embedding a FIPS validated product has always been acceptable, the new implementations of the guideline results in weakened product hardening and a movement away from the standards original intent.

FIPS modules can form the basis for a good security solution, but the more you extend the functionality, the more you open the product up to risk.

("FIPS Inside" used to secure a crypto library, leaving multiple vulnerabilities)

Corsec Security Inc.
13921 Park Center Rd., Suite 420, Herndon, VA 20171

FIPS Validated vs "FIPS Inside":

To some vendors, both FIPS Validated and "FIPS Inside" can be viable options in security. To the U.S. government, or other governments, or to the Commercial world, these are not options. FIPS validation provides a certain level of security assurance; "FIPS Inside" doesn't. And this is critical especially when thinking about who controls important aspects of the targeted solution.

The optimal scenario for any certification is that the vendor of the device also controls the targeted subcomponent. However, when relying on a third party's software solution, as is the case with "FIPS Inside", the path presents its share of very real pitfalls. To help we have generated a comparison between the two:

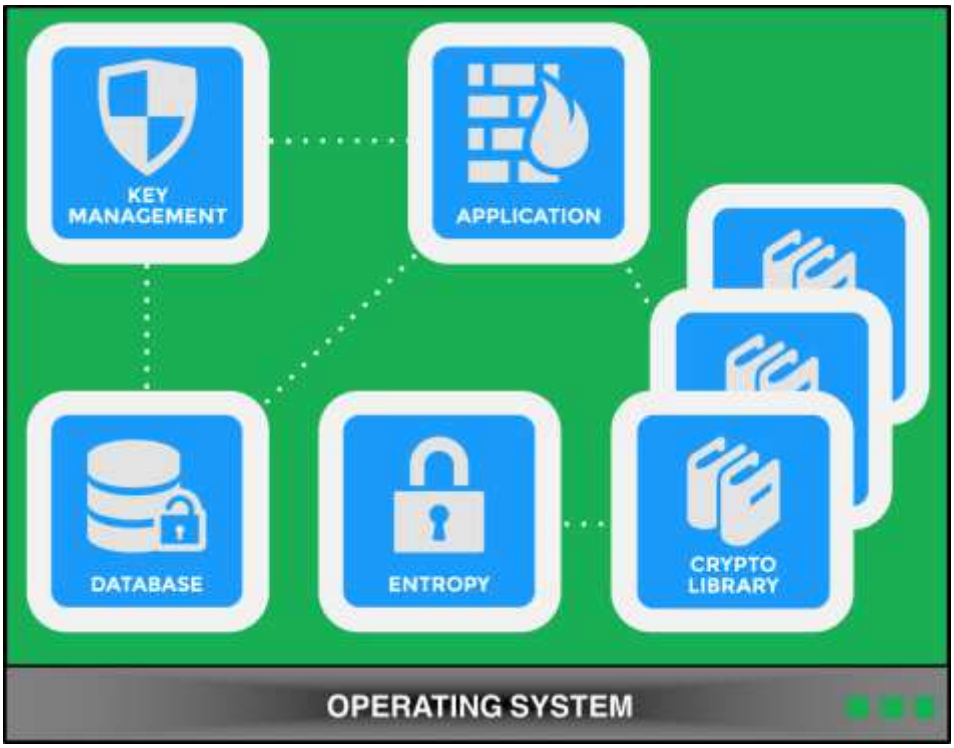
	FIPS Validated	*"FIPS Inside"*
Security Assurance	Independently tested by an accredited lab whose work was reviewed and approved by an oversight body of representatives from the U.S. and Canada: Provide assurance that a cryptographic module is in conformance to the standard.	When a vendor relies on another vendor's certificate, the product is not specifically tested nor is it approved by a third party for assurance: Considerably weakens assurance claims.
Business Risk	You control the schedule, maintenance and version of your own product. If you decide to make changes to your product, you are fully aware of the revocations and changes needed in order to conform to compliance. Eliminates unknown degradation as a result of third party conformance to standards.	Third party validations face expiration and revocation, eliminating FIPS-validated crypto functionality claims. Reliance on third party developers that conformance issues are important enough to fix AND re-validate in a suitable timeframe. Potential loses in revenue and opportunities.
Brand + Reputation Impact	Full validation and accreditation of all crypto claims. Proof of complete validation through accredited labs and governments Demonstrated brand hardening and organizational commitment to security	Without a full understanding of a crypto library's integration, additions to the solution's codebase are difficult to make, creating claims of security based on "trust" that a third party has engineered it to work, as opposed to an organizational guarantee that the product's development and security claims are valid.
Market Differentiation	Proof to customers that that the product's due diligence was performed and there is organizational ownership of security. Significant security posturing against "FIPS Inside" compliant products in the marketplace.	Without an independent FIPS validation (assurance accepted industry-wide), security capabilities and viability for processing SBU (sensitive but unclassified) information is questioned.
Time	Usually between 12-14 Months	Potentially 4-6 Months

Should I Validate My Entire Product?

Factors such as convenience, resource availability, time-to-market, sustainability, long- and short-term costs, benefits, and risks must all be weighed to determine the most viable course of action. While integrating a third party crypto service solution in order to meet FIPS requirements seems like the best choice (and sometimes, it actually is), there are a growing number of business-related drawbacks to this path that must be identified and weighed.

Choosing a path with these drawbacks without careful consideration could impact your validation status and ability to compete for years to come.

Contact Corsec to understand the difference between complete protection and pseudo-security.



(A fully secured product, with multiple sources of encryption, all FIPS 140-2 validated)

Secure Product, Secure Brand, Secure Bottom Line

Corsec Security Inc.
13921 Park Center Rd., Suite 420, Herndon, VA 20171