‘FIPS Inside’
A Strategic Advantage for FIPS 140-2 Validation

A Paper from SafeLogic

SafeLogic Inc.

530 Lytton Ave, Suite 200

Palo Alto, CA 94301

www.SafeLogic.com

Background

A FIPS 140-2 validation may be completed for either a cryptographic module as a component of a product or for a standalone product. SafeLogic's CryptoComply modules exemplify the former; customers embed our product to achieve FIPS 140-2 compliance for hardware or software modules. The SafeLogic RapidCert process delivers a FIPS 140-2 validation for the module in use in that customer's name for full transparency to their end user. Some people refer to this as 'FIPS Inside', meaning that there is a validated module inside a larger product.

Federal agencies are mandated to require procured products to use FIPS 140-2 validated encryption modules for any cryptographic functions. Note that this mandate does not demand that the entire product receive validation. In fact, cryptographic testing is irrelevant for product features outside of the encryption module itself and can create undue complication in the validation process, as well as trigger otherwise unnecessary and costly revalidation efforts in the future. There are significant advantages to the 'FIPS Inside' approach, and SafeLogic provides additional value for all FIPS 140-2 needs. These are some of the common discussion points and questions.

Benefits of Using a FIPS 140-2 Validated Module

Strategy	Benefit
Leverage existing FIPS 140-2 validated crypto modules	Reduce or even avoid the FIPS validation process by leveraging centralized certificates instead of one for each product variation.
Well-defined and minimized cryptographic boundaries	Allows for easier product updates (including product updates and fixes for security vulnerabilities). Need to make a non-FIPS relevant change or enhancement? Make those changes outside the boundary, keeping your product in full compliance while remaining at the cutting edge. Only updates specific to the encryption module will require a revalidation.
Offload the FIPS maintenance to the crypto module vendor (including new guidance and algorithm transitions)	Get more longevity from your certificate. Vendors don't need to continually re-engage costly consultants for "guidance" or to revalidate for non-cryptographic updates to the product. SafeLogic simply pushes updates to customers as needed and ensures that compliance is maintained.
Project and schedule risk are reduced	Your engineering resources will spend less time figuring out FIPS 140 requirements and implementing new code. They can specialize in improving the product, not reinventing the wheel of compliance. Your sales resources have something to sell quicker and on a more reliable development cycle.
Reduced time to market	By leveraging CryptoComply and SafeLogic's RapidCert process, product vendors can receive a FIPS 140-2 Level 1 certificate in as little as 6-8 weeks.
Stepping stone to hardware Level 2 validations if required	Some end users will require Level 2 validations. If the product contains software, then an embedded validated module provides the necessary features and functions for algorithms and most self-tests. The gap-up effort to Level 2 is quicker and easier as a result, SafeLogic can assist, and the intermediate Level 1 validation strengthens sales and competitive positioning in the meantime.

Misperceptions of 'FIPS Inside'

Claim	Response
A standalone product FIPS validation is better than leveraging a FIPS validated encryption module	FIPS 140-2 validation, for better or worse, is a checkmark, not a ranking. Unless a customer specifically requires a Level 2 or higher validation, Level 1 meets the mandate, while Level 2 testing requirements simply slow down the process. This increases the likelihood that the product is obsolete or at a competitive disadvantage by the time it is validated, backfiring on the vendor's efforts to supersede a rival. Further, a larger, more comprehensive testing boundary increases the risk for revalidation due to the sheer number of moving parts. These are all advantages for a consultant, but not for a vendor.
A standalone product FIPS validation is more secure than leveraging a FIPS validated encryption module	The more narrow the certification boundary, the more flexible and agile the product will be. A larger boundary will yield a more frequent debate over whether to make security updates or not, based upon a reluctance to revalidate the product. By limiting the certification boundary to the core encryption module, very few product updates would necessitate revalidation. Thus, products can make revisions as needed, without requiring revalidation, keeping up with the latest security research and gaining a competitive advantage.
Federal agencies prefer standalone product validations over leveraging a FIPS validated encryption module	Federal procurement officers don't see FIPS 140-2 validation as a differentiator. Rather, it is a checkmark prerequisite that they have been mandated to confirm. As long as the deployed encryption is in FIPS mode, the product has qualified for procurement.
The product may not be using the embedded module correctly	SafeLogic has not experienced this objection from any customer feedback, government policy, or end-user discussions. If such a question does arise, FIPS Testing Labs provide services to independently verify and provide an attestation to the correct use of an embedded FIPS cryptographic module in a product. SafeLogic is happy to assist in this process, should it be required.
Entropy analysis not included in the FIPS validation	This is an evolving element of FIPS 140-2 validation. The entropy sources are typically the same for FIPS module components and standalone products. In the event independent, third-party attestation is required, FIPS Testing Labs provide services to independently verify the entropy sources for the supported operating environments of modules that are components of product. Again, SafeLogic is happy to assist in this process, should it be required.

Contact Information

For any questions on this document, please contact:

Doug Rossie
VP Business Development and Partnerships
SafeLogic Inc.
Email: Doug@SafeLogic.com
Phone Number: (703) 829-5290

About SafeLogic

SafeLogic's product line is focused on standards-based cryptographic engines designed for use in Cloud, mobile, wearable, IoT, server, workstation, and appliance environments. These modules have been fully validated to FIPS 140-2 standards and offer drop-in OpenSSL and Bouncy Castle compatibility, a variety of connectors to accommodate unique product architecture, and instant compliance for federal deployments to SafeLogic customers.

Even better, SafeLogic modules include RapidCert, the industry's only FIPS 140-2 validation service that provides a certificate in the customer's name, while drastically accelerating the timeline, requiring no additional engineering effort, zero interaction with testing labs, and at a fixed cost.

SafeLogic's customers are among the most influential and innovative companies in technology today, from startups to the Fortune 100.

SafeLogic was established in 2012, is privately held and is headquartered in Palo Alto, California.

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301

(844) 4-ENCRYPTION

www.SafeLogic.com

www.Twitter.com/SafeLogic