certicom™

Certicom Security for Government Suppliers

developing products to meet the US Government FIPS 140-2 security requirement

THE PROBLEM

How can vendors take advantage of the lucrative but complex government communications space? In 2002, US Federal Government spending on IT security doubled from the previous year to approximately $2.5 billion. More than $700 million of that was set aside for cyber initiatives. Government spending for 2003 maintains this high level of funding.

However, the National Institute of Standards and Technology (NIST) specifies security requirements for any system protecting sensitive but unclassified information in the Federal Information Processing Standards (FIPS). These standards, such as FIPS 140-2, are binding on US government agencies. Any product sold to the US government must comply with one or more of the relevant FIPS publications. The Government of Canada, through the Communications Security Establishment (CSE), worked with NIST to develop these standards and has adopted a similar policy.

FIPS validation is an independent verification that the secure technologies used by government agencies meet a predetermined security profile. Any Original Equipment Manufacturer (OEM) or application developer wishing to enter the government space, or grow its existing revenue there, must have FIPS validation for its solution.

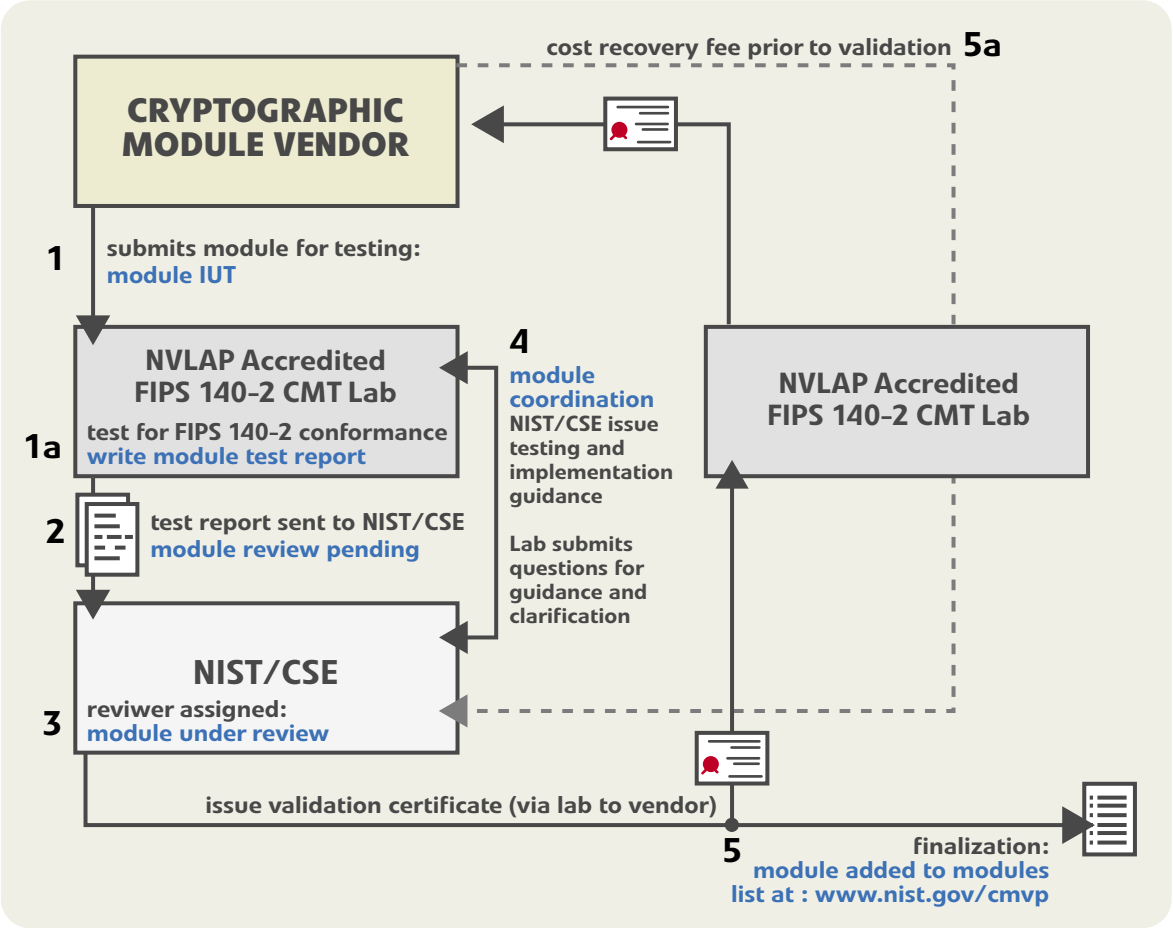
NIST has accredited several labs to test vendor products and technologies for FIPS validation but high demand combined with the thorough testing process results in lengthy waiting periods that can be over two years.

Moreover, the complexity of building to the FIPS 140-2 standard means that 96% of tested cryptographic modules and 65% of tested security algorithms contain FIPS errors[1]. So vendors can spend time and money developing a solution that requires FIPS-validation for the government market, then submit it to a testing process that can take years, and afterwards learn that their solution is flawed and cannot be FIPS-validated without improvements. This is a truly daunting barrier to entry in this valuable market space.

FIPS continue to evolve and incorporate new technologies for the future. Among these is Elliptic Curve Cryptography (ECC), a highly efficient form of public key cryptography that offers the same high security of other technologies but with much smaller key sizes. This results in higher speeds and lower power consumption, as well as memory and bandwidth savings.

Certicom is an ECC pioneer and market leader. Certicom's ECC technology has now been licensed by the US National Security Agency (NSA) to be implemented as a crucial technology for mission critical national security information. Government suppliers are well-advised to ensure their secure solutions keep pace with these new technologies as they become part of FIPS.

[1] NIST survey of accredited FIPS laboratories.



FIPS 140-2 Testing and Validation Flowchart

THE SOLUTION

For most vendors, there are two important forms of FIPS validation. The first validates only the encryption techniques used by a particular solution. This includes encryption algorithms, hash algorithms and digital signatures. For example: DES, 3DES, AES, DSA and SHA1. In this case FIPS identifies how these are defined, and how they must be implemented to achieve validation.

The second, higher level, and more important validation is FIPS 140-2. This standard specifies eleven security areas that must be met by a "cryptographic module" used inside a security system that protects information. A cryptographic module can be hardware, firmware or software that carries out cryptographic functions like encryption, authentication techniques or random number generation. A cryptographic module performs the security services for a particular product.

To receive FIPS 140-2 validation, a cryptographic module must:

- **have a well-defined crypto boundary so that all sensitive security information remains within the cryptographic core of the product;**
- **use FIPS-approved algorithms with correct implementation and an intact crypto boundary.**

The product may have other security functionality outside the crypto module but this would not be FIPS 140-2 validated. Certicom offers two solutions for easing or ensuring the FIPS validation process for your device or application: Security Builder® Crypto™-C and Security Builder GSE™.

Security Builder Crypto-C simplifies and accelerates your FIPS validation process by providing:

- **plug and play encryption, public keys and other security mechanisms**
- **small code size that is ideal for constrained and wireless environments as well as traditional platforms**
- **FIPS-validated algorithm implementations for proven security**

Government suppliers that require FIPS 140-2 validation find the Security Builder GSE developer toolkit even more attractive. It provides a complete FIPS 140-2 validated cryptographic module that you can incorporate directly into your products. Thus, you avoid the lengthy and costly FIPS approval process entirely.

Security Builder GSE has earned FIPS 140-2 validation certificate #316 for Windows 98 and Windows CE 3.0 and certificate #351 for Palm 4.1 from NIST's Cryptographic Module Validation Program. This achievement makes Security Builder GSE the first solution to receive the designation for use on both PC-based and multiple wireless operating systems.

The Security Builder developer toolkits also have a concise and intuitive API for desktop and wireless applications, dramatically reducing time-to-market and providing interoperable end-to-end security.

THE IMPLEMENTATION

FIPS 140-2 identifies eleven areas for a cryptographic module used inside a security system that protects information:

- **cryptographic module specification**
- **cryptographic module ports and interfaces**
- **roles, services and authentication**
- **finite state model**
- **physical security**
- **operational environment**
- **cryptographic key management**
- **electromagnetic interference/electromagnetic compatibility (EMI/EMC)**
- **self tests**
- **design assurance**
- **mitigation of other attacks**

The standard also provides four increasing, qualitative levels of security, from 1 to 4 (1 being the lowest) for these eleven areas and then assigns a single overall rating. The different levels provide increasing levels of security as follows:

Level 1: No physical security mechanisms are required in the module beyond the requirement for production-grade equipment.

Level 2: Tamper evident physical security or pick resistant locks. Level 2 also provides for role-based authentication.

Level 3: Tamper resistant physical security. Level 3 provides for identity-based authentication.

Level 4: Physical security provides an envelope of protection around the cryptographic module and protects against fluctuations in the production environment.

The rating depends on how many of the eleven FIPS 140-2 requirements the cryptographic module meets. The four security levels address a range of implementation scenarios. The security level of a cryptographic module is determined by:

- **appropriate security for the requirements of the application**
- **the environment in which the module operates**
- **the security services the module provides**

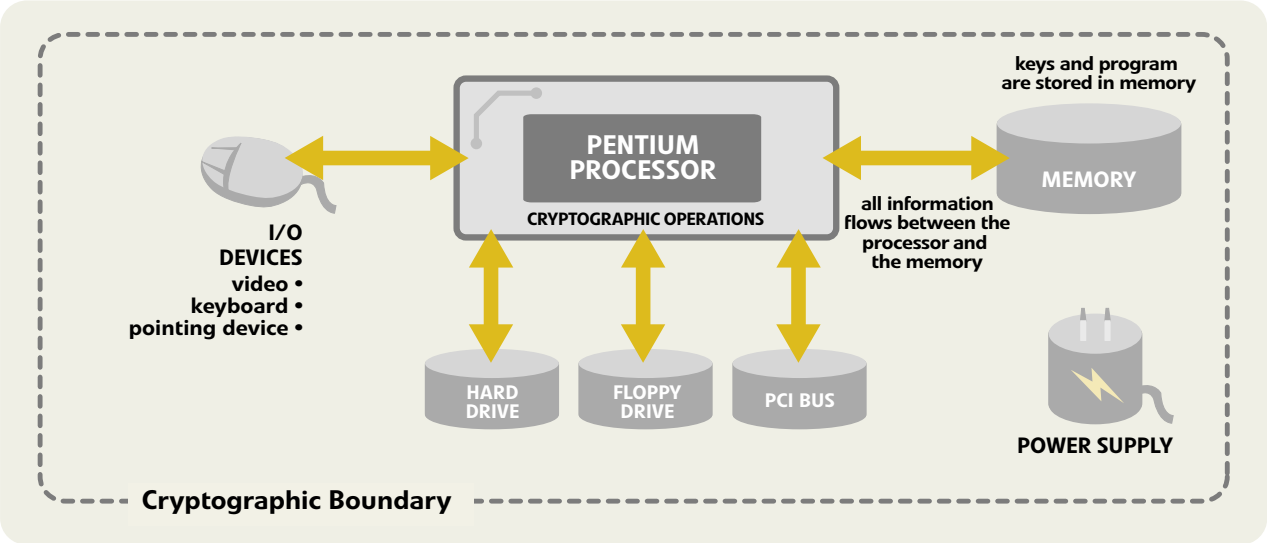
Security Builder GSE is designed to address each of the eleven FIPS areas within a well-defined crypto boundary that uses properly implemented and approved FIPS algorithms.

Security Builder GSE FIPS Validated Algorithm Implementations

Security Builder GSE implements DES, 3DES, DSA, SHA-1, and AES as FIPS approved algorithms. Vendor affirmed implementations include ECDSA, RSA and HMAC.

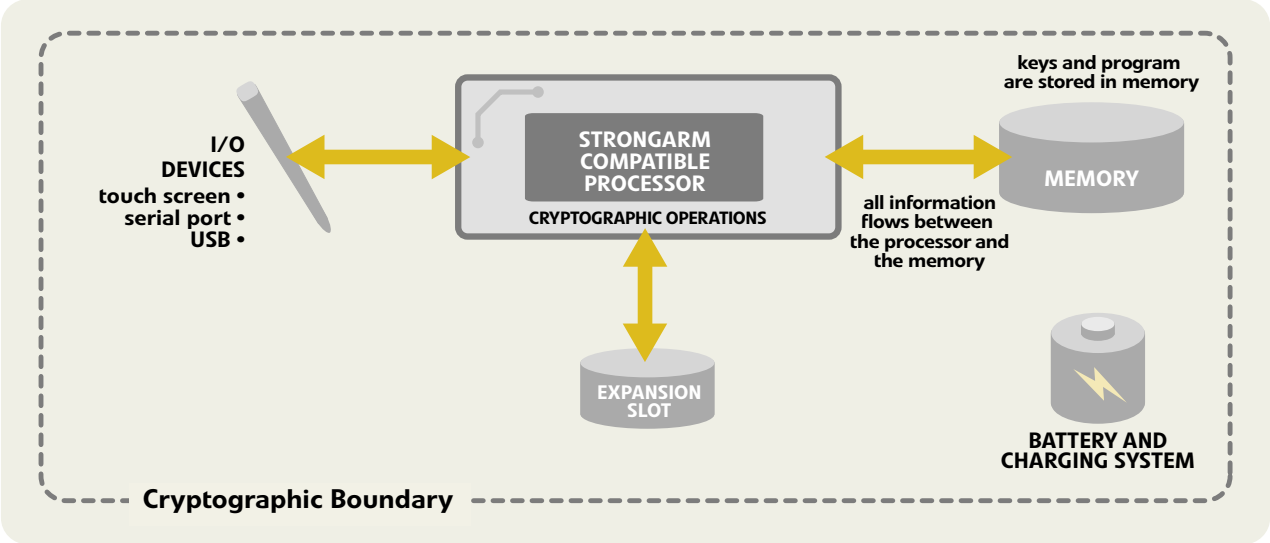
Security Builder GSE cryptographic boundary

Security Builder GSE is validated against FIPS 140-2 Level 1 for three representative C modules: **Windows® 98** (representative server platform), **Windows CE** (representative embedded platforms), and **Palm OS** (representative embedded platforms). The Security Builder GSE module is supplied in the form of shared libraries and is a multi-chip stand-alone module. The cryptographic boundary for these platforms appear below.



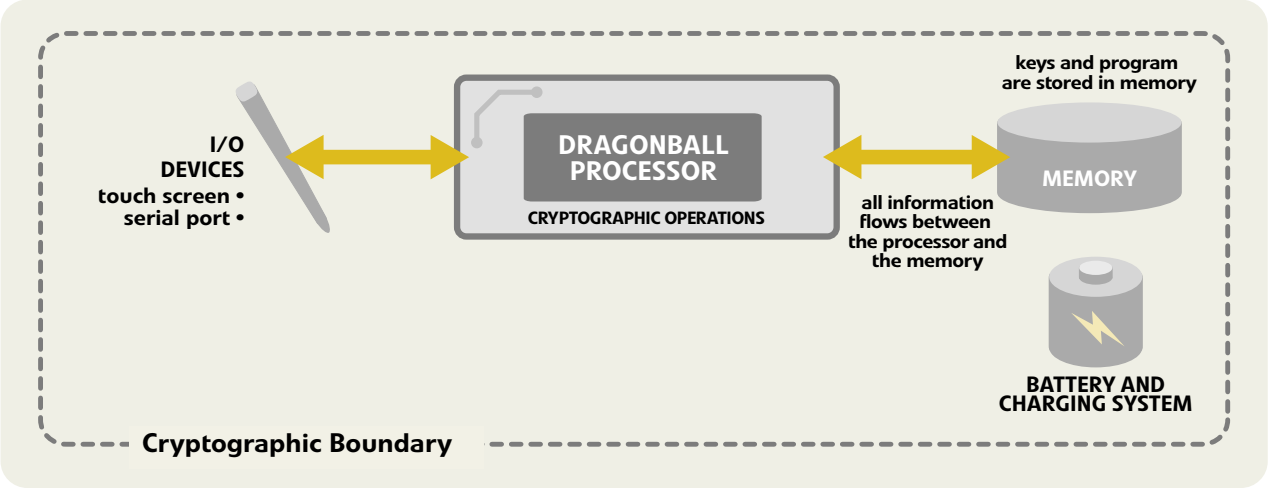
Windows 98 and compatible systems

For Windows 98, the crypto boundary is an IBM-compatible PC, running the Windows 98 operating system (or a compatible version of the operating system), and the Security Builder GSE module.



Windows CE and compatible systems

The crypto boundary for the Windows CE platform is a Windows CE based PDA (such as Pocket PC and Handheld PC), running the Windows CE 3.0 operating system (or a compatible version of the operating system) on the StrongARM-compatible processor, and the Security Builder GSE module.



Palm OS 4 systems

The crypto boundary for the Palm OS platform is a Palm OS compatible PDA running Palm OS 4.1 (or a compatible version of the operating system) on a Dragonball processor, and the Security Builder GSE module. The boundary of the module also contains the Palm OS DLL.

Security Builder GSE can run on all of these platforms to meet all FIPS 140-2 Level 1 physical security and operating system specifications. The module can also be used in applications requiring higher levels of FIPS 140-2 validation when it is combined with additional security mechanisms such as tamper-evident or tamper-proof chassis.

Security Builder GSE is interfaced via API function calls. These provide the interface to the cryptographic services for which the parameters and return codes provide the input/output data and status conditions. The API function calls are used to provide FIPS 140-2 Level 1 validated cryptographic services.

RESULTS

Government suppliers that integrate solutions which already hold FIPS validation reduce or eliminate the time and expense of the lengthy validation process from their development schedule. This significantly accelerates the ability of these vendors to enter the lucrative government market.

Whether government suppliers chooses to integrate FIPS validated algorithms into their own cryptographic modules, or if they prefer to use an existing FIPS 140-2 validated cryptographic module, they now have a cost-effective, timely method of adhering to the standards their government customers are required to follow.

In addition to advocating this approach, Certicom puts it into practice: Security Builder GSE is used to ensure Certicom's movian security applications meet the FIPS 140-2 requirement. Likewise, customers including LRW, Digital, Bluefire Security and Synchrologic have benefited by integrating Security Builder GSE into their existing applications.

about certicom

Certicom is a leading provider of wireless security solutions, enabling developers, governments and enterprises to add strong security to their devices, networks and applications. Designed for constrained devices, Certicom's patented technologies are unsurpassed in delivering the strongest cryptography with the smallest impact on performance and usability.

North America 1.800.561.6100
EMEA +44 20 7484 5025
International +1.905.507.4220
E-mail info@certicom.com
www.certicom.com

certicom™