Meeting Security Certification Requirements with Certicom and QNX

Rick Pitz, Product Manager, Security Toolkit, Certicom
Yi Zheng, Product Manager, Safety and Security Products, QNX Software Systems
sales@certicom.com, yheng@qnx.com

Introduction
As government agencies, health care providers and financial institutions deploy increasingly complex network-oriented services, the range of devices accessing these systems continues to expand. Concurrent with this development, there is a growing focus in these sectors on information security and privacy: organizations are investing enormous sums to satisfy data security requirements for everything from servers and network equipment to laptops, smartphones and printers. For example, over the next five years, the U.S. federal government will invest more than $500 billion on Information Technology (IT)\(^1\), with a sizeable portion of this money directed to the Crypto Modernization Program and activities related to encryption and key management.

To help reduce the complexity and costs of its expanding networking and security needs, the U.S. federal government has published strict standards and interoperability requirements: Federal Information Processing Standard (FIPS) 140-2 *Security Requirements for Cryptographic Modules*. This cryptographic security standard has been adopted by several other governments, and is becoming a reference standard in healthcare, finance and the emerging smart grid sector. Under the U.S. government’s Crypto Modernization Program, the implementation of other advanced cryptographic techniques, such as Elliptic Curve Cryptography\(^2\), is growing and expected to influence the future of security.

To compete in these markets, software and device vendors must demonstrate that their products meet Federal Information Processing Standard (FIPS) validated cryptography requirements, a long, complex and costly endeavor that must be revisited with each product upgrade. Vendors must also ensure that upgrades, no matter how trivial, do not compromise their products’ FIPS security compliance, as they must also continuously monitor the standards themselves to ensure that their products keep up with evolving requirements—FIPS 140-3, which is set to supersede FIPS 140-2, is already available in draft form.

Of the many and diverse components that make up today’s software systems, two are most important for the system’s security:

- an OS that meets strict safety requirements for dependability\(^3\)
- a FIPS-validated cryptography module

\(^2\) ECC in particular provides key strengths capable of long-term data protection quite suitable for sensitive personal information such as electronic medical records.
\(^3\) Dependability = Reliability (responds correctly) + Availability (responds when required)
In this paper we examine some key challenges associated with the FIPS 140-2 validation process, and describe how the QNX® Neutrino® RTOS and the Certicom Security Builder Government Security Edition (GSE) cryptographic library can help ease the burden of building and delivering FIPS 140-2 compliant software.

COTS and Security
Like other organizations, government agencies would like to be able to use commercial off-the-shelf (COTS) products in order to take advantage of the expertise and cost savings offered by competitive vendors. To be eligible for use by these agencies, however, these COTS vendors’ products must meet stringent security requirements established by (in the U.S.) organizations such as the Department of Defense (DoD), National Security Agency (NSA), and the National Institute of Standards and Technology (NIST). FIPS 140-2 is the common denominator in the most important computer security directives; the DoD, for instance, refers to this standard in directives governing the communication of sensitive data.

The health care and financial services sectors are similarly affected by information security requirements, especially with the burgeoning number of disclosures of Personally Identifiable Information. Data security requirements in these industries are driven by government legislation, including the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act for health care providers, and the Gramm-Leach-Bliley Act (GLBA) rules on consumer privacy for banks and financial companies. These requirements naturally steer vendors to FIPS 140-2 for guidance on cryptography and data security.

HIPAA regulations state that “Valid encryption processes for data in motion are those that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2.”

This same document specifies that data at rest should be protected in accordance with NIST Special Publication 800-111, which recommends the use of FIPS certified crypto algorithms. Further, the HITECH act even promotes the use of proven security technology by providing audit relief to organizations using FIPS certified products.

The importance of FIPS 140-2 does not end here, though. As critical infrastructure systems, such as gas pipeline distribution and smart grid control systems, become more networked, these industries are likely to adopt similarly strict controls on the cryptography used to protect their data in transit, creating more demand for FIPS certified cryptography solutions.

To capture a larger part of this growing market, or even to maintain their current positions, COTS vendors that have not traditionally required a high level of security expertise have no

---

4 A quick search for FIPS 140-2 on the DoD web site brings up, for example, Instruction 8500.2 “Information Assurance (IA) Implementation” (Feb. 6, 2003), and contract announcement 650-06 (July 10, 2006), which includes in one section the following: “DoD 8500 also cited another updated requirement for FIPS 140-2 security requirements for cryptographic modules.”

5 Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for purposes of the Breach Notification Requirements under Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009, US Department of Health and Human Services, April 17, 2009.

choice but to expand their understanding of current and developing security standards and cryptography technologies, while closely monitoring evolving FIPS requirements. They must also find ways to meet the considerable challenge of supporting these requirements in embedded systems.

A Solid Foundation

A fundamental requirement of any secure system is that it run on a dependable OS. Building a secure system on an OS that cannot provide dependability guarantees is very much like building a bank vault with a dirt floor. Someone will eventually notice and exploit this fundamental weakness.

Key characteristics that make the QNX Neutrino RTOS the ideal OS for Certicom’s GSE cryptographic library include:

**Realtime dependability guarantees**: only a realtime operating system (RTOS) is designed expressly for systems that must respond correctly and predictably to requests in a timely manner.\(^7\)

**Microkernel architecture**: with the QNX Neutrino RTOS’s microkernel architecture, applications, device drivers, filesystems and networking stacks all reside outside the kernel in separate address spaces, and are thus isolated from both the kernel and each other. A fault in one component will not bring down the entire system, and recovery mechanisms can restart the failed processes.

**Pre-emptible lower-priority kernel calls**: to meet realtime commitments, the QNX Neutrino RTOS allows low priority kernel calls to be pre-empted by higher priority processes. Time windows during which preemption may not occur are extremely brief. Further, there is an upper bound on how long preemption is held off and interrupts disabled, allowing developers to ascertain worst-case latencies.

**Priority inheritance**: the QNX Neutrino RTOS implements *priority inheritance*, a technique for preventing priority inversions (the problem that, infamously, plagued the Mars Pathfinder project in July 1997\(^8\)) by assigning the priority of a blocked higher-priority task to the lower-priority thread doing the blocking until the blocking task completes.

**Adaptive partitioning**: the QNX Neutrino RTOS uses adaptive partitioning to prevent processes or threads from monopolizing CPU cycles and starving other processors or threads. With adaptive partitioning, developers can allocate guaranteed budgets of CPU time to processes and threads, and a dynamic scheduling algorithm dynamically reassigns CPU cycles from partitions that are not using them to partitions that can benefit from extra processing time. Partition budgets are enforced only when the CPU is running to capacity. All available cycles are used if they are needed, but when processes in more than one partition compete for cycles, the partitioning enforces resource budgets and prevents resource starvation.

---

\(^7\) For a more complete discussion of realtime OSs, see Paul Leroux, “Exactly When do You Need and RTOS?”, QNX Software Systems, 2009.

High-availability framework: no system is absolutely fault-free; to ensure continued availability, the QNX Neutrino RTOS supports a high availability framework that includes a watchdog that monitors processes for failures; automatic mechanisms that restart failed processes without a reboot; mirror processes that perpetually stand ready to take over the watchdog’s duties if needed; and a programming interface that lets the system designer determine how the watchdog will respond to specific failures.

Multiprocessor capabilities: to ensure both stability during and after migration, and efficiency on multicore systems, the QNX Neutrino RTOS uses bound multiprocessing (BMP), a QNX-specific extension of processor affinity (or thread affinity) that allows developers to specify runmask inheritance for threads. By allowing developers to set runmasks that restrict not just the specified threads but also their child threads to specific cores, BMP helps protect a system migrated to multicore from latent bugs or design features, such as FIFO scheduling, that render code written for single-core processors unreliable on multicore systems, and it helps solve problems, such as cache thrashing, that are commonly associated with symmetric multicore processing. Developers migrating systems to multicore can bind entire thread hierarchies to a single processor to ensure that there are no unpleasant surprises in the new environment.

FIPS 140-2

In the U.S., requirements for government security are regulated by FIPS publications. NIST develops these publications for use across all government agencies. It develops and issues new FIPS publications when there are compelling federal government requirements for new security and interoperability standards.

FIPS 140-2 describes the U.S. federal government cryptography requirements that software and hardware products must meet for sensitive but unclassified use. FIPS 140-2 refers to the validation of the complete module that applications must use to perform the specified cryptographic functions. See “FIPS Validation” below. Other FIPS, such as FIPS 186-2, which describes the use of the Elliptic Curve Digital Signature Algorithm (ECDSA), and FIPS 197, which specifies the Advanced Encryption Standard (AES), are specific implementations of cryptographic algorithms that are included in a FIPS 140-2 validated module.

In 2002, the Federal Information Security Management Act (FISMA) removed a provision that allowed government agencies to issue waivers for the purchase of non-FIPS approved products. This removal meant that, henceforth, FIPS 140-2 validation became mandatory for all products that implement cryptography and are sold to the U.S. federal government. Without FIPS 140-2 validation, products will not be considered by U.S. government customers. In addition, outside the U.S., countries such as the United Kingdom, and Canada through its Communication Security Establishment (CSE), have adopted FIPS 140-2 for their security requirements.

Similarly, while FIPS validation is not always required of applications in the health care and financial sectors, it is nonetheless often a requirement. For instance, it is required for medical installations in U.S. government facilities where wireless technology is deployed to transport patient data. And where FIPS validation is not explicitly required, it is still highly recommended when data security is needed. In short, FIPS-validated products enjoy a competitive advantage in these markets.
FIPS 140-2 Validation

For most vendors, there are two levels of FIPS validation. The first level validates the encryption techniques used by specific algorithms, such as those referred to in FIPS 186-2 and FIPS 197. These algorithms include symmetric encryption algorithms such as AES, DES, 3DES and RSA; hash algorithms such as SHA-1; and digital signatures such as RSA and ECDSA. FIPS specifies how these algorithms are defined, and how they must be implemented to achieve validation. The NIST's Cryptographic Algorithm Validation Program (CAVP) performs these validations.

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 running inside a secure system to protect information in that system. This cryptographic module can be hardware, firmware or software. It assumes responsibility for the security services for the system in which it is used, performing cryptographic functions such as encryption, authentication and random number generation.

![Figure 1: The FIPS 140-2 Validation Process](image-url)

FIPS 140-2 defines four levels of security, from 1 to 4 (with 4 being the most secure) for each of the eleven security areas it specifies; it then assigns a single overall rating for the security module. For more detailed information about these levels, please refer to Certicom’s application note: “Certicom Security for Government Suppliers”, available at www.certicom.com/fips.

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 at least one FIPS-approved algorithm with correct implementation and an intact crypto boundary

The process for validating either an algorithm or a FIPS 140-2 cryptographic module is outlined in Figure 1 above. At least one algorithm used in the FIPS module must be validated by the CAVP prior to entering the FIPS 140-2 validation process through the
CMVP. The entire FIPS module must then be validated through the Cryptographic Module Validation Program (CMVP), which like the CAVP is operated by NIST. All tests under CMVP are conducted by one of the Cryptographic Modules Testing (CMT) laboratories accredited under the National Voluntary Laboratory Accreditation Program (NVLAP).

Market Entry Barriers and Issues
While the government market is attractive and lucrative, for many vendors the FIPS validation process represents a significant barrier to entry. The choices available to vendors hoping to sell to government agencies (or for that matter many health care and financial institutions) are limited: they can either build a product from the ground up, or they can buy a FIPS-140-2 validated cryptographic module from a commercial vendor.

Anyone considering building should note that the validation process takes from eight to 12 months, requires the commitment of several developers, and costs some $50,000 just for the cost of the initial validation. To this initial expense must be added costs of $10,000 to $15,000 for each subsequent submission of the same module (updates, bug fixes, correction of initial errors, etc.). Thus, factoring in development costs, module validation runs easily over $100,000.

Note also that when submitting a cryptographic software module for validation, the vendor must provide the following documentation: security policy, finite state machine, software module descriptions, source code listing for all software within the cryptographic boundary, description of module roles and services, description of key management life-cycle, and algorithm conformance certificates. Validation is platform specific: individual validation certificate numbers are required for each platform. Moreover, any change or addition to a validated product imposes a new validation cycle on that product, along with additional costs.

Further, building a cryptographic module to the FIPS 140-2 standard is not only complex; it has a high failure rate. According to NIST, 48% of cryptographic modules submitted by new applicants and 20% of returning applicant modules contain security flaws. A full 30% of algorithms tested by NIST do not conform to the FIPS standard9. This failure rate suggests that companies may spend considerable time and money developing a solution that requires FIPS validation, then submit it to a testing process that can last up to a year, only to learn that their solution is flawed and cannot be FIPS-validated without further work and expense.

Finally, the cost of FIPS validation doesn’t end when a product receives its first validation. In-house expertise is needed to monitor evolving security standards and industry trends, which may dictate changes to the product to meet market demand, or keep pace with new FIPS requirements. The FIPS 140-2 standard is updated every five years, with new algorithms added to improve the standard, align it with industry trends, and make it more robust. Although existing validations remain in effect when the FIPS standard changes, if a vendor wants to take advantage of the new algorithms in the standard, his product needs to be updated and submitted once again for validation.

Instead of attempting to build their own cryptographic modules, vendors can choose to purchase a pre-validated cryptographic module, which they can then incorporate in their

---

9 NIST survey of accredited FIPS laboratories.
products. The benefits of this approach include FIPS 140-2 validation while bypassing the validation process altogether, minimal development costs, short time to market, and development efforts focused on core competencies. The following considerations will help ensure the correct choice of cryptographic module:

**Extensible architecture:** a platform that offers a common API makes it easier to support new algorithms and security protocols with minimal code re-writes.

**Update flexibility:** using a pre-validated module allows the product vendor to make changes to his product or solution and maintain FIPS validation by re-using the same module for security. The FIPS module supplier assumes responsibility for monitoring the FIPS standard, making the changes to the module and validating the updated module. The product vendor only needs to replace the FIPS module in his product to maintain FIPS validation.

**Platform flexibility:** if FIPS 140-2 validation will be needed for multiple system platforms, the FIPS module supplier must offer validated security modules for all required platforms.

**Resource Constraints:** using a FIPS validated module that has been designed specifically for resource-constrained devices can significantly improve system performance by reducing CPU bandwidth and memory requirements. This gain is especially true in mobile devices where battery life is of major concern.

**Conclusion**

Given the barriers and the benefits associated with developing a FIPS-validated product, finding a reliable FIPS implementation that will get the product to market quickly and with the least amount of risk can mean the difference between success and failure.

QNX Software Systems and Certicom have partnered to provide a shared object module library that gives developers an easy and cost-effective way to take advantage of Certicom's Security Builder GSE FIPS validated cryptographic libraries. This solution enables device manufacturers and independent software vendors to offer their customers solutions with FIPS 140-2 security-certified technology on a proven RTOS foundation.
About Certicom

Certicom, a wholly owned subsidiary of Research In Motion Limited (RIM) (Nasdaq: RIMM; TSX: RIM), manages and protects the value of content, applications and devices with government-approved security. Adopted by the National Security Agency (NSA) for government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the global leader in ECC, Certicom’s security offerings are currently licensed to hundreds of multinational technology companies, including IBM, General Dynamics, Motorola and Oracle. Founded in 1985, Certicom’s corporate office is located in Mississauga, Ontario, Canada. Visit www.certicom.com.

About QNX Software Systems

QNX Software Systems Limited is the leading global provider of innovative embedded technologies, including middleware, development tools, and operating systems. The component-based architectures of the QNX® Neutrino® RTOS, QNX® Momentics® Tool Suite, and QNX® Aviage™ middleware family together provide the industry’s most reliable and scalable framework for building high-performance embedded systems. Global leaders such as Cisco, Daimler, General Electric, Lockheed Martin, and Siemens depend on QNX technology for vehicle telematics and infotainment systems, industrial robotics, network routers, medical instruments, security and defense systems, and other mission- or life-critical applications. The company is headquartered in Ottawa, Canada, and distributes products in over 100 countries worldwide. Visit www.qnx.com.

© 2011 Certicom Corp. and QNX Software Systems Limited, subsidiaries of Research In Motion Limited. All rights reserved.


QNX, Momentics, Neutrino, Aviage, Photon and Photon microGUI are trademarks of QNX Software Systems Limited, which are registered trademarks and/or used in certain jurisdictions, and are used under license by QNX Software Systems Limited. All other trademarks belong to their respective owners.

302207 MC411.94