WP467 (v1.1) December 9, 2016

A FIPS 140-2 Primer for the Zynq-7000 All Programmable SoC

By: Lester Sanders and Ed Peterson

The high level of integration, hardware and software programmability, wide range of built-in security features, and extensive supporting documentation make the Zynq®-7000 AP SoC ideal for use in cryptographic modules that are to be certified under the FIPS 140-2 or ISO/IEC 19790 security standards.

ABSTRACT

In 2002, the Federal Informational Security Management Act directed that the Federal Informational Processing Standard (FIPS) 140-2 be used for products that use cryptography to protect sensitive but unclassified information. Examples of sensitive information are financial and health records. Cryptographic products purchased by federal agencies are required to be certified by NIST to the requirements in FIPS 140-2.

Two programs used in FIPS 140-2 validation are the Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP). Developing a FIPS 140-2 certified product requires that an original equipment manufacturer (OEM) use an independent test lab for CMVP and CAVP certification.

Xilinx FPGAs have been used in projects that comply with these standards for over 10 years. This white paper provides a primer on the FIPS 140-2 certification of a product that uses Zynq-7000 All Programmable SoCs. This white paper also explores certification under the similar international ISO/IEC 19790 security standard.

Introduction

The National Institute of Standards and Technology (NIST) Computer Security Division and the Communications Security Establishment Canada (CSEC) administer the Cryptographic Module Validation Program (CMVP). A FIPS 140-2 certified product typically consists of hardware and software included in an enclosure. Typically, an OEM integrates hardware and software cryptographic modules into the top-level cryptographic module, which then comprises the end product in an enclosure. Cryptographic modules use FIPS 140-2 approved algorithm(s), often the Advanced Encryption Standards (AES) or Rivest Shamir Adleman (RSA) algorithm. The approved algorithm is certified in the Cryptographic Algorithm Validation Program (CAVP).

Vendors and OEMs obtain CAVP and CMVP certification using independent Cryptographic and Security Testing (CST) labs. The labs are accredited by the National Voluntary Laboratory Accreditation Program (NVLAP). The CMVP FIPS 140-2 certification process typically takes 9–12 months. The certification process is expedited if the final cryptographic product consists of certified cryptographic algorithms and cryptographic modules. When a FIPS 140-2 certified algorithm is used in a cryptographic module, the OEM must make the case to the CST that the certified algorithm/module used is not modified.

The Zynq-7000 AP SoC Security section describes security in Zynq-7000 devices. FIPS 140-2 provides security requirements in areas such as cryptographic boundary, cryptographic ports, physical security, key management roles, self-test, and services. In many cases, the FIPS 140-2 security requirement is in the domain of the OEM's top-level cryptographic module. The Zynq-7000 AP SoC security functionality can be used to meet all or some of the module cryptographic requirements, however additional protections (e.g., anti-tamper coatings) might be required outside of the Zynq device for module/system level certification.

The CMVP Overview section describes the four levels of security defined in FIPS 140-2. It also provides details on the Zynq-7000 AP SoC's functionality as it applies to the FIPS 140-2 security requirements. The CAVP Overview provides background information on the CAVP and shows certified cryptographic algorithms used in Xilinx FPGAs and in the Zynq-7000 AP SoC. The ISO / IEC 19790 section takes a look at the international standard and how it compares with FIPS 140-2.

Zynq-7000 AP SoC Security

Two characteristics of the Zynq-7000 AP SoC that facilitate FIPS 140-2 certification are its high level of integration and its hardware and software programmability. The high level of integration provides a cryptographic module boundary, which can reduce the number of levels of hierarchy in the final cryptographic product. The programmability shortens FIPS 140-2 certification time by allowing quick changes to resolve OEM – CST issues.

The Zynq-7000 AP SoC integrates a feature-rich ARM® Cortex™-A9 based processing system (PS) and 28nm Xilinx programmable logic (PL) in a single device. Figure 1 shows the Zynq-7000 AP SoC major hardware components: nonvolatile memory (NVM) controllers, double data rate (DDR) memory controller, mask-programmed bootROM, on-chip memory (OCM), central processing unit (CPU), system-level control register (SLCR), device configuration interface (DEVCI), eFUSE array, and the AES/HMAC engine.(1)

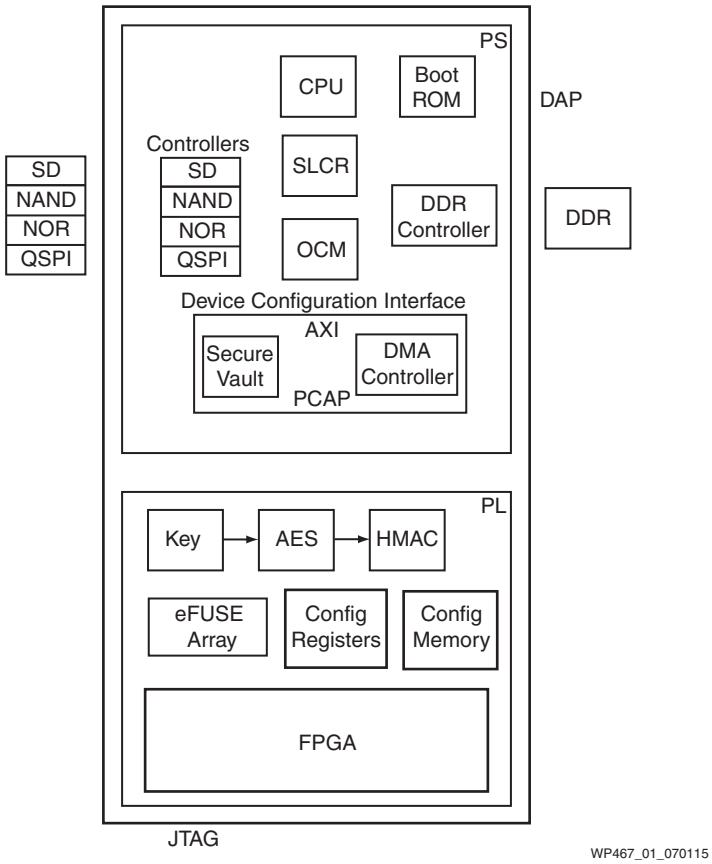

Figure 1: **Zynq-7000 AP SoC Security Functions**

The secure storage in the Zynq-7000 AP SoC security perimeter includes 256KB OCM, up to 3MB AXI block RAM (depending on the particular device), and PL configuration memory. The OCM memory address and control bus signals are not available externally at all; there is very limited access to the on-chip address and control signals.

The storage of the symmetric 256-bit AES cryptographic key in either eFUSE or battery-backed random access memory (BBRAM) is secure and programmable only through the JTAG port. To protect the cryptographic key, the Zynq-7000 AP SoC provides methods to control access to the JTAG port, including the capability to permanently disable access. See Table 1. The storage of the 256-bit hash of the user-defined 2048-bit RSA public key is in eFUSE memory. This unmodifiable SHA-256 hash links the RSA public key to the device to enable authentication of the first-stage boot loader (FSBL) to establish a root-of-trust. [Ref 1]

1. The AES/HMAC engine is only available for boot code decryption and symmetric authentication, not for application layer cryptography.

Table 1: **Zynq-7000 AP SoC Security Features Summary**

	Built-in Silicon Features
Passive Features	Confidentiality w/ AES-256 (BBRAM/eFUSE)
	Secure Configuration/Boot (PL/PS)
	Hardened Readback Disable
	Symmetric Key Authentication
	Public Key (Asymmetric) Authentication
Active Features	SEU Checking
	JTAG Disable/Monitor (BSCAN)
	Internal Key Clear
	Internal Configuration Memory Access
	Unique Identifier (Device DNA)
	Unique Identifier (User eFUSE)
	On-chip Temperature/Voltage Monitors
	PROGRAM_B Intercept
	Permanent JTAG Disable

The Zynq-7000 AP SoC provides boot and run-time security using the AES and RSA cryptographic algorithms.[Ref 2] When power is applied, device-level tests by masked programmed bootROM code ensure secure startup. Methods exist that periodically do a run-time integrity check on system memory.[Ref 3] RSA public key authentication is used by the bootROM code, and each hardware and software partition is authenticated using RSA in the secure boot. The Zynq-7000 AP SoC uses a hardened decryptor to decipher partitions encrypted using the AES standard.

As shown in Figure 2, the Zynq-7000 AP SoC boot process uses "chain of trust" to ensure a secure boot process so that security at run-time (application execution) can be achieved.

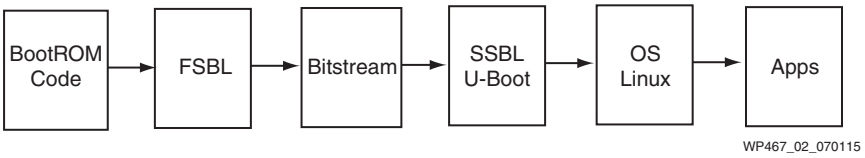

Figure 2: **Secure Boot Chain of Trust**

Isolation and access control are fundamental tenets of computer security. Using the SLCR, the Zynq-7000 AP SoC allows isolation by locking security subsystems when not in use. The SLCR is also used to ensure certain security settings are maintained throughout the secure boot process to include when the application is running. The security-critical settings are "sticky" and when initially set by the FSBL cannot be later changed without performing a device reset or power cycle. The FSBL is defined and customized by the user—Xilinx provides a standard FSBL as a baseline.

ARM® TrustZone provides a system approach to security by isolating secure applications from non-secure applications, preventing access to or corruption of the secure applications. TrustZone is integrated into the Zynq-7000 AP SoC's ARM Cortex-A9 processors, extending to the PS and PL intellectual property (IP) using the AXI bus. TrustZone defines "secure world" and "normal world" for a trusted execution environment and a rich operating system. TrustZone can be used for

isolation and access control.[Ref 4] Access control is a focus of the cryptographic module security policy, a security requirement described in the CMVP Overview.

The JTAG port is disabled by default. If the user decides to activate it, then it is important to realize that the JTAG port provides access to input/outputs (I/Os), registers, and memory—all items that can be exploited by an adversary. Zynq-7000 AP SoCs use a multi-level hierarchy to disable access to the JTAG ports. The JTAG port can be permanently disabled by a one-time programmable (OTP) eFUSE bit. The SLCR provides a second level of dynamically enabling/disabling the DAP and JTAG ports. As with most security-related control bits, the SLCR bits for disabling the DAP/JTAG ports are triplicated and sticky.

As an additional layer of tamper protection, the Xilinx Security Monitor (SecMon) can be instantiated into Zynq-7000 devices to provide run-time protection against a variety of tamper attacks. SecMon provides clock, JTAG port, voltage, and temperature monitoring and generates alarms if out-of-bounds activity is detected (SecMon also dynamically blocks the JTAG port). SecMon can respond to a tamper detection by performing functions such as BBRAM key erasure and zeroization of the PL configuration memory contents. SecMon can also take tamper input from external elements to provide a centralized system-level tamper detection and system response such that it can be used as the starting point to meet tamper requirements in higher levels of security (e.g., 3 and 4).[Ref 5]

The Xilinx Isolation Design Flow (IDF) uses an implementation methodology that isolates functions in the PL and controls fault propagation.[Ref 6] IDF can be used to address physical and logical separation of security functions in Security Levels 2, 3, and 4.

CMVP Overview

The participants in the FIPS 140-2 certification process are the semiconductor vendor, the CST, the CMVP/CAVP Authority, and the OEM. Most of the tasks in CMVP/CAVP certification are performed by the vendor (or OEM) and the CST.

- The OEM produces the end product, which typically integrates multiple cryptographic modules in an enclosure.
- The vendors in this space are companies like Xilinx, QNX, Green Hills, and Wind River.
- There are approximately twelve CST labs in the US, and approximately twenty worldwide.

FIPS 140-2 certification requires extensive documentation. Certification starts with the OEM selecting a CST lab and providing the documentation described in FIPS PUB 140-2, Appendix A.[Ref 7] Since the Zynq-7000 AP SoC has a very large number of users, much of the documentation is available. The availability of low-cost Zynq-7000 AP SoC evaluation boards allows almost immediate testing of hardware and software relative to a large cryptographic boundary. The testing can be done at the CST facility or by the vendor.

FIPS PUB 140-2 defines four levels of security and eleven security requirements. Most of the security requirements can be tested to a specified security level. The principle drivers defining the different security levels are the operating system and the anti-tamper (AT) requirements. The overall FIPS 140-2 certification level is *the lowest level attained in all of the security requirements*. Most FIPS 140-2 certifications are to Security Levels 1 and 2.

The Common Criteria for Information Technology Security Evaluation (CC) is an international standard (ISO/IEC 15408) for computer security certification. The CC uses a Protection Profile (PP), a document that identifies the security requirements for a category of consumer need. CC lists seven Evaluation Assurance Levels (EALs), with EAL1 being the least stringent. FIPS 140-2 includes EAL requirements in Security Levels 2, 3, and 4. Xilinx operating system partners Green Hills, QNX, and Wind River products meet EALs that exceed the requirements of FIPS 140-2 Security Level 4.

- **Security Level 1** is the lowest FIPS 140-2 level defined. There are no physical security requirements on the cryptographic module. The operating system does not require evaluation.
- **Security Level 2** includes physical security requirements for tamper attacks. These requirements are addressed with coatings or seals that are broken if access is attempted. For a single-chip cryptographic module, opaque tamper-evident coating on chip or enclosure is required. A pick-resistant lock can be used on removable enclosures. The operating system must meet the functional requirements specified in the CC PP and be evaluated to CC EAL2 or higher.
- **Security Level 3** requires more advanced tamper detection, and includes the requirement to zeroize critical security parameters (CSP) when an enclosure is opened. Identity authentication is required. The operating system must meet the functional requirements specified in the CC PP and be evaluated to CC EAL3 or higher.
- **Security Level 4** increases the tamper detection further. Cryptographic modules can be used in unprotected environments, i.e., outside the security perimeter of a guarded facility. Two-factor authentication is used. For a single-chip cryptographic module, hard opaque removal resistant coating on chip is required. Protection against noninvasive attacks, such as Differential Power Analysis (DPA), is specified. The operating system must meet the functional requirements specified in the CC PP and be evaluated to CC EAL4 or higher.

The eleven FIPS 140-2 security requirements are summarized here followed with a high level explanation of how Zynq-7000 can be used to satisfy each.

1. **Cryptographic Module Specification.** The cryptographic module (including the cryptographic boundary) is defined, along with approved algorithms, modes of operation, and security policy. A cryptographic module can operate in FIPS mode and non-FIPS mode, and it can execute approved algorithms such as AES and RSA, and non-approved algorithms such as the Data Encryption Standard. The documentation requirements include the cryptographic boundary, which defines what is included and excluded, physical ports and logical interfaces, and the control/status signals of cryptographic modules. A list of approved and non-approved cryptographic functions is provided. The documentation must include a block diagram of the hardware components. Appendix A in FIPS PUB 140-2 summarizes the documentation requirements.[Ref 7]

   The following Zynq-7000 device attributes facilitates the creation of this specification in a timely manner:

   - The high level of feature integration within the device helps to provide a well-defined crypto boundary.
   - The existing embedded on-chip crypto algorithms (AES and RSA) are FIPS-approved and have passed CAVP.

- The hardware and software programmability allows for additional FIPS-approved algorithms, bypass/non-FIPS modes, etc.
- Extensive documentation (e.g., XAPP1175[Ref 2], XAPP1223[Ref 8], and WP468[Ref 9]) can provide additional information on topics such as the proper use of crypto keys, enhancing device security, etc.

2. **Cryptographic Module Ports and Interfaces.** The cryptographic module must have four logical interfaces: data input, data output, control, and status. For Security Levels 1 and 2, the ports used to input plaintext cryptographic keys can be shared with other ports. For Security Levels 3 and 4, the ports used to input cryptographic keys must be physically and logically separated. For secure boot, the plaintext cryptographic key is input into the Zynq-7000 AP SoC using the JTAG port and stored in BBRAM or eFUSEs. The Zynq-7000 device provides hierarchical control of access to the JTAG port. Since this is a plaintext key load, it has to be performed in a secure facility.

   For the application layer, the ports used for cryptographic key(s) are user defined on the Zynq-7000 device. In this case, the keys can be plaintext or ciphertext depending on the user's programmable implementation (e.g., the user can instantiate a secure key exchange function in the PL for a ciphertext (black) key load). These cryptographic "mission" keys are typically used for secure communication channel(s) (voice, data, video, packets, etc.). For security Levels 3 and 4, the user defines an access controlled port for key loading (not JTAG). This is similar to the DS101/DS102 port (military radios), SafeNet USB key loader, or Motorola KVL key loader (which is a variation on RS-232 serial). These mission keys can be loaded daily, weekly, or periodically. There is also Over the Air Rekeying (OTAR) required by most radio systems that can be implemented in the programmable Zynq-7000 device.

3. **Roles, Services, and Authentication.** This section addresses the ability of the cryptographic module to identify two types of operators: role-based and identity-based. The operator(s) perform services such as loading the plaintext cryptographic key. Security Level 1 does not require authentication. Security Level 2 requires role-based authentication to control access to the cryptographic module. Security Levels 3 and 4 require identity-based authentication. Setting up the key management organization and facility to meet this requirement is principally the responsibility of the OEM.

   BootGen, the Xilinx image generation tool, supports a variation on the split knowledge referenced in FIPS 140-2, i.e., the encryption and authentication can be done on different servers by different operators. The Zynq-7000 AP SoC provides RSA authentication, starting with the FSBL and including all partitions loaded into the embedded system. BootGen supports a user-defined field (UDF) in the Authentication Certificate for identity authentication on the partitions loaded. If the UDF is used, the user must modify the FSBL to implement the identity check. Additionally, authenticated application code residing on the PS can implement role-based / user-based authentication schemes.

4. **Finite State Model.** The operation of a cryptographic module is specified with a finite state model that includes power on/off, cryptographic officer services, cryptographic key/CSP entry, user, self-test, and error states.

   The Zynq-7000 AP SoC's bootROM state diagram provides a basis for the Finite State Model (FSM) for secure boot.[Ref 10] Post secure boot, any user defined security features (PS software or PL design) will be included in this FSM.

5. **Physical Security.** The Physical Security requirements defines three embodiments of the cryptographic module: single chip, multiple chip embedded, and multiple chip stand-alone. It defines tamper evidence and tamper response as physical security mechanisms for responding to attempts at unauthorized access to the cryptographic module. Tamper evidence leaves a visible sign of tampering. A tamper response is action such as zeroizing a key/CSP after a tamper event is detected.

   Security Level 1 physical security requirements are met with production grade components with standard passivation. Security Level 2 requires tamper-evident mechanisms. Security Level 3 requires strong enclosures with tamper detection and response. Security Level 4 adds environmental requirements, specifying functionality when the voltage and/or temperature is deliberately or accidentally changed so that it is outside of the specified operating range.

   With a wide a range of security functions built into Zynq-7000 AP SoCs (e.g., Keyclear, System Monitor for environmental monitoring, etc.), many of these requirements can be easily met. Xilinx application note XAPP1084, *Developing Tamper Resistant Design with Xilinx Virtex®-6 and 7 Series FPGAs* provides detailed information on these security features and how to use them.[Ref 11]

   Additionally, the SecMon IP from Xilinx provides tamper monitoring and response functions (e.g., JTAG port monitoring and BBRAM key zeroization). It does this by taking advantage of the active security features described in XAPP1084 and combines them into a single IP block. SecMon can also be leveraged to provide the foundation for system-level zeroization response due to extensibility via additional system tamper event inputs. Since SecMon is part of the overall user design functionality must be integrated at the system level by the OEM.

   Other physical security requirements are the responsibility of the OEM, since the OEM provides the coatings and enclosures for the underlying cryptographic devices and functions.

6. **Operational Environment.** The operational environment refers to the management of the software, firmware, and hardware, i.e., the operating system.

   The Zynq-7000 AP SoC has a number of options in terms of the operational environment, such as:

   - The ARM Cortex-A9 with dual processors can be operated in single processor, symmetric dual processor, and asymmetric dual processor modes.
   - Monolithic or Microkernel operating systems can be used
   - Run-time security features can include: memory management unit (MMU), TrustZone, and Hypervisor enforced protections.

   Security Level 1 requires restricting access to the cryptographic keys. The Zynq-7000 AP SoC limits access to the eFUSE and BBRAM cryptographic keys, providing mechanisms for protecting the software installed. It also includes an approved integrity check of the FSBL using approved RSA cryptography. User-defined mechanisms must be implemented to restrict access to the session keys used by the application layer.

   Security Levels 2–4 require an operating system that is evaluated to CC EALs 2–4, respectively. Operating systems that meet these requirements are available from Xilinx software ecosystem members, including Green Hills, QNX, and Wind River.

7. **Cryptographic Key Management.** This security requirement addresses random number generators (RNGs), key generation, key establishment, and key entry. Keys can be entered using manual (e.g., keyboard) or automated (smartcard) methods. For Security Levels 1 and 2, the private key must be entered in encrypted form when automated entry is used. If entered manually, the private key is entered in plaintext form. For Security Levels 3 and 4, private keys must be entered in encrypted form when using automated methods, and in either encrypted or split-knowledge form, when manual methods are used. If a key is stored in plaintext, it must be zeroizable.

   As mentioned previously, the key used for secure boot is in plaintext (red) form and must be loaded into on-chip BBRAM or eFUSEs within a secure facility. Only the BBRAM key can be zeroized because the eFUSE key is one time programmable (OTP).

   The Zynq-7000 AP SoC does not have a built-in RNG in silicon to create application layer session keys. However, an RNG can be implemented in the PL to create keys within the device. For loading external application layer session keys, the interface port is user defined and can be a plaintext or ciphertext (black) key load depending on the user's implementation.

8. **Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC).** Cryptographic modules must conform to the EMI/EMC requirements specified by **Section 47, Code of Federal Regulations, Part 15, Subpart B,** *Unintentional Radiators, Digital Devices*.[Ref 12] The requirement is Class A for Security Levels 1 and 2 and Class B for Security Levels 3 and 4.

   This requirement does not apply at the Zynq-7000 device level. Compliance at the board / module level is required. Employing power supply decoupling and signal integrity best practices help with compliance. This requirement does not exist in the ISO/IEC 19790 international security standard.

9. **Self Tests.** The cryptographic module must perform power-up and conditional self tests to ensure that the module functions correctly. The power-up tests are: (a) cryptographic algorithm, (b) software integrity, and (c) critical functional tests. As an example, the AES cryptographic algorithm test is a type of known-answer test (KAT).

   A KAT of the AES algorithm is not automatically executed by the Zynq-7000 device at power-up. However, a KAT can be added to the RSA-authenticated FSBL user code.

   The conditional test requires that an approved authentication mechanism be used when software is loaded. The Zynq-7000 device's RSA authentication is approved and is run at boot time on all partitions loaded. The RSA authentication can be run periodically during run time. [Ref 3] If included, SecMon IP is continually performing configuration memory health checks in the background as well as internal watchdog checks.

   In addition to cryptographic and security self-tests, Xilinx provides extensive Built In Self Tests (BIST) and device driver self-test software, which can be run at startup or periodically, for testing the overall health of the system.

10. **Design Assurance.** Design Assurance ensures that the cryptographic module is properly tested, configured, delivered, installed, and developed. Documentation that relates the security policy with the hardware, software, and firmware components of the cryptographic module is required from the OEM.

Security Level 2 requires a functional specification that describes the cryptographic module and its interfaces. Security Level 3 requires the use of a high-level language to describe the security functions within the device. Security Level 4 requires formal models of the security policy.

In terms of the Zynq-7000 device itself, Xilinx follows best-in-class processes and procedures to ensure the highest quality at all stages of production. The Xilinx Quality Manual can be used as supporting documentation to help meet this requirement.[Ref 13]

For the programmable portions of a Zynq-7000 AP SoC enabled system, the documentation includes source code (e.g., C/C++) for the PS and HDL (e.g., Verilog or VHDL) for the PL. The user is responsible to ensure a quality process is followed for all the programmable user designs and supply the applicable supporting documentation.

11. **Mitigation of Other Attacks.** Cryptographic modules are subject to attacks such as power analysis, timing analysis, fault induction, and TEMPEST. FIPS 140-2 does not provide testable requirements for these attacks.[Ref 7]

    The use of authenticated soft security functions can be implemented in the PS or PL to mitigate attacks such as differential power analysis (DPA). Xilinx White Paper WP468, *Leveraging Asymmetric Authentication to Enhance Security-Critical Applications Using Zynq-7000 All Programmable SoCs* provides some examples as to how the security of a Zynq-7000 device can be enhanced.[Ref 9]

Table 2 provides a Zynq-7000 AP SoC "scorecard" in terms of satisfying the prior eleven FIPS 140-2 security requirements (i.e., what the relative risk level is). Unless noted otherwise, the achievability is for security levels 1-4.

Table 2: **Zynq-7000 AP SoC FIPS 140-2 Scorecard**

FIPS 140-2 Security Requirements	
Coverage Areas	**Achievability Level with Zynq-7000 AP SoC**
1. Crypto Module Specification	Low Risk
2. Cryptographic Module Ports and Interfaces	Low Risk
3. Roles, Services and Authentication	Medium Risk
4. Finite State Model	Low Risk
5. Physical Security	L1-3: Low Risk L4: Medium Risk
6. Operational Environment	Low Risk
7. Cryptographic Key Management	Medium Risk
8. EMI / EMC	n/a
9. Self-Tests	Medium Risk
10. Design Assurance	Low Risk
11. Mitigation of Other Attacks	Low Risk

CAVP Overview

Participants in CAVP are the vendor, CST, and the CAVP validation. The CST laboratory independently tests cryptographic algorithms using the Cryptographic Algorithm Validation System (CAVS) test tool. Either the vendor or the CST is allowed to perform the tests. CSTs are accredited under the NVLAP. The algorithms can be tested in a hardware environment or in simulation. The validation process typically takes 1–3 months. A list of accredited labs can be found on the NIST IFT Computer Security Resource Center website.[Ref 14] Also provided on this site are tests such as KATs.[Ref 15]

The AES and RSA cryptography in Zynq-7000 devices are approved cryptographic algorithms shown on the CAVP validation list.[Ref 16] Authentication by the Hash Message Authentication Code (HMAC) provides assurance in the form of symmetric authentication that the image has not been altered or replaced, either by accident or intentionally. In Zynq-7000 devices, HMAC is run on partitions on which AES is run. The Zynq-7000 devices always perform AES and HMAC together.

Table 3 lists the NIST validation numbers for the Zynq-7000 devices.

Table 3: **NIST CAVP Validation List**

CAVP Validation List	Validation Number
AES	2363
RSA	1224
HMAC	1465
SHA-256	2034

ISO / IEC 19790

While other governments recognize and use FIPS 140-2, a US government-produced standard is not appropriate for all international security projects. The ISO/IEC 19790 international standard is nearly identical to FIPS 140-2 in the four security levels and eleven security requirements, with some changes in terminology. ISO/ IEC 24759 is similar to NIST's *Derived Test Requirements*[Ref 17], which outlines tests needed to achieve FIPS 140-2 certification. As of this writing, the CST Labs are not certifying to ISO/IEC 19790.

Various authorities have developed validation programs for testing against ISO/IEC 19790 requirements. For instance, Japan operates a cryptographic module validation program named JCMVP, and Korea operates a cryptographic module validation program named KCMVP. Spain, Turkey, and others have also developed programs or are in development. Most of the programs are similar in structure to USA/Canadian CMVP for FIPS 140-2. The overall goal is the mutual recognition by different programs to meet the needs of worldwide commercial sectors.

ISO 19790 differs from FIPS 140-2. Table 4 provides a summary of the changes to ISO19790. Most notably, the Software / Firmware and Non-Invasive Security sections are new, and the EMC/EMI section has been removed.

Table 4: **Changes to ISO 19790**

Section	Overview of ISO 19790 Changes
Cryptographic Module Specification	New modes of operation: Hybrid, Normal, Degraded; Indicator is required when approved security mode is used.
Cryptographic Module Interfaces	Control interface is updated. Trusted channels are defined.
Roles, Services, and Authentication	On demand module versioning. Update of software load. Default authentication must be changed after initial use. Authentication strength increased.
Finite State Model	Moved to Life Cycle Assurance section, essentially unchanged.
Software/Firmware Security	Zeroization of temperature values. Integrity test can use an independent module. At Level 2, only executable (not source) code is evaluated. Level 2: Expanded audit records. Levels 3, 4: Digital signatures replace keyed hashes.
Operational Environment	Level 2: Discussion of SSPs, audit records which must be maintained has expanded
Physical Security	Enclosure, encapsulation material, tamper seal changes. Change in EFP/EFT at levels 3, 4.
Non-Invasive Security	Section is new, optional. Levels 1, 2 require non-invasive security mechanisms documented. Levels 3, 4 require testing to metrics in Annex F, which are not yet defined.
Sensitive Security Parameter Management	Sensitive Security Parameter: Hashes of passwords, RBG state information are CSPs. Encrypted SSP entered manually cannot be displayed in plaintext. CSPs entered wirelessly must be encrypted. Expanded requirements of zeroization. Multi-factored authentication for Level 4.
EMC/EMI	Removed.
Self-Tests	Algorithm tests must be run before first use. Pre-operational tests. Levels 3, 4 require periodic self-tests, with an error log.

Table 4: **Changes to ISO 19790**

Section	Overview of ISO 19790 Changes
Life Cycle Assurance	Description of functional tests. Automated security diagnostic tool is required. Procedures for secure sanitization, secure destruction of the module. Level 4 requires operator authentication, removes requirement for formal modeling.
Mitigation of Other Attacks	Similar to FIPS 140-2.

Table 5 provides a Zynq-7000 SoC "scorecard" in terms of satisfying the eleven ISO/IEC 19790 security requirements (i.e., what the relative risk level is). Unless noted otherwise, the achievability is for security levels 1-4.

Table 5: **Zynq-7000 AP ISO/IEC 19790 Scorecard**

ISO/IEC 19790 Security Requirements	
Coverage Areas	**Achievability Level with Zynq-7000 AP SoC**
1. Cryptographic Module Specification	Low Risk
2. Cryptographic Module Interfaces	Low Risk
3. Roles, Services and Authentication	Medium Risk
4. Software/Firmware Security	Low Risk
5. Operational Environment	Low Risk
6. Physical Security	L1-3:Low Risk L4: Medium Risk
7. Non-Invasive Security	Low Risk
8. Sensitive Security Parameter Management	Medium Risk
9. Self-Tests	Medium Risk
10. Life-Cycle Assurance	Low Risk
11. Mitigation of Other Attacks	Low Risk

Conclusion

The certification of a cryptographic module against the FIPS 140-2 or ISO/IEC 19790 standards can be an arduous and time-consuming process. A Zynq-7000 AP SoC-enabled system can alleviate many of the difficulties in the certification process due to these key points:

- High level of integration
- Wide range of built-in hard security functions
- Ability to add-in authenticated soft security functions
- Hardware and software authenticated programmability
- AES, HMAC and RSA algorithms already validated by CAVP
- Mature development environments and extensive supporting documentation
- Rich partner eco-system for both the PS and PL

To help meet time-to-market demands, the combination of these key attributes makes the Zynq-7000 AP SoC an attractive solution to consider when architecting a cryptographic module that is required to adhere to stringent security standards.

References

1. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Descriptions of SHA-256, SHA-384, and SHA-512*. Accessed November 29, 2016. https://web.archive.org/web/20130526224224/http:/csrc.nist.gov/groups/STM/cavp/documents/shs/sha256-384-512.pdf
2. Xilinx Application Note XAPP1175, *Secure Boot of Zynq-7000 All Programmable SoC*.
3. Xilinx Application Note XAPP1225, *Run Time Integrity Check of Zynq-7000 All Programmable SoC System Memory*.
4. Xilinx User Guide UG1019, *Programming ARM TrustZone Architecture on the Xilinx Zynq-7000 All Programmable SoC: User Guide*.
5. Xilinx Product Brief, Security Monitor IP*: Industry-Leading Programmable Device Security Protecting IP and Mission Critical Data*.
6. Xilinx Application Note XAPP1086, *Developing Secure and Reliable Single FPGA Designs with Xilinx 7 Series FPGAs Using the Isolation Design Flow*.
7. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Security Requirements for Cryptographic Modules (FIPS PUB 140-2)*. May 2001. (Supersedes FIPS PUB 140-1, January 1994.) Retrieved 15 June 2015.
8. Xilinx Application Note XAPP1223, *Changing the Cryptographic Key in Zynq-7000 AP SoC*.
9. Xilinx White Paper WP468, *Leveraging Asymmetric Authentication to Enhance Security-Critical Applications Using Zynq-7000 All Programmable SoCs*.
10. Xilinx User Guide UG585, *Zynq-7000 AP SoC: Technical Reference Manual*.
11. Xilinx Application Note XAPP1084, *Developing Tamper Resistant Designs with Xilinx Virtex-6 and 7 Series FPGAs*.
12. *Unintentional Radiators, Digital Devices,* Section 47, Code of Federal Regulations, Part 15, Subpart B.
13. *Xilinx Quality Manual*, QAP0002.
14. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Cryptographic And Security Testing (CST) Laboratories*. Updated June 2015. Retrieved 15 June 2015.
15. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)*. Updated November 2002. Retrieved 15 June 2015.
16. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Algorithm Validation Lists*. Retrieved 15 June 2015.
17. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*. DRAFT January 2011, no update. Retrieved 15 June 2015.

Further Reading

1. Xilinx Application Note XAPP1223, *Changing the Cryptographic Key in Zynq-7000 AP SoC*
2. Xilinx White Paper WP365, *Solving Today's Design Security Concerns*
3. Wikipedia, *Cryptographic Module Validation Program*. Retrieved 15 June 2015.
4. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *CAVP Management Manual*. Draft 1.0 June 2009, no update. Retrieved 15 June 2015.
5. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Frequently Asked Questions for the Cryptographic Algorithm Validation Program Concerning the Validation of Cryptographic Algorithm Implementations*. Updated May 2016. Retrieved 8 July 2016.
6. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*. Updated June 2016. Retrieved 8 July 2016.

Revision History

The following table shows the revision history for this document:

Date	Version	Description of Revisions
12/09/2016	1.1	Updated Zynq-7000 AP SoC Security.
07/29/2016	1.0	Initial Xilinx release.

Disclaimer

Automotive Applications Disclaimer