Zynq UltraScale+ MPSoC: A FIPS 140-3 Primer

WP543 (v1.0) February 4, 2022

Abstract

The high level of integration, hardware and software programmability, wide range of built-in security features, and extensive supporting documentation make the Zynq® UltraScale+™ MPSoC ideal for use in cryptographic modules that are certified under the FIPS 140-3 security standard.

In 2019, the Secretary of Commerce approved Federal Information Processing Standards Publication (FIPS) 140-3 *Security Requirements for Cryptographic Modules*. FIPS 140-3 supersedes FIPS 140-2 and is the new gold standard for products that employ cryptography to protect sensitive but unclassified information. Examples of sensitive information are financial and health records. The transition to the new standard has started and in 2026, the National Institute of Standards and Technology (NIST) will require cryptographic products purchased by federal agencies to be FIPS 140-3 certified. Two programs used in FIPS 140-3 validation are the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP). Developing a FIPS 140-3 certified product requires that an original equipment manufacturer (OEM) use an independent test lab for CMVP and CAVP certification. This white paper is a primer on the FIPS 140-3 certification of a product that uses Zynq UltraScale+ MPSoCs.

Introduction

The NIST Computer Security Division and the Communications Security Establishment Canada (CSEC) administer the CMVP. A FIPS 140-3 certified product usually consists of hardware and software/firmware included in an enclosure. Typically, an OEM integrates hardware and software/firmware cryptographic modules into the top-level cryptographic module, which then comprises the end product in an enclosure. Cryptographic modules use FIPS 140-3 approved algorithms, such as the advanced encryption standards (AES) or the Rivest Shamir Adleman (RSA) algorithm. The approved algorithm is certified in the CAVP.

In March 2019, the United States Department of Commerce approved the FIPS140-3 *Security Requirements for Cryptographic Modules* [REF 1] to succeed FIPS140-2 [REF 2]. FIPS140-3 represents the formal adoption of the International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 19790:2012/Cor 1:2015 standard to replace FIPS 140-2. The ISO 24759:2017 standard serves as the derived testing requirements and the NIST Special Publication (SP) 800-140A-F series serves as the requirements for the CMVP. Clarifications and guidelines to the ISO are provided in the *Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program* [REF 3].

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 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 140-3 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 UltraScale+ MPSoC Security section describes security in Zynq UltraScale+ MPSoCs. FIPS 140-3 provides security requirements in areas such as cryptographic boundary, cryptographic ports, software/firmware security, physical security, key management roles, self-test, and services. In many cases, the FIPS 140-3 security requirement is in the domain of the OEM's top-level cryptographic module. The Zynq UltraScale+ MPSoC security functionality can be used to meet most 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 140-3. It also provides details on the Zynq UltraScale+ MPSoC’s functionality as it applies to the FIPS 140-3 security requirements. The CAVP Overview provides background information on the CAVP and shows certified cryptographic algorithms used in Xilinx FPGAs and in the Zynq UltraScale+ MPSoC.

Zynq UltraScale+ MPSoC Security

Built on TSMCs 16FinFET Plus (16FF+) process, the Zynq UltraScale+ MPSoC integrates Xilinx programmable logic (PL) and an Arm®-based processing system (PS) that includes an application processing unit containing two or four Cortex®-A53 cores (APU subsystem) and a real-time processing unit containing two Cortex-R5F cores (RPU) in a single device.

The Zynq UltraScale+ MPSoC provides a number of features to help secure not only the hardware but the software applications running on it. These features include a hardened physical unclonable function (PUF), user-accessible hardened cryptographic blocks, asymmetric authentication, side-channel attack protection, and other silicon-based anti-tamper protections. See *Accelerating Cryptographic Performance on the Zynq UltraScale+ MPSoC* (WP512) and *Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices* (XAPP1323) for details. Xilinx also offers an intellectual property (IP) known as Security Monitor (SecMon) to provide runtime protection against a variety of tamper attacks. [REF 7].

Xilinx classifies the security features as either passive or active. In general, passive features are either part of the tool flow or built into the device and do not require you to do anything extra in your SoC design. Passive features are also temporal in nature and come into effect at the following phases of the operating life of the Zynq UltraScale+ MPSoC:

- Pre-boot
- During boot
- Post-boot

In contrast, active security features are required to be included in the SoC design. These features only come into effect after the Zynq UltraScale+ MPSoC has been securely booted and the design becomes active. The security features fall into three main categories:

- Prevention (e.g., JTAG port disabling)
- Detection (e.g., on-chip temperature and voltage monitoring)
- Response (e.g., key zeroization)

The following table summarizes the security features of the Zynq UltraScale+ MPSoC (see *Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices* (XAPP1323)).

Table 1: **Zynq UltraScale+ MPSoC Built-in Security Features**

Zynq UltraScale+ MPSoC Security Features	Type	Category
Image/bitstream confidentiality (symmetric)	Passive	Prevention
Volatile on-chip 256-bit BBRAM AES key storage	Passive	Prevention
Non-volatile on-chip 256-bit eFUSE AES key storage	Passive	Prevention
PUF-enabled black key storage (internal eFUSEs)	Passive	Prevention
Write-only key load with integrity check (BBRAM and eFUSE)	Passive	Prevention
Image/bitstream authentication (symmetric)	Passive	Prevention
Image/bitstream authentication (asymmetric)	Passive	Prevention
Non-volatile 384-bit eFUSE public key hash storage to enable RSA authentication	Passive	Prevention
DPA side-channel attack protections	Passive	Prevention
Obfuscation of the user AES key loading and storage	Passive	Prevention
Hardened readback disabling circuitry	Passive	Prevention
Design for test (DFT) boot mode permanent disable	Passive	Prevention
Uninterruptible internal clock source for CSU	Passive	Prevention
Error correction code (ECC) on PS memories	Passive	Prevention

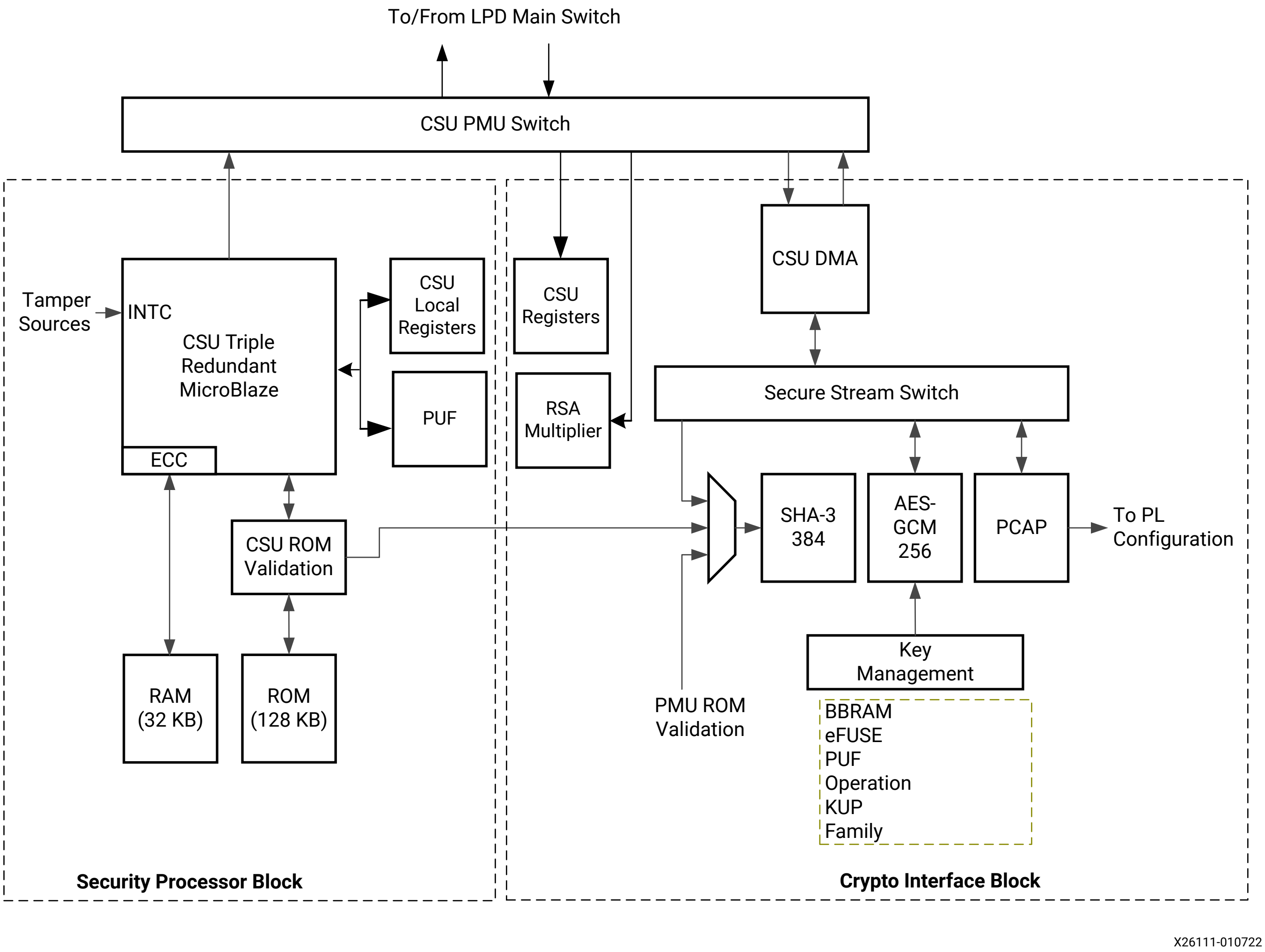
Table 1: **Zynq UltraScale+ MPSoC Built-in Security Features** *(cont'd)*

Zynq UltraScale+ MPSoC Security Features	Type	Category
Triple-mode redundancy (TMR) in PS critical operations	Passive	Prevention
JTAG port permanent disable (eFUSE)	Passive or active	Prevention or response
JTAG port temporary disable	Passive or active	Prevention
JTAG port monitor	Active	Detection
PL configuration memory integrity checking	Active	Detection
Unique identifiers (device DNA and user eFUSE)	Active	Detection
On-chip temperature and voltage monitors/alarms	Active	Detection and response
PL configuration memory clearing	Active	Response
Uninterruptible internal clock source on PL STARTUP block	Active	Detection
Key agility (BBRAM only)	Active	Prevention and response
BBRAM key zeroize (erase + verify)	Active	Response
CSU tamper monitor and response	Active	Detection and response
Public key revocation	Active	Response
Non-volatile (eFUSE) tamper event logging	Active	Response
User accessible crypto blocks	Active	Prevention
Arm TrustZone	Active	Prevention and detection
Arm v8 cryptography extensions	Active	Prevention and detection
Xilinx memory protection unit (XMPU)	Active	Prevention and detection
Xilinx peripheral protection unit (XPPU)	Active	Prevention and detection
AXI/APB isolation block (AIB)	Active	Prevention and response
AXI timeout block (ATB) in interconnects	Active	Detection and response
System memory management unit (SMMU)	Active	Prevention and detection
Global 3-state (GTS) enable (PL I/O only)	Active	Response
Global set-reset (GSR) enable (PL I/O only)	Active	Response

At the center of the device security is the hardened configuration security unit (CSU), shown in the following figure. The CSU consists of two main blocks, the secure processor block (SPB) and the crypto interface block (CIB), shown on the left and right of the figure, respectively. The SPB contains a triple-redundant MicroBlaze™ processor for controlling boot operation, an associated ROM, a small private RAM, a PUF, and the necessary control/status registers required to support all secure operations. The CIB contains engines for supporting and accelerating the following cryptographic operations:

- AES-GCM, SHA-3, and RSA
- Direct memory access (DMA) controller
- Processor configuration access port (PCAP) interface

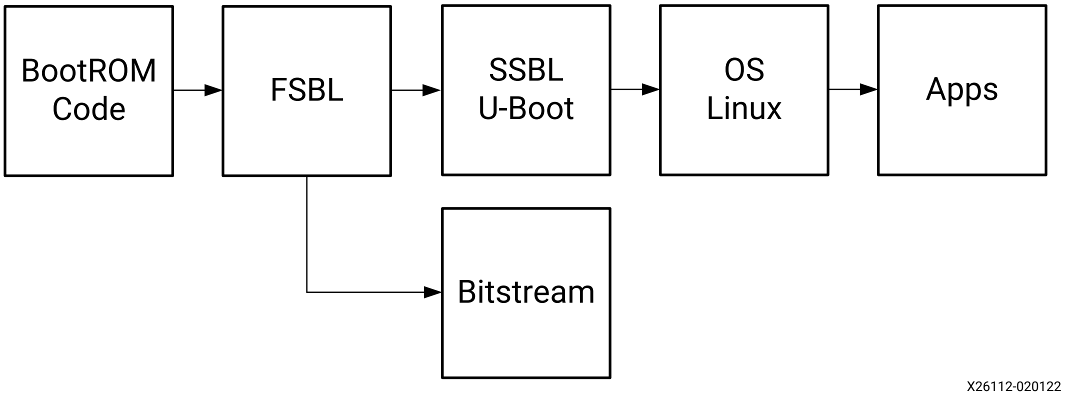
Figure 1: **Configuration Security Unit Block Diagram**



The CSU ensures the secure boot of the device by supporting the authentication and confidentiality of the partitions in the boot image. This also includes the secure storage and management of the cryptographic keys. After boot, the CSU is used for tamper monitoring and response of the device. At runtime, the crypto engines of the CSU can also be used by PS/PL applications to accelerate cryptographic operations. Access to the CSU can be restricted to specific applications with the XPPU.

The following figure illustrates a typical Zynq UltraScale+ MPSoC boot process that builds a *chain of trust* to ensure a secure boot process so that security at runtime (application execution) can be achieved. The chain of trust is maintained assuming each loaded component is either immutable (for example, boot ROM code) or is properly authenticated.

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



Secure boot is defined as authenticating PS/PL images (use of encryption is optional unless confidentiality is required for boot products). Image authentication (using RSA) ensures that an image came from a trusted source and has not been modified. The Zynq UltraScale+ MPSoC builds the chain of trust by supporting the authentication of the very first piece of user code that is loaded on the SoC, which is the first stage boot loader (FSBL). To this end, the device also checks the integrity of the immutable boot ROM code (using SHA-3), which brings up the FSBL. Along with integrity and authentication, the Zynq UltraScale+ MPSoC also provides confidentiality of the images (using AES-GCM) to protect against attacks such as cloning, over-building, and reverse engineering. There are a number of other security features such as black key storage and side-channel attack countermeasures that add to the robustness of the Zynq UltraScale+ device secure boot process.

Unlike previous generations, the Zynq UltraScale+ MPSoC provides a PUF. The PUF, among other functions, serves as a generator of a die-unique AES key-encryption key (KEK) that can be used to encrypt/decrypt the symmetric 256-bit AES key that decrypts the partitions of the boot image. That is, the Zynq UltraScale+ MPSoC encrypts the symmetric AES key using the KEK to further protect it, before storing it in non-volatile eFUSEs. Furthermore, the device stores the 384-bit SHA-3 hash of the user-defined 4096-bit RSA public key in the eFUSE bits. This unmodifiable SHA-3 hash links the RSA public key to the device to enable authentication of the FSBL to establish a root-of-trust. User-defined cryptographic keys (AES keys and the hashes of RSA keys) can be stored in the on-chip eFUSEs or battery-backed RAM (BBRAM). The programming of BBRAM and eFUSEs is achieved using software that runs on the PS, which uses the Xilinx Secure Key (XilSKey) library (see *Zynq UltraScale+ MPSoC: Software Developers Guide* (UG1137)).

Arm TrustZone combined with XPPU and XMPU 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 UltraScale+ MPSoC Arm Cortex-A53 processors, extending to the PS and PL using the AXI bus. TrustZone defines *secure world* and *normal world* for a trusted execution environment and a rich operating system. For more details, see *Isolate Security-Critical Applications on Zynq UltraScale+ Devices* (WP516). TrustZone can be used for isolation and access control. Access control is a focus of the cryptographic module security policy, which is a security requirement described in CMVP Overview.

As an additional layer of runtime tamper protection, the Xilinx SecMon IP [REF 7] can be implemented in Zynq UltraScale+ MPSoCs to provide runtime protection against a variety of tamper attacks. SecMon provides clock, JTAG port, voltage, temperature, and configuration monitoring, and generates alarms if out-of-bounds activity is detected (SecMon IP also blocks the JTAG port). SecMon can respond to tamper detection by performing functions such as BBRAM key zeroization and zeroization of the device. SecMon can also take tamper input from external elements to provide a centralized system-level tamper detection and system response.

The isolation design flow (IDF) (see *Isolation Design Flow for UltraScale+ FPGAs and Zynq UltraScale + MPSoCs* (XAPP1335)) is supported for static and reconfigurable PL applications with Zynq UltraScale+ MPSoCs. The IDF methodology allows the designer to logically isolate the secure from the non-secure functions implemented in the PL.

CMVP Overview

The participants in a FIPS 140-3 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 are companies such as Xilinx, QNX, Green Hills, and Wind River.
- There are twelve CST labs in the U.S. and twenty-one worldwide.

FIPS 140-3 certification requires extensive documentation. Certification starts with the OEM selecting a CST laboratory and providing the documentation described in the standard. Because the Zynq UltraScale+ MPSoC has a very large number of users, most of the documentation is available. The availability of cost-optimized Zynq UltraScale+ MPSoC 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 140-3 specifies a wide spectrum of requirements a cryptographic module must meet to address a diversity of application environments. The requirements are categorized into eleven distinct requirement areas/sections, and for each section, the standard defines four security levels that gradually enhance the security mechanisms of the module. 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 140-3 certification level is the lowest level attained in all of the security requirements. Most FIPS 140-3 certifications are to security levels 1 and 2, which are described below.

Compared to FIPS 140-2, FIPS 140-3 defines the same sections of security requirements as its predecessor with the following exceptions:

- The *Electromagnetic Interference/Electromagnetic Compatibility* (EMI/EMC) section in FIPS 140-2 has been removed from FIPS 140-3.
- The *Finite State Model* section of FIPS 140-2 becomes a subsection and part of the *Life-cycle Assurance* section of FIPS 140-3.

- FIPS 140-3 introduces two sections to the standard, the *Software/Firmware Security* and *Non-invasive Security* sections, by grouping related requirements already existing in FIPS 140-2 and specifying new ones.
- The FIPS 140-2 *Cryptographic Key Management* and *Design Assurance* sections have been renamed in FIPS 140-3 as *Sensitive Security Parameter Management* and *Life-cycle Assurance*, respectively.

Another important change in FIPS 140-3 is the removal of all references to the Common Criteria for Information Technology Security Evaluation (CC). CC is an international standard (ISO/IEC 15408) for computer security certification and identifies and documents security requirements based on consumers' needs. CC defines seven Evaluation Assurance Levels (EALs) and unlike FIPS 140-2, which includes EAL requirements in Security Levels 2 to 4, in FIPS 140-3 all the references to EALs have been removed.

The four security levels of FIPS 140-3 are summarized as follows.

- **Security Level 1 (SL1):** Is the lowest FIPS 140-3 level defined and specifies the basic security requirements for a cryptographic module. There are no requirements for authentication nor for physical security in SL1 and, consequently, it is appropriate for modules that are to be deployed in an environment that already provides these security features.
- **Security Level 2 (SL2):** Adds on to SL1 by including requirements for minimum role-based authentication and protection against tamper attacks. This allows cryptographic modules to be deployed in modifiable environments capable of supporting role-based access. Tamper protection involves the use of tamper-evident coatings or seals or pick-resistant locks on removable covers or doors.
- **Security Level 3 (SL3):** Enhances further the mechanisms SL2 specifies for protection against unauthorized access and includes additional requirements for non-invasive mitigation methods and life-cycle assurances. It requires the use of strong enclosures and tamper detection/response circuitry (e.g., zeroization of all the sensitive security parameters (SSPs)). SL3 also takes authentication up a level, by requiring identity-based authentication. Furthermore, at SL3, all cryptographic modules should include features for environmental failure protection (EFP) or undergo rigorous environmental failure testing (EFT).
- **Security Level 4 (SL4):** Is the highest FIPS 140-3 level and includes all the security features the lower levels specify, as well as extended features. Indicatively, SL4 introduces multi-factor identity-based authentication for all services that use trusted channels. Furthermore, SL4-certified cryptographic modules with SSPs should be able to detect and respond to all unauthorized attempts at physical access. Also, at SL4, the modules are required to include EFP and special environmental protection features to ensure that security is not compromised when they are forced to operate outside of their normal operating range. SL4 is appropriate for modules that are to be deployed in physically unprotected environments.

FIPS 140-3 Requirement Sections

This section summarizes the eleven FIPS 140-3 requirement sections and provides a high-level explanation of how the Zynq UltraScale+ MPSoC can be used to satisfy each.

Cryptographic Module Specification

This section specifies the requirements for the proper definition of the cryptographic module along with approved algorithms, modes of operation, and security policy. A cryptographic module is defined with one of the following module types:

- Hardware
- Software
- Firmware
- Hybrid software
- Hybrid firmware

The two hybrids are modules that are composed of either a software or firmware component and a disjoint hardware component (that is, the software/firmware component is not contained within the hardware component). Furthermore, this clause specifies requirements for the cryptographic boundary. This boundary defines what is included and excluded, physical ports and logical interfaces, and the control/status signals of modules. A FIPS-approved normal mode of operation of the module should use at least one service that employs an approved security function specified in the standard.

***Note*:** Non-security-relevant functions and components can be included within the cryptographic boundary and used in an approved normal mode of operation, provided that they do not compromise the security of the module.

To help troubleshoot potential issues, FIPS 140-3 also introduces the degraded mode of operation in addition to the normal mode as specified in FIPS 140-2. Upon entering an approved degraded mode of operation, the module is allowed to operate even if it can only offer a subset of its functions due to an error that has occurred. The module is allowed to enter the degraded operation mode only if it successfully passes all pre-operational self-tests (see requirements in Self-tests).

The following Zynq UltraScale+ MPSoC attributes facilitate the creation of this specification in a timely manner:

- Built-in isolation mechanisms to provide the implemented functions with a well-defined, hardware-enforced cryptographic boundary.
- A hardware rooted chain of trust to ensure the secure boot of the system.
- A hardened unit (CSU) dedicated to implementing the SHA-3, RSA, and AES-GCM cryptographic algorithms that 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 (*Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices* (XAPP1323), *Isolation Design Flow for UltraScale+ FPGAs and Zynq UltraScale+ MPSoCs* (XAPP1335), *Isolation Methods in Zynq UltraScale+ MPSoCs* (XAPP1320), *External Secure Storage Using the PUF v1.0 Application Note* (XAPP1333), and *Zynq UltraScale+ Device Technical Reference Manual* (UG1085)) can provide additional information on how to use the device's features to isolate security functions, develop tamper-resistant designs, generate cryptographic keys, etc.

Cryptographic Module Interfaces

The cryptographic module should have the following logical interfaces specified in FIPS 140-2 plus a Control output interface introduced in FIPS 140-3.

- Data input
- Data output
- Control input
- Status output
- Control output (introduced in FIPS 140-3)

The addition of the control output interface aims to enable the exchange of commands among modules. All non-software modules should also have a power interface if power is not managed within the cryptographic boundary. Furthermore, FIPS 140-3 introduces the concept of trusted channels (similar to the trusted paths specified in FIPS 140-2) to specify the secure exchange of plaintext critical security parameters (CSPs) among modules. For SLs 1 and 2, there are no requirements for the use of trusted channels. However, for SLs 3 and 4, the exchange of plaintext CSPs requires the use of trusted channels. The trusted channels should have either their physical ports physically separated from all other ports or their logical interfaces logically separated from all other interfaces. Depending on the security level (SL3 or SL4), there are specific requirements for authentication of all the services that use the trusted channel and for its protection against eavesdropping and physical/logical tampering.

The designer of the cryptographic module is responsible for the implementation of the requested ports and for the interfaces that are used for transferring keys to and from the device. The Zynq UltraScale+ MPSoC is composed of four major power domains. Three of the power domains provide power to the PS and the fourth is used to power the device's PL, which is known as the PL power domain (PLPD). Consequently, PL-only modules can be isolated from PS-based applications post-boot. If the designer opts to repurpose the hardened cryptographic engines of the CSU (see Figure 1), the module can take advantage of the Zynq UltraScale+ MPSoC's security features. Data from the PS/PL are DMA'ed to the CSU and then distributed to the appropriate cryptographic engine using the CSU's secure stream switch. Cryptographic keys can be updated at runtime using the CSU's key management facility. As discussed in Zynq UltraScale+ MPSoC Security, access to the engines can be hardware-controlled using the XPPUs. Furthermore, the CSU along with the RPU and the platform management systems are powered by the same domain (low-power domain) and, consequently, the module can be power-isolated from the PL and the rest of the PS system.

Roles, Services, and Authentication

The cryptographic module should be able to support distinct roles for its operators and the corresponding services the latter can access. In particular, the module should support at a minimum a crypto officer role and, optionally, a user role and a maintenance role. In FIPS 140-2, only the maintenance role is optional. There are no authentication requirements for SL1 modules. At SLs 2 and 3, the module should employ role-based authentication and identity-based authentication, respectively. At SL4, the clause adds an additional layer of security by requesting the modules to employ multi-factor identity-based authentication. Also, the module should expose the following services to operators:

- Module version and status
- Security functions
- Zeroization
- Self-test

FIPS 140-3 also introduces requirements for module self-initiated security functions that require no operator intervention at runtime. The requirements of this clause also cover the secure loading of software/firmware from an external source to the module.

Bootgen (see *Bootgen User Guide* (UG1283)), the Xilinx image generation tool, supports a variation on the split knowledge referenced in FIPS 140-3. For example, the encryption and authentication can be done on different servers by different operators by using Bootgen in the hardware security monitor (HSM) mode. The Zynq UltraScale+ MPSoC provides RSA asymmetric 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. Also, authenticated application code residing on the PS can implement role-based/user-based authentication schemes. Runtime device health checks, tamper response involving auto-triggered SSPs zeroization, and SoC lockdown are also part of the self-initiated security functions the Zynq UltraScale+ MPSoC provides to the operator.

Software/Firmware Security

FIPS 140-3 introduces this new section of requirements by grouping all the software/firmware requirements for integrity and loading of tests that are in FIPS 140-2. The section also introduces a few new requirements and allowances. At all security levels, integrity tests should be applied to a software/firmware module either by the module itself or by another validated and approved module. The tests should be able to be triggered using only interfaces specified in the standard, and all temporary values generated during a test should be zeroized upon completion of the test. Error correction codes (at minimum 16-bit in length) are still acceptable but only at SL1 and only for software/firmware components within a hardware module or within a disjoint hardware component of a hybrid module. For software/firmware modules at SL1, the only acceptable integrity methods are based on either message authentication codes (MACs) or digital signatures. At SL2, using hash-based MACs (HMACs) or digital signatures is mandatory for integrity. However, at SL3 and 4, only digital signatures are allowed. The clause also requires that the modules should contain only binaries and should be able to disable any debug interfaces allowing the inspection of the code.

The Zynq UltraScale+ MPSoC supports the secure boot of the SoC by providing confidentiality, integrity, and authentication of the PS/PL images using FIPS-approved cryptographic algorithms. The hardware rooted chain of trust starts with the device power-up when the metal-masked PMU/CSU boot ROM code is about to be executed. Since the boot ROM code is immutable with an adequate lifetime per FIPS 140-3 implementation guidelines, it does not need an integrity check. Nevertheless, the boot ROM code is hashed using the CSU's hardened SHA-3 engine, and the resulting checksum is checked against the golden copy that is also stored on the device. If the cryptographic checksums match, the CSU starts executing the part of its boot ROM code that authenticates the FSBL bootloader using RSA asymmetric digital signatures with SHA-3 hashing, which also verifies the integrity of the bootloader. The CSU also includes an RSA multiplier to accelerate public/private key operations. To provide confidentiality, the operator can encrypt the FSBL using the AES algorithm. In this case, the CSU uses the AES engine to decrypt it. Next, the FSBL takes over to boot other parts of the SoC, either in the PS or PL, and it is up to the operator to properly utilize the device's security facilities to maintain the chain of trust up to the application layer. The SoC also provides support for symmetric authentication that is based on the AES-GCM algorithm. The JTAG interface is the centerpiece of the debug features the Zynq UltraScale+ MPSoC provides for PS/PL development. By default, the JTAG port initially starts out disabled and is only enabled if a non-secure boot mode is detected or post secure boot by authenticated software. The device also provides an eFUSE that the operator can program to permanently disable the JTAG interface.

Operational Environment

The operational environment of a cryptographic module is defined as the management of the software, firmware, and hardware required for the module to operate. Most of the FIPS 140-2 requirements for operating systems are also in FIPS 140-3. At all security levels, the OS should provide complete process separation to the module to prevent any unauthorized access to the module's SSPs. At SL2, to protect the module's SSPs, the OS should also implement either role-based access controls or, at a minimum, a robust mechanism for defining new groups and assigning restrictive permissions. The authentication mechanisms of the OS should meet the requirements outlined in Roles, Services, and Authentication. In addition, the module, with the help of the OS, should provide an auditing mechanism for capturing and recording events that can potentially expose data the module manages. Other than how requirements are organized in this clause, the most noteworthy change in FIPS 140-3 is that the requirement for validation of the OS to CC EAL2 or higher has been removed.

The Zynq UltraScale+ MPSoC has built-in hardware mechanisms that limit unauthorized access to the device’s eFUSE- and BBRAM-stored cryptographic keys. Furthermore, it supports the secure installation of software by implementing in hardware FIPS-approved algorithms for image confidentiality, integrity, and authentication (see requirements in Software/Firmware Security). However, the Arm-based PS system of the Zynq UltraScale+ MPSoC protects the OS during execution by enforcing hardware-based isolation with security mechanisms that are built into the CPU (e.g., XPPU, XMPU, SMMU combined with the Arm TrustZone security, memory protection unit (MPU), secure virtualization, etc.) At the OS/application layer, mechanisms must be implemented to use the device's security facilities to restrict access to the module's SSPs and to provide support for auditing system events.

Physical Security

The cryptographic module should employ mechanisms to restrict unauthorized physical access to the module and to prevent unauthorized modifications of its state to protect its data components and SSPs within the cryptographic boundary. The requirements in this clause define the single-chip, multiple-chip embedded, and multiple-chip standalone embodiments of the cryptographic module. SL1 requirements are met with production-grade components with standard passivation. SL2 requires the addition of tamper-evident technology and mechanisms to prevent the direct observation of critical information about the internal operations of the module (opaqueness). SL3 requires the addition of strong or hard enclosures with mechanisms for detecting and responding to tampering attempts at removable covers and doors and for resistance to direct probing via openings or entry points. A tamper response should involve the immediate zeroization of all the unprotected SSPs of the module upon detection. SL4 extends the SL3 requirements to require the use of detection and response mechanisms to the entire enclosure.

Compared to its predecessor, FIPS 140-3 moved the requirement for uniquely numbered or independently identifiable tamper-evident seals to SL3. Also, all cryptographic modules should either implement EFP features or undergo rigorous EFT at SL3. At SL4, the modules should implement EFP features and mechanisms for protection against fault induction. Both EFP features and EFT testing aim to ensure that the security of the module will not be compromised when the module is forced to function (accidental or induced) outside its specified normal operating range. Another change in FIPS 140-3 is that any tamper-evident material used for opaqueness should either be opaque or translucent within the visible spectrum.

With a wide range of security functions built into the Zynq UltraScale+ MPSoC (e.g., CSU for secure installation/boot of software and installation of cryptographic keys, hardware-based protection units for memory (XMPU) and peripherals (XPPU), etc.), many of these requirements can be easily met. The Xilinx application notes *Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices* (XAPP1323), *Isolation Design Flow for UltraScale+ FPGAs and Zynq UltraScale+ MPSoCs* (XAPP1335), and *Isolation Methods in Zynq UltraScale+ MPSoCs* (XAPP1320) provide detailed information on these security features and how to use them.

In addition, the Xilinx SecMon IP 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 *Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices* (XAPP1323) 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. Because SecMon is part of the overall user design functionality, it must be integrated at the system level by the OEM.

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

Non-invasive Security

FIPS 140-3 introduces this new section to specify requirements to protect the cryptographic module against attacks that do not require physical access to the module. The requirements are yet to be defined although they are expected to outline test metrics for the evaluation of countermeasures against non-invasive attacks such as single/differential power analysis (SPA/DPA), voltage/clock glitching, etc.

Although the list of non-invasive attacks a module should be able to mitigate and the specific evaluation metrics are yet to be defined, the Zynq UltraScale+ MPSoC includes built-in DPA countermeasures (see *Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices* (XAPP1323)).

To protect against DPA attacks, it is extremely important to reduce the amount of side-channel data an adversary can collect on any one key. To this end, the device authenticates images (before decrypting them) to detect random (or invalid) images the adversary loads on the device in an attempt to increase the amount of information the side-channel leaks. Furthermore, each image is broken up into multiple smaller blocks and each block is encrypted using its own unique user-defined key to reduce the amount of data that can be collected for a single key. The device also employs a key rolling technique to avoid having to store all the decryption keys on the chip. In this technique, only the decryption key for the first block of the image is stored in on-chip memory while all the other keys are stored in the blocks of the image (i.e., each block contains the decryption key of the next block). To mitigate glitching attacks, the Zynq UltraScale+ MPSoC implements the following countermeasures to continuously monitor the health of the device at runtime:

- CSU/PMU triple redundant processors
- ECC on PS and DDR memories
- SHA integrity checks on immutable ROM code
- SecMon IP

Sensitive Security Parameter Management

This section addresses random bit generators (RBGs) and SSP management that encompasses the entire lifecycle of SSPs (e.g., SSP generation, SSP establishment, SSP entry/output, SSP storage, and SSP zeroization). SSPs consist of CSPs (e.g., secret and private keys, passwords, RBG state information, etc.) and public security parameters (PSPs) that are explicitly defined for the first time in FIPS 140-3 to also address public keys, public-key certificates, etc. Unlike CSPs whose confidentiality and integrity should be ensured, for PSPs, there are only integrity-related requirements in this clause. SSPs can be entered into or output from the cryptographic module either electronically/automatically (e.g., via a smart card/tokens, PC card, etc.) or directly/manually (e.g., entered via a keyboard or output via a visual display). Manual entry/output of SSPs should be through interfaces specified in the standard and SSPs that are entered unencrypted into the module can be temporarily displayed to allow for visual verification. At SLs 1 and 2, the input or output of CSPs, key components, and authentication data can be in either encrypted or plaintext form, provided they are maintained within the operational environment and meet the operational environment requirements. At SL3, CSPs that enter or leave the cryptographic module should either be encrypted or use trusted channels (see Cryptographic Module Interfaces). SL4 requires that the module should also use multi-factor separate identity-based operator authentication for entering or outputting key components. At all security levels, unprotected SSPs stored in plaintext form should be zeroizable. SL4 also extends this requirement to encrypted SSPs. At SL1, the zeroization of plaintext SSPs can be performed procedurally by the operator of the module. At SLs 2 and 3, the module by itself should zeroize plaintext SSPs when they are no longer needed. Furthermore, at SL4, the zeroization of SSPs should be non-interruptible and occur in a sufficiently small time period to prevent their recovery.

The (CSP) AES decryption key (see Software/Firmware Security) is stored in plaintext (red) form on the device in either the BBRAM or non-volatile eFUSEs during the provisioning of the device (i.e., prior to field deployment). The red key is transferred via a write-only path to the BBRAM/eFUSEs upon which a key integrity check is performed. Both BBRAM and eFUSEs do not provide a physical readback path for the red key, whereas the key is only usable by the AES-GCM engine during secure boot. To further guard the red key, the operator can use the PUF, available in the Zynq UltraScale+ MPSoC, to generate a die-unique KEK and use it to AES-encrypt the red key. The PUF-encrypted red key (or now, black key) can be stored in the on-chip eFUSEs. The red keys stored in BBRAM can be zeroized. The eFUSE-stored keys cannot be zeroized because they are one-time programmable (OTP). Registers holding the red key are immediately zeroized after they are used to decrypt the first block of an image. The AES keys that are required to decrypt the remaining blocks of the image are provided with the image (see the key rolling technique discussed in Non-invasive Security). For the PSPs, the RSA public/private key pair that is used during secure boot for the asymmetric authentication of an image is created off the device by the operator. Secure boot requires only the public key (which has no value to an adversary) to be on the device. Due to limited space, the public key is hashed using SHA-3 and stored in on-chip eFUSEs while the full public key is provided with the image. During secure boot, the device rehashes the provided public key and compares the resulting hash with the hash value stored in eFUSEs to verify its integrity. The Zynq UltraScale+ MPSoC can accommodate two 384-bit hashes of primary public keys (PPKs), which are write-protected and can be individually revoked in case of a tamper event. To limit the use of the two PPKs, the PPKs are only used to authenticate secondary public keys (SPKs) and the SPKs, in turn, to authenticate the image. SPKs are also provided with the image and the operator is responsible for creating them along with their private counterparts. Zynq UltraScale+ MPSoCs support up to 32 SPKs and they can also be revoked upon a tamper event.

The Zynq UltraScale+ MPSoC does not have a built-in RBG in silicon to create application layer session keys. However, an RBG 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 (red) or ciphertext (black) key load depending on the implementation. Also, a hardware security module (HSM) IP that provides secure key management and additional cryptographic processing to the Zynq UltraScale+ MPSoC is available from Silex Insight [REF 15] (a Xilinx partner).

Self-tests

The cryptographic module should run pre-operational and conditional tests by itself without any external intervention to verify that it runs as expected. Before the module starts outputting any data via the data output interface, it should have successfully passed all pre-operational self-tests to ensure it functions correctly. The pre-operational self-tests include tests for the cryptographic algorithm if the module contains a hardware component, including the hybrids types (see requirements in Cryptographic Module Specification). If the module has a software/firmware component, tests for software/firmware integrity are also necessary. For example, the AES cryptographic algorithm test is a type of known-answer test (KAT). Also, the clause requires self-tests for bypass mechanisms and for other critical functions provided by the module. Conditional self-tests should be executed whenever they are required by a security function that is about to be invoked. At SLs 3 and 4, FIPS 140-3 introduces the requirement for error logs to be kept with information, at a minimum, for the most recent error event upon a failing self-test so it can be examined by an authorized operator. If a module fails a self-test, it should enter an error state and either output an error message or allow the operator to determine that the module has entered an error state implicitly through an unambiguous procedure documented in the standard.

The hardened cryptographic functions of the Zynq UltraScale+ MPSoC do not automatically execute pre-operational KATs at the power-up of the device. However, a KAT can be added to the RSA-authenticated FSBL user code. The conditional test requires that an approved authentication mechanism is used when software is loaded. The Zynq UltraScale+ MPSoC's RSA authentication is approved and is run at boot time on all partitions loaded. The RSA authentication can be run periodically during runtime. 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 start-up or periodically for testing the overall health of the system and SecMon IP.

Life-cycle Assurance

Life-cycle assurance ensures that the cryptographic module is properly designed, developed, tested, configured, delivered, installed, disposed, and documented by the vendor. An important change in this FIPS 140-3 clause is the addition of requirements for vendor testing of the module to ensure that it operates in accordance with the module security policy and functional specifications. At SLs 1 and 2, the vendor should specify and document the functional testing performed on the module. At SLs 3 and 4, the vendor should also specify and document the low-level testing performed on the module. The low-level testing details are not defined yet. FIPS 140-3 also dives deeper into the proper way of disposing of the module when it is no longer needed. At SLs 1 and 2, there are requirements for sanitization of the module, such as removing SSPs so that they cannot be distributed to other operators. At SLs 3 and 4, the vendor should also specify and document procedures for the secure destruction of the module.

For the Zynq UltraScale+ MPSoC, Xilinx follows best-in-class processes and procedures to ensure the highest quality at all stages of production. The *Xilinx Quality Manual* (QAP0002) can be used as supporting documentation to help meet this requirement. For the programmable portions of a Zynq UltraScale+ MPSoC 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 designer is responsible for ensuring that a quality process is followed for all the programmable user designs and for supplying the applicable supporting documentation.

Mitigation of Other Attacks

This section captures attacks and mitigations that are not defined elsewhere in the standard without providing any testable requirements and metrics for evaluation. SLs 1, 2, and 3 require that the list of attacks the cryptographic module is designed to mitigate should be included in the module's supporting documents so it will be evaluated when requirements and associated tests are developed. SL4 requires that the details of the developed mitigation mechanisms and methods to test their effectiveness should be documented, too.

Additional security functions can be implemented in the PS or PL to mitigate attacks that are not currently covered by the standard. The designer is responsible for adequately documenting the attacks the module mitigates and the methods developed to test its effectiveness.

Zynq UltraScale+ MPSoC FIPS 140-3 Scorecard

The following table provides a Zynq UltraScale+ MPSoC *scorecard* for satisfying the eleven FIPS 140-3 security requirements (i.e., the relative risk level). Unless noted, the achievability is for SLs 1 to 4.

Table 2: **FIPS 140-3 Security Requirements**

FIPS 140-3 Security Requirements	
Coverage Area	**Achievability Level with Zynq UltraScale+ MPSoC**
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	SL1-3: Low Risk, SL4: 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

CAVP Overview

The participants in a CAVP validation are the vendor and the CST lab. The CST lab independently tests cryptographic algorithms using the CAVS test tool. Either the vendor or the CST lab is allowed to perform the tests. CST labs are accredited under the NVLAP. The algorithms can be tested in a hardware environment or in simulation. A list of accredited labs can be found on the NIST IFT Computer Security Resource Center website [REF 17]. Also provided on this site are tests such as KATs [REF 18]. The AES and SHA cryptography used in Zynq UltraScale+ MPSoCs are approved cryptographic algorithms shown on the CAVP validation list [REF 19]. The following table lists the NIST validation numbers for the Zynq UltraScale+ MPSoC.

Table 3: **NIST CAVP Validation List**

CAVP Validation List	Validation Number
SHA3/384	SHA-3 20
Zynq UltraScale+ MPSoC AES-GCM Core	AES 4438
Zynq UltraScale+ MPSoC XilSecure Library	A1940

The RSA algorithm used in the Zynq UltraScale+ MPSoC has the following two variances from the NIST standard:

- Uses a non-standard RSA modulus (4096 rather than 1024, 2048, or 3072).
- Omits the additional *01* appended to the message when using SHA3.

These slight variances are applied to boot and configuration cryptographic operations. Consequently, user implementations are not hampered by these limitations and nothing precludes the user`s ability to implement cryptographic algorithms that are fully compatible with the NIST standard. For more information on the variances of the RSA algorithm used in the Zynq UltraScale+ MPSoC, see the *Variances Against NIST Cryptographic Standards for UltraScale, UltraScale+, and Zynq UltraScale+ Devices* (XTP475), available on the Xilinx Design Security Lounge.

Conclusion

The certification of a cryptographic module against the FIPS 140-3 standard can be an arduous and time-consuming process. A Zynq UltraScale+ MPSoC-enabled system can alleviate many of the difficulties in the certification process for these reasons:

- High level of integration.
- Wide range of built-in hard security functions.
- User-accessible hardened cryptographic blocks.
- Silicon-based anti-tamper protections.
- Side-channel attack protection.
- Cryptographic algorithms already validated by CAVP.
- Mature development environments and extensive supporting documentation.

- Rich partner ecosystem for both the PS and PL.

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

References

These documents provide supplemental material useful with this guide:

1. National Institute of Standards and Technology, Information Technology Laboratory, *Security Requirements for Cryptographic Modules (FIPS PUB 140-3)*. March 2019. (Supersedes FIPS PUB 140-2, May 2001.) Retrieved April 1, 2021.
2. National Institute of Standards and Technology, Information Technology Laboratory, *Security Requirements for Cryptographic Modules (FIPS PUB 140-2)*. May 2001. (Supersedes FIPS PUB 140-1, January 1994.) Retrieved April 1, 2021.
3. National Institute of Standards and Technology, Canadian Centre for Cyber Security, *Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program*. November 2021. Retrieved December 1, 2021.
4. *Accelerating Cryptographic Performance on the Zynq UltraScale+ MPSoC* (WP512).
5. *Isolate Security-Critical Applications on Zynq UltraScale+ Devices* (WP516).
6. *Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices* (XAPP1323).
7. Product Brief, Security Monitor IP: *Industry-Leading Programmable Logic Device Security Protecting IP and Mission Critical Data*.
8. *Zynq UltraScale+ MPSoC: Software Developers Guide* (UG1137).
9. *Isolation Design Flow for UltraScale+ FPGAs and Zynq UltraScale+ MPSoCs* (XAPP1335).
10. *Isolation Methods in Zynq UltraScale+ MPSoCs* (XAPP1320).
11. *External Secure Storage Using the PUF v1.0 Application Note* (XAPP1333)
12. *Zynq UltraScale+ Device Technical Reference Manual* (UG1085).
13. *Bootgen User Guide* (UG1283)
14. *Variances Against NIST Cryptographic Standards for UltraScale, UltraScale+, and Zynq UltraScale+ Devices* (XTP475) (available on the Xilinx Design Security Lounge).
15. Silex Insight, Hardware Security Module [For Xilinx FPGA].
16. *Xilinx Quality Manual* (QAP0002).
17. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: Testing Laboratories. Updated June 2020. Retrieved September 1, 2021.
18. 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 September 1, 2021.

19. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: Cryptographic Algorithm Validation Program. Updated March 8, 2021. Retrieved September 1, 2021.

Revision History

The following table shows the revision history for this document.

Section	Revision Summary
02/04/2022 Version 1.0	
Initial release.	N/A

Please Read: Important Legal Notices

The information disclosed to you hereunder (the "Materials") is provided solely for the selection and use of Xilinx products. To the maximum extent permitted by applicable law: (1) Materials are made available "AS IS" and with all faults, Xilinx hereby DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE; and (2) Xilinx shall not be liable (whether in contract or tort, including negligence, or under any other theory of liability) for any loss or damage of any kind or nature related to, arising under, or in connection with, the Materials (including your use of the Materials), including for any direct, indirect, special, incidental, or consequential loss or damage (including loss of data, profits, goodwill, or any type of loss or damage suffered as a result of any action brought by a third party) even if such damage or loss was reasonably foreseeable or Xilinx had been advised of the possibility of the same. Xilinx assumes no obligation to correct any errors contained in the Materials or to notify you of updates to the Materials or to product specifications. You may not reproduce, modify, distribute, or publicly display the Materials without prior written consent. Certain products are subject to the terms and conditions of Xilinx's limited warranty, please refer to Xilinx's Terms of Sale which can be viewed at https://www.xilinx.com/legal.htm#tos; IP cores may be subject to warranty and support terms contained in a license issued to you by Xilinx. Xilinx products are not designed or intended to be fail-safe or for use in any application requiring fail-safe performance; you assume sole risk and liability for use of Xilinx products in such critical applications, please refer to Xilinx's Terms of Sale which can be viewed at https://www.xilinx.com/legal.htm#tos.

AUTOMOTIVE APPLICATIONS DISCLAIMER

AUTOMOTIVE PRODUCTS (IDENTIFIED AS "XA" IN THE PART NUMBER) ARE NOT WARRANTED FOR USE IN THE DEPLOYMENT OF AIRBAGS OR FOR USE IN APPLICATIONS THAT AFFECT CONTROL OF A VEHICLE ("SAFETY APPLICATION") UNLESS THERE IS A SAFETY CONCEPT OR REDUNDANCY FEATURE CONSISTENT WITH THE ISO 26262 AUTOMOTIVE SAFETY STANDARD ("SAFETY DESIGN"). CUSTOMER SHALL, PRIOR TO USING

OR DISTRIBUTING ANY SYSTEMS THAT INCORPORATE PRODUCTS, THOROUGHLY TEST SUCH SYSTEMS FOR SAFETY PURPOSES. USE OF PRODUCTS IN A SAFETY APPLICATION WITHOUT A SAFETY DESIGN IS FULLY AT THE RISK OF CUSTOMER, SUBJECT ONLY TO APPLICABLE LAWS AND REGULATIONS GOVERNING LIMITATIONS ON PRODUCT LIABILITY.

Copyright