AMD
XILINX

Single Chip FIPS 140-3 on Zynq UltraScale+ MPSoC

WP548 (v1.0) November 3, 2022

Abstract

Data security is a primary concern across all markets, especially communications. A certified cryptographic module that provides off-the-shelf cryptographic functions and programmable interfaces is essential. The high level of integration, hardware, and software programmability, and the inclusion of iDirect Government certified IP makes the Zynq® UltraScale+™ MPSoC an ideal solution. This white paper describes a novel approach to enable a secure execution environment (SEE) on the Zynq UltraScale+ MPSoC architecture for FIPS 140-3 certification.

Introduction

iDirect Government has a history of operating FIPS 140-2 certified cryptography in its satellite communications products. Starting with the e8000 series of products, iDirect Government has developed, and certified, its cryptographic products with cryptographic module validation program (CMVP) and fielded these products in United States Department of Defense (DoD) networks.

The 9000 series of remote terminals and defense line cards (DLCs) took this development a step further with the inclusion of a separate printed circuit board (PCB) assembly used as an external cryptographic module, with accompanying IP, that are certified under FIPS 140-2 Level 3.

iDirect Government's next generation of remote terminals feature an extension of this modular development and leverage the programmable security features of the Zynq UltraScale+ MPSoCs. Moving from a separate printed circuit board (PCB) assembly to an on-chip solution further improves modularity as well as size, weight, and power (SWaP). In conjunction with iDirect Government's field tested and previously certified IP, the Zynq UltraScale+ MPSoCs can further enhance next-generation products with support for FIPS 140-3.

Introduction to Secure Execution Environment

This section details the difference between a traditional trusted execution environment (TEE) leveraging unique features of the Zynq UltraScale+ MPSoC and the iDirect Government secure execution environment (SEE) solution.

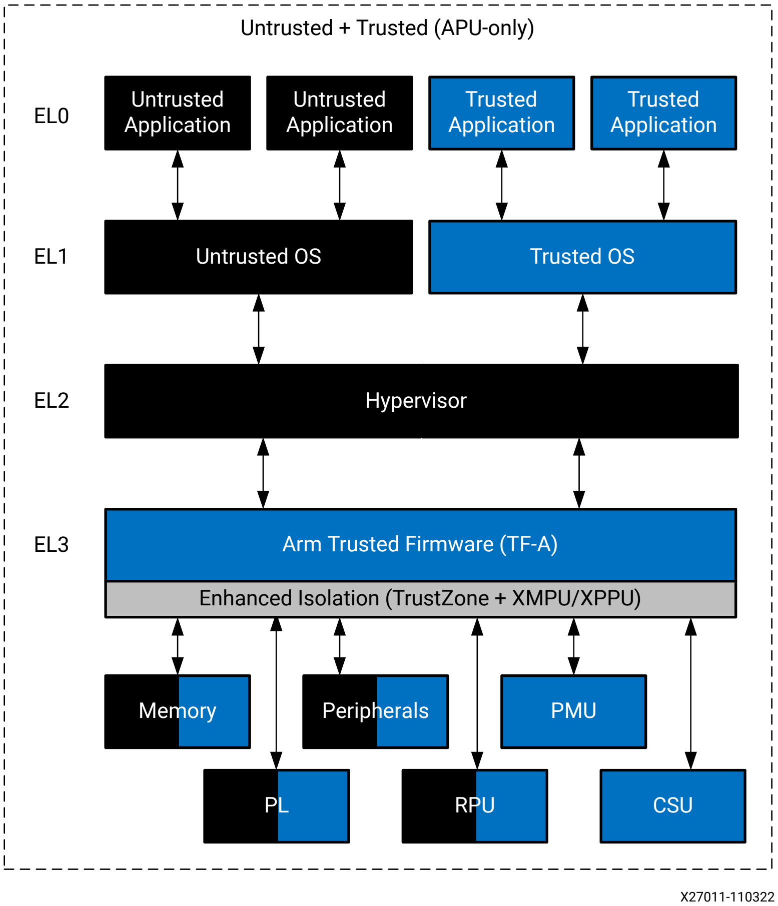
Trusted Execution Environment

One mechanism for isolating the trusted world from the untrusted world is by leveraging Arm® trusted firmware for the Cortex® processors (TF-A) to create a trusted and untrusted environment on the same processor. The application processing unit (APU) on the Zynq UltraScale+ MPSoC is an Armv8 Cortex®-A53 and therefore fully supports unique exception levels (EL) to isolate secure and non-secure domains.

This isolation is reliant on TF-A software to act as the arbiter between trusted and untrusted domains by adding AXI4 protection bits to the transactions. As detailed in the following figure, you can see that an untrusted (colored in black) application must go through the TF-A to request access to trusted (colored in blue) memory or peripherals.

On the Zynq UltraScale+ MPSoC, TF-A is further enhanced by the Xilinx peripheral protection unit (XPPU) and memory protection unit (XMPU). The use of the XMPU and XPPU on the Zynq UltraScale+ MPSoC adds a hardware backed element to the functionality of the TF-A. As shown in the following figure, any transaction originating from a trusted application on the APU (master of the transaction in this case) is permitted to access a trusted peripheral. Any other master (RPU for example) is blocked from accessing this peripheral by the XMPU/XPPU.

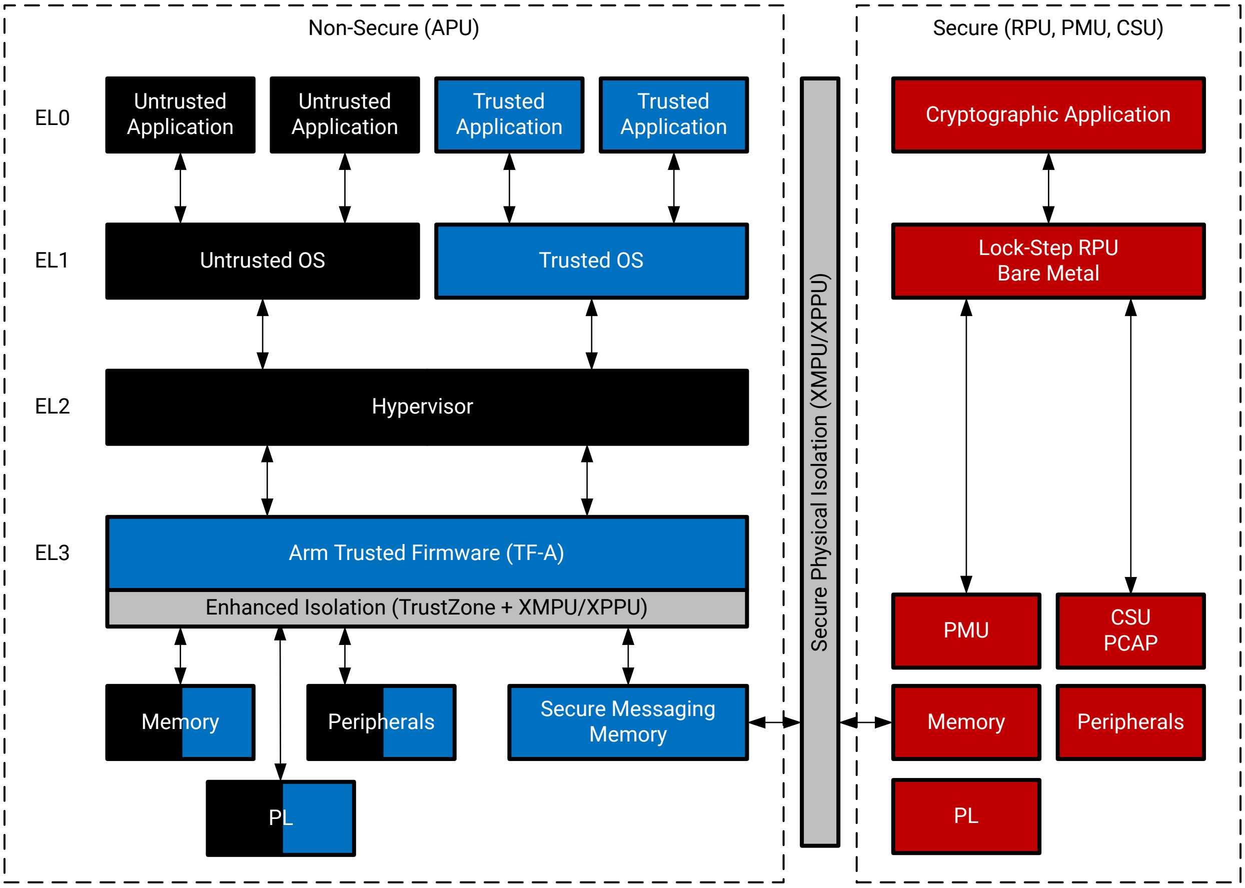
Figure 1: **Trusted Execution Environment with Zynq UltraScale+ MPSoC Enhanced Isolation**



Secure Execution Environment

Unfortunately, in a TEE, even with enhanced isolation provided by the Zynq UltraScale+ MPSoC, the system relies on the proper operation of TF-A execution levels. For example, if an exploit is exercised to elevate an untrusted applications execution level, even with the enhanced isolation of Zynq UltraScale+ MPSoC (XMPU), a nefarious application would not be prevented from accessing trusted memory or peripherals. Using the previous figure, if an untrusted application exploits TF-A software and raises its execution level, it can still bypass the XMPU because this transaction is still originating from the APU at EL3. Because the master ID is the same as the APU, the XMPU or XPPU will fail to block the transaction. The secure execution environment (SEE), proposed by iDirect Government's architecture, provides a physically isolated secure cryptographic sub-system for hosting the systems cryptographic functions. As shown in the following figure, the secure cryptographic sub-system (colored in red) is physically isolated (via XMPU/XPPU) from the rest of the system. Regardless of the state of the TF-A, any transaction originating from the APU is denied access to secure peripherals or memory. This hardware-backed solution leverages Zynq UltraScale+ MPSoC multiprocessor architecture to provide a physically and logically isolated environment for non-secure and secure domains. The physical isolation of the APU and RPU (as well as their associated memories and peripherals) allows the iDirect Government architecture to maintain a strict, logical separation between non-secure application code and secure, FIPS 140-3 certified cryptographic module software.

Figure 2: **Secure Execution Environment with Zynq UltraScale+ MPSoC Enhanced Isolation**

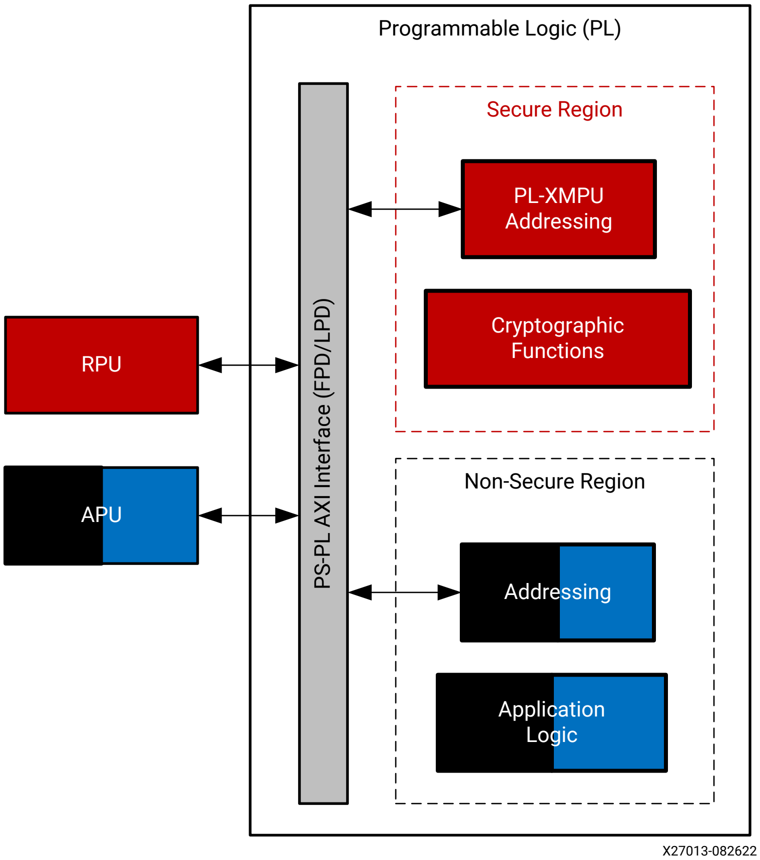


X27012-110322

Programmable Logical Isolation

The SEE extends from the processing system into the programmable logic (PL). As shown in the following figure, the iDirect Government SEE is leveraging features of the Zynq UltraScale+ MPSoC programmable logic to isolate non-secure application logic from secure cryptographic logic in the PL. A soft version of the XMPU is implemented in the secure region of the PL to ensure that any transaction from the processing system to secure logic in the PL only responds to transactions originating from the secure domain (RPU). The logic contained in the secure PL region remains fixed and FIPS 140-3 certified regardless of any changes made to logic contained in the non-secure PL region. The non-secure PL region includes application logic such as iDirect Government's satellite waveform modulators and demodulators, which can be updated independently of the secure PL region.

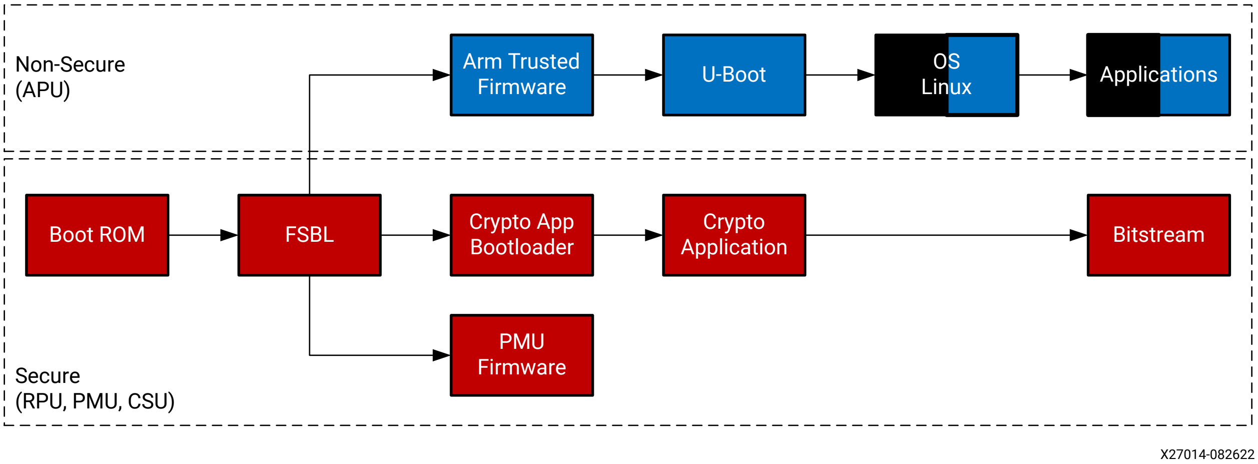
Figure 3: **Programmable Logic Isolation**



Authenticated Boot with RPU as Root of Trust and Secure Processing System

In iDirect Government's SEE, the RPU is the secure processor ensuring root of trust as well as maintaining the logical isolation of the system. The RPU executes the first stage boot loader (FSBL) and configures XMPU/XPPU isolation control registers, which ensures that the root of trust extends from boot ROM all the way to the cryptographic application. The following figure illustrates the boot flow in iDirect Government's SEE. The FSBL executes on the RPU that hands off to the cryptographic application. All non-secure software is executed solely on the APU, ensuring that secure peripherals and memory cannot be accessed.

Figure 4: **Boot Sequence and Root of Trust**



iDirect Government Cryptographic Application

iDirect Government has over 10 years of experience building and maintaining FIPS 140-2 certified cryptographic modules and telecommunications equipment. Their cryptographic application is fielded in thousands of satellite remote terminals and communication hub deployments throughout the world for the U.S. DoD customers, as well as foreign ministries of defense (MoDs). The following is a high-level overview of the architecture and collaboration with Xilinx on the next-generation Zynq UltraScale+ MPSoC application.

High-level Description

The cryptographic application is responsible for the configuration, control, and monitoring of the hardware and programmable logic. Upon execution, the software initializes, verifies the software image residing in secure flash, and performs a series of self-tests. If the initialization succeeds, the software enters the normal operation state. If initialization fails, the software enters the critical error state.

The critical error state supports the ability to load new software and provide status. No critical security parameters (CSPs) or cryptographic functions are available. The normal operation mode supports two sub-modes: limited and full-featured.

When the software enters the normal operation state, by default it is in the limited sub-mode which supports the ability to load new software, load a device bitstream, and provide status. No CSPs or cryptographic functions are available. As discussed in the next section, the software can enter full-featured mode when the device bitstream is authenticated, loaded into the PL, and verified. If anything fails along the way, the software remains in limited mode.

The full-featured mode supports cryptographic functions including the encryption and decryption of all data. Periodic tests are performed in full-featured mode to continue verification of the programmable logic and software. If any tests fail, the software moves to the critical error state. Full-featured mode also supports the ability to update CSPs.

A request to load a device bitstream while in full-featured mode causes the software to return to limited-mode after the new bitstream is authenticated, but before it is loaded and verified.

Secure Message Interface

As shown in Figure 2: Secure Execution Environment with Zynq UltraScale+ MPSoC Enhanced Isolation, the non-secure software (APU) communicates with the cryptographic application using a well-defined, shared memory messaging interface. All messages sent to the cryptographic application are authenticated.

Messages are written to the non-secure DRAM and the cryptographic application is notified of an outstanding message. Upon notification, the software copies the message into the secure DRAM, authenticates, and processes the message. The copy to the secure DRAM is necessary to verify the message is not altered during or after the authentication phase by an untrusted entity.

Authenticated FPGA Configuration

To maintain control over the authenticity of programmable logic's images, the iDirect Government's cryptographic application is developed to be the sole master of PL configuration. This isolation configuration ensures that only iDirect Government signed and authenticated bitstreams can be configured. The cryptographic application running on the RPU receives a device configuration message from the modem software running on the APU. Requests to load a bitstream are processed when the software is in limited or full-featured mode. A device configuration message requests the cryptographic application to copy the programmable logic image into secure DRAM memory, authenticate the RSA signature, and load the image into the PL. As with messages, the copy to secure DRAM is necessary to verify the bitstream is not altered during or after the authentication phase. As described previously, once a device bitstream is loaded into the secure PL region and verified using a set of known answer tests (KAT), the software enters full-featured mode.

FIPS 140-3 Requirements Matrix

The following table summarizes eleven sections of FIPS 140-3 requirements and provides a high-level explanation of using the Zynq UltraScale+ MPSoC with iDirect Government SEE and IP can satisfy each requirement. The iDirect Government's FIPS 140-3 cryptographic module provides a FIPS 140-3 Level 3 solution by leveraging a proven cryptographic application and using the physical isolation and physical security features of the Zynq UltraScale+ MPSoC.

Refer to the *Zynq UltraScale+ MPSoC: A FIPS 140-3 Primer* (WP543) for more detailed explanation of each requirement and how a Zynq UltraScale+ MPSoC system can be leveraged to resolve each requirement.

Table 1: **FIPS 140-3 Requirements Matrix**

FIPS 140-3 Requirement	Description	iDirect Government Solution
Cryptographic module specification	A clear border is defined between software, hardware, firmware, hybrid software, and hybrid firmware.	The SEE defined by iDirect Government has a well-defined border between the secure RPU/PL environment and the unsecure APU/PL environment. Leveraging the Zynq UltraScale+ MPSoC XMPU/XPPU and proprietary iDirect Government cryptographic software.

Table 1: **FIPS 140-3 Requirements Matrix** *(cont'd)*

FIPS 140-3 Requirement	Description	iDirect Government Solution
Cryptographic module interfaces	Five logical interfaces exist between the cryptographic module and the unsecure world: data input, data output, control input, control output, and status output.	Leveraging iDirect Government's SEE, previously certified cryptographic software and Zynq UltraScale+ MPSoC isolation features, these five interfaces can be logically separated and maintained during all levels of operation as defined in the FIPS 140-3 standard.
Roles, services, and authentication	The cryptographic module should be able to support distinct roles for its operators and corresponding cryptographic services.	iDirect Government's cryptographic software supports three roles and services: secure, limited, and factory mode. Each operating role provides a range of none, limited, or full access to cryptographic services.
Software/firmware security	A cryptographic module shall implement an authenticated chain of trust and ensure authenticity of its cryptographic services via runtime tests.	Leveraging the authenticated boot feature of the Zynq UltraScale+ MPSoC, the iDirect Government's cryptographic software can be authenticated from boot ROM to execution. The SEE messaging interface is authenticated and cryptographic services are continuously monitored to ensure authenticity.
Operational environment	The operational environment of a cryptographic module must be authenticated and access to its sensitive security parameters (SSPs) must be ensured.	The Zynq UltraScale+ MPSoC authenticated boot ensures authenticity through execution of the cryptographic software. iDirect Government's secure messaging interface ensures that only authorized users can access cryptographic services after they have been validated.
Physical security	The cryptographic module must employ mechanisms to ensure authenticated access to SSPs within the cryptographic boundary.	iDirect Government's secure messaging interface is authenticated by a username and password with each message being authenticated during transit. Each device image is signed and authenticated before being configured. After configuration the cryptographic algorithms in firmware and software are validated using FIPS accepted KAT tests.
Non-invasive security	FIPS 140-3 introduces a new section to mitigate against attacks that do not require physical access such as single/differential power analysis (SPA/DPA).	Xilinx publishes guidelines on AES key rolling to mitigate simple/differential power analysis (SPA/DPA) vulnerabilities. iDirect Government's cryptographic software and firmware implements similar mitigations to limit the effectiveness of SPA/DPA attacks.
Sensitive security parameter management	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).	iDirect Government's previously certified cryptographic software already implements an approved key management schema, over-the-air key distribution protocol and AES-256 engine. iDirect Government's cryptographic software also implements an approved DBRNG and TRNG source to ensure that the SEE has access to sufficient entropy for key generation.
Self-tests	The cryptographic module runs pre-operational and conditional tests by itself, requiring no external intervention to assure the operator that it is performing as expected.	iDirect Government's cryptographic software executes pre-operational KATs on boot before becoming fully operational. The tests can also be executed on request via the secure messaging interface. It is with the already defined authentication and integrity checks performed on the software executables and programmable logic images.
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.	Using the best-in-class processes and procedures implemented by Xilinx during Zynq UltraScale+ MPSoC manufacturing, test, and distribution, iDirect Government provides extensive documentation to both the certifying body as well as end customers to support and maintain the product line.

Table 1: **FIPS 140-3 Requirements Matrix** *(cont'd)*

FIPS 140-3 Requirement	Description	iDirect Government Solution
Mitigation of other attacks	This section captures attacks and types of mitigation that are not defined elsewhere in the standard. It does not provide testable requirements and or metrics for evaluation. Security levels 1, 2, and 3 require that the list of attack(s) the cryptographic module is designed to mitigate should be included in the module's supporting documents to be evaluated when requirements and associated tests are developed.	Additional security functions can be implemented in the processing system or PL to mitigate attacks that are not currently covered by the standard. iDirect Government's cryptographic software employs a variety of additional protections to ensure the integrity of customer data. Additional PL features can also be implemented to ensure authenticity of the bitstream as well as runtime PL configuration memory fault detection.

Conclusion

This white paper explored how iDirect Government has developed a secure execution environment capable of a FIPS 140-3 certification. By leveraging the architectural features of the Zynq UltraScale+ MPSoC and iDirect Governments previously certified cryptographic application, a strong cryptographic module can be created using only a single Zynq UltraScale+ MPSoC and associated peripherals. This paper was written in collaboration with our partner iDirect Government.

References

These documents provide supplemental material useful with this guide:

1. ARM Cortex-A Series Programmer's Guide for ARMv8-A
2. Arm Software GitHub Trusted Firmware-A
3. 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 1 April 2021.
4. 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 1 April 2021.
5. *Isolation Methods in Zynq UltraScale+ MPSoCs* (XAPP1320)
6. *Zynq UltraScale+ Device Technical Reference Manual* (UG1085)
7. *Xilinx Quality Manual* (QAP0002)
8. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Testing Laboratories*. Updated June 2020. Retrieved 1 September 2021.
9. 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 1 September 2021.
10. National Institute of Standards and Technology (NIST), Information Technology Laboratory, Computer Security Resource Center: *Cryptographic Algorithm Validation Program*. Updated 8 March 2021. Retrieved 1 September 2021.

11. *Zynq UltraScale+ MPSoC: A FIPS 140-3 Primer* (WP543)

About iDirect Government

iDirect Government, LLC, a U.S. corporation, delivers secure satellite-based voice, video and data applications with anytime and anywhere connectivity in the air, at sea and on land. iDirect Government's advanced satellite IP solutions are used for critical ISR, airborne, maritime and COTM communications to support force protection, logistics, situational awareness, disaster recovery and emergency response. Building on more than 15 years of global satellite communications experience, iDirect Government provides the most bandwidth-efficient, scalable and highly secure platform to meet specialized applications of multiple federal, state and local government agencies, including the Department of Defense, both domestically and abroad. iDirect Government has been a trusted partner of the U.S. government for more than 17 years. All its employees are U.S. citizens, with a third being U.S. military veterans and more than 60% holding U.S. security clearances.

iDirect Government's specialized technology includes transmission security (TRANSEC), Communication Signal Interference Removal (CSIR™) anti-jam technology and Open Antenna Modem Interface Protocol (OpenAMIP). All Defense-grade products sold by iDirect Government are designed, developed, assembled, programmed and verified within the United States.

For more information, please visit http://www.idirectgov.com and follow iDirectGov on Twitter athttps://twitter.com/idirectgov, Facebook at https://www.facebook.com/idirectgov, and Instagram athttps://www.instagram.com/idirectgov/. See iDirectGov on YouTube at https://www.youtube.com/channel/UCReL2Mi-yyX0sNNu-Dq0erw.

Revision History

The following table shows the revision history for this document.

Section	Revision Summary
11/03/2022 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