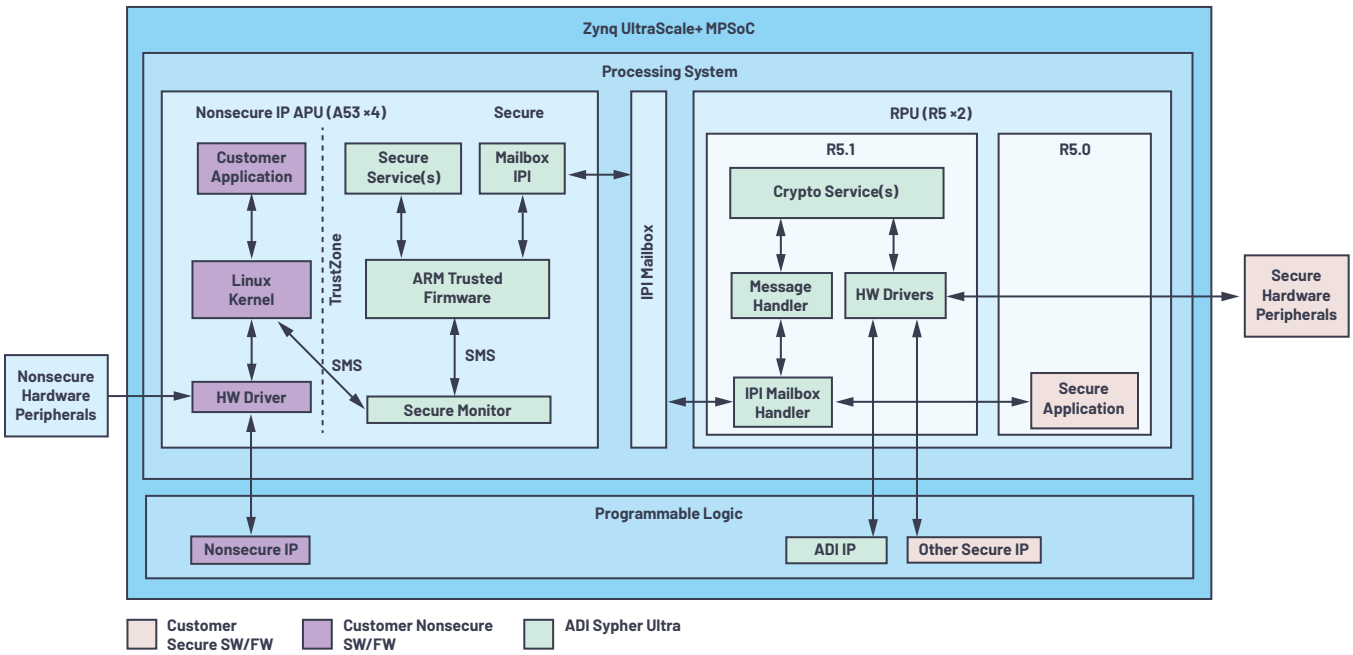
Sypher Ultra

Secure Execution Environment

System Overview

The Sypher™ Ultra secure execution environment (SEE) is a robust cryptographic system with multiple layers of security controls that reside between the Xilinx® system and the end application. This means that minimal security expertise or hardware is required. Secure APIs enable easy and seamless integration of a secure environment with your application. This eliminates the worry of compromising secure processes, reduces implementation and testing risk, reduces design cost and time to market, and frees up engineering resources. In conjunction with the Xilinx Zynq® UltraScale+™ MPSoC, the Sypher Ultra SEE enables secure computation, privacy, and data protection and isolation.



VISIT ANALOG.COM/CYBERSECURITY

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Features

Secure Boot

- **Bridges the Gap:** Provides the link between boot ROM and the end application, enabling and utilizing the inherent cryptographic algorithms within the ZUS+ (AES-256 GCM, RSA-4096, SHA-3-384) to ensure confidentiality, integrity, and authentication of all booted and executed elements.
- **Lean:** Using the inherent ZUS+ features enables efficient resource utilization.
- **Availability:** Power-on health checks are performed to ensure proper system execution.

Secure Update

- **Validated:** Automatically loads, verifies, and stores security related update files into non-volatile memory.
- **Trusted:** Enables signature/hash verification of all security related update files using RSA-4096 and SHA-3.
- **Flexible:** Utilizes The Update Framework (TUF) to maintain the security of the software update system, providing protection even against attackers that compromise the repository or signing keys.

Secure Key Storage

- **External Storage:** Secure external application key storage for keys of variable size.
- **Uses PUF:** Utilizes physical unclonable function (PUF) technology for initial key generation.
- **RNG:** Robust key generation using hardware true random number generator (TRNG).
- **NIST Compliant Encryption:** Secure key storage using NIST compliant AES-256 GCM engine to provide authenticated encryption/decryption.
- **Protection:** Prevents unauthorized access of sensitive data.

Secure Internal Communication

- **ARM® TrustZone®:** Trusted Sypher Ultra and third-party/customer security related application software is isolated from untrusted application software.
- **Seamless:** Handles switching from the nonsecure state to the secure state and vice versa.

Target Applications

Sypher Ultra can be used in any application utilizing the ZUS+ family of MPSoCs, such as:

- Industrial systems
- Automotive
- Aerospace and defense
- Healthcare

Package

The Sypher Ultra Secure Execution package includes the following items:

- User guide
- Reference design
- Build environment
- API document
- User template image

For more information about Sypher Ultra, email: secure-products@analog.com

And visit analog.com/cybersecurity

Xilinx Zynq UltraScale+ MPSoC Compatibility/Utilization

Parameter	Constraint/Compatibility
ZUS+ Compatibility	
Device Type	CG, EG, EV
Device Size	ZU2, ZU3, ZU4, ZU5, ZU6, ZU7, ZU9, ZU11, ZU15, ZU17, ZU19
Speed Grade	-2 or better
Resource Utilization	
APU (A53) Subsystem	>5%[1]
RPU (R5) Subsystem	50%[2]
Programmable Logic	
CLB Flip Flops	3888 FF
CLB LUTs	1944 LUT
Block RAM	0
Ultra RAM	0
DSP Slices	0
PL External I/O	0
Global Clock Buffers (BUFG)	0
External Interfaces	
PS DDR[3]	See Xilinx data sheet: DC and AC Switching Characteristics (DS925) for compatible DDR
Boot Flash	See Xilinx answer record 65463 (AR#65463[4]) Validated parts: MT25QU512ABB MT25QU01GBBB

[1] Portion of APU used by Security Driver to communicate with Sypher Ultra application.
[2] One of the two R5 processors: R0 reserved for exclusive Sypher Ultra usage.
[3] Minimum 64 MB used by Sypher Ultra.
[4] xilinx.com/support/answers/65463.html