

Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ iSE > SCZ\_iSE\_XZU+\_BA471

# HARDWARE SECURITY MODULE (HSM)

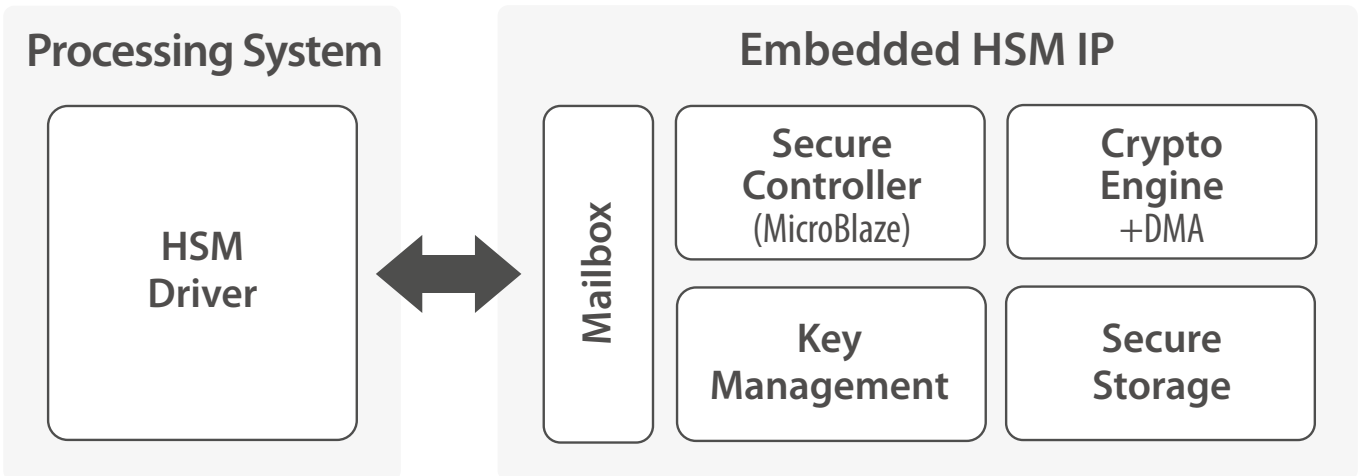
The HSM IP module is a Hardware Security Module for a wide range of applications. It is developed, validated and licensed by Secure-IC (partner of Xilinx) as an FPGA-based IP solution dedicated to the Xilinx Zynq UltraScale+ MPSoC platform.

As the connectivity of industrial systems is growing, so is the need for data integrity and system authentication. A very important aspect of this embedded security is a hardware security module (HSM), a security enclave that provides secure key management and cryptographic processing.

This HSM IP module removes the need for a dedicated HSM device and it incorporates 2 solutions:

- The **HSM hardware IP**, to be implemented in programmable logic and ready to interface with the Zynq UltraScale+ processing system.
- A **software stack** containing the HSM firmware, HSM driver code and an interface layer allowing integration.

## HARDWARE SECURITY MODULE (HSM) For Xilinx Zynq UltraScale+ MPSoC



### Features

- ✓ Secure key provisioning
- ✓ Secure key storage
- ✓ Secure counter
- ✓ Flexible anti-tampering
- ✓ Easy to integrate (AXI interface)
- ✓ Cryptographic operations offload
  - PK engine
  - Symmetric engine
  - Random number generator
- ✓ Flexible and scalable platform



### Applications

- ✓ Automotive
- ✓ Industrial
- ✓ Defence
- ✓ Smart metering
- ✓ IoT
- ✓ eHealth
- ✓ Banking & finance

## Configurable, scalable and flexible solution

The hardware security module can be scaled and configured to match any requirement, even for the most demanding applications. The size and performance of the solution can be adapted for a perfect application fit while leaving room in the FPGA for other critical applications.

## Xilinx Zynq UltraScale+ MPSoC platform

Xilinx's SoC portfolio integrates the software programmability of a processor with the hardware programmability of an FPGA, providing you with unrivaled levels of system performance, flexibility, and scalability. The portfolio gives your designs overall system benefits of power reduction and lower cost with fast time to market. Unlike traditional SoC processing solutions, the flexible programmable logic provides you with optimization and differentiation, allowing you to add the peripherals and accelerators you need to adapt to a broad base of applications.



## Deliverables

- |                                 |                               |                                   |                           |
|---------------------------------|-------------------------------|-----------------------------------|---------------------------|
| ✓ FPGA netlist or encrypted RTL | ✓ HSM firmware                | ✓ HSM driver                      | ✓ Self-checking testbench |
| ✓ Simulation model              | ✓ Reference simulation script | ✓ Reference implementation script | ✓ Documentation           |

V1.2

**SECURE-IC**  
THE SECURITY SCIENCE COMPANY

### HEADQUARTERS

Digital Park B - ZAC Atalante Via Silva  
801 avenue des Champs Blancs  
35510 Cesson-Sévigné - France  
+33 (0)2 99 12 18 72 - [contact@secure-ic.com](mailto:contact@secure-ic.com)

**EMEA**  
[sales-EMEA@secure-ic.com](mailto:sales-EMEA@secure-ic.com)

**AMERICAS**  
[sales-US@secure-ic.com](mailto:sales-US@secure-ic.com)

**APAC**  
[sales-APAC@secure-ic.com](mailto:sales-APAC@secure-ic.com)

**JAPAN**  
[sales-JAPAN@secure-ic.com](mailto:sales-JAPAN@secure-ic.com)

**CHINA**  
[sales-CHINA@secure-ic.com](mailto:sales-CHINA@secure-ic.com)

CONTACT US

[www.secure-ic.com](http://www.secure-ic.com)