SECURE-iC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

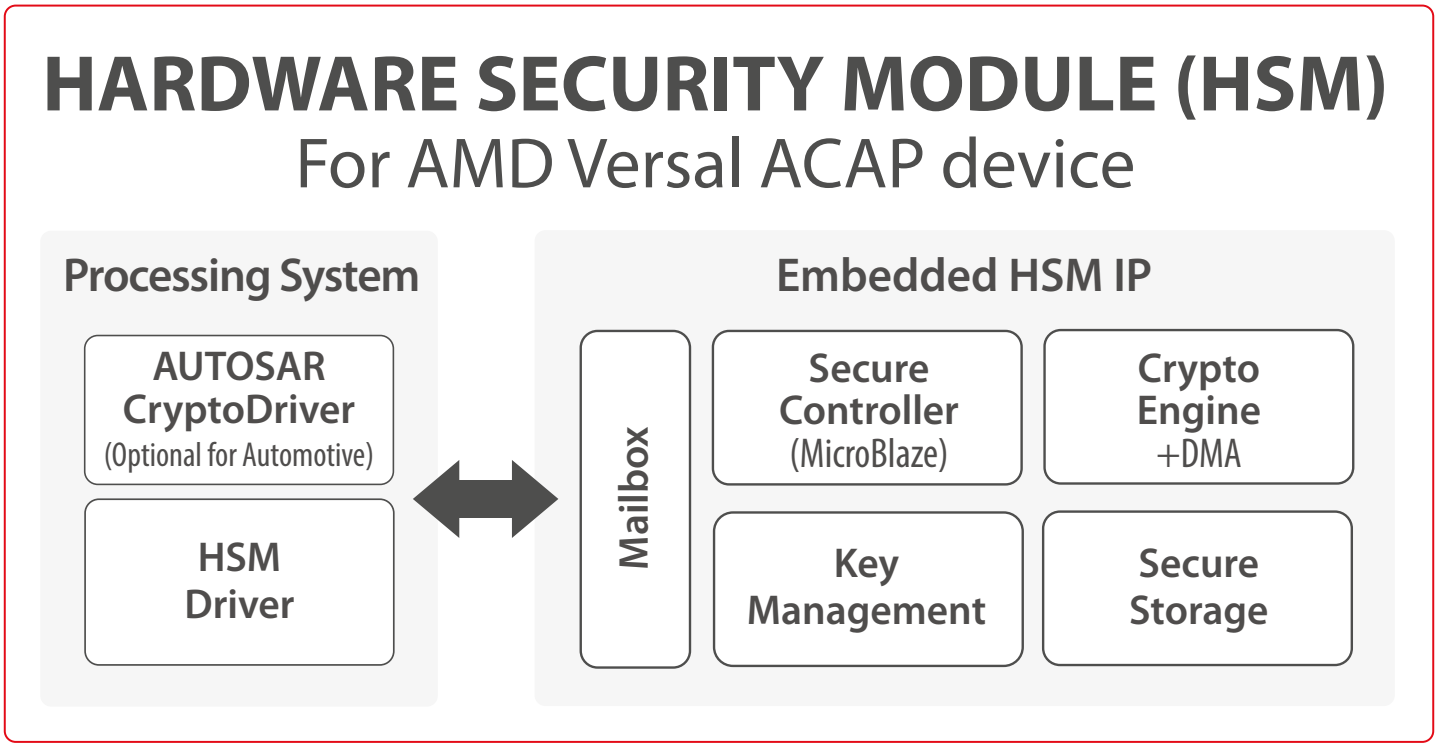
Securyzr™ > Securyzr™ Secure HW Solutions > Securyzr™ iSE > SCZ_iSE_XVS_BA472

HARDWARE SECURITY MODULE (HSM)

The HSM IP module is a Hardware Security Module for a wide range of applications. It is developed according to the guidelines set out by the EVITA project and is meant to be implemented on a AMD Xilinx Versal ACAP device. It supports TrustZone.

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 of the AMD Versal ACAP.
• A **software stack** containing the HSM firmware, HSM driver code and an interface layer allowing integration into the AUTOSAR framework, for automotive applications.



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

ISO 26262 SUPPORTS

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 VERSAL ACAP Platform

Versal® adaptive compute acceleration platforms (ACAPs) combine Scalar Engines, Adaptable Engines, and Intelligent Engines with leading-edge memory and interfacing technologies to deliver powerful heterogeneous acceleration for any application.

Built on the TSMC 7 nm FinFET process technology, the Versal portfolio platform combines software programmability and domain-specific hardware acceleration with the adaptability necessary to meet today's rapid pace of innovation.

Deliverables

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

V1.1

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

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

CONTACT US

www.secure-ic.com