SECURE DEBUG HARDWARE IP

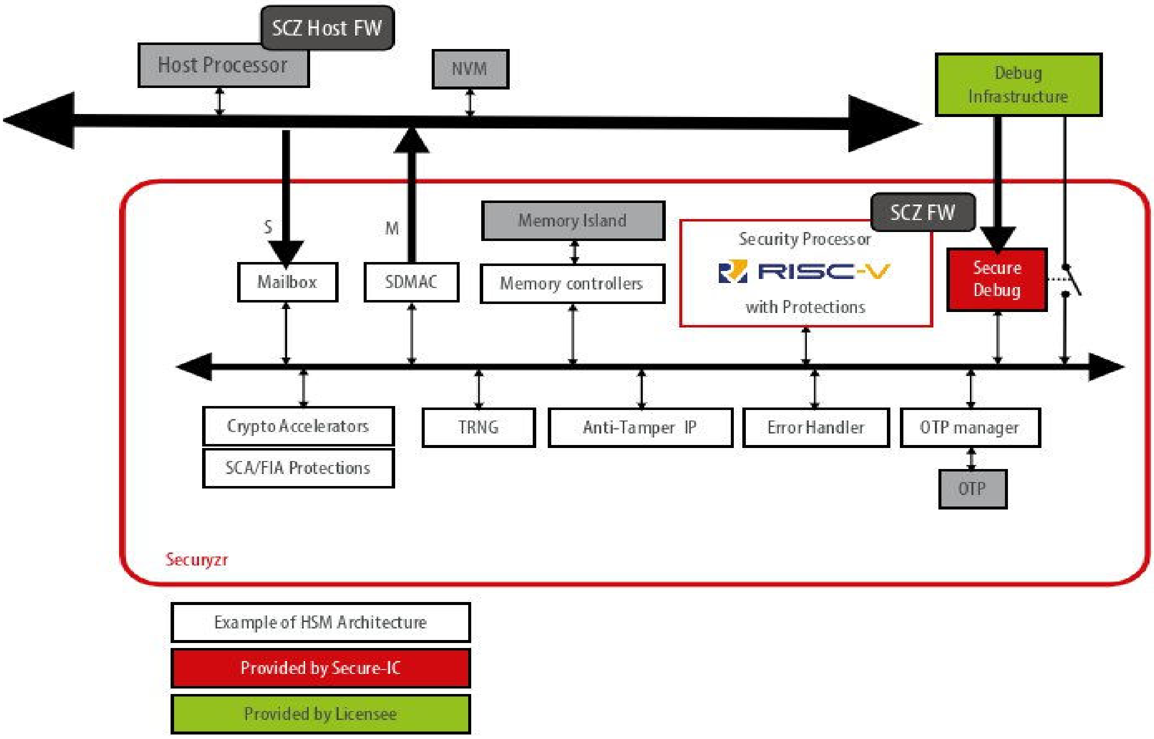
The Secure Debug IP provides isolation between 2 domains. It will ensure isolation between the HOST System on one hand, and the HSM System on another hand. Both (HOST and HSM) can access the IP through an AXI Slave interface.

Secure-IC's Secure Debug IP is a hardware IP that provides:

- Hardware Authentication scheme between the HOST and the HSM.
- Communication interface between the HOST and the HSM, mainly for the purpose of the maintenance of the System-on-Chip.

This IP is controlled by a HOST through an AXI Slave Interface. The purpose of the Secure Debug IP is to provide the following services:

- Get life-cycle information from the HSM.
- Provide a Hardware Authentication scheme.
- Allow only one HOST to be logged in at the same time.
- Allow to open the HSM debug port only if life cycle mode values allow it.
- Receive Maintenance requests (first programming, update, lifecycle ...) from an external user.



Activities

- First Programming
- Debug purpose
- Key injection/generation
- On-site Firmware injection/update
- Get life-cycle information from the HSM
- Provide a Hardware Authentication scheme
- Allow only one Host to be logged at the same time
- Open the HSM debug port only if life cycle mode values allow it
- Receive Maintenance requests (First programming, update, lifecycle…) from an external user

Technology

As a front-end module, Secure Debug can be deployed in any ASIC's techno node which Secure-IC has experience with:

- 130nm /65nm /55nm /40nm /28nm /16nm /12nm /10nm /7nm /5nm /3nm

Markets

AUTOMOTIVE & SMART MOBILITY	CONSUMER ELECTRONICS	DEFENSE & SPACE	SEMI CONDUCTORS	SERVER & CLOUD	INDUSTRY & FACTORY AUTOMATION

Applications

✓ Set-Top Box ✓ SSD	✓ Secure Flash memory ✓ Mobile	✓ IUICC

Deliverables

✓ RTL code	✓ SW Drivers	✓ Scripts for implementation	✓ Self-checking RTL test-bench	✓ Documentation

V4.0

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

TAIWAN
sales-TAIWAN@secure-ic.com

CONTACT US
www.secure-ic.com