Press Release

Eurosmart publishes PP-0117 Secure Sub-System SoC Protection Profile: Tiempo Secure IP products are ready!

The new protection profile PP-0117 brings the security of Secure Elements to Subsystems inside a System-on-Chip; Tiempo Secure CC EAL5+ certified TESIC Secure Element IP already complies with the newly published specification.

Grenoble, France – April 5, 2022 – Eurosmart, the voice of the digital security industry, provides technical contributions to all stakeholders in the market in the form of specifications that guarantee interoperability and security. For years, Common Criteria Protection Profile PP-0084 was the reference for security as it defined the Target of Evaluation for the certification of secure microcontrollers used originally by the smartcard industry. The industry organization Eurosmart just released a new Protection Profile PP-0117, which specifies security rules for hardware secure enclaves as a part of a System on Chip.

The BSI, the German Federal Office for Information Security, has just completed the certification of Eurosmart’s PP-0117 Version 1.5 for Secure Sub-System in System-on-Chip (3S in SoC) for conformance to the Common Criteria (CC). The Target of Evaluation (TOE) is the Secure Sub-System (3S) integrated in a System on Chip (SoC) defined by in PP-0117.

Tiempo Secure participated in the elaboration of the PP-0117 specification from its very inception. As such, the semiconductor security expert company has been able to work with all the prestigious stakeholders in Eurosmart and share its expertise with all developers of the PP-0117 version 1.5 specifications.

Tiempo Secure TESIC Secure Element IP has been developed according to these guidelines and already integrated into a silicon chip that has been certified Common Criteria EAL 5+ by the CEA Leti ITSEF (Information Technology Security Evaluation Facility).

Consequently, Tiempo Secure TESIC is the first Secure Element IP on the market to be compliant with Eurosmart’s PP-0117 Protection Profile for Secure Sub-System in System-on-Chip (3S in SoC) and to have already achieved the Common Criteria EAL 5+ certification.

Serge Maginot, Tiempo Secure CEO, declares: "The new Protection Profile PP-0117 is becoming the reference for up-to-date security architectures, which include a secure element IP inside a System on Chip. We are glad to see that our vision of secure element IP is now recognized by the whole industry."

Tiempo Secure TESIC IP is CC EAL5+ certification-ready. Tiempo Secure offers all services for the writing of CC-compliant documentation, the preparation of customer chip samples and boards for evaluation, the support of ITSEF labs during customer chip evaluation and certification, and the interactions with the national cybersecurity agency to obtain the CC certificate.

For more information on Eurosmart's PP-0117 Protection Profile for Secure Sub-System in System-on-Chip (3S in SoC) : https://www.eurosmart.com/bsi-completes-evaluation-of-eurosmarts-secure-sub-system-in-system-on-chip-protection-profile-pp-0117.

About Tiempo Secure:

Tiempo Secure is an independent SME headquartered near Grenoble, France, founded in 2007, with customers in Europe, North America and Asia. It specializes in the development of intellectual property (IP) in microelectronics and in embedded software for securing connected objects.

The company offers a wide range of Secure Elements (TESIC family) ready to be integrated into "System-on-Chip" (SoC) components, and allowing maximum security (Common Criteria EAL5+ certified) of connected components: authentication on networks with integrated SIM (iSIM/iUICC), payment (EMVCo), government or private identification, web authentication (FIDO 2), smart car access, communication with autonomous vehicles (V2X HSM).

For more information: www.tiempo-secure.com.

Contact:
Tiempo Secure
Email: sales@tiempo-secure.com, Tel: +33 4 76 61 10 00