Press Release

Tiempo Secure announces TESIC RISC-V Secure Element IP and development kit

Building upon its longstanding expertise in semiconductor design, Tiempo Secure is proud to announce its TESIC RISC-V Secure Element IP, which brings an unprecedented level of security to embedded systems, it is certification-ready for Common Criteria EAL 5+ level, and makes SoC development easy thanks to its integration with the complete RISC-V ecosystem. Tiempo Secure also introduces its Development Kit allowing all RISC-V developers to build their own SoC benefitting from the security brought by its technologies.

Grenoble, France – March 8, 2023 – As security is increasingly the central issue of any SoC (System on Chip) development, for example taking into account initiatives like the Cyber Resilience Act, Tiempo Secure has decided to enrich the RISC-V community with security expertise by developing a new version of its TESIC Secure Element IP based on a RISC-V microcontroller. Given the global evolution from software to hardware based security, this new development combines the best of both worlds as it inherits the security features that have made TESIC one of the most recognized Secure Element IP platforms with the advantages of the RISC-V widely developed ecosystem, including an extensive offer in terms of development tools adopted by a large community of developers. It is fully adapted to any design that requires a Secure Enclave, Secure Element or Root of Trust that is highly protected against side channel, perturbation and fault attacks.

Applications include secure and certified GSMA iSIM and iUICC, EMVCo payment, hardware wallets, FIDO2 web authentication, V2X HSM protocols, smart car access, secured boot, secure OTA firmware updates, secure debug and more.

Tiempo Secure TESIC RISC-V Secure Element IP is based on a 32-bit RISC-V processor core implementing the RISC-V instruction set architecture (ISA) specification "RV32IMCB." Tiempo Secure TESIC RISC-V Secure Element IP inherits the security aspects from the whole TESIC family. It specifically includes sophisticated data masking capabilities, which protect data on-the-fly, while they are exchanged between the microcontroller and the rest of the world. This provides protection against side channel attacks such as simple power analysis (SPA) or differential power analysis (DPA). The Tiempo Secure TESIC RISC-V Secure Element IP also includes register protection features including error detection and correction: the microcontroller register file and status registers are protected against perturbation and glitch attacks, amongst others. As it builds upon the existing TESIC range, Tiempo Secure TESIC RISC-V Secure Element IP is certification-ready for Common Criteria CC EAL 5+ level for protection profiles PP 0084 and PP 0117.

In addition, Tiempo Secure introduces the Tiempo Secure TESIC RISC-V Development Kit, that allows developers to explore the product features and develop their firmware, including access to the Secure Element. The Development Kit includes the RISC-V microcontroller and the Secure Element, along with software tools: compiler, linker and debugger based on GNC GCC /GDB, RISC-V toolchain and development environment (IDE) CC EAL5+ and EMVCo certified CryptoLibrary, as well as the CC EAL5+ and EMVCo certified boot loader. It is perfectly integrated with the RISC-V ecosystem, which means developers will instantly be able to use it and to build their own embedded systems.

By choosing Tiempo Secure TESIC RISC-V Secure Element IP, developers of SoCs will benefit from the highest level of security protecting their design, their data and that of their customers, as Tiempo Secure's expertise in security is at the heart of the development of this latest product. In addition, the fact that Tiempo Secure TESIC RISC-V Secure Element IP is built on a standard RISC-V microcontroller, allows developers to benefit from the latest technologies for embedded systems, along with a full development tool ecosystem.

Mikael Dubreucq, Tiempo Secure VP Global Sales and Marketing, states: "By introducing the Tiempo Secure TESIC RISC-V Secure Element IP and its Development Kit, we are bringing the utmost security features to the already rich RISC-V ecosystem. The Development Kit will accelerate integration and development of the Tiempo Secure Element into SoCs."

About Tiempo Secure:

Tiempo Secure is an independent SME headquartered near Grenoble, France, founded in 2007, with customers in Europe, North America and Asia. They specialize 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