Press Release

Tiempo Secure lowers entry barriers to securing the Internet of Things with its CC EAL5+ grade Secure Element IP macro dedicated to secure Systems-on-Chip

Tiempo Secure announces the availability of its CC EAL5+ grade Secure Element IP, allowing plug-and-play integration into Systems-on-Chip, supporting iUICC and other advanced security functions, thus providing the IoT solutions developers with the industry's highest level of security.

Grenoble, France – February 25, 2019 – Tiempo Secure, a semi-conductor specialist focusing on high-end secure products, is now expanding its offer to propose various levels of integration for its Common Criteria EAL5+ grade Secure Element IP for the Internet of Things. Tiempo Secure TESIC Series of Secure Elements is now available in a variety of forms, from classical discrete semiconductor chips to ready-for-integration hardware IP macros.

The Secure Element IP macro is dedicated to System-on-Chip (SoC) designers who are now able to include integrated SIMs (iSIM or iUICC) and other Secure Element functions into their design with a minimal NRE cost. Tiempo Secure Element IP macro includes the same Secure Element features as the company's CC EAL5+/EMVCo certified chips, ensuring the same security level is integrated into the final design regardless of the choice of implementation.

For developers of chips requiring a high level of security, like IoT connection devices, Tiempo Secure Element IP allows an easy plug-and-play integration and, with its dedicated CC EAL5+ certified cryptographic library, includes all authentication, encryption and signature functions along with countermeasures (in software, hardware logic and hardware layout) against state-of-the-art physical side-channel and intrusion attacks. Consequently, Tiempo Secure can commit on the CC EAL5+ (CC EAL4, EMVCo, and/or FIPS140-2) certification of customer chips integrating its Secure Element IP macro.

Security features supported by the Secure Element IP macro with the highest, government-grade, security level possible are the secure iSIM/iUICC functions as well as secure encryption key management, secure Over-The-Air (OTA) firmware update, secure, trusted and measured boot, hardware binding, anti-cloning and sealing/unsealing functions.

"Offering the highest level of security to IoT developers through the integration of a Secure Element IP seems to be the right approach for secure SoC. With our knowledge of Tiempo's know-how in security, we are convinced that Tiempo will provide the right answers for an effective and efficient CC EAL5+ evaluation of these SoC products," says Elisabeth Crochon, Director of CESTI LETI (ITSEF, Information Technology Security Evaluation Facility), a security evaluation lab accredited by the ANSSI (the French National Cybersecurity Agency).

Serge Maginot, CEO, Tiempo Secure, adds: "Our Secure Element IP macro and its associated secure software libraries leverage the security expertize and IP that we developed for our own secure microcontroller chips for the Governmental and Banking markets, chips that have been CC EAL5+ and EMVCo certified since 2016. This allows us to propose to SoC developers the most appropriate solution for an embedded Secure Element that reaches the highest security targets for their IoT chip platform."

The Secure Element IP macro is available from now on from Tiempo under a licensing model. Like all Tiempo Secure products, the Secure Element IP is built upon Tiempo's patented fully asynchronous design technology, which offers highest security and ultra-low power consumption. It incorporates all the needed security functions such as secure secret storage, secure Over The Air (OTA) firmware update, and state-of-the-art cryptography systems.

Tiempo Secure will be present during the Mobile World Congress, in Barcelona, Spain, on February 25-28, 2019, and during Embedded World, in Nuremberg, Germany, on February 26-28, 2019. Feel free to give us a call to set up a meeting.

<u>About Tiempo Secure:</u>
Tiempo Secure is an independent company founded by semiconductor industry experts having unique experience in the development of secure microcontrollers and embedded secure software. The company has already designed Common Criteria EAL5+ and EMVCo certified secure microcontroller chips, available in contact and dual interface mode, for Government ID and High-end Banking applications. Tiempo Secure is expanding its roadmap by offering CC EAL5+ proven/certified Secure Elements for the IoT market, either as companion chips or as hard IP macros that are easy to integrate into application/SoC chips.

The company is headquartered in Montbonnot, near Grenoble, France. More information can be found on www.tiempo-secure.com

<u>Contact:</u>
Serge Maginot, CEO, Tiempo Secure,
Email: sales@tiempo-secure.com, Tel: +33 4 76 61 10 00