Press Release

First SoC ever to pass CC EAL5+ certification thanks to Tiempo Secure TESIC Secure Element IP

Tiempo Secure is the developer of the Secure Element IP TESIC constituting the Target of Evaluation of Sequans' Monarch 2 LTE-M and NB-IoT chip, which has just been certified CC EAL 5+ PP0084 by the ANSSI after a security evaluation completed by the CEA-Leti.

Grenoble, France – December 1st, 2021 – For the first time in the world, a complex System-on-Chip (SoC) such as Sequans 5G-ready LTE-M and NB-IoT Monarch 2 platform for the Internet of Things has just received the Common Criteria (CC) EAL 5+ certification with a Target of Evaluation based on Tiempo Secure TESIC Secure Element IP.

Traditionally, Common Criteria certifications cover standalone secure microcontroller chips for smartcard and ID applications. Only recently they also started to be considered for larger chips but those were always entirely designed by companies having the necessary and rare expertise to secure the design at the highest level required by these certifications. In the present case, Sequans has chosen to integrate CC EAL5+ ready TESIC Secure Element IP in its own Monarch 2 System-on-Chip. The whole SoC was presented for certification with the Secure Element designed by Tiempo Secure being the Target of Evaluation.

This achievement demonstrates not only the security level reached by Tiempo Secure TESIC but also the ability for an SoC developer to integrate Tiempo's IP in its own product and obtain the CC EAL 5+ certification. It is the first time that a SoC reaches the CC EAL5+ level of certification. In addition, this CC certificate also validates a flexible architecture with secure access to an external flash memory.

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.

Serge Maginot, Tiempo Secure CEO, declares: "We are very proud to see that years of team efforts in delivering a full offer of CC EAL5+ ready Secure Element IP to our customers are recognized by an independent and reputable security lab and a government cybersecurity agency delivering official certification. This is the foundation for all our customers to integrate our IP into their designs in order for them to obtain highest level of

chip security and certification, such as Sequans with its world-first CC EAL5+ IoT platform Monarch 2."

Sebastien Falgayrettes, Head of Massive IoT Product Management at Sequans, adds: "We are very happy to see our Monarch 2 LTE-M and NB-IoT platform receive the first CC EAL 5+ certification thanks to Tiempo Secure's TESIC Secure Element IP, allowing powerful support for integrated SIM (iUICC) and for securing application data."

Sequans' Monarch 2 chip, including Tiempo's TESIC Secure Element, has been certified at CC EAL5+ level using the protection profile PP0084 with package loader 2, enriched with security functional requirements coming from the protection profile PP0117 (package for Passive External Memory) by the ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information - National Agency for the Security of Information Systems) on November 11th, 2021 (certificate #ANSSI-CC-2021_53).

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