Press Release

Tiempo Secure and GreenWaves Technologies demonstrate Secure Element role as Master in an embedded system

GreenWaves Technologies and Tiempo Secure have demonstrated the advantages of giving the role of Master to a Secure Element integrated in a System-on-Chip: this architecture significantly enhances the security of the SoC, while making the implementation more efficient.

Grenoble, France – April 12, 2023 – Tiempo Secure and GreenWaves Technologies are proud to have demonstrated how a Secure Element brings additional security in a project supported by the French Government, the community of communes Grésivaudan and the Auvergne Rhone Alpes Region. While in classical architecture, developers of SoCs (System-on-Chips) usually use their CPU as the core application processor and call Secure Element functions when needed, the partnership between Tiempo Secure and GreenWaves Technologies turns the tables and demonstrates a better architecture where the Secure Element is in control of the boot process. The prototype combines a Tiempo Secure Element with a GreenWaves ultra-low power RISC-V based Application Processor targeting IoT and hearables markets.

A Secure Element is a small component, based on a secure architecture already used in billions of SIM cards and banking cards daily. It has limited and controlled I/O, a limited and protected memory and implements physical security features; as such it constitutes a secure environment, which can be certified to the highest levels of Common Criteria.

As the Master of the SoC the Secure Element is the first to boot when the device is started thus guaranteeing that only valid software is used to start the SoC and making it substantially more resistant to hacking attempts. The fact that the boot of the whole device is controlled by the Secure Element makes it resistant to side channel attacks and fault injection attacks. The TESIC IP Secure Element boot is based on AES-256, which means that it is future proof to quantum computers attacks. Access to mass memory, generally Flash, is controlled by the Secure Element, thus preventing any unauthorized access to data. For instance, the coefficients of a neural network for noise reduction stored in the external Flash memory of a GreenWaves processor would be protected by the secret keys securely stored in the Secure Element.

In addition, this architecture allows to store the boot code in a rewritable memory, not in a ROM, allowing to update it in a secure manner during the lifecycle of the object. More generally, data needed by the SoC are stored in a non-volatile memory shared between the Secure Element and the Application Processor, bringing more flexibility to memory allocation and reducing area and therefore cost.

The project (SECURE-RISC-V) has been conducted with the support of the French government-sponsored *Programme d'Investissements d'Avenir* – "Investments for the Future Program" – *Action Renforcement des Pôles de Compétitivité* – "Reinforcement of business clusters" –, co-sponsored by the community of communes Grésivaudan, and the *Appel à projets PSPC-Régions n°1* – "Call for projects PSPC-Regions #1" – from the Auvergne Rhone Alpes Region.

Sebastien Riou, Applications Manager for Tiempo Secure, declares: "This collaboration with GreenWaves has been extremely profitable for both parties: it has allowed us to iron out all potential issues in giving the role of Master to the Secure Element, and to demonstrate the benefits of this architecture in a very concrete case."

Eric Flamand, Co-founder and CTO of GreenWaves Technologies, adds: "Tiempo Secure integrated secure element to boot a SoC allows to simplify drastically security architecture, replacing many critical parts such as ROM code, PUF and TRNG with a single IP."

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

About GreenWaves Technologies:

GreenWaves is a fabless semiconductor company founded in 2014 and based in Grenoble, France. We design and market ultra low power processors for energy constrained products such as hearables, wearables, IoT & medical monitoring products.
GreenWaves' system-on-chips enable companies to develop and bring to market products with new to world features enabled by state of the art machine learning and digital signal processing techniques. Our leading edge development tools enable audio and machine learning developers to productively harness the power of GAP processors.
GreenWaves GAP9 processor powers features such as neural network based noise removal and adaptive noise cancellation, multi-channel spatial sound and listening enhancement technologies in next generation earbuds and headphones with market leading energy efficiency.
For more information, visit www.greenwaves-technologies.com

Contact:
GreenWaves Technologies, Email: sales@greenwaves-technologies.com