Andes Technology and Tiempo Secure Announce Strategic Partnership to Enhance RISC-V Platform Security up to CC EAL5+ Certification

Andes Technology Corporation, a leading supplier of outstanding efficiency, low-power, high performance 32/64-bit embedded CPU cores, including a broad family of RISC-V cores, has entered into a strategic partnership with Tiempo Secure, a unique supplier of ISO/IEC 15408 standard CC (Common Criteria) EAL5+ (Evaluation Assurance Level) grade secure element IP, to bring the RISC-V based security solution up to CC EAL5+ certification.

HSINCHU (Taiwan) and GRENOBLE (France) – October 2, 2019 - The rise of IoT is driving serious concern about security, including at the edge device level. According to recent Ericsson research, by 2024, there will be more than 22 billion connected IoT devices. While security based on logical separation mechanism is commonly deployed, it is admitted that there is some limitation in term of security certification. Furthermore, security integration into the IoT ecosystem could become complex.

The alternative is to enable security from a tamper resistant and certified hardware as a security enclave (Secure Element IP) into the MCU or SoC design.

Tiempo Secure has developed a Secure Element IP (TESIC) as a hard macro integrating CC EAL5+ grade state-of-the-art security countermeasures and security sensors against side channel and intrusion attacks. The integration of this Secure Element IP into a RISC-V SoC will bring the security of this SoC up to CC EAL5+ security, without compromising on power consumption.

"Andes Technology offers RISC-V based ultra-compact processor with the outstanding performance and low power consumption available on the market," said Dr. Charlie Su, CTO and Executive VP of Andes Technology. "Integrating Tiempo Secure's CC EAL5+ security enclave into AndesCore N22 solution will now allow our customers to address the most security critical applications on the IoT market."

"By working with Andes Technology we're able to dramatically enhance the security that developers need to protect their IoT ecosystems based on RISC-V," said Serge Maginot, CEO of Tiempo Secure. "The plug-and-play integration of TESIC, our CC EAL5+ grade Secure Element IP, into the RISC-V cores of Andes Technology will enable RISC-V developers to easily integrate certified security features, such as secure boot, secure firmware update or iUICC stack, into their system."

Once the Secure Element IP from Tiempo Secure is embedded into the RISC-V based AndesCore N22 designed by Andes Technology, the whole system can pass the highest level of security certification, including CC EAL4+/EAL5+ PP0084 and FIPS 140-2. It also solves the problem of security integration into the IoT ecosystem.

About Andes Technology

Andes Technology Corporation is a world class creator of innovative high-performance/low-power 32/64-bit processor cores and associated development environment to serve the rapidly growing global embedded system applications. The company delivers superior low power CPU cores, including the comprehensive RISC-V V5 family of processor cores, with integrated development environment and associated software/hardware solutions for efficient SoC design. Up to the end of 2018, the cumulative volume of Andes-Embedded™ SoCs has reached 3.5 billion with 2018 alone contributing over 1 billion. Andes Technology's comprehensive CPU line includes entry-level, mid-range, high-end, extensible and security families. For more information, please visit www.andestech.com

About Tiempo Secure

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 and certified Common Criteria EAL5+ and EMVCo secure microcontroller chips, available in contact and dual interface mode, for Government ID and High-end Banking applications. Tiempo Secure is now offering CC EAL5+ proven/certification-ready Secure Elements for the IoT market, either as companion chips or as hard IP macros that are easy to integrate into application/SoC chips, allowing the customer chips to pass CC EAL5+ and other security standard certification.

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