Press release
Communiqué de presse
Comunicato stampa
新闻稿 / 新聞稿
プレスリリース
보도자료

P4533S

Secure Manager from STMicroelectronics combines HW and SW to simplify development of secure embedded applications

- *Delivers market's first out-of-the-box, certified MCU protection for customer embedded developments*
- *Leverages Arm® TrustZone® and a range of ST and partner-developed technology to comply with PSA Certified Level 3 & Global Platform SESIP3 security specs*

Geneva, Switzerland, March 7, 2023 – STMicroelectronics (NYSE: STM), a global semiconductor leader serving customers across the spectrum of electronics applications, has announced its STM32Trust TEE Secure Manager. It is the first microcontroller system-on-chip security solution that simplifies embedded application development to assure out-of-the-box protection. First used in the new STM32H5, the STM32TrusTEE Secure Manager saves developers writing and validating their own code while providing security services developed according to best practices.

"*The growing emphasis on application security and customers' need to deliver certified secure, high-performance applications quickly, encouraged us to work closely with ST Authorized Partner ProvenRun to build the STM32Trust TEE Secure Manager,"* said Ricardo De Sa Earp, Executive Vice President General-Purpose Microcontroller Sub-Group, Microcontrollers and Digital ICs Group. *"The Secure Manager keeps users, assets, and data secure by enhancing and simplifying the addition of valuable security services to customer developments while easing their certifications."*

As a lead development partner with Arm, ST supported the development of the Cortex®-M33 core to comply with the PSA Level 3 security specifications. In addition, ST has collaborated with Microsoft Azure on middleware with strong security and worked with ProvenRun in the development of the STM32Trust TEE Secure Manager, powered by the company's ProvenCore-M secure Trusted Execution Environment Operating System.

"We have enthusiastically co-developed the Secure Manager with ST to bring it into a mass-market, easy-to-use security solution within the STM32Cube ecosystem," said Dominique Bolignano, President & Founder of ProvenRun. *"We trust that the integration of our ProvenCore-M technology will support customers' efforts to dramatically increase the security robustness of their applications over time."*

Further, ST has pre-qualified the Kudelski IoT keySTREAM™ root of trust, from ST Authorized Partner Kudelski IoT, on the Secure Manager to allow remote credential lifecycle management services. The result is a plug-in security solution providing security services that include isolation, cryptography, key storage, and initial attestation.

"Digital identities, provisioning and credentials management are at the heart of security for IoT devices. The pre-integration and validation of our IoT keySTREAM within ST's Secure Manager increases device security while relieving the manufacturer's pain of managing credentials in complex and insecure production environments by enabling in-field, zero-touch provisioning," said Hardy Schmidbauer, SVP of Kudelski IoT.

Following its inclusion in the STM32H5, ST plans to make the STM32Trust TEE Secure Manager available on a broad range of STM32 MCU series.

For further information please go to https://www.st.com/stm32trustee-sm

About STMicroelectronics

At ST, we are more than 50,000 creators and makers of semiconductor technologies mastering the semiconductor supply chain with state-of-the-art manufacturing facilities. An integrated device manufacturer, we work with more than 200,000 customers and thousands of partners to design and build products, solutions, and ecosystems that address their challenges and opportunities, and the need to support a more sustainable world. Our technologies enable smarter mobility, more efficient power and energy management, and the wide-scale deployment of the Internet of Things and connectivity. ST is committed to becoming carbon neutral by 2027. Further information can be found at www.st.com.

For Press Information Contact:

Michael Markowitz
STMicroelectronics
Tel: +1 781 591 0354
Email: michael.markowitz@st.com