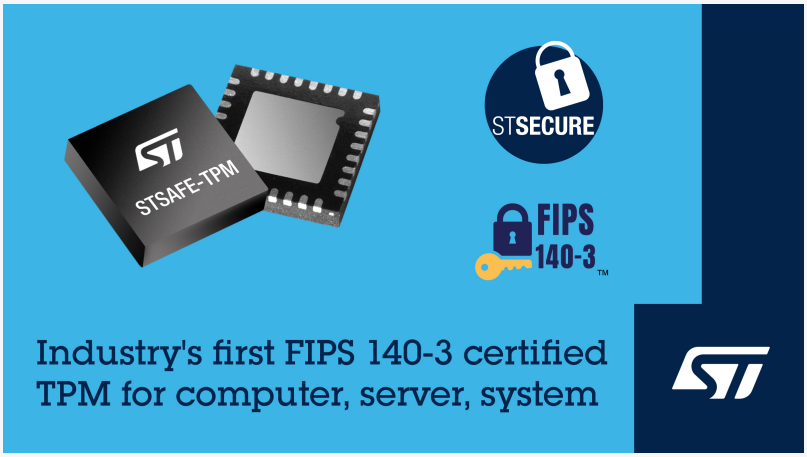
STMicroelectronics delivers industry’s first FIPS 140-3 certified TPMs for computer, server, and embedded systems

State-of-the-art protection certified to latest standard for information security certification, globally recognized and mandatory for US federal procurement



Industry’s first FIPS 140-3 certified TPMs from ST

GENEVA, SWITZERLAND, September 17, 2024 /EINPresswire.com/ -- STMicroelectronics today announced the FIPS 140-3 certification of STSAFE-TPM trusted platform modules (TPMs), the first standardized cryptographic modules on the market to receive this certificate.

The newly certified TPMs, the ST33KTPM2X, ST33KTPM2XSPI, ST33KTPM2XI2C, ST33KTPM2I and ST33KTPM2A provide cryptographic asset protection to meet security and regulatory requirements for critical information systems. They are used in PCs, servers and network-connected IoT devices, as well as medical and infrastructure high-assurance equipment. The ST33KTPM2I is qualified for long lifetime industrial systems. ST33KTPM2A commercialized under the name STSAFE-V100-TPM leverages an AEC-Q100 qualified hardware platform required for automotive integration.

FIPS 140-3 is the latest version of the federal information processing standards (FIPS) specifications for cryptographic modules, superseding FIPS 140-2. “All FIPS 140-2 certificates are scheduled to expire in September 2026,” commented Laurent Degauque, Marketing Director, Connected Security, STMicroelectronics. “By achieving FIPS 140-3, our TPMs are uniquely ready for new designs and let customers create secure, interoperable equipment with extended product and certification lifetimes.”

The products support use cases like secure boot, remote/anonymous attestation, and secure storage with an extended user memory of 200kBytes. In addition, each product supports secure firmware update to add new cryptographic algorithms like PQC and maintain state-of-the-art cryptographic asset protection.

The STSAFE-TPM devices are compliant with multiple industry security standards. These include Trusted Computing Group TPM 2.0 applicable to trusted platform modules, Common Criteria EAL4+, passing the CC framework's most stringent vulnerability analysis (AVA_VAN.5), and now FIPS 140-3 level 1 with physical security level 3. They offer cryptographic services (ECDSA & ECDH up to 384 bits, RSA up to 4096 including key generation, AES up to 256 bits, SHA1, SHA2 and SHA3), standardized by TCG and compatible with software stacks under FIPS 140-3 certification.

ST also offers provisioning services to load device keys and certificates to reduce the total solution cost and time to market and to guarantee the security of the supply chain.

For more information, visit www.st.com/st33ktpm

Alexander Jurman
STMicroelectronics International NV
Alexander.Jurman@st.com
