SecEdge Unveils Embedded TPM for STM32 Microprocessors

SEC-TPM™ Accelerates CRA Compliance with Embedded TPM for STM32 MPUs without Hardware Redesign

SEATTLE, WA, UNITED STATES, January 13, 2026 /EINPresswire.com/ -- SecEdge, a leader in digital security for edge devices, today announced the availability of its SEC-TPM™ foundational device security solution for STMicroelectronics' STM32 microprocessors (MPUs). SEC-TPM™ enables a TPM 2.0-compliant Firmware Trusted Platform Module (fTPM), seamlessly integrated into the STM32 Board Support Package (BSP), operating within a secure execution environment.

SecEdge and STMicroelectronics announced the availability of SEC-TPM foundational device security solution for STMicroelectronics' STM32 microprocessors.

SEC-TPM is a Trusted Computing Group (TCG) TPM 2.0 Compliant Firmware Trust Platform Module (TPM), TCG Vendor ID: 0x5ECE, enclosed in the STM32 MPU hardware secure execution environment using Arm® TrustZone™.

> " SecEdge Inc. knowledge of the ST portfolio and key expertise can help customers meet design challenges and shorten development time."
>
> *Alessandro Maloberti, Partner Ecosystem Director, STMicroelectronics*

SEC-TPM includes an extensive suite of additional device security features:
• Device security for new and existing deployments
• AI model protection at rest
• Secure key storage
• Secure cloud integration
• 2 factor authentication for secure connectivity (SEC-VPN™) partner contribution

"We are pleased to extend SEC-TPM solution coverage to the STM32 platform, forging a secure foundation for Edge AI," said Sami Nassar, CEO of SecEdge. "Our fully integrated, software-defined TPM 2.0 solution for STM32 MPUs enables trusted,

scalable deployment of intelligent systems worldwide easing the path to CRA compliance and advanced AI model lifecycle management and security."

"SecEdge Inc. knowledge of the ST portfolio and key expertise can help customers meet design challenges and shorten development time," said Alessandro Maloberti, Partner Ecosystem Director, STMicroelectronics. "ST's review and vetting of ST Authorized Partners has enabled us to build a strong ecosystem of qualified and skilled partners who can enhance customers' developments with advanced technologies and multiple services to accelerate the design of their projects and solutions."

AVAILABILITY
The SEC-TPM development kit is now available for immediate download at www.secedge.com/sec-tpm-kits, enabling developers to download, run, test and evaluate SEC-TPM.

The SEC-TPM software-defined upgrade for STM32 microprocessors is offered under a per-chip licensing model and can be sourced through a broad network of authorized ST distributors and system-on-module (SOM) vendors.

SecEdge's leading partners include Arrow Electronics, Ubiquitous AI, and EDOM.

"We are delighted to partner with SecEdge to distribute SEC-TPM solutions for STM32 MPU platforms worldwide," said Mark Tzeng, Vice President of EDOM Technology. "With our technical expertise and ecosystem resources, EDOM will help customers adopt a seamless security solution that comply with global cybersecurity standards."

ADDRESSING KEY INDUSTRY CHALLENGES
SEC-TPM tackles critical security and operational challenges while delivering significant advantages:
• Supports both greenfield and brownfield deployments, ensuring seamless integration across new and existing systems without board redesign or additional hardware.
• Ensures quantum resistance (PQC), for future-proof security implementations.
• Enables compliance with key industry standards, including EU CRA, IEC 62443-4-2, NIST 800-183/193, and NISTR8259.
• Enables new capabilities in alignment with critical requirements in today's edge deployments, including AI model protection and secure IPSec VPN connectivity.

ABOUT SecEdge
SecEdge™ is a digital security leader for edge devices, providing advanced security software solutions for edge AI, compute, and control applications. Renowned for its award-winning AI model protection, the SecEdge platform delivers a complete chip-to-cloud security solution, including device-level security, zero-trust networking, and secure data control and management

For more information, visit www.secedge.com.

ABOUT STMICROELECTRONICS
STMicroelectronics, a global semiconductor leader serving customers across the spectrum of electronics applications created the ST Partner Program to speed customer development efforts by identifying and highlighting to them companies with complementary products and services. Moreover, the program's certification process assures that all partners are periodically vetted for quality and competence. For more information, please visit www.st.com/partners

Jennifer Walken
SecEdge, Inc.
+1 408-462-1376
jennifer.walken@secedge.com
Visit us on social media:
LinkedIn
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/880669983