EINPRESSWIRE

SecEdge Joins TCG-Approved Vendors with SEC-TPM™, a Groundbreaking TPM 2.0 Solution for Arm® TrustZone™-Enabled Silicon

SEC-TPM™ stands as an industry first, pioneering security in Edge AI and enhancing application data privacy for confidential computing

TRUSTED® COMPUTING GROUP
Industry First for Edge AI Security.
SEC eDGE
Digital Security to the Edge
SEC-TPM™

SEATTLE, WA, UNITED STATES, November 19, 2024 / EINPresswire.com/ -- AI security and data privacy have received a major boost today as SecEdge joined the Trusted Computing Group (TCG) approved vendor community in support of SEC-TPM™. SEC-TPM is a TPM 2.0 firmware TPM solution, as specified by the TCG, who created the original TPM 25 years ago.

This Trusted Platform Module (fTPM) solution sets a new standard for device security by supporting a wide range of silicon compatible with Arm® TrustZone™ architectures and delivering end-to-end software management.

> “
> SecEdge’s SEC-TPM uses the utility of TPMs in key focal areas, including AI security and application data privacy, which are critical for the future of confidential computing.”
>
> *Joe Pennisi, President & Chairman of Trusted Computing Group (TCG)*

"SecEdge’s SEC-TPM uses the utility of TPMs in key focal areas, including AI security and application data privacy, which are critical for the future of confidential computing," said Joe Pennisi, President and Chairman of Trusted Computing Group (TCG).

SEC-TPM is a turnkey firmware TPM solution that integrates seamlessly into existing hardware environments, providing robust security features for edge devices. SEC-TPM enables enhanced security for AI models, extending the use of TPMs into Edge AI to protect applications, and ensuring data integrity with the next level of confidential computing in data privacy.

The SEC-TPM solution uses hardware security and software provisioning services to facilitate secure deployments for ARM TrustZone-enabled devices. Through a hardware root-of-trust (RoT), the solution also provides second-factor authentication for Virtual Private Network (VPN) tunnel solutions, including SecEdge's SEC-VPN™.

"We took a mature standard, TPM 2.0, and made it the de facto security solution for a wide range of silicon and devices," said Sami Nassar, President and Co-CEO at SecEdge. "The SEC-TPM solution provides crypto-agility, reduces cost, and improves performance of traditional solutions, as well as enabling critical security capabilities in AI model protection and secure data connectivity."

SEC-TPM is available now. More information is available at www.secedge.com/sec-tpm.

ABOUT SECeDGE

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

To learn more about SecEdge security solutions, visit www.secedge.com or email us at info@secedge.com.

ABOUT TRUSTED COMPUTING GROUP

TCG is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry specifications and standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. More information is available at the TCG website, www.trustedcomputinggroup.org. The organization offers a number of resources for developers and designers at https://develop.trustedcomputinggroup.org/.

Follow TCG on Twitter (https://x.com/TrustedComputin) and LinkedIn (https://www.linkedin.com/company/trusted-computing-group).

Jennifer Walken
SecEdge, Inc.
jennifer.walken@secedge.com
Visit us on social media:
Facebook
X

LinkedIn