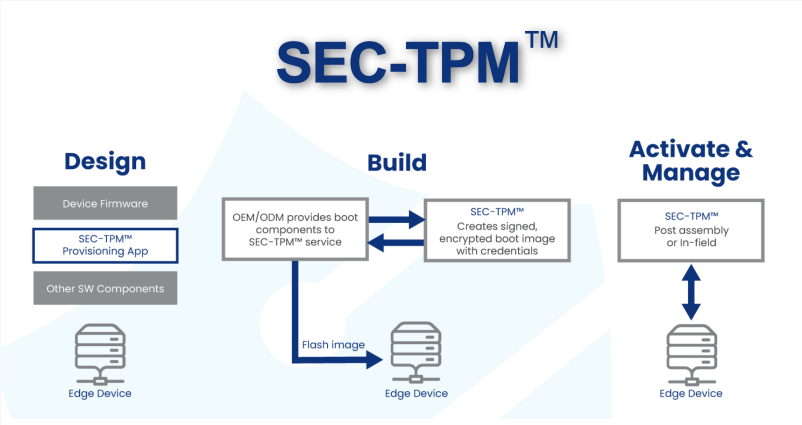
Sec Edge Introduces Industry's First fTPM Security Solution for NVIDIA Jetson Edge AI and Robotics Platform

Sec Edge announces SEC-TPM, a transformative turnkey solution with in-field trust provisioning and management for the NVIDIA JetPack SDK



Sec Edge SEC-TPM™ is a software-as-a-service solution that provides a Trusted Computing Group (TCG) 2.0 Compliant firmware TPM (fTPM), enclosed in a hardware secure execution environment, with a post-assembly trust provisioning service.

SEATTLE, WA, USA, November 28, 2023 /EINPresswire.com/ -- Digital security leader Sec Edge announced today that it has collaborated with NVIDIA in the development of firmware Trusted Platform Module (fTPM) solutions for implementation in the NVIDIA JetPack SDK 6.0 release for the NVIDIA Jetson platform, among other products and solutions for both companies. Sec Edge also announced the SEC-TPM™ turnkey software-as-a-service solution, which provides a TCG 2.0-compliant fTPM in a hardware-secure execution enclosure with a post-assembly Trust Provisioning service.

> We are excited to provide the industry's first quantum-resistant embedded TPM solution...available supporting the latest NVIDIA JetPack SDKs."
>
> *Sami Nassar, Sec Edge President & co-CEO*

A Disruptive Solution to the Traditional Discrete TPM Chip

SEC-TPM provides a hardware root-of-trust in an NVIDIA System-on-Chip hardware-secure execution enclosure. The solution is future-proof through crypto-agility, enabling quantum-resistant algorithms. SEC-TPM runs on the Jetson Orin's powerful applications processor, providing higher performance and easier implementation.

Turnkey In-field Provisioning and Management

Device makers can easily deploy and manage the solution using the SEC-TPM turnkey

implementation and management service. The service provides in-field trust provisioning, ensuring a secure supply chain, a zero-trust chip-to-cloud connection, and a secure remote management system.

Industry and Regulation Compliance

The solution allows device makers to meet industry compliance specifications, supporting TCG, NIST, CRA for the IoT, and the Azure Edge Secured Core Certification, among others.

Value-Added Applications

SEC-TPM is based on the technology foundation powering Sec Edge products, including the award-winning EmSPARK™ Security Suite, which provides device security, AI model protection, and chip-to-cloud data security for platforms like NVIDIA Jetson for edge AI and robotics. By enabling the transition to firmware, the solution delivers a crypto-agile, managed solution that is higher-performing than a traditional hardware TPM for cybersecurity applications like edge AI, IoT, and secure OpenBMC.

SEC eDGE™
Digital Security to the Edge

Sec Edge announces SEC-TPM™, a turnkey software-as-a-service solution.

NVIDIA®

Sec Edge has collaborated with NVIDIA in the development of firmware Trusted Platform Module (fTPM) solutions for implementation in the NVIDIA JetPack SDK 6.0 release for the NVIDIA Jetson platform.

“We are excited to provide the industry’s first quantum-resistant embedded TPM solution that doesn’t require a secure manufacturing environment,” said Sami Nassar, CEO at Sec Edge. “The solution is available today supporting both NVIDIA JetPack 5.0 and JetPack 6.0 releases.”

More information on the SEC-TPM solution is available on the Sec Edge website. Sec Edge is a member of the NVIDIA Partner Network. SEC-TPM is available for all NVIDIA Jetson hardware partners and customers.

About SEC eDGE

Sec Edge is a digital security SaaS Platform leader for IoT and Edge devices, providing advanced security solutions for Edge AI, Compute, Control and on-demand cellular IoT data connectivity. The Sec Edge software-as-a-service platform provides a complete solution including device-level security, zero-trust networking, and secure data control and management, with connectivity via broadband internet or on-demand cellular data available anywhere.

To learn more about Sec Edge security solutions, visit www.secedge.com or email info@secedge.com.

###

Jennifer Walken
Sec Edge, Inc.
email us here
Visit us on social media:
Twitter
LinkedIn
