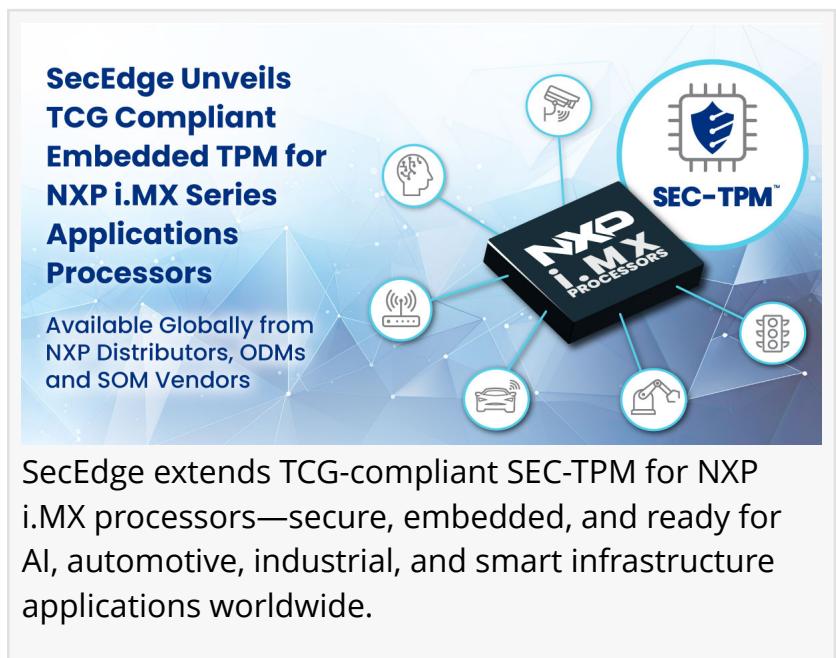


SecEdge Unveils Embedded TPM for NXP i.MX 6, 7, 8 and 9 Series Applications Processors

SEC-TPM™ delivers embedded TCG TPM 2.0+ functionality without the need for an external IC

SEATTLE, WA, UNITED STATES,
November 19, 2025 /

EINPresswire.com/ -- SecEdge, a leader in digital security for edge devices, today announced the availability of its [SEC-TPM™](#) foundational device security solution for [NXP® Semiconductors i.MX 6, 7, 8 and 9 series of applications processors](#). SEC-TPM™ enables a TPM 2.0-compliant Firmware Trusted Platform Module (fTPM), seamlessly integrated into the NXP i.MX Board Support Package (BSP), operating within a secure execution environment.



SecEdge Unveils TCG Compliant Embedded TPM for NXP i.MX Series Applications Processors

Available Globally from NXP Distributors, ODMs and SOM Vendors

SecEdge extends TCG-compliant SEC-TPM for NXP i.MX processors—secure, embedded, and ready for AI, automotive, industrial, and smart infrastructure applications worldwide.

“We are pleased to extend SEC-TPM solution coverage to the NXP Semiconductors i.MX 6, 7, 8 and 9 families,” said Sami Nassar, CEO of SecEdge. “Our fully integrated, software-defined TPM 2.0 solution leveraging NXP’s advanced hardware security brings robust device security capabilities to edge devices that face tight space, performance and cost constraints, while also enabling advanced AI model lifecycle management and security.”

“

SecEdge’s SEC-TPM is extending the adoption of the TPM 2.0 standard into platforms like NXP i.MX, enabling features such as AI model protection, as well as preparing for TPM post-quantum cryptography.”

Joe Pennisi, President and Chairman, Trusted Computing Group

“SecEdge has been a trusted [part of NXP’s Partner Program](#) since 2020, collaborating with us to advance embedded security and offer our customers managed solutions accelerating the deployment of security in the field,” said Denis Noël, Senior Director, Strategy and Marketing, Secure Connected Edge, at NXP Semiconductors. “The introduction of SEC-TPM may remove the need for a separate hardware TPM, providing a standards-compliant,

software-defined option for device protection that simplifies design and reduces cost. Built on NXP's advanced security architecture, it utilizes the EdgeLock® Secure Enclave in select i.MX applications processors—a dedicated security unit physically isolated from the rest of the System-on-Chip and protecting sensitive security operations, including secure device boot, secure device updates, upgrades of feature such as SEC-TPM install, as well as key management, device attestation and other cryptographic functions.”

“SecEdge’s SEC-TPM is extending the adoption of the TPM 2.0 standard into platforms like NXP i.MX, enabling features such as AI model protection, as well as preparing for TPM post-quantum cryptography,” said Joe Pennisi, president and chairman of the Trusted Computing Group (TCG).□

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 NXP i.MX 8 and 9 series of applications processors is offered under a per-chip licensing model and can be sourced through a broad network of authorized NXP i.MX distributors and system-on-module (SOM) vendors.

SecEdge’s leading partners include Arrow Electronics, Ubiquitous, and Variscite.

“By delivering standard TPM 2.0 functionality, this solution enables our customers to meet critical industry specifications, including the upcoming Cyber Resilience Act,” said Ofer Austerlitz, VP of Business Development and Sales at Variscite. “It provides a seamless path to best-in-class security and compliance — whether for new designs or existing deployments — all through a simple software upgrade.”

ADDRESSING KEY INDUSTRY CHALLENGES

SEC-TPM™ tackles critical security and operational challenges while delivering significant advantages:

- Offers an alternative to discrete TPM hardware, potentially reducing costs, saving board space, and simplifying inventory—without compromising security.
- Enhances system performance by leveraging the powerful NXP i.MX 6, 7, 8 and 9 series of applications processors, surpassing traditional discrete TPMs.
- Enables new capabilities in alignment with critical requirements in today’s edge deployments, including AI Model protection and secure IPsec VPN connectivity.
- Supports both greenfield and brownfield deployments, ensuring seamless integration across new and existing systems.

- 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.

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 SecEdge □ <https://www.secedge.com/>.

Jennifer Walken

SecEdge, Inc.

jennifer.walken@secedge.com

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/866141234>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2025 Newsmatics Inc. All Right Reserved.