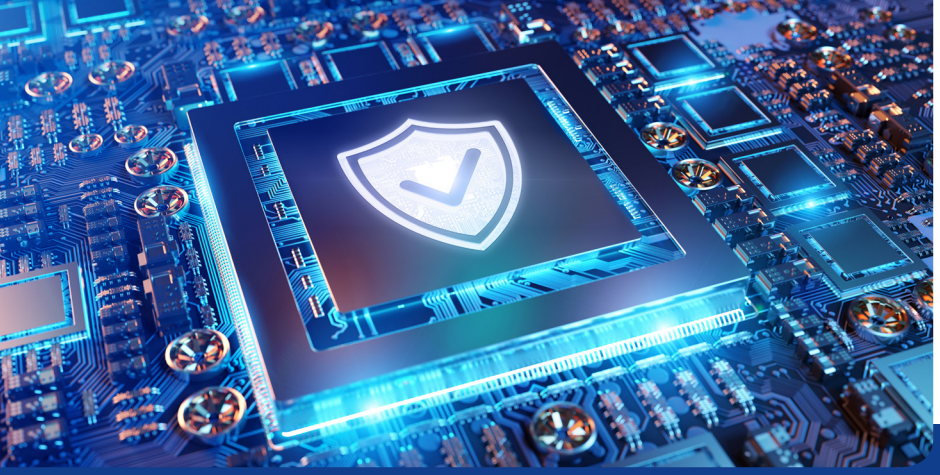
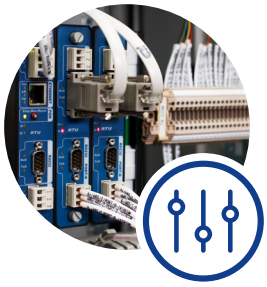


NXP EdgeLock™
SE050

Use Case:
Beyond Trusted Platform Module (TPM)

In the IoT, where resource-constrained edge devices require flexible crypto functionality in lightweight implementations, a traditional TPM, designed for the architectures and lifecycles of powerful PC and tablet devices, may not be the best choice. A secure element, equipped with TPM functionalities, can add high-level protection in a format better suited for IoT operation.

APPLICATIONS



Industrial PLCs

Robots

Sensors/Actuators

CHALLENGE

For more than a decade, the computing industry has relied on a special type of secure crypto-processor, called a Trust Platform Module (TPM), to provide hardware-based protection of PCs, laptops, networking equipment, and other computing devices.

In computing, the TPM is mainly used to securely store the credentials required for user password protection, disk encryption and trusted execution. TPM chips include indeed Product Configuration Registers (PCRs), which allow tracking the installed SW and system configuration and help ensure the computing platform's trustworthiness over time. TPM functionality is specified as ISO/IEC 118889, and TPM operation is certified by the Trusted Computing Group (TCG), an industry organization formed by leading computer-platform companies.

PLUG&TRUST

NXP

Securing tomorrow's IoT. *Today.*

Devices operating in the Internet of Things (IoT) face some of the same risks as network-connected computers. Nevertheless, from the IoT perspective, adding even a compact TPM to the design can create excess overhead in terms of size of the SW stack and platform resources required to drive the TPM while still not providing the flexibility and crypto functionality required to support IoT-specific tasks, such as creating a secure network connection, onboarding on multiple cloud, storing multiple keys to authenticate data or securely connect to multiple other devices, and so on. These were not use cases foreseen for traditional computing TPMs. What's more, because of the different threat model and form factor associated with IoT devices, an IoT device requires features that aren't typically provided by a traditional TPM, such as secure binding to the host controller (leveraging, for example, Secure Channel Protocol 03 or SCP03 standardized by Global Platform), a small footprint to fit in compact devices or programmability to adapt the security logic to the type of IoT device.

To address the specific needs of the IoT, developers can provide TPM functionality with a secure element that's purpose-built for IoT operation.

SOLUTION

The EdgeLock SE050 is a tamper-resistant secure element, with a pre-installed applet optimized for IoT use cases, that brings TPM functionality to IoT applications. The entire EdgeLock SE050 secure element family, from entry level to high end, provides TPM-like functions, such as secure cryptographic processing, and secure key storage, as well as unique ID generation and storage. It also includes attestation capabilities and PCRs to remotely verify device health and ensure trust. The big advantage that the EdgeLock SE050 has over traditional TPMs is that it supports more IoT-relevant features, a wider variety of development and usage models, and can be used in tiny sensors as well as powerful IoT equipment such as edge computing platforms.

The EdgeLock SE050 goes beyond baseline TPM operation to provide special support for IoT operation, including a more flexible approach to managing credentials and user policies. More user/policy combinations are possible per credential object, and the IC supports secure binding to a host MCU (using standard SCP03 protocol). The IC supports the ability to freeze keys (and thereby avoid deletion by other stakeholders), configure access-right policies on the large on-chip memory, and, in combination with NXP EdgeLock 2GO service, supports management of keys and digital certificates over the air, in the field. The IC also supports multi-tenancy, where multiple stakeholders (such as equipment manufacturers, maintenance or infrastructure operators) can use the same EdgeLock SE050 secure element to securely store their sensitive data and credentials.

To simplify integration and save on development time, the EdgeLock SE050 supports secure binding to the processor, not only on the platform level but also at the application level. The small memory footprint works well with IoT formats and makes the implementation more cost-effective.

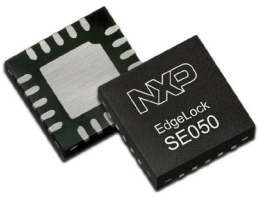
To power lighter IoT nodes, the thin Plug & Trust middleware that runs on the host microprocessor or microcontroller is optimized in size. Also, to enable fast migration from a traditional TPM to an EdgeLock SE050, the Plug & Trust middleware provides a TSS adaptation layer for easy integration into the TPM Software Stack (TSS). Pre-integration of multiple controller, processor, and crypto libraries, including OpenSSL and mbedTLS, is another feature that reduces effort and saves time during development.

The EdgeLock SE050 is part of NXP EdgeLock Assurance Program and provides certified security according to Common Criteria framework with EAL6+ AVA_VAN.5 resistance level at hardware but also at operating system level. The EdgeLock SE05x secure elements are also designed for scalability, and can easily be configured to support existing and upcoming standards, such as CHIP (Connected Home over IP) for Smart Home, DLMS-COSEM for Smart Metering, ISA/IEC 62443 for Industrial Control Security and the Open Platform Communication United Architecture (OPC UA), which defines data-exchange standards for industrial communication.

LEARN MORE

The NXP Design Community site offers helpful hints, easy-to-follow how to's, and detailed application notes for use with the EdgeLock SE050. The EdgeLock SE050 Product Page links to detailed specs, designs tools & software, training & support, and more.

- **NXP Design Community**
  https://community.nxp.com/community/identification-security/secure-authentication/overview
- **EdgeLock SE050 Product Page**
  https://www.nxp.com/SE050



Find more information on **www.nxp.com/SE050**

Date of release: April 2021

PLUG &TRUST