NXP EdgeLock™ SE050

Use Case: *Secure Communication*

Every communication with cloud, edge, and server platforms, as well as with IoT MCUs and MPUs, needs to be protected in integrity, authenticity and confidentiality. A secure element, equipped with a toolbox of crypto algorithms and common communications protocols, enables secure Plug & Trust communication.

APPLICATIONS

Industrial

Smart Home

Smart City

CHALLENGE

Whenever digital systems exchange data, it creates an opportunity for malicious actors to reveal secrets, steal private information, or mount an attack. Each time data is transmitted or received, between the various parts of a device or between the device and its environment (other devices, edge nodes, cloud services, etc.), the communication has to be made secure. To do this effectively, device communications need to meet three essential security requirements: confidentiality, integrity, and authenticity.

Confidentiality is about keeping secrets secret. Devices working in the IoT, to support industrial processes, Smart City applications, or home automation, collect and transmit data that needs to be kept confidential at all times. Symmetric cryptographic algorithms, such as AES, rely on keys shared between the sender and receiver, and protect against eavesdropping and data theft.

PLUG&TRUST

NXP

Securing tomorrow's IoT. *Today.*

Integrity means data remains unchanged during transport, and software executes without modification. Various techniques, including cryptographic hash functions (SHA), digital signatures, and message tags (MACs), allow to verify that data arrives untouched and that software is in its original state.

Authenticity involves verifying identities, to confirm the source of data or software, and control access to sensitive operations. Asymmetric cryptographic algorithms, such as RSA and ECC, give the sender and receiver their own key pairs (public and private), and ensure transmissions are coming from the right sender, while digital signatures and hash functions assign digital "fingerprints" that establish trust and support non-repudiation.

Designing, developing, and implementing a well-architected framework for secure communications, to ensure confidentiality, integrity, and authenticity, is a significant undertaking that requires detailed knowledge of advanced techniques. To save time and effort, while still delivering certified security protections in embedded designs, developers can use a secure element, a dedicated platform for ensuring secure communication.

SOLUTION

The EdgeLock SE050 is a tamper-resistant secure element that helps to ensure the confidentiality, integrity, and authenticity of device communications. Designed for flexibility, scalability, and quick integration, the EdgeLock SE050 uses certified security and standards compliance to make strong security accessible to every developer.

The EdgeLock SE050 comes with certified hardware and cryptographic algorithms already in place, and offers a middleware stack that simplifies integration and strengthens the security of embedded architectures, even those that use an MCU/MPU already equipped with high-level protections. The EdgeLock SE050 solution also includes a support package that makes it easy to deploy common communication protocols, such as TLS and Global Platform SCP03, while enabling secure Plug & Trust communication with cloud, edge, and server platforms.

Built as a turnkey, off-the-shelf security solution, the EdgeLock SE050 provides a secure, tamper-resistant environment that's closed off from the rest of the system, so critical operations take place in an isolated, protected part of the system. The on-chip security software uses a built-in crypto library and hardware crypto coprocessors, and provides a comprehensive set of cryptographic algorithms, including, among others, AES, 3DES, ECC, and KDF. The EdgeLock SE050 comes with pre-provisioned keys and credentials and is ready to work with NXP's EdgeLock 2GO service for credential management, which also offers secure credential injection at an NXP trusted facility, so developers don't have to create their own PKI infrastructure or handle and manage credentials.

The EdgeLock SE050 can be used to support binding and secure boot, by validating authenticity and integrity of firmware, and by ensuring that only signed software is executed in the IoT device. The EdgeLock SE050 can also store and protect the mission-critical cryptographic keys used to verify authenticity of firmware images prior to execution. To secure network communications, developers can code their own TLS algorithms or use the secure sample code provided within the Plug & Trust middleware. The EdgeLock SE050 also offers a pre-installed IoT applet that delivers TPM-like capabilities, for hardware-based protection of sensitive credentials.

The EdgeLock SE050 is independently certified at CC EAL 6+ (AVA_VAN.5), meets IEC-62443 security requirements, and is FIPS 140-2 CMVP certified to the top software layers. The result is a high level of assurance, even when operating in high-threat environments.

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

community.nxp.com/community/identification-security/secure-authentication/overview

Application Notes

- Ease ISA/IEC 62443 compliance with EdgeLock SE05x
- Binding a host device to EdgeLock SE05x
- EdgeLock SE05x to implement TPM-like functionality
- EdgeLock SE05x to enhance the MCU boot sequence security

User Guide

Plug & Trust MW Documentation

EdgeLock SE050 Product Page

www.nxp.com/SE050

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

Date of release: May 2021