EdgeLock™ SE050: IoT Secure Element product family

Plug & Trust: Enhanced IoT security with maximum flexibility

The EdgeLock SE050 product family of Plug & Trust devices offers enhanced CC EAL 6+ based security, for unprecedented protection against the latest attack scenarios.

KEY BENEFITS

- Plug & Trust for fast and easy design-in with complete product support package
- Ready-to-use example codes for key use cases
- Easy integration with different MCU & MPU platforms and OSs (Linux, RTOS, Windows, Android)
- Turnkey solution for system-level security without the need to write security code
- Supports compliance to new security standards like OPC-UA, IEC62443, OCF and GDPR (Privacy)
- Real end-to-end security, from edge to cloud
- Trust anchor for IoT devices with secure credential injection at hardware level

KEY FEATURES

- Flagship 40nm NXP IntegralSecurity architecture
- CC EAL 6+ based HW and OS as safe environment to run pre-installed NXP IoT applets, supporting full encrypted communications, and secured lifecycle management
- RSA & ECC functionalities, high key length and future proof curves, e.g. brainpool, Edwards and Montgomery
- AES & 3DES encryption and decryption
- HMAC, CMAC, SHA-1, SHA-224/256/384/512 operations
- HKDF, MIFARE® KDF, PRF (TLS-PSK)
- Support of main TPM functionalities
- Secured flash user memory up to 50kB
- I2C slave (High speed mode, 3.4Mbps), I2C master (Fast mode, 400kbps)
- SCP03 (bus encryption and encrypted credential injection on applet and platform level)
- Contactless interface for late-stage parameter configuration of unpowered devices
- Standard (-25 to +85 °C) and extended temp range for industrial applications (-40 to +105 °C)
- Small footprint HX2QFN20 package (3x3 mm)

The EdgeLock SE050 product family includes pin-to-pin compatible configurations (A, B, C) with use case driven feature sets.

USE CASES

- Secure, zero-touch connection to public/private clouds, edge computing platforms, infrastructure
- Device-to-device authentication
- Device integrity protection and attestation
- Device traceability and proof-of-origin
- Secure data protection and multi-user key storage for multi-application environments
- Late-stage parameter configuration
- Wi-Fi credential protection
- MIFARE support for secure access
- Authentication in blockchain
- Secure credential provisioning
- Secure access to IoT services
- Sensor data protection

TARGET APPLICATIONS

- Smart Industry
- Smart Home
- Smart Cities
- Smart Supply Chains

SECURING TODAY'S IOT APPLICATIONS

Connecting an edge device to the IoT introduces risk, since the device can serve as an illicit point of entry to the network. To provide the necessary levels of IoT security for the latest IoT applications, and protect against the latest attack scenarios, NXP developed the EdgeLock SE050 product family that delivers next-generation functionality with a very high degree of flexibility.

The EdgeLock SE050 doesn't compromise on performance and is optimized for industrial applications. A pre-installed flexible applet eliminates the need to write security code and the scalable, ready-to-deploy software has built-in protections that prevent unwanted modification.

END-TO-END CHAIN OF TRUST

With the EdgeLock SE050 IoT devices incorporate security from the start, not as a bolt-on or afterthought. Credentials, preinjected as the root of trust, are stored in hardware and fully isolated from external software access. There's no need to handle keys at untrusted stages of the supply chain. IoT devices and services are protected from unauthorized access, hacking, overwriting, deleting, manipulation, and other forms of tampering.

With this, NXP supports trust throughout the product lifecycle, from production to the field. Die-individual keys and certificates are injected at NXP certified manufacturing facilities, or by a qualified partner.

COMPLETE PLUG & TRUST PRODUCT SUPPORT PACKAGE

Delivered as a ready-to-use solution, the EdgeLock SE050 includes a complete product support package that simplifies design-in and reduces time-to-market. NXP eases the design process in several ways.

In addition to libraries for different MCUs and MPUs, the support package also offers integration with the most common OSs including Linux, Windows, RTOS, and Android.

Time-saving design tools, such as example codes for major use cases, extensive application notes, and compatible development kits for i.MX and Kinetis® microcontrollers, accelerate the final system integration.

FLEXIBLE CONFIGURATIONS

To support scalability and service the broadest range of use cases in IoT applications, the EdgeLock SE050 is available in different configurations, including versions with support for sensors directly attached to the EdgeLock SE050 via I2C Master or contactless interfaces. The following are example use cases:

- **Secure Cloud Onboarding** – Use zero-touch secure connectivity, based on proven, hardware-based security algorithms, to connect with public and private clouds.
- **Device-to-Device Authentication** – Ensure only authorized devices connect to a given network, site, or service with mutual authentication and hardware-protected keys.
- **Protect Sensor Data** – Verify that data was collected locally before encrypting and transmitting it securely to the host MCU/MPU along to the cloud or server for treatment and analysis.
- **Late-Stage Parameter Configuration** – Use the contactless interface (ISO/IEC 14443) to set application parameters of unpowered devices.
- **Support Secure Operation for MIFARE products** – Store the master key and derive multiple keys for different users and/or sessions for environments e.g. based on MIFARE DESFire®.
- **Secure Wi-Fi Connection** – Securely set up WPA2 Wi-Fi connection. Use key derivation for multiple session keys to securely connect to a Wi-Fi router, without having the master key leave the EdgeLock SE050.
- **Device ID for Blockchain Transactions** – Deploy blockchains seamlessly by using the EdgeLock SE050's unique ID to authenticate real-world assets, prove transaction ownership, and verify signatures as transactions are logged in the blockchain.

SE050 Variant	Orderable Part Number	Description	Temperature Range	12NC
SE050C1	SE050C1HQ1/Z01SCZ	ECC, RSA, AES, 3DES, MIFARE KDF, CL-IF, I2C Master	-25 to +85 °C	9353 869 87472
SE050C2	SE050C2HQ1/Z01SDZ	ECC, RSA, AES, 3DES, MIFARE KDF, CL-IF, I2C Master	-40 to +105 °C	9353 869 88472
SE050B1	SE050B1HQ1/Z01SEZ	RSA, AES, 3DES	-25 to +85 °C	9353 869 85472
SE050B2	SE050B2HQ1/Z01SFZ	RSA, AES, 3DES	-40 to +105 °C	9353 869 86472
SE050A1	SE050A1HQ1/Z01SGZ	ECC, AES, 3DES	-25 to +85 °C	9353 867 22472
SE050A2	SE050A2HQ1/Z01SHZ	ECC, AES, 3DES	-40 to +105 °C	9353 869 84472
SE050 Dev Kit	OM-SE050ARD	SE050 Arduino compatible development kit	-40 to +105 °C	9353 832 82598

More information on www.nxp.com/SE050

Date of Release: June 2019

PLUG&TRUST

NXP