PLUG & TRUST: ENHANCED IoT SECURITY WITH HIGH FLEXIBILITY

The EdgeLock SE050 secure element (SE) product family provides a trust anchor in IoT devices. This ready-to-use secure element offers enhanced Common Criteria EAL 6+ and FIPS 140-2 certified security for strong protection against the latest attack scenarios, and an extended feature set for a broad range of IoT use cases.

KEY BENEFITS

- Plug & Trust for fast and easy design-in with complete product support package and example codes for a broad range of use cases
- Extended user memory with dynamic file system to store credentials for multiple applications running on one chip
- Easy integration with different MCU/MPU platforms and OSs (Linux®, RTOS, Android®)
- Turnkey solution to reach system-level security with any MCU/MPU without the need to implement security nor handle critical keys and credentials
- Supports compliance to many security standards like IEC 62443, DLMS/COSEM, OPC-UA and ISO15118-2
- Real end-to-end security, from edge to cloud
- Trust anchor for IoT devices with secure credential injection at hardware level

KEY FEATURES

EdgeLock SE050 is available in different configurations. The available features* depend on the chosen configuration:

- EdgeLock SE050E, Common Criteria (CC) certified EAL 6+ with extended range of ECC and symmetric cryptographic options
- EdgeLock SE050F, Common Criteria (CC) EAL 6+ and FIPS certified (140-2 security level 3 for OS and applet and security level 4 for the physical security of the hardware) with support of FIPS approved algorithms
- EdgeLock 2GO enabled for flexible credential customization and over-the-air key management to meet various application requirements

Product features*:

- ECC cryptographic support of extended set of ECC curves, including NIST (up to 521 bit key length), Brainpool, Twisted Edwards and Montgomery
- RSA up to 4096Bits
- 3DES and AES (AES modes: CBC, CTR, ECB, CCM, GCM)
- HMAC, CMAC, GMAC, SHA-1, SHA-224/256/384/512
- HKDF, MIFARE® KDF, PRF (TLS-PSK)
- DRBG/TRNG compliant to NIST SP800-90A/B
- Support of main TPM functionalities
- Secured flash user memory up to 50kB
- Contactless interface for late stage parameter configuration of unpowered devices
- I^2C target (up to high speed mode, 3.4 Mbit/s), I^2C controller (fast mode, 400 kbit/s)
- Secure binding with host MCU/MPU, and bus encryption
- Secure credential injection with end-to-end encryption
- Advanced access control policies to credentials and data stored on chip
- Extended temperature range for industrial applications (-40 to +105 °C)
- Small and very thin footprint HX2QFN20 package (3 × 3 mm) with max 0.33 mm height

** Features vary according to the specific variant (EdgeLock SE050E, EdgeLock SE050F or EdgeLock 2GO Custom)*

TARGET APPLICATIONS

- Industrial
- Energy Management Systems and Smart Metering
- EV Chargers and Battery Systems
- Smart Home and Routers
- Mobile Accessories and Gaming
- Smart City. Infra & Transportation
- Security Systems and Surveillance Cameras
- Healthcare
- Communication Infrastructure

SECURING TODAY'S IOT APPLICATIONS

Connecting an edge device to the IoT poses risk, since the device can serve as an illicit entry point to the network. To provide the necessary levels of IoT security, 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 are stored in hardware and fully isolated from external software access. There's no need to handle confidential keys at untrusted stages of the supply chain. IoT devices and services are protected from unauthorized access and manipulation, physical attacks and tampering.

With this, NXP enables 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.

The extended free user memory allows customers to dynamically store credentials to enable multiple applications running on one chip.

COMPLETE PLUG & TRUST PRODUCT SUPPORT PACKAGE

Delivered as a ready-to-use solution, the EdgeLock SE050 comes with a complete product support package that simplifies design-in and reduces time-to-market.

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

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

USE CASE ENABLEMENT

- **Secure Credential Provisioning and Protection** – Secure provisioning of credentials at certified hardware level and SE customization without the need for a customer to set up a costly PKI infrastructure.
- **Secure Cloud Onboarding** – Use zero-touch secure connectivity, based on proven, hardware-based security algorithms, to connect with public and private clouds.
- **Device Integrity Protection, Attestation and Traceability** – Verify the originality and integrity of the devices with protection of the credentials stored in the secure storage of the SE. Use the credentials to attest device and data, as well as manage access to the devices.
- **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 sensitive data was collected locally by encrypting it prior to transmission to the host MCU/MPU and ultimately to the cloud or server for treatment and analysis.
- **Qi 1.3 Wireless Charging Authentication** – Integrate the EdgeLock SE050 into your wireless charger to securely store the private key and certificate of the charger and prove it is an authentic Qi-certified product.
- **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.
- **Matter Ready** – Provide the necessary cryptographic functions to support the upcoming Matter standard for connecting smart home devices.

SE050 Variant	Orderable Part Number	Description	Temperature Range	12NC
SE050E2	SE050E2HQ1/Z01Z3Z	Mainstream ECC variant (AES, 3DES, MIFARE KDF, I²C Controller)	-40 to +105 °C	9354 343 82472
SE050F2	SE050F2HQ1/Z018HZ	FIPS variant (ECC, RSA, AES, 3DES, CL-IF, I²C Controller)	-40 to +105 °C	9354 284 44472
SE050E Dev Kit	OM-SE050ARD-E	SE050E Arduino compatible development kit	-40 to +105 °C	9354 332 66598
SE050F Dev Kit	OM-SE050ARD-F	SE050F Arduino compatible development kit	-40 to +105 °C	9354 357 63598

www.nxp.com/SE050

Date of Release: May 2022
Document Number: EDGELOCKSE050FS REV 0