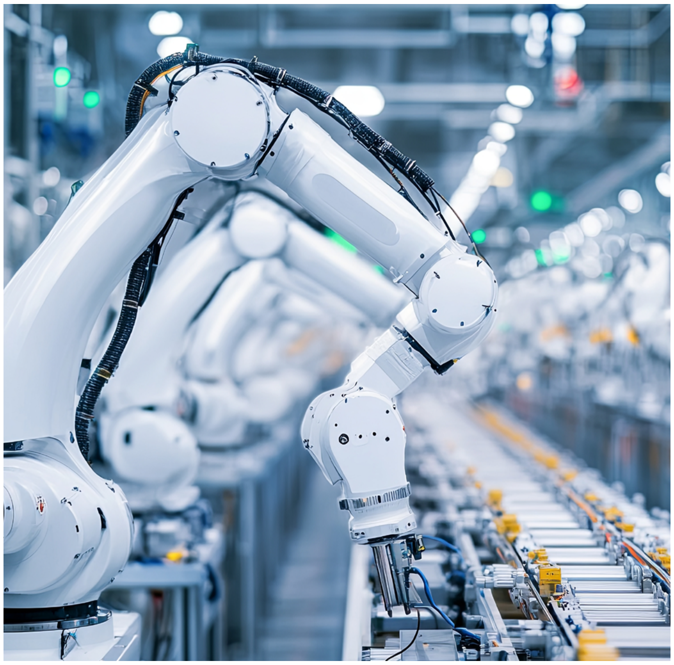
Proven, easy-to-use IoT security solution with support for updatability and custom applets

These extensions to the widely trusted EdgeLock® SE050 IoT secure element platform support applet updatability to ensure device resiliency and navigate dynamic cybersecurity regulations.



Key benefits

- Certified trust anchor for IoT devices with secure credential injection at hardware level
- Fast, easy deployment with Plug & Trust support package
- Future-proof security with SEMS Lite support for IoT applet updates
- Increased options for crypto operations with expanded support for elliptic curves
- Flexibility with optional custom applet addition

Edgelock SE051 extensions

- IoT security solutions with updatability for fast time-to-market and customization
  - SE051A/C with pre-installed IoT applet and full SW enablement for fast deployment
- SEMS Lite for convenient IoT applet updatability
- Expanded crypto agility by GMAC, AES, CCM and GCM
- Flexible user memory
  - SE051A/C: 46 KB user memory with PERSO options to go up to 104 KB

Edgelock SE050 platform features

- CC EAL6+ certified solution for IoT deployments
- Flagship 40 nm NXP IntegralSecurity architecture
- Crypto agility: RSA & ECC functionalities, high key length and future-proof curves (e.g. Brainpool, Edwards, Montgomery)
- AES and 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
- I^{2}C target (High-speed mode, 3.4 Mbit/s), I^{2}C controller (Fast-mode, 400 kbit/s)
- GlobalPlatform SCP03 (bus encryption and encrypted credential injection on applet and platform level)
- Contactless interface for late-stage parameter configuration of unpowered devices
- Extended temp range for industrial applications (-40 to +105 °C)
- Small and thin footprint HX2QFN20 package (3×3 mm)

The EdgeLock SE051 is an updatable extension of the EdgeLock SE050 Plug & Trust secure element family, which delivers proven security certified to CC EAL 6+, with AVA_VAN.5 up to the OS level. Designed for the latest IoT security requirements, it includes various countermeasures against the most recent attack scenarios. For easy design-in, the EdgeLock SE051 comes with already known features from the popular EgdeLock SE050 device, with a pre-installed IoT applet and the Plug & Trust support package. The support package includes the Plug & Trust middleware, widely integrated across microcontrollers and microprocessors, and known communication stacks such as Open SSL, mbedTLS and many more.

Flexibility and maintenance with SEMS LITE

The EdgeLock SE051 supports a lightweight, IoT-optimized version of the GlobalPlatform Secure Element Management Service (SEMS), making it possible to either update the EdgeLock SE051's IoT applet with various items, including updates for security maintenance in the field, applet upgrades, or deploy newly developed applets post-shipment.

The SEMS Lite process begins when the Update Manager, a software module running in the host, downloads the SEMS Lite update script from the OEM's backend and forwards it to the SEMS Lite Agent for execution.

The SEMS Lite Agent, an abstraction layer between the Update Manager and the EdgeLock SE051, queries the state of the system, loads the SEMS Lite script into the EdgeLock SE051, tracks update progress and recovers the system in case the update fails. The SEMS Lite Applet, pre-installed on the EdgeLock SE051, handles the update request together with the Update Manager and the SEMS Lite Agent running on the host.

OEMs can also download scripts directly from NXP's EdgeLock 2GO cloud service.

Pre-loaded IoT and perso applets

In addition to the SEMS Lite Applet, the EdgeLock SE051A/C versions are shipped pre-loaded with an IoT applet that supports GlobalPlatform Amendment H. Updates and upgrades can be triggered using the Amendment H API. The original applet will save its state and user data during any updates or upgrades in progress.

All versions of the EdgeLock SE051 also include a personalization (PERSO) applet, which allows users to configure certain platform features through the supported communications interfaces.

It can, for instance, be used to change the I^{2}C target address or delete OS modules that aren't needed for the present use case to save user memory.

Edgelock 2GO — ready

To support common IoT use cases, such as device onboarding to public clouds, the EdgeLock SE051A/C comes with pre-injected unique keys and certificates. The EdgeLock SE051A includes one ECC device – individual key pair and certification. The EdgeLock SE051C includes several options, including device – individual and device-unique key pairs as well as certificates in RSA and ECC format.

Plug and trust support package

To help simplify development and shorten time-to-market, NXP supplies a complete Plug & Trust support package for the EdgeLock SE051. This is especially of value for customers that do not have deep security expertise in-house and don't want to invest in the development of secure software code. Using the Plug & Trust middleware and pre-installed IoT applet on top of the IC's operating system means customers can rely on NXP's IoT security expertise and can scale this as a horizontal security solution across platforms, applications, and use cases. The package includes the EdgeLock SE051 enablement middleware, an EdgeLock SE051 Arduino-compatible development kit, and support for a wide range of MCU/MPU evaluation boards, along with demo codes for Wi-Fi, MIFARE, and cloud onboarding, as well as a full selection of documentation.

Ordering information

SE051 variant	Orderable part number	Temperature range	12NC
SE051C2	SE051C2HQ1/Z01XDZ	-40 to +105 °C	935414457472
SE051A2	SE051A2HQ1/Z01XEZ	-40 to +105 °C	935414458472
SE051A/C dev. kit	OM-SE051ARD	-40 to +105 °C	935399187598

nxp.com/SE051