NXP EdgeLock® SE05x secure elements and EdgeLock A5000 secure authenticator

Use Case: *Matter Security*

A turnkey solution, based on discrete, security-certified components that can be plugged into any type of device architecture, is a straightforward and scalable way to implement Matter security. The EdgeLock SE05x/A5000 solution extends Matter's connectivity security to provide additional protections – such as secure device administration and device management, support for device integrity, and secure storage of user data – that OEMs and consumers need.

MATTER AND SECURITY OF SMART HOME DEVICES

Implementing Matter Security

As smart home has evolved, so have the risks of cyberattacks on smart-home devices. The network-connected devices used to control home environments have the potential to expose private information, put personal safety at risk, and disrupt the services we depend on. What's more, these devices are also subject to counterfeiting and manipulation in the supply chain, a fact that puts the reputations of device manufacturers and service providers at risk, too.

The new Matter specification, a widely backed industry standard for smart-home interoperability, leverages strong, thoroughly tested industry-standard cryptographic algorithms and addresses security in several ways. Matter devices must get their genuity verified at commissioning, protect user ownership, and connect securely with the Matter ecosystem. Device attestation credentials are required for onboarding, as are Over-the-Air (OTA) updates, so devices can stay current with evolving threats.

As a result, building a Matter device involves implementing a number of security mechanisms. This includes generation and pre-installation of well-defined cryptographic material (keypairs and digital certificates). Developers must also implement a number of hardware and firmware elements, such as true random-number generation, cryptographic-key protection, an encryption engine, and crypto accelerators.

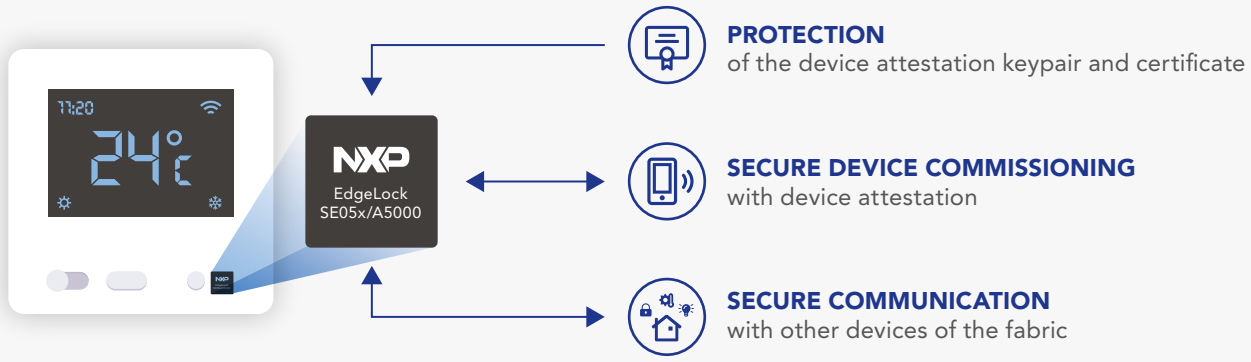
NXP EdgeLock Secure Elements and Secure Authenticator

NXP EdgeLock SE05x secure elements (SE) and the EdgeLock A5000 secure authenticator (SA) provide a turnkey solution to address Matter security requirements. Equipped with an I²C interface to connect to any type of processor, these Plug & Trust security components provision Matter attestation keys and certificates to the device and provide hardware-accelerated execution of Matter authentication protocols.

PLUG&TRUST NXP

Securing tomorrow's IoT. *Today.*

BLOCK DIAGRAM



EdgeLock SE05x/A5000 for Matter

As a result, OEMs can simplify product development, accelerate manufacturing and compliance to Matter security specifications, and avoid investment and cost of ownership in specialized equipment for credential provisioning.

Beyond supporting what's specified in the Matter standard, the EdgeLock SE05x/A5000 delivers certified security with tamper resistance, with Common Criteria EAL 6+ certification and protection from the latest attack scenarios, including advanced hardware attacks.

NXP's EdgeLock SE05x/A5000 solutions for Matter support Linux, FreeRTOS, Zephyr, and other RTOSs, support multiple use cases, and provide a uniform framework with optimal performance across multiple device types. The EdgeLock SE05x/A5000 can be used in NXP's Matter development platforms, including a Linux-based, multi-connectivity platform built around the NXP i.MX 8M Mini application processor, 88W8987 Wi-Fi/Bluetooth solution and K32W0x multiprotocol wireless MCU.

EdgeLock SE05x/A5000 solutions are pin-to-pin compatible and offer a scalable API for security services. The entire portfolio is supported by the NXP EdgeLock 2GO service for credential management.

The EdgeLock A5000 provides Matter device attestation based on ECC cryptography and NIST P-256 curve (with key functions such as ECDSA, ECDH, and True Random Number Generation). This ready-to-use solution is available with pre-injected and customized Matter attestation credentials, and has enough memory to store other credentials, such as those used to securely connect the device to a SW update server based on TLS protocol for example.

The EdgeLock SE050E builds on the A5000's capabilities with a range of additional security functions, including a wide choice of ECC curve options for compliance with other ecosystems and requirements, as well as TPM functions, Wi-Fi Key Derivation Function (KDF), and extended memory for secure storage of user data.

The EdgeLock SE051W, which combines Matter device attestation with support for secure ranging based on Ultra Wideband (UWB), is designed for use in smart locks and other presence-based access systems. It supports updatability using NXP SEMS Lite to cope with potential future updates of the Matter standard and includes a contactless NFC interface that enables late-stage Matter device configuration.

The EdgeLock SE051H is designed to meet the security requirements of Matter by supporting the necessary algorithms and cryptographic functions (including SPAKE2+), while enabling the simplicity of device onboarding via NFC. So developers can deliver products that are secure yet easy to deploy by delivering a better user experience.

THE RIGHT BUILDING BLOCKS

NXP is one of the few semiconductor companies that helped define the Matter specification, and is one of the first to offer Matter-certified and compliant development platforms and products. We are also one of the first semiconductor manufacturers to have been granted trusted Product Attestation Authority (PAA) status by the Connectivity Standards Alliance (CSA). The NXP EdgeLock 2GO service can issue Matter device attestation certificates for the OEM products and offers flexible options for device provisioning. The EdgeLock SE05x/A5000 solution, supported by the EdgeLock 2GO service, is an innovative approach that enables peace of mind while simplifying security.

EDGELOCK SE05X/A5000 SOLUTION GUIDE

	EDGELOCK A5000 Secure authenticator	**EDGELOCK SE050E** General-purpose secure element	**EDGELOCK SE051W** Secure element with UWB ranging support	**EDGELOCK SE051H** Secure element with extended Matter support
Matter support	▸ Provisioning of Device Attestation Certificate ▸ Certificate-based authentication (ECC P-256)	▸ Provisioning of Device Attestation Certificate ▸ Certificate-based authentication (ECC P-256)	▸ Provisioning of Device Attestation Certificate ▸ Certificate-based authentication (ECC P-256)	▸ Provisioning of Device Attestation Certificate ▸ Provisioning of Passcode verifier ▸ Certificate-based authentication (ECC P-256) ▸ Device commissioning via NFC ▸ Password-authenticated key exchange (SPAKE2+)
SEMS Lite technology (Applet updatability for potential updates of the Matter standard)	No	No	Yes	Yes
Other use cases supported beyond Matter	▸ Device onboarding to cloud ▸ Protection of user data	▸ Device onboarding to cloud ▸ Protection of user data and user privacy ▸ Device integrity (TPM) ▸ Certificate-based Wi-Fi authentication	▸ SUS and FIRA applet for secure UWB ranging ▸ Device onboarding to cloud ▸ Protection of user data and user privacy ▸ Device integrity (TPM) ▸ NFC-based device configuration ▸ Certificate-based Wi-Fi authentication	▸ Device onboarding to cloud ▸ Protection of user data and privacy ▸ Device integrity (TPM) ▸ NFC-based device configuration ▸ Certificate-based Wi-Fi authentication
Available User memory (kB)	8	50	20	16
Availability	In mass production	In mass production	In mass production	In mass production

Same packaging, all pin-to-pin compatible

Find more information on **nxp.com/iotsecurity**

Date of release: February 2023