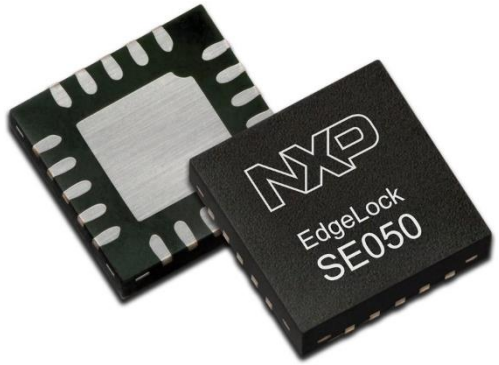
EdgeLock™ SE050

PLUG&TRUST secure element family



JORDI JOFRE

27/08/19

jordi.jofre@themobileknowledge.com

PUBLIC

SECURE CONNECTIONS FOR A SMARTER WORLD

Agenda

- EdgeLock SE050 key features.
- Plug & Trust secure element product portfolio.
- EdgeLock SE050 product variants.
- EdgeLock SE050 use cases.
- EdgeLock SE050 secure provisioning.
- EdgeLock SE050 support package.

September 3rd, 10 AM CEST and 08 AM PDT

Session 2: Getting started with EdgeLock SE050 support package

https://attendee.gotowebinar.com/rt/6794463289897864706

PLUG&TRUST

Security is at the core of enabling trust

IoT **security** is becoming more important as the number of connected devices increase.

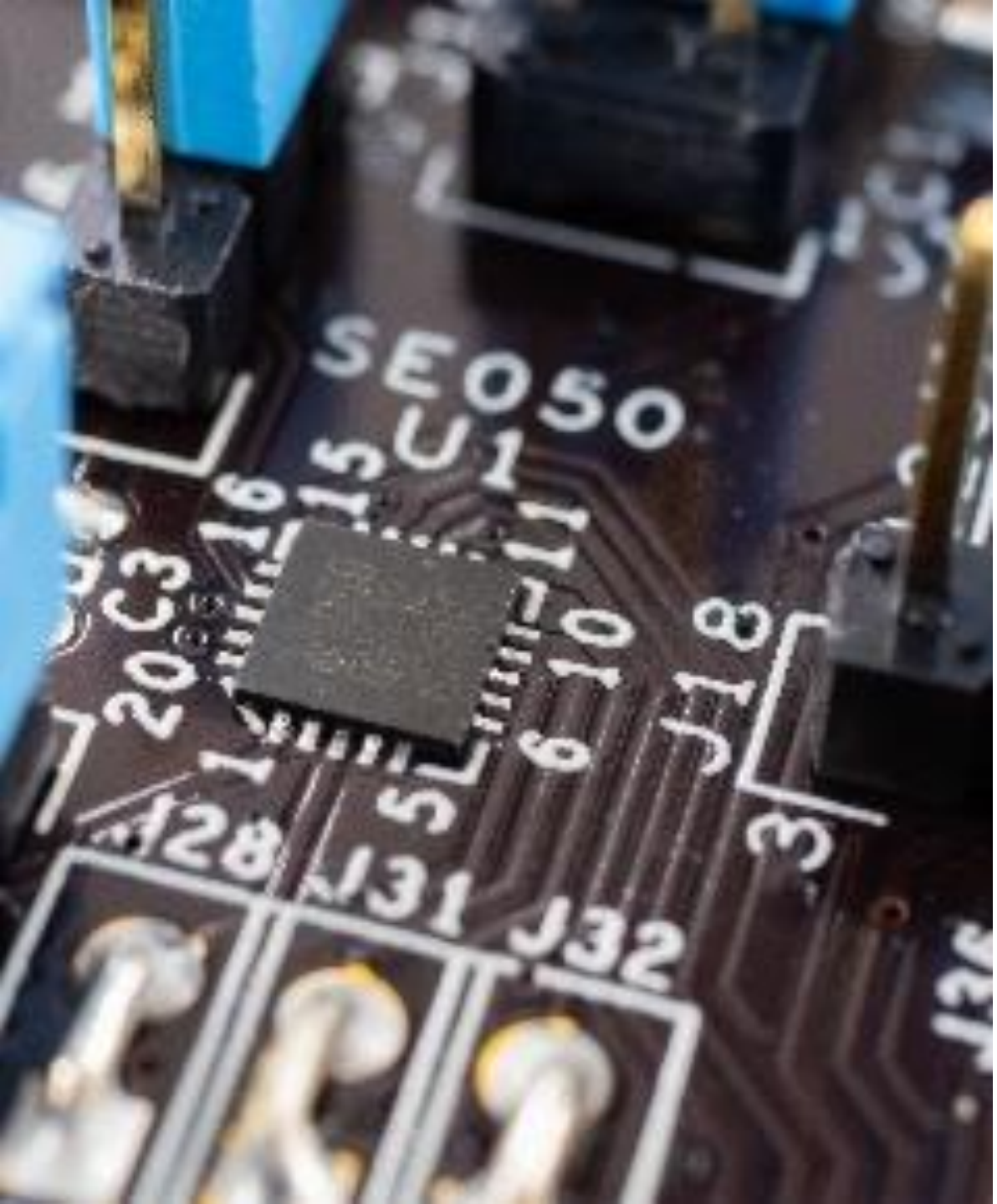
IoT presents an exciting environment for innovation, but also **security challenges**.

IoT solutions need to be built on **a secure foundation** to ensure integrity, confidentiality, authenticity, availability and end-user safety.

Security is the **value enabler** to deliver trust and it is essential for business growth.

NEW

EdgeLock SE050 Plug & Trust Secure Element family



EdgeLock SE050

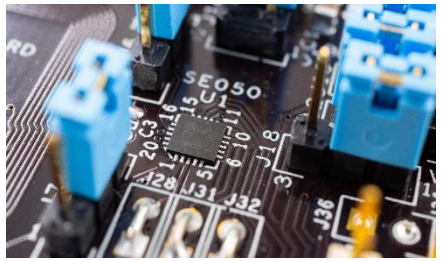
Enhanced IoT security with maximum flexibility

- ECC and RSA crypto support
- Root of trust at the IC level
- CC EAL 6+ certified solution
- Maximum flexibility.
  Pre-integration with SW connectivity stacks, IoT public clouds and NXP MCUs/MPUs.

NXP PLUG&TRUST

A tamper resistant HW to safely store keys and credentials

PLUG&TRUST



NXP IoT security App

Secure OS (JCOP 4)

SE050 HW

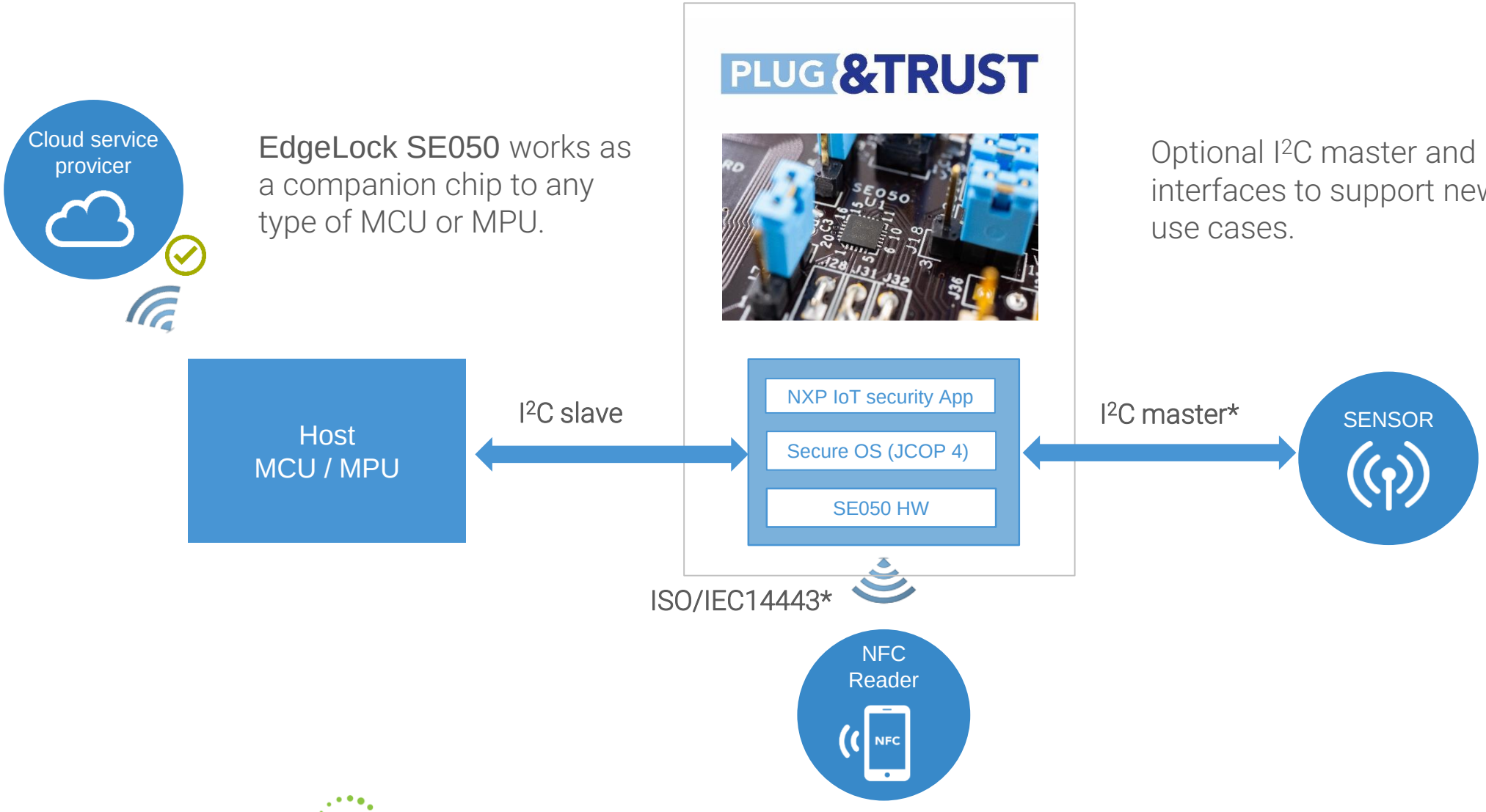
Crypto support

ECC algorithms	ECDSA, ECDH, ECDHE, ECDAA, EDDSA
ECC curves	NIST (192 to 512 bit) BrainPool (160 to 512 bit) Koblitz Secp (160 to 256 bit) Montgomery curve25519 Twisted Edwards (for Ed25519)
RSA	Encrypt/Decrypt/Sign/Verify 1024-2048-3072-4096 bits
Symmetric	AES 128/192/256, (T)DES
Hashing	SHA1, SHA224/256/384/512
MAC	HMAC, CMAC
KDF	TLS KDF, TLS PSK, Wi-Fi KDF (PBKDF2) OPC_UA KDF, MIFARE

EdgeLock SE050 file system allows us to store "secure objects"

A physically isolated IC for performing critical security functions and crypto operations **without the need to write security code or expose keys**.

A trusted HW that can be added to any IoT architecture



EdgeLock SE050 Plug & Trust for IoT

Customer benefits

- Plug & Trust for fast and easy design-in with complete product support package
- 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
- Compliance to new security standards like OPC-UA, IEC62443, OCF and GDPR
- Real end-to-end security, from sensor to cloud
- Trust anchor for IoT devices with secure credential injection at hardware level

Product overview & 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 & DES 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
- Standard (-25 to +85 °C) and extended temp range for industrial applications (-40 to +105 °C)
- The EdgeLock SE050 product family includes pin-to-pin compatible configurations 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 configuration & personalization via ISO14443
- Wi-Fi credential protection
- MIFARE support for secure access
- Authentication in blockchain
- Secure credential provisioning
- Secure access to IoT services
- Sensor data protection

Packaging

- Small footprint HX2QFN20 package (3x3 mm)

Interfaces

- I2C slave (High-speed mode, 3.4Mbps), I2C master (Fast mode, 400kbps)
- ISO14443

Plug & Trust
secure element portfolio

Plug & Trust secure element portfolio

Product positioning

EdgeLock SE050

Offers enhanced Common Criteria EAL 6+ security certification to secure high-performance IoT applications.

More flexibility, use cases, and extended support package.

Optimized for industrial applications, secure end-to-end channel and cloud onboarding.

★ Flagship product

A71CH

Ready-to-use solution providing a root of trust at the IC level and delivers chip-to-cloud security out of the box*.

NXP's Plug & Trust portfolio streamlines the deployment of IoT services and onboarding of IoT end nodes and edge nodes to the cloud while achieving the most effective security levels.

* A71CH (Watson, IBM, AWS, Azure)
A71CL (Alibaba, Baidu clouds)

Plug & Trust secure element portfolio

Product features comparison

ECC (ECDSA/ECDH/ECDHE 256p), Hash (HMAC) SHA (SHA256), Key derivation (HKDF, PRF (TLS-PSK))	**Cryptography**	ECC (ECDSA/ECDH/ECDHE/ECDAA), **RSA (up to 4096),** Hash (HMAC, CMAC) SHA (SHA-1/224/256/384/512) AES (128, 256) & DES encryption/ decryption, Key derivation (HKDF, PBKDF, Wi-Fi KDF,OPC_UA KDF, PRF (TLS-PSK)
ECC NIST P-256	**ECC crypto curves**	ECC NIST (192 to 521-bit), Brainpool (160 to 512-bit), Koblitz (160 to 256 bit), Edward (Ed25519), Montgomery (Curve25519)
I2C Slave (400kbps)	**Interfaces**	I2C Slave (3.4Mbps), I2C Master, (fast mode 400kbps), ISO/IEC 14443 interface
4 kB	**User memory**	50 kB
SCP03 (bus encryption + encrypted credential injection)	**Secure interface**	SCP03 (bus encryption + encrypted credential injection on applet & platform level)
4x4mm (HVSON-8), 2x2mm (CSP)	**Packaging**	3x3mm (HX2QFN20)
-40…+90 ºC	**Temperature range**	-40…+105 ºC
1.62…3.6V	**Voltage range**	1.65…3.6V (5V possible)

Common Criteria

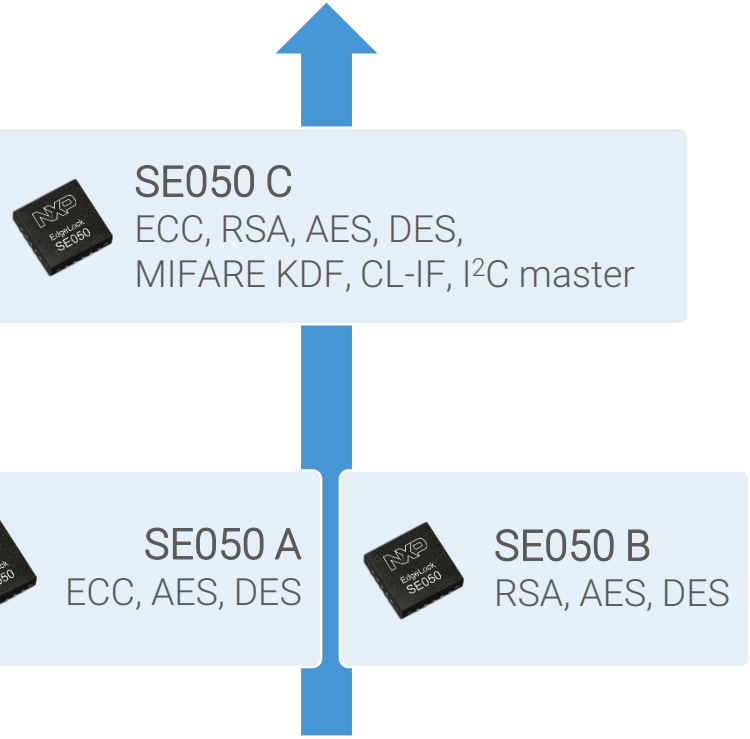
CC EAL 6+

Training Mobile Knowledge

NXP PLUG&TRUST

EdgeLock SE050 product variants

EdgeLock SE050 product variants

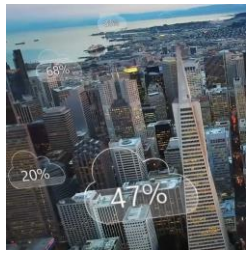


Group	Feature	SE050 A	SE050 B	SE050 C
ECC algorithms	ECDSA	Yes	No	Yes
	ECDH	Yes	No	Yes
	ECDHE	Yes	No	Yes
	ECDAA	No	No	Yes
	EDDSA	No	No	Yes
ECC curves	ECC NIST (192 to 512 bit)	Yes	No	Yes
	ECC BrainPool (160 to 512 bit)	Yes	No	Yes
	Koblitz (160 to 256 bit)	Yes	No	Yes
	Montgomery curve25519	No	No	Yes
	Twisted Edwards (for Ed25519)	No	No	Yes
RSA	RSA (up to 4096 bit)	No	Yes	Yes
Symmetric	(T)DES	Yes	Yes	Yes
	AES (128-256 bit)	Yes	Yes	Yes
Key derivation	TLS KDF, TLS PSK	Yes	Yes	Yes
	MIFARE DESFire KDF	No	No	Yes
	WiFi KDF (PBKDF2)	Yes	Yes	Yes
	OPC_UA KDF	Yes	Yes	Yes
Interfaces	I²C slave	Yes	Yes	Yes
	I²C master	No	No	Yes
	ISO/IEC14443	No	No	Yes

A family concept meeting the needs of different use cases

EdgeLock SE050 use cases

New use cases with EdgeLock SE050 on top of A71CH



Secure Cloud Onboarding

Device-to-device authentication

Attestation & Proof of device origin

Known from A71CH

New on SE050

Sensor data protection

Late-stage parameter configuration

Wi-Fi credential protection

Secure Access Module

Device ID for Blockchain

Trusted platform module

SE050 is converging secure sensing, secure connections to multiple cloud services, and integrity protection of a trusted IoT platform.

Secure cloud onboarding

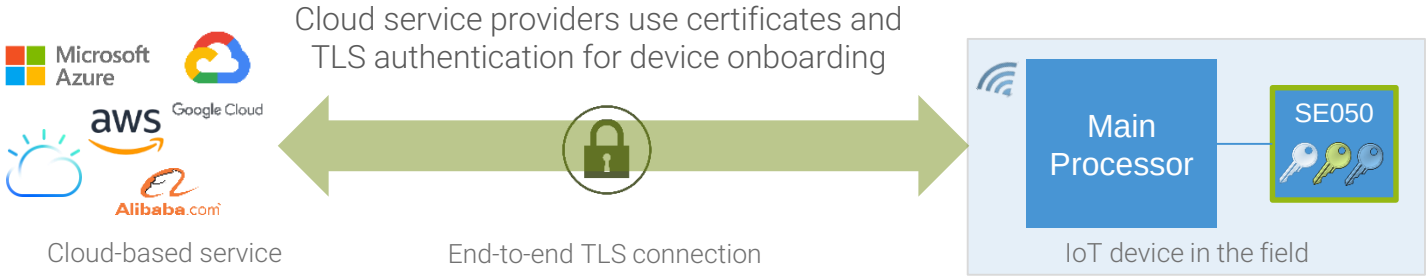
Secure, zero-touch connection to public/private clouds, edge computing platforms and infrastructure.

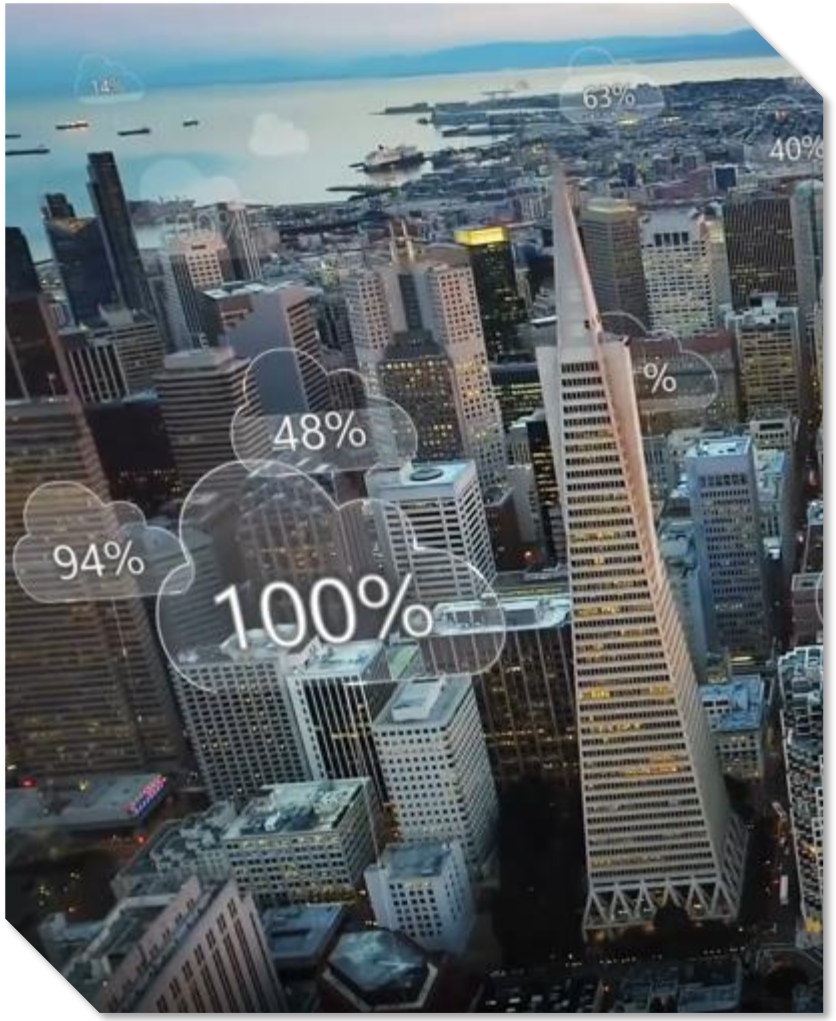
Use of SE050:

- SE050 provides end-to-end security, from chip to edge to cloud.
- SE050 protects the credentials used to establish a TLS link with the cloud service provider. Keys are never exposed to any party during the lifetime of a device.
- SE050 supports TLS version 1.3 and pre-shared key cipher suites using either symmetric keys or ephemeral keys.

Key applications:

- Smart industry
- Smart home





Device-to-device authentication and attestation

Mutually authenticate devices, prevent electronic counterfeiting and verify proof-of-origin to operate securely.

Use of SE050:

- SE050 supports secure and scalable hardware root of trust authentication for devices.
- SE050 provides protection against side attack channel and tampering on the private keys.
- SE050 prevent non-authorized tools from connecting to my device or network

Key applications:

- Industrial devices and control systems.
- Standalone security systems (OTP, cloud keys)

Authenticity is proved by the verification of signed random numbers

Certificates are used to bind public key with its owner.

Sensor data protection

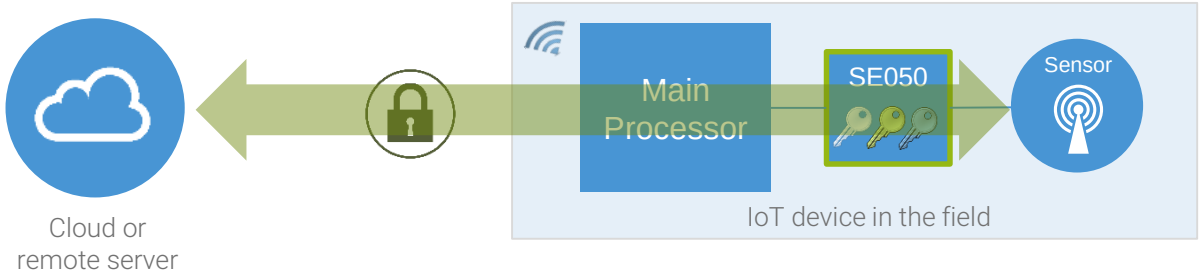
Set up a secure, end-to-end connection from sensor or actuator to local gateway or cloud-based service.

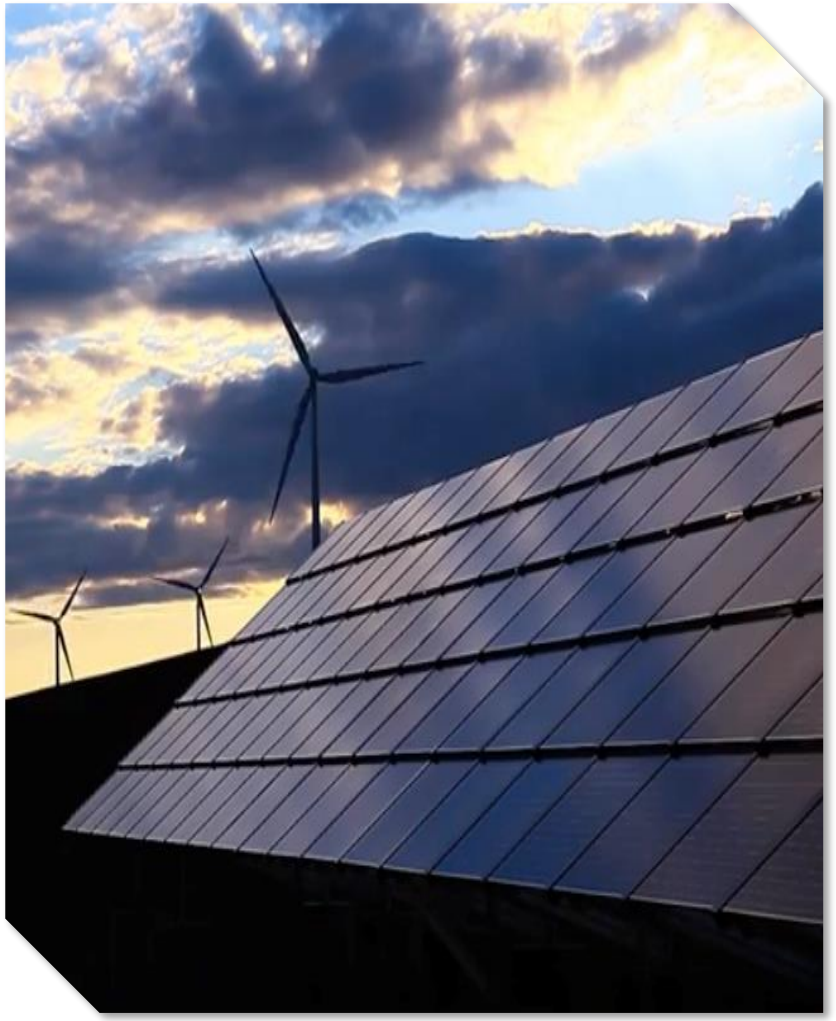
Use of SE050:

- SE050 has the task to guarantee the privacy and the authenticity of the data extracted by sensor.
- SE050 encrypts and signs the sensor data by default before forwarding it.
- SE050 is directly connected to the critical sensor and ensures data is collected privately and cannot be manipulated.

Key applications:

- Smart Energy (e.g., solar panels).
- Access to machines / robots (e.g., temperature, sensor).
- Sensors used in robots
- User authentication via Pin Pad.





Late-stage parameter configuration

Set configuration parameters without powering the device using an NFC phone or contactless reader.

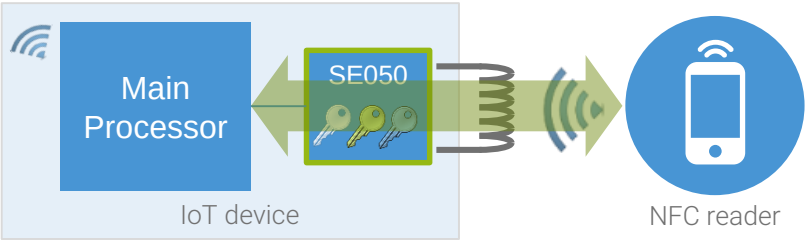
Use of SE050:

- SE050 integrates an ISO/IEC14443 interface.
- SE050 contactless interface can be used to configure IoT devices, install a setup or enter data.
- SE050 allows generic IoT products to be set up and configured in the last step (e.g., certain customers or use cases).

Key applications:

- Home appliances
- Consumer kits.
- Lighting management system

NFC reader writes info into SE050 shared file system, host reads this info, and writes answer back into shared file system



Wi-Fi credential protection

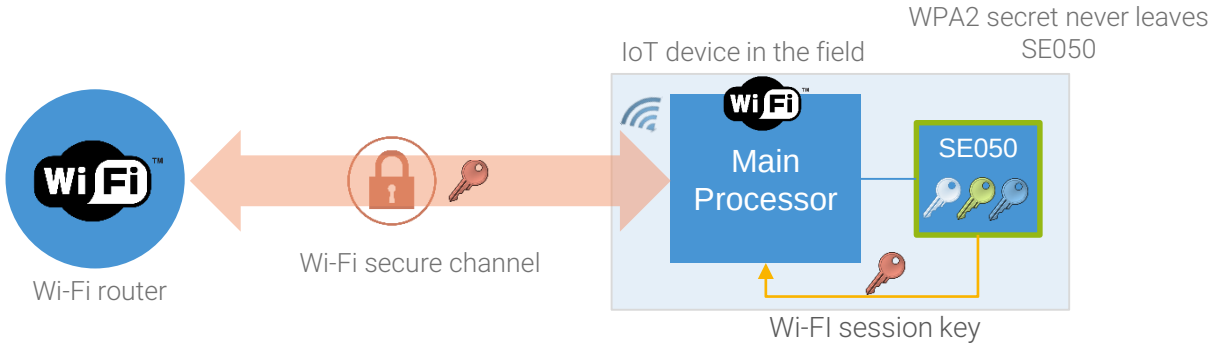
Secure access to networks. Authenticate and validate devices connecting to a WLAN or Wi-Fi router.

Use of SE050:

- SE050 supports the WPA2-PSK (PBKDF2) and WPA2-EAP-TLS security protocols.
- SE050 protects the WPA2 passphrase or secret key and generates the Wi-Fi session key to connect to the Wi-Fi router used for the WPA2 connection setup.

Key applications:

- Routers
- Gateways
- Critical IoT devices connected via WiFi.



Secure Access Module

Securely manage user credentials and enhance the protection of your facilities or specialized machinery.

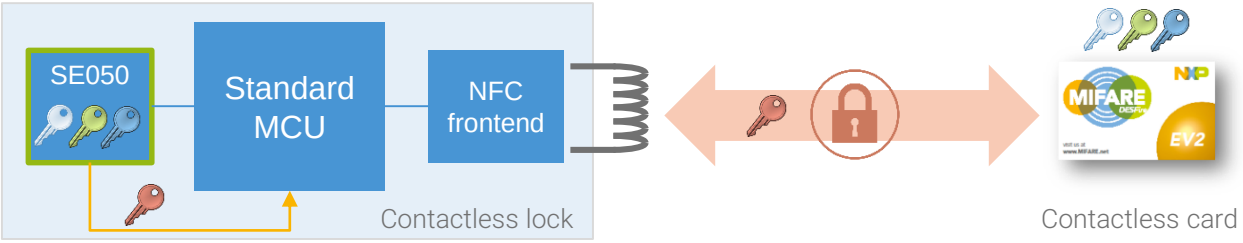
Use of SE050:

- SE050 supports secure operation for MIFARE DESFire product.
- SE050 protects the secret key used to set up a secure channel with a MIFARE credential.
- SE050 supports MIFARE key derivation function, authentication and session key generation.

Key applications:

- Smart factories.
- Machine access
- Smart door lock.

1. The MCU uses SE050 to authenticate the MIFARE credential.
2. SE050 calculates and exports the MIFARE session key to the MCU.
3. The MCU implements the MIFARE command set and secure messaging.



MIFARE temporary session key

Device ID for Blockchain

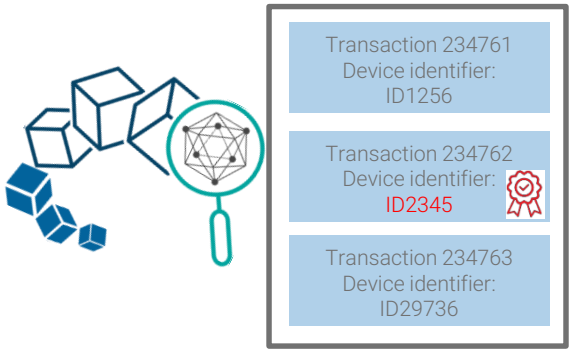
Use the SE050 unique ID to associate real-world assets to their counterpart in the blockchain, generate and own the key pair to authenticate to the blockchain and sign the transaction requests

Use of SE050:

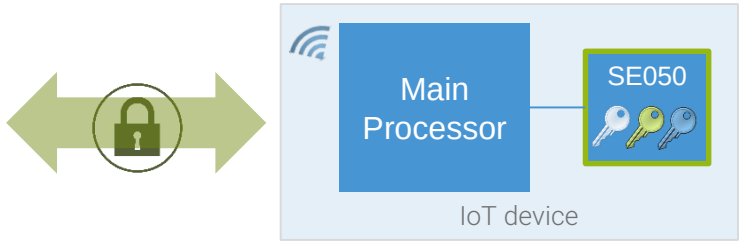
- SE050 supports Blockchain applications by providing a unique identifier.
- SE050 acts as the link between the real-world asset and references to this real-world asset in the transactions of the blockchain.
- SE050 protects the public-private key pair needed to prove ownership of transactions.

Key applications:

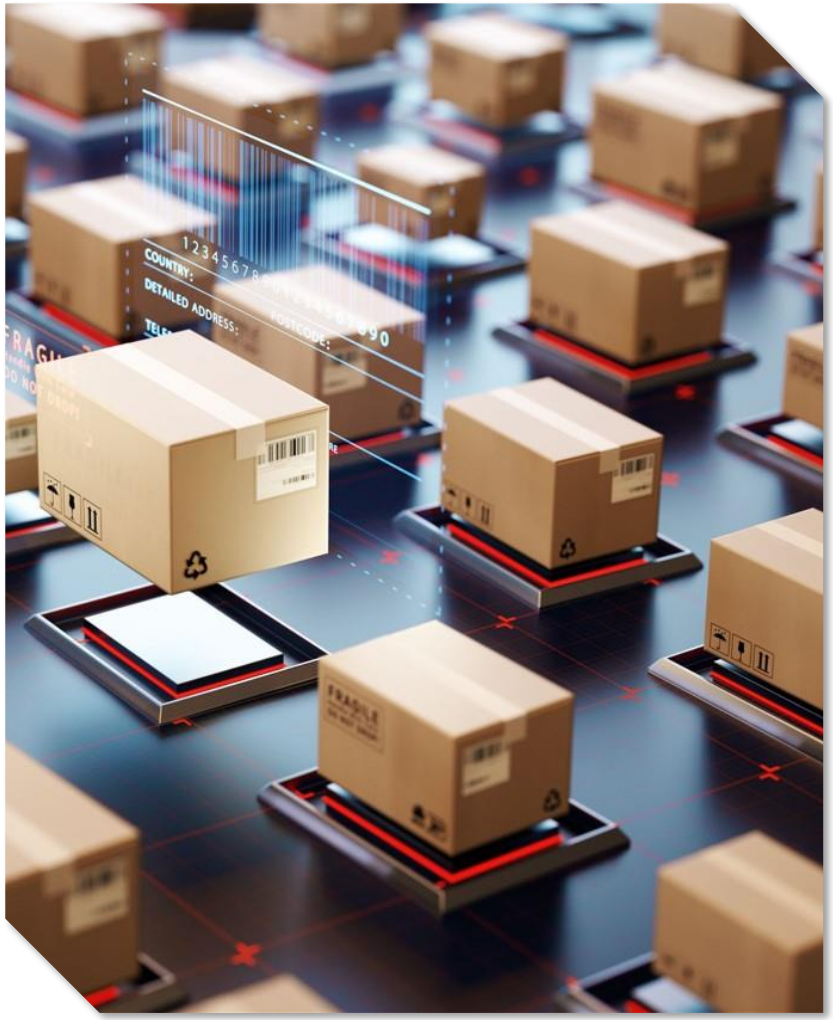
- Logistics.
- Traceability.
- Tagging.



Main processor presents data to SE050, SE050 prepares transaction request and signs it*.



*Other variants are possible



TPM-like functionality

EdgeLock SE050 combines main TPM-like functionality with increased flexibility and support of more security use cases.

Use of SE050

- SE050 supports TPM-like functionality with crypto-co-processing, NV key storage, random sources, monotonic counters, unique identifiers, platform configuration registers (PCRs), anonymous attestation, privacy enablement, authorization and boot flow protection.
- SE050 has been designed to meet IoT use cases as opposed to TPM, designed for computing.

What SE050 brings over TPM:

- Tiny Plug & Trust middleware (10 kB) on host MCU/MPU to manage access and policies.
- Integration with common IoT OS and HW
- Multi Cloud support based on RSA, ECC, 50kB dynamic memory for certificates & keys.
- Smaller footprint 3x3mm (TPM = 5x5mm).
- Secure interface binding with host processor (SCP03 secure channel).
- Multi-tenancy – Flexible credential management with higher granularity.
- More user/policy combination per credential object (4 instead of 1).
- Key pre-injection solution for zero-touch X509-based cloud onboarding.
- Fast adaption to new upcoming standards (e.g., IEC 62443, OPC-UA).

EdgeLock SE050
end-to-end secure channel protection

End-to-end secure channel protection

Secure channels of user sessions provide end-to-end protection, from application (cloud service, maintenance operator tool, MCU)

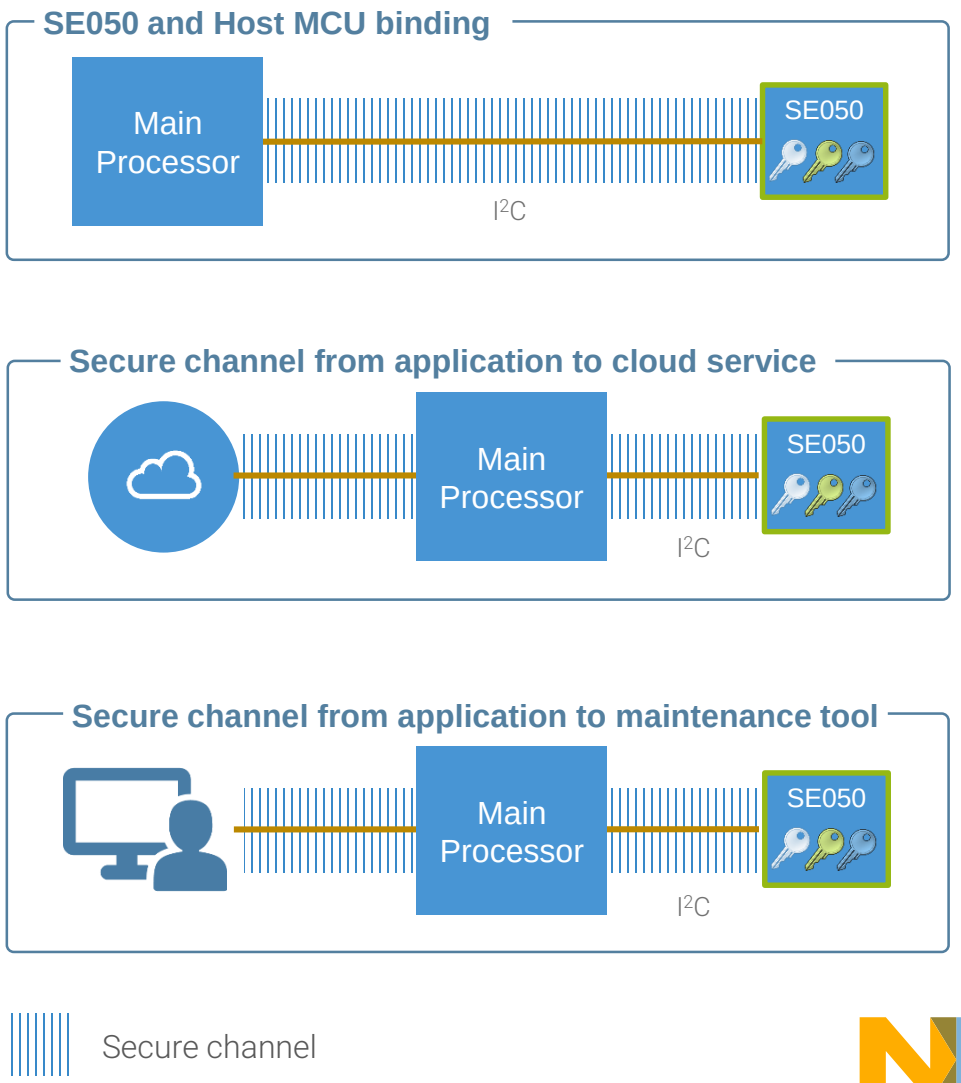
SE050 enables the user to set up an end-to-end secure channel protection using either SCP03 or FastSCP

SCP03 is based on shared AES128 keys (3 keys):

- 1 for message authentication
- 1 for message encryption
- 1 to wrap new authentication/encryption keys

FastSCP is based on ECC P-256 bits key pairs to set-up the secure channel.

- Pre-sharing of public keys (ECDH) is required



EdgeLock SE050 secure provisioning

EdgeLock™ SE050 secure provisioning

SE050 EASE OF USE CONFIGURATION

SE050 variants come pre-provisioned with keys which can be used for all major use cases not requiring customer specific credentials.

NXP TRUST PROVISIONING

NXP TP offers customized and secure injection of die-individual keys and credentials into SE050 on behalf of the OEM. This service is available for high volume orders.

NXP DISTRIBUTORS

NXP has agreements with distributors and third-party partners to offer customized and secure injection of die-individual keys and credentials into SE050 for orders of any size.

EdgeLock SE050 ease of use configuration

SE050 EASE OF USE CONFIGURATION

SE050 variants come pre-provisioned with keys which can be used for all major use cases not requiring customer specific credentials

*Check AN12436 – SE050 configurations for more details

- SE050 pre-configuration for ease of use allows you to offload the cost of ownership, secure element personalization and the complexity of key management.
- SE050C1/C2 includes a combination of key pairs and certificates suitable for most of the use cases (cloud onboarding, secure sensing, Wi-Fi protection, etc):
  - An ECC key pair and certificate for attestation.
  - An RSA key pair and certificate for attestation.
  - 4 RSA key pairs and certificates.
  - 2 ECC key pairs and certificates.
- SE050A/B come with a subset of keys (ECC or RSA only)

All SE050 variants are offered off-the-shelf pre-provisioned for ease of use. This means that for many of the use cases and cloud services customers are not required to program additional credentials.

EdgeLock SE050 support package

EdgeLock SE050 Plug & Trust support package

EdgeLock SE050 Plug & Trust middleware

EdgeLock SE050 enablement

Pre-integration to Main OS & MCU, MPU

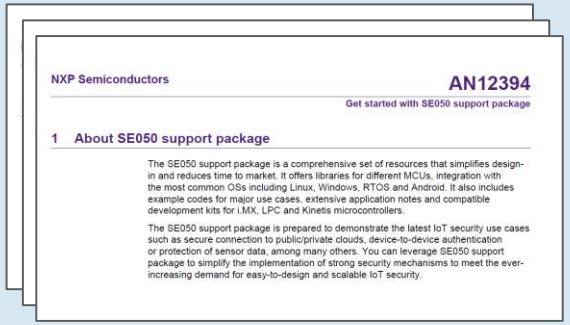
Android™, Linux®, RTOS	Linux, Windows®, macOS®	
Use Case Based Example Codes		
PKCS11	Android KeyMaster	OPC-UA	MQTT
Arm® mbed™ TLS	OpenSSL	TLS
API		

Supported evaluation MCU/MPU boards

SE050 Arduino compatible development kit

Demo codes

Documentation



NXP Semiconductors

AN12394

Get started with SE050 support package

1 About SE050 support package

The SE050 support package is a comprehensive set of resources that simplifies design-in and reduces time to market. It offers libraries for different MCUs, integration with the most common OSs including Linux, Windows, RTOS and Android. It also includes example codes for major use cases, extensive application notes and compatible development kits for i.MX, LPC and Kinetis microcontrollers.

The SE050 support package is prepared to demonstrate the latest IoT security use cases such as secure connection to public/private clouds, device-to-device authentication or protection of sensor data, among many others. You can leverage SE050 support package to simplify the implementation of strong security mechanisms to meet the ever-increasing demand for easy-to-design and scalable IoT security.

MORE INFO

September 3rd, 10 AM CEST and 08 AM PDT

https://attendee.gotowebinar.com/rt/6794463289897864706

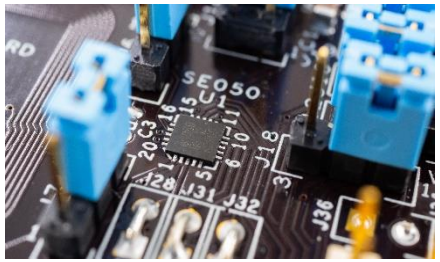
NXP PLUG&TRUST

Last words

EdgeLock SE050 – a Root of Trust enabling new use cases

PLUG &TRUST

Out-of-the-box Solution



NXP IoT security App

Secure OS (JCOP 4)

SE050 HW

I²C slave | ISO/IEC 14443 | I²C master

Flagship 40nm architecture and CC EAL 6+ certified state of the art security concepts strongly protect against most recent attack scenarios. Additional features enable use cases to answer multiple application needs in IoT and especially industrial needs.

Enhanced security

- 40nm Flagship Technology with IntegralSecurity 3.0
- CC EAL 6+ VAN5 certified HW & OS
- RSA & ECC functionalities
- Future proof curves & higher key length
- Encrypted communication via SCP
- Symmetric ciphers for encryption/decryption

Absolute flexibility

- Product family with multiple solutions for various new use cases
- Flexible applet with dynamic 50kB user memory
- Multiple interfaces – I2C Slave, I2C Master, ISO14443
- Plug & Trust: Easy integration with multiple MCU/MPU platforms & OS, major Cloud integration
- OPC-UA support & easy compliance for IEC62443

Product website: www.nxp.com/SE050

Development kit: www.nxp.com/ OM-SE050ARD

NXP PLUG &TRUST

EdgeLock SE050 ordering details

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

For more info check out www.nxp.com/SE050

Time for Q & A

MobileKnowledge

MobileKnowledge is a team of HW, SW and system engineers, experts in **smart, connected and secure** technologies for the IoT world. We are your ideal **engineering consultant** for any specific support in connection with your **IoT** and **NFC** developments. We design and develop secure HW systems, embedded FW, mobile phone and secure cloud applications.

Our services include:

- **Secure hardware design**
- **Embedded software development**
- **NFC antenna design** and **evaluation**
- **NFC Wearable**
- **EMV L1 pre-certification support**
- **Mobile** and **cloud application development**
- **Secure e2e system design**

MIFARE Accredited Training Partner

Approved Engineering Consultant NXP

MOBILE WORLD CAPITAL™ BARCELONA

www.themobileknowledge.com

mk@themobileknowledge.com

We help companies leverage the **secure IoT revolution**

NXP PLUG&TRUST

PLUG &TRUST

SECURE CONNECTIONS
FOR A SMARTER WORLD