EdgeLock™ SE050: NXP's New Generation Plug & Trust Solution to Secure IoT Edge

Denis NOEL

Head of Marketing
IoT Security

June 2019 | Session AMF-SOL-T3649

SECURE CONNECTIONS FOR A SMARTER WORLD

Agenda

- The relevance of HW security & Trust Anchoring in IoT
- Introduction to EdgeLock SE050
- SE050 Plug & Trust unique value proposition
- Illustration of SE050 features across Industrial, Smart City and Smart Home use cases
- SE050 Plug & Trust Family overview

IoT Edge requires HW Security with Trust Anchoring

IoT is about

- Real-time autonomous systems controlling critical world states
- Data collection & injection into ubiquitous AI engines with the risk of data poisoning
- Smart manufacturing and the need for business continuity

This drives the need for Trust Anchoring at Edge

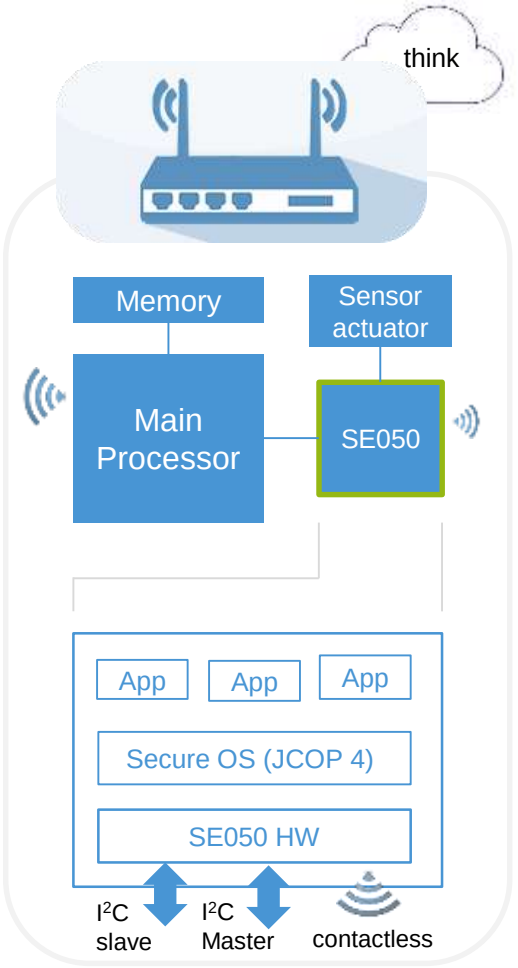
- Trust anchor means a reliable foundation, tamper resistant
  - Physical isolation in space and time of critical security functions (all remote & local attacks exploit absence of isolation)
  - Binding of keys and credentials to a trusted issuer/source
- Trust Anchoring
  - Reduces SW effort & maintenance cost
  - Reduces liability of the SW vendors in multi tenant systems

NXP introduces EdgeLock SE050, a Trust Anchor for IoT…

- EdgeLock SE050 is an Embedded Secure Element
  - Discrete HW Tamper resistant security component
  - State-of-the-art security, certified
  - Dedicated environment to host security functions (isolation)
  - Companion chip to any type of MCU, MPU and AP

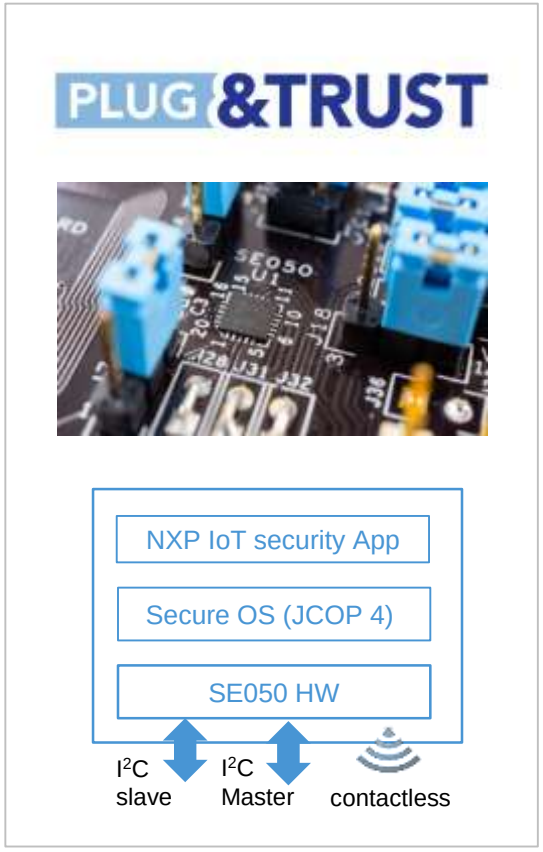
- Secure sub-system on IoT Edge:
  - Can host different secure Apps with different APIs
  - Standardized Apps management interface (Global Platform)
  - Separation of application domains

- Platform with multiple interface options:
  - I2C for MCU/MPU
  - Master I2C interface
  - Contactless ISO14443 (NFC)



…EdgeLock SE050 Plug & Trust for out-of-the-box solutions

- EdgeLock SE050 with pre-integrated IoT security Apps
  - Out-of-the-box experience for IoT developers
  - Rich API to meet different IoT use cases
  - Pre-integration into NXP MPUs and MCUs
  - Pre-integration into embedded SW stacks
  - Pre-integration with major IoT Public Clouds
- EdgeLock SE050 Plug & Trust is a product family
  - Different IoT security Apps with different features & configurations
  - Cross-compatible API
  - Same packaging across family



EdgeLock SE050 Plug & Trust is a convergence IoT product

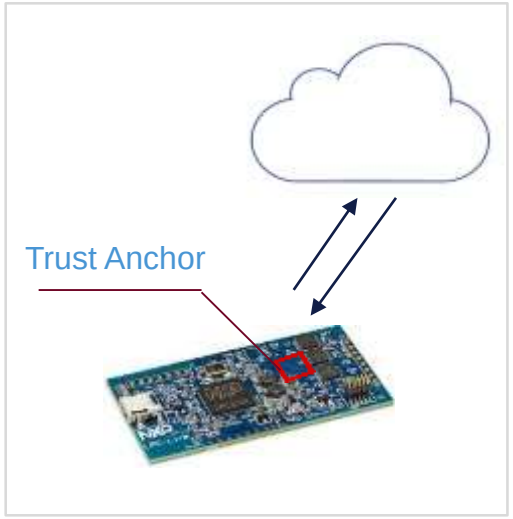
Secure connection to multiple Cloud services and devices

Secure sensing and actuation

Functionality typical to Trusted Platform Modules, such as remote SW attestation

EdgeLock SE050 is a certified and unique security solution

- Security Certification
  - Common Criteria, EAL6+ certified (HW and OS)
- Root of Trust credentials pre-injection in certified infrastructure
- Flexibility with configurable access control and large memory
- Performance with support of long key lengths and expanded ECC curve set
- Easy of deployment of security



EdgeLock SE050 Plug & Trust

Illustration of SE050 use cases across

different IoT application examples

EdgeLock SE050 for Industry 4.0

To protect integrity of Industrial infrastructures, SE050

- Secures device manufacturing and supply chain
- Supports access control management
- And provides with reliable traceability and trusted sensing capability

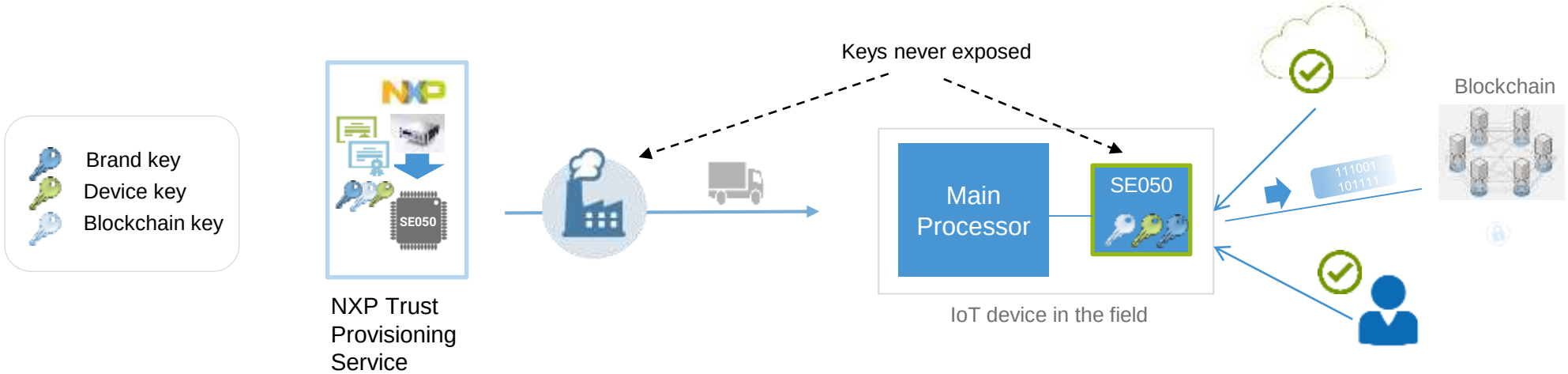
Traceability emerge as priority across the Industry

- Supply Networks are seen as a growing risk in Industrial
  - Untrusted manufacturing
  - Device credentials and SW exposed during manufacturing
  - Counterfeit products = reliability issue
    - Trojan horse into infrastructure
    - Low performance and quality
    - Warranty cost
- Infrastructure owners need to control their assets
  - Which devices are attached (origin, HW/SW state, history)
  - Log commissioning events

EdgeLock SE050 secures manufacturing & enable traceability

Use SE050 to

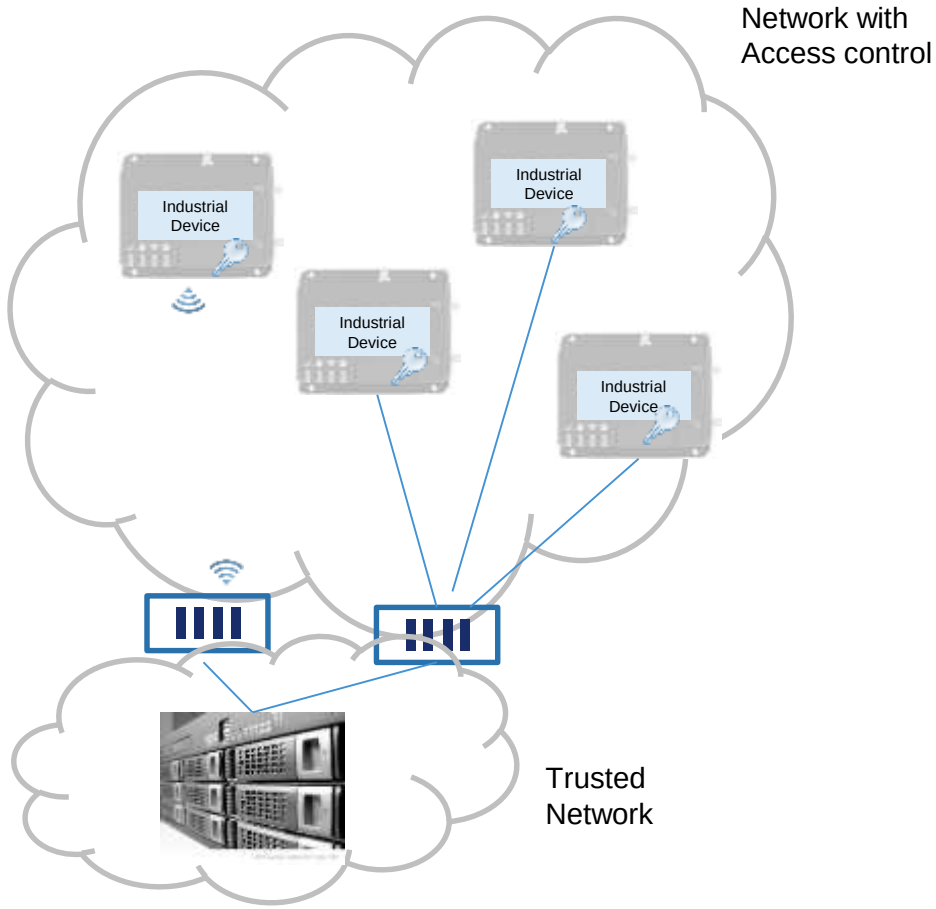
- Authenticate device vendor origin
- Make sure device credentials are never exposed in manufacturing and throughout supply chain
- Attest the SW running on a device when connected in the infrastructure
- Log install & commissioning events into Blockchains for traceability



EMS = Electronic Manufacturing Service

Controlled Access to Industrial Networks

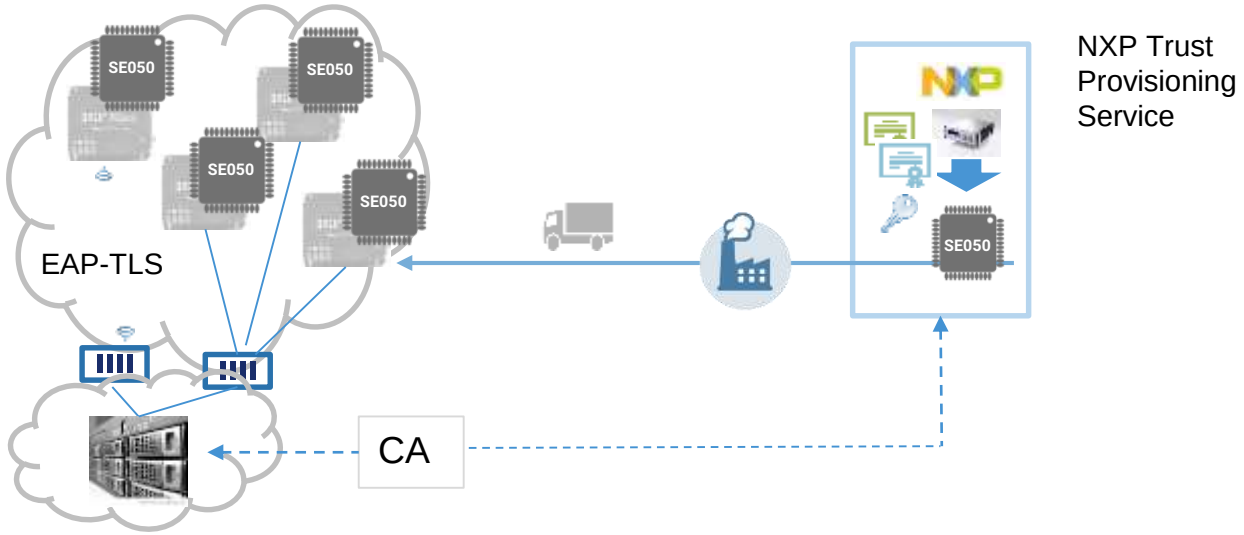
- Industrial networks can be very sensitive and require access control
- Example illustrates 802.1X infrastructure with authentication based on EAP-TLS
- This protocol allows to authenticate each device separately and set up a specific key for data exchange
- A central server authenticates and authorizes devices to join network
- It requires a key management infrastructure



EdgeLock SE050 secures access to networks

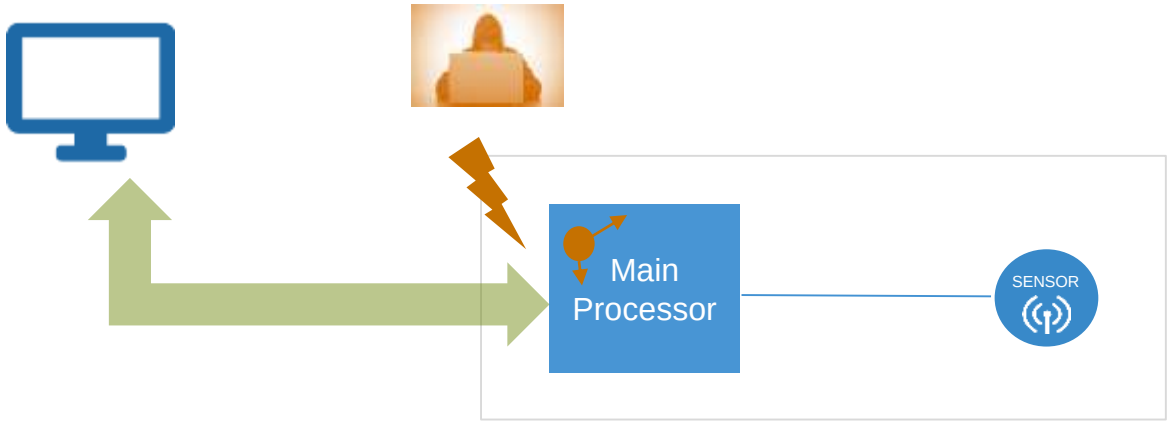
Use SE050 to

- Implement EAP-TLS protocol
- Pre-provision in the device keys and certificates, as well as certification authority certificates (before commissioning)
- Easily comply to IEC 62443 security requirements and achieve SL3
- Support OPC-UA standard

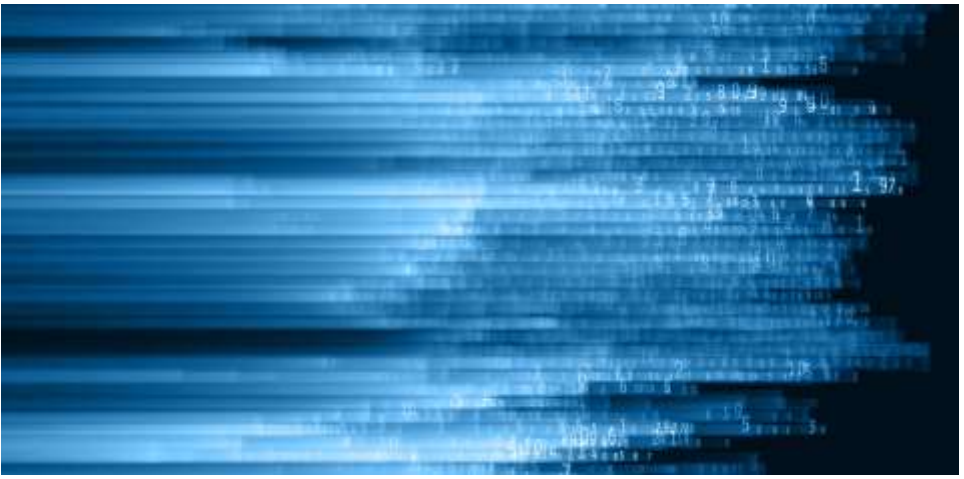


Data collection in Industrial systems is critical

- Data from some sensors distributed across an industrial infrastructure can be extremely critical
- This data could reflect the state of actuators or monitoring a system or process
- Sensor platforms are however prone to (remote) attacks compromising integrity of their SW
- This results in possible data manipulation



EdgeLock SE050 enables secure sensing

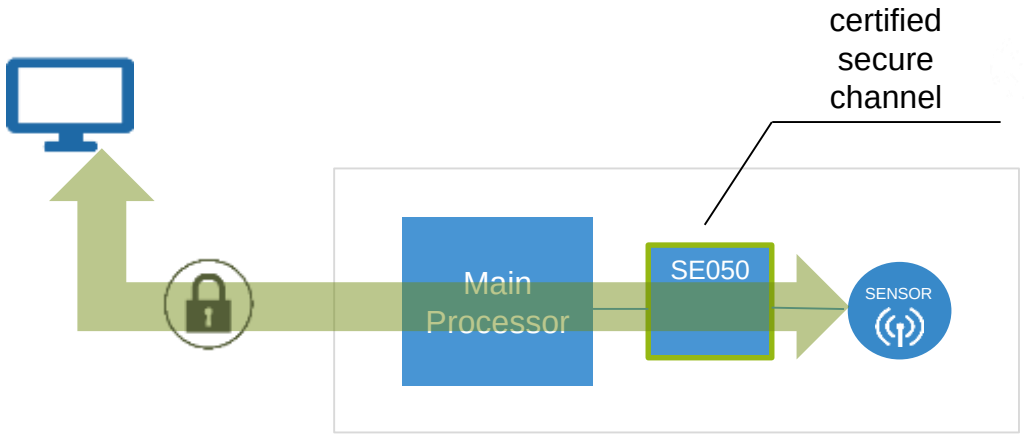


Use SE050 to

Set up a secure, end-to-end connection

from sensor or actuator

to local gateway or cloud based service



- SE050 is directly connected to the critical sensor
- Proof of Origin: SE050 authenticates the sensor
- Local Encryption: SE050 encrypts and signs the sensor data by default before forwarding it

EdgeLock SE050 for Smart Cities

SE050 provides with the necessary trust, adaptability and scalability to support deployment of Services leveraging IoT:

- Secure multi-cloud connectivity
- High performance versatile cryptography
- Secure service transactions

EdgeLock SE050 supports 4k crypto for IP cameras

Use SE050 to

- Generate signatures on video stream (up to 4k RSA)
- Set up secure TLS and SSH connections
- Secure Apps running on the IPcam platform
- Set configuration parameters in the camera, before commissioning and without powering the device

Secure access of IPcam to multiple servers, such as
- Time/timestamp Server
- Supervisory station
- Directory server

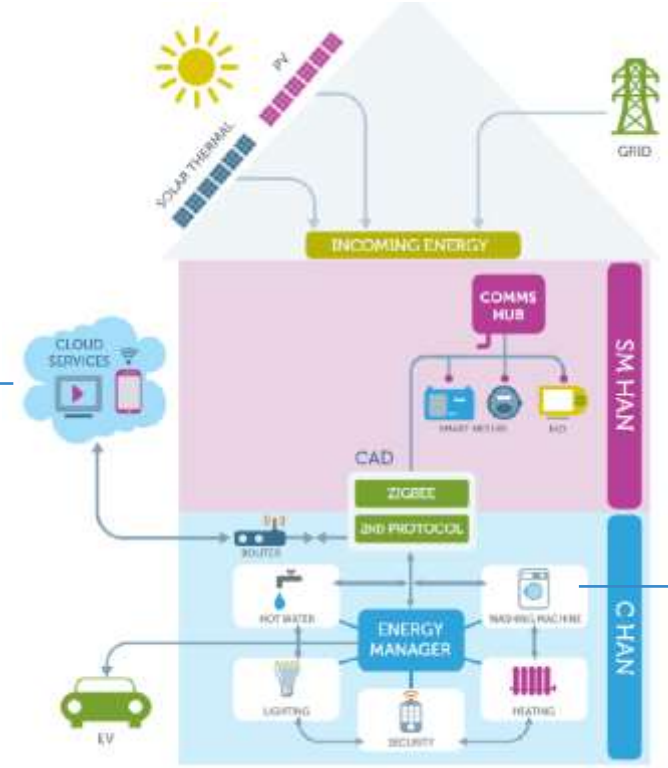
Authenticate video stream for integrity protection

Provide secure key store to other Apps running on the camera platform

EdgeLock SE050 securely bridges energy ecosystems

Use SE050 to

- Seamless connect to service operators hosted on private or Public Clouds (including AWS, Watson IoT, Azure or Google GCP)
- Manage charging transactions and billing to various operators



Use SE050 to

Zero-touch connect to Smart Grid and energy retailers

Use SE050 to

Authenticate towards home/external devices.

SE050 supports to OCF security

EdgeLock SE050 for Smart Home

SE050 brings

- To consumers the protection of their Privacy & assets
- While at the same time providing home appliance OEMs with protection of their return on investment in connectivity

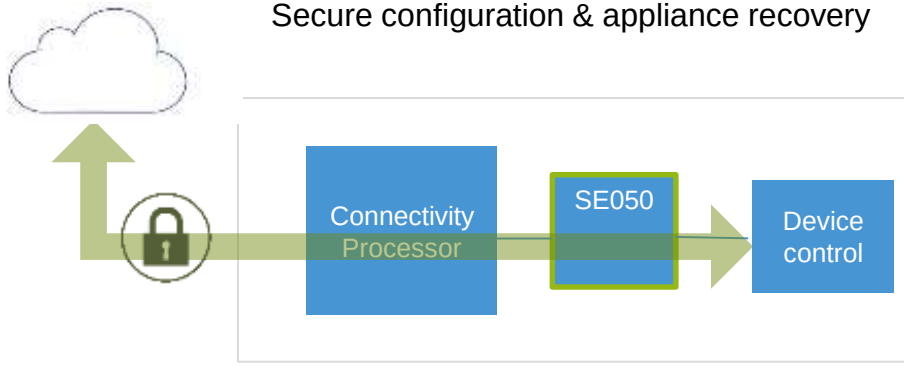
EdgeLock SE050 secures deployment of connected appliances

Use SE050 to

- Manage connection to WiFi network and WPA2 passphrase for user
- Zero-touch onboard appliance onto Cloud service (TLS connections)
- Issue certificate to connect devices together in the home (local CA)
- Comply with OCF security
- Recover compromised devices leveraging SE050 as secure channel
- Configure zero-power appliance before commissioning

Seamless onboarding on Cloud service

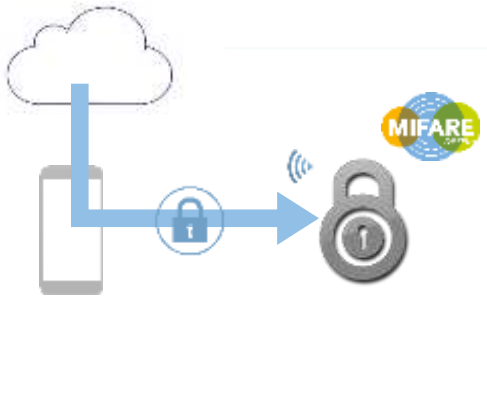
Secure configuration & appliance recovery



EdgeLock SE050 powers Smart Locks

Use SE050 to

- Secure connect smart lock to Cloud services
- Securely manage user credentials
- Encrypt and decrypt lock commands



Enrollment & Pairing

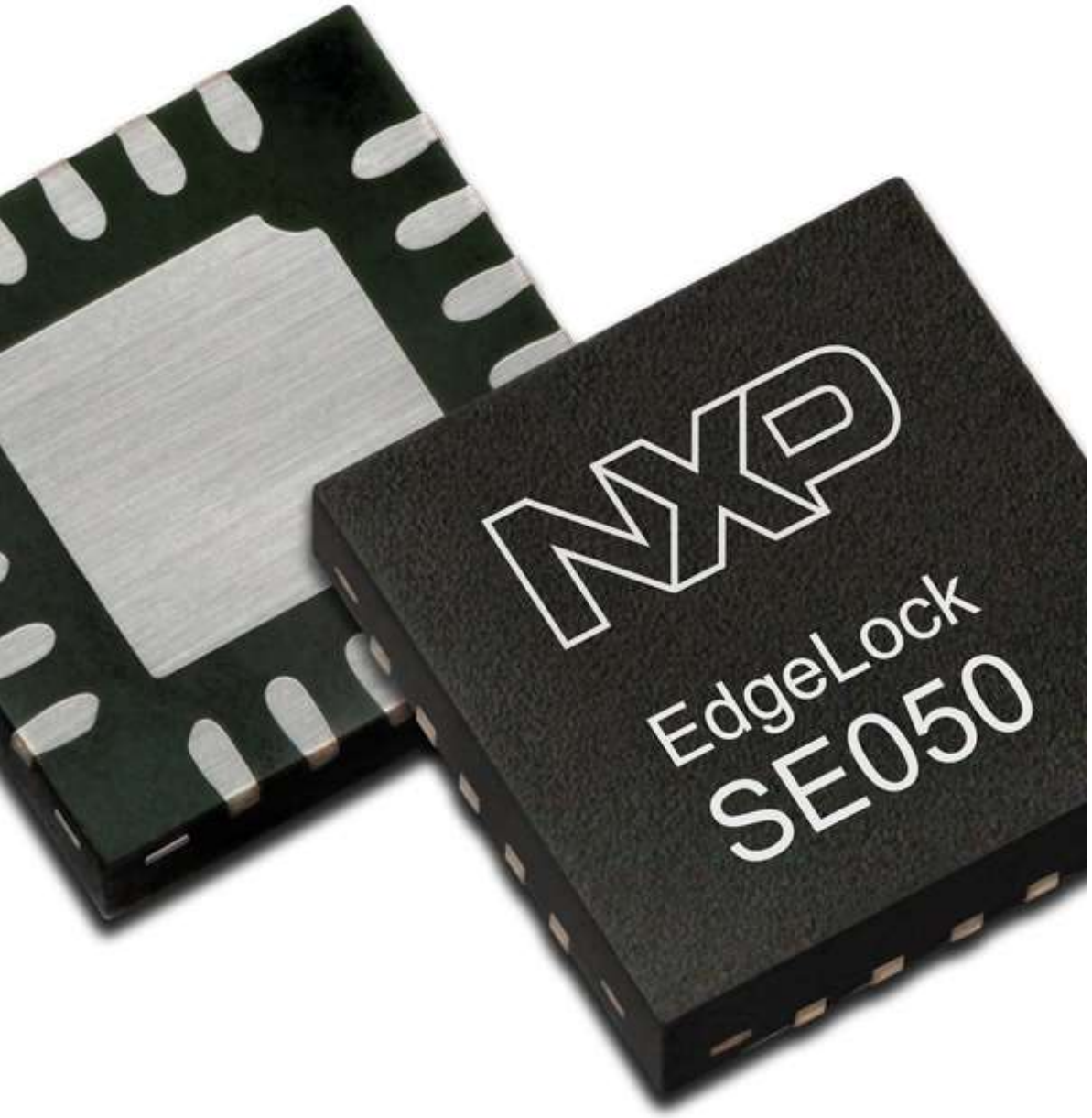
Secure configurations and lock/unlock

Monitoring, alerts and management

EdgeLock SE050 Plug & Trust

A family of Secure Elements to address each & every specific application

in a cost effective way, out-of-the box



EdgeLock SE050 Plug & Trust Key Features

Security

	NXP IntegralSecurity Architecture Certified Common Criteria EAL6+ Secure OS JCOP 4

Secure Storage

User memory	50 kB (Dynamic File system)

Packaging

Package	HX2QFN20 (3x3mm)
Temperature	-25…+85 ºC, -40…+105 ºC

HW/SW Integration

SW	mbedTLS 2.13.1, OpenSSL 1.1, Android Key Master, Windows10 IoT, Amazon FRTOS 1.4.0
Processors	i.MX 6UL, i.MX8, i.MX RT1050, LPC55s, K64F, Hikey 960

Cloud Integration

SE050 A/B/C	Work with Azure, AWS, Watson IoT, Google Cloud Platform

Microsoft Azure · amazon webservices · IBM Watson · Google Cloud Platform

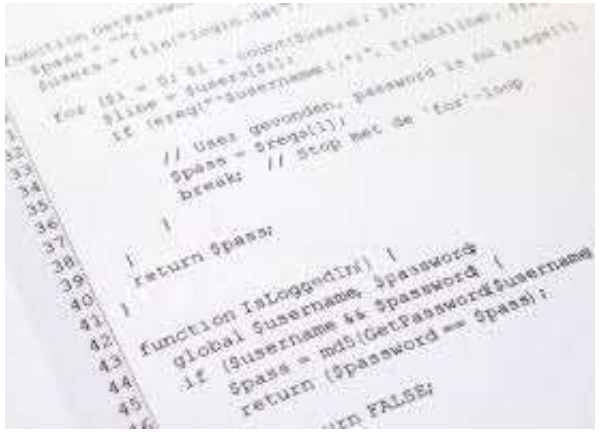
EdgeLock SE050 Plug & Trust Family

	 SE050A	 SE050B	 SE050C
Crypto support			
ECC algorithms	ECDSA, ECDH(E)	-	ECDSA, ECDH(E), EDDSA, ECDAA, ED25519
ECC curves	NIST P-192/224/256/384/521 BrainPool 160/192/224/256/320/384/512 Koblitz Secp160k1/192k1/224k1/256k1	-	NIST P-192/224/256/384/521 BrainPool 160/192/224/256/320/384/512 Koblitz Secp160k1/192k1/224k1/256k1 Curve25519, ECC_BN_P256
Hashing	SHA1, SHA224/256/384/512	SHA1, SHA224/256/384/512	SHA1, SHA224/256/384/512
RSA	-	Encrypt/Decrypt/Sign/Verify 1024-2048-3072-4096 bits	Encrypt/Decrypt/Sign/Verify 1024-2048-3072-4096 bits
Symmetric encryption	AES 128/192/256, (T)DES	AES 128/192/256, (T)DES	AES 128/192/256, (T)DES
MAC	HMAC, CMAC	HMAC, CMAC	HMAC, CMAC
KDF	TLS-PSK, WiFi WPA2	TLS-PSK, WiFi WPA2	TLS-PSK, WiFi WPA2, OPC-UA, MIFARE
Interfaces			
	Host I^2C plain/encrypted - 3.4Mbpcs	Host I^2C plain/encrypted - 3.4Mbpcs	Host I^2C plain/encrypted - 3.4Mbpcs Secondary I^2C Master – 400kbps contactless ISO14443
Root of Trust credentials			
	NXP Proof of Origin Key/certificate	NXP Proof of Origin Key/certificate	NXP Proof of Origin Key/certificate Key Attestation certificate Cloud connection keys/certificates Ready-to-use RSA 4k key sets

EdgeLock SE050 Plug & Trust: Product support Package

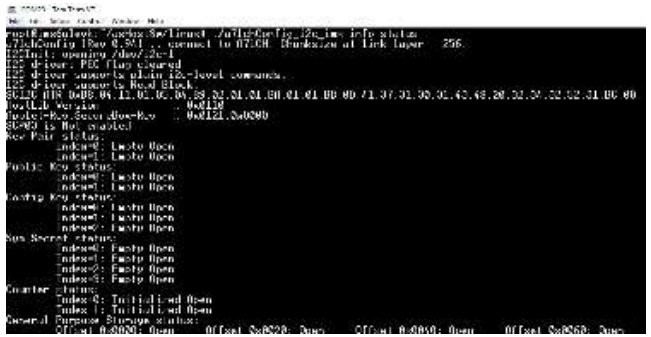
SE050 development boards

SE050 Host software package



AppNotes,Webinars,Videos,Community

SE050 Configure tool



SE050 Demo Framework

SE050 API usage examples

SECURE CONNECTIONS
FOR A SMARTER WORLD