

EdgeLock™ SE050: NXP's new generation Plug & Trust solution to secure IoT Edge

Matthias Michael VIERTLER

Technical Support SAPAC
IoT Security

July 2019 | Session NXP TechDay



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

Why a Secure Element (SE) in IoT?



IoT ecosystem

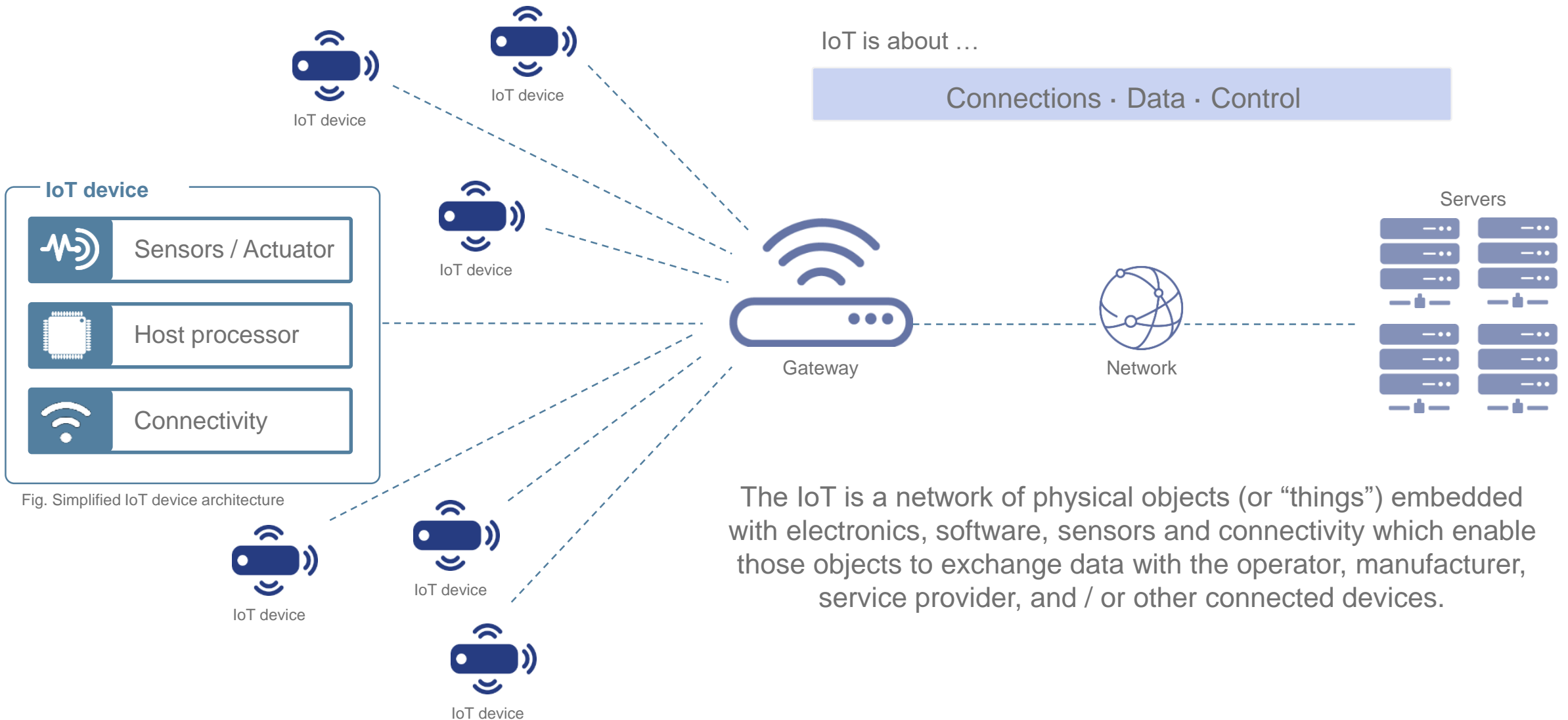


Fig. Simplified IoT device architecture

The IoT is a network of physical objects (or “things”) embedded with electronics, software, sensors and connectivity which enable those objects to exchange data with the operator, manufacturer, service provider, and / or other connected devices.

IoT devices are vulnerable to security threats

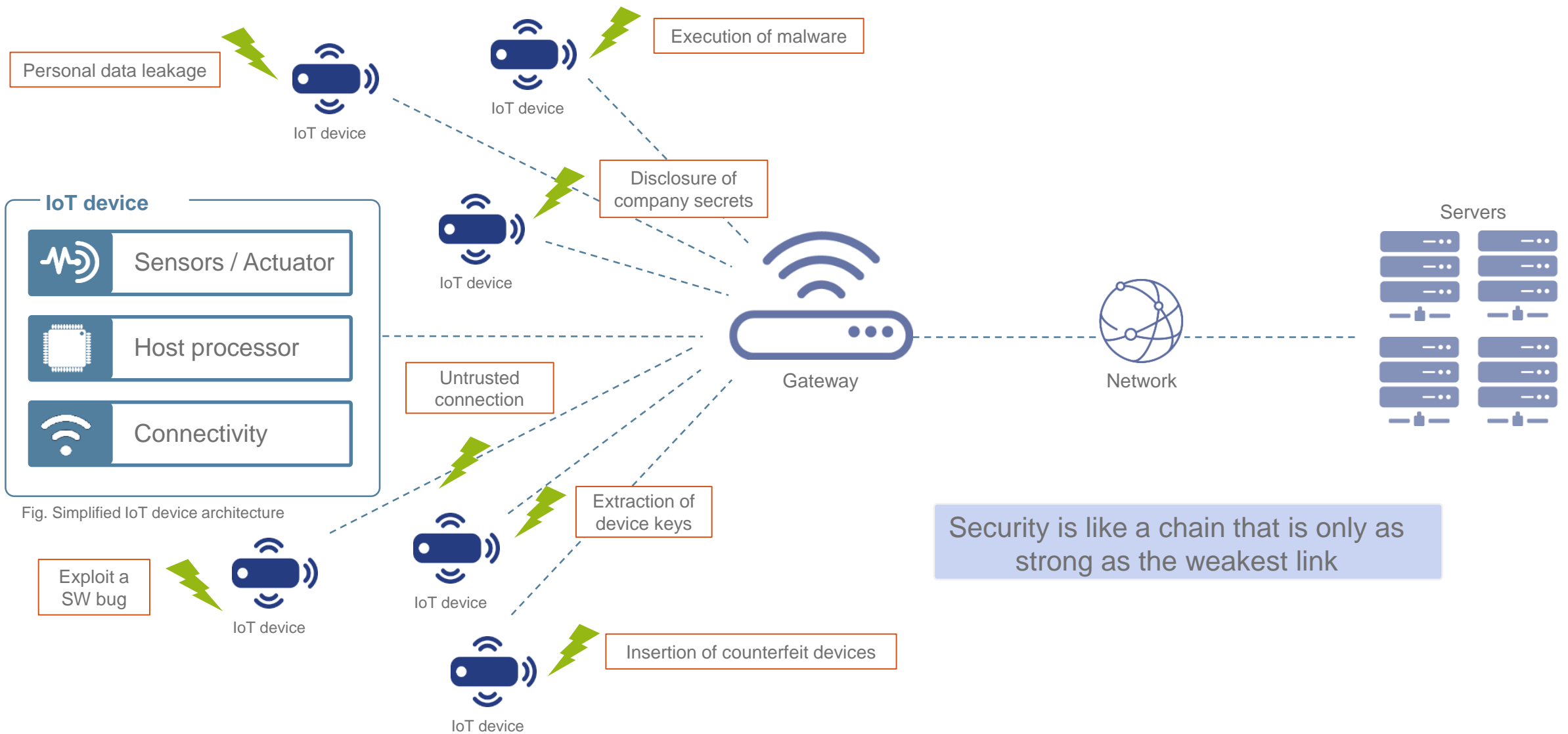


Fig. Simplified IoT device architecture

Security is like a chain that is only as strong as the weakest link

IoT devices must follow a secure-by-design approach

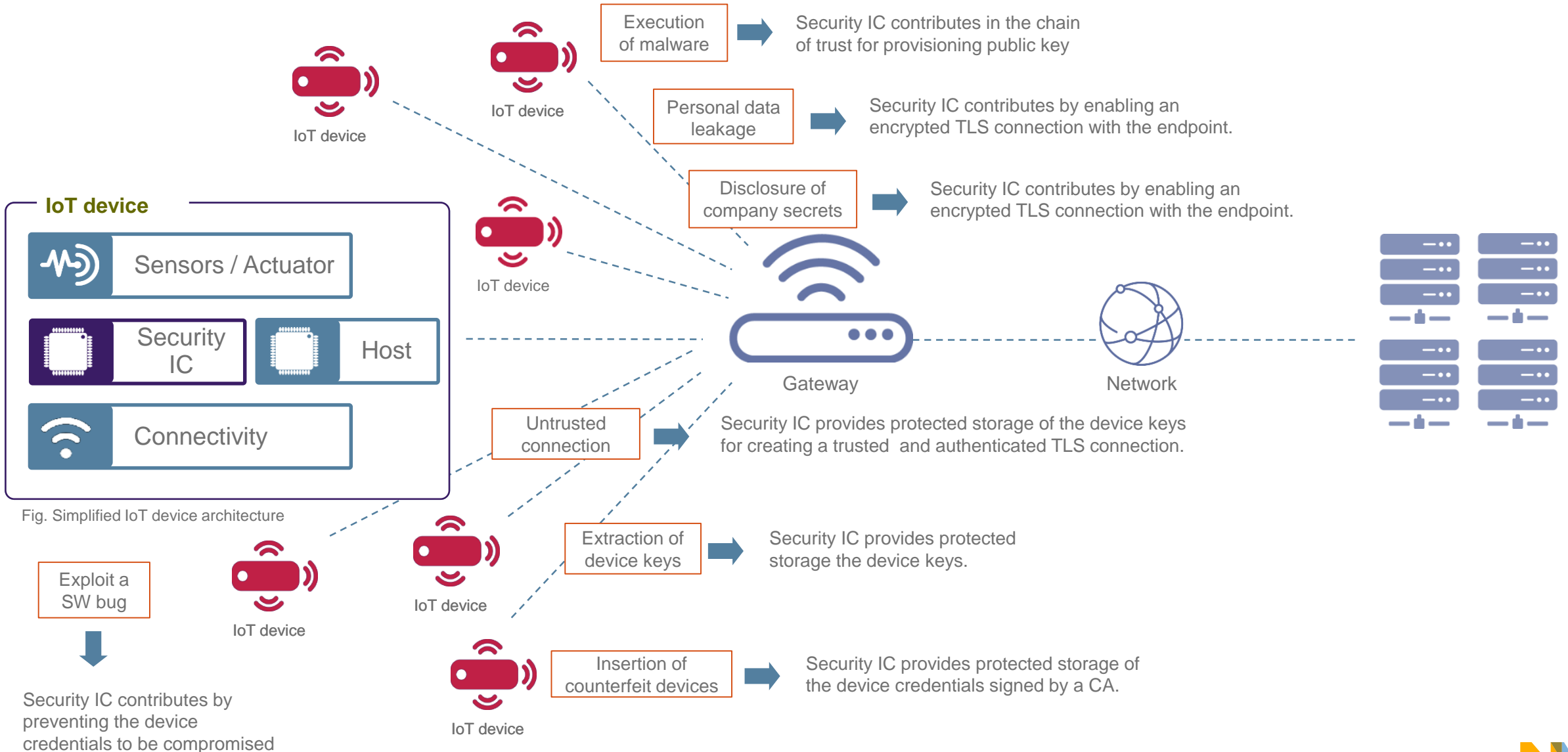


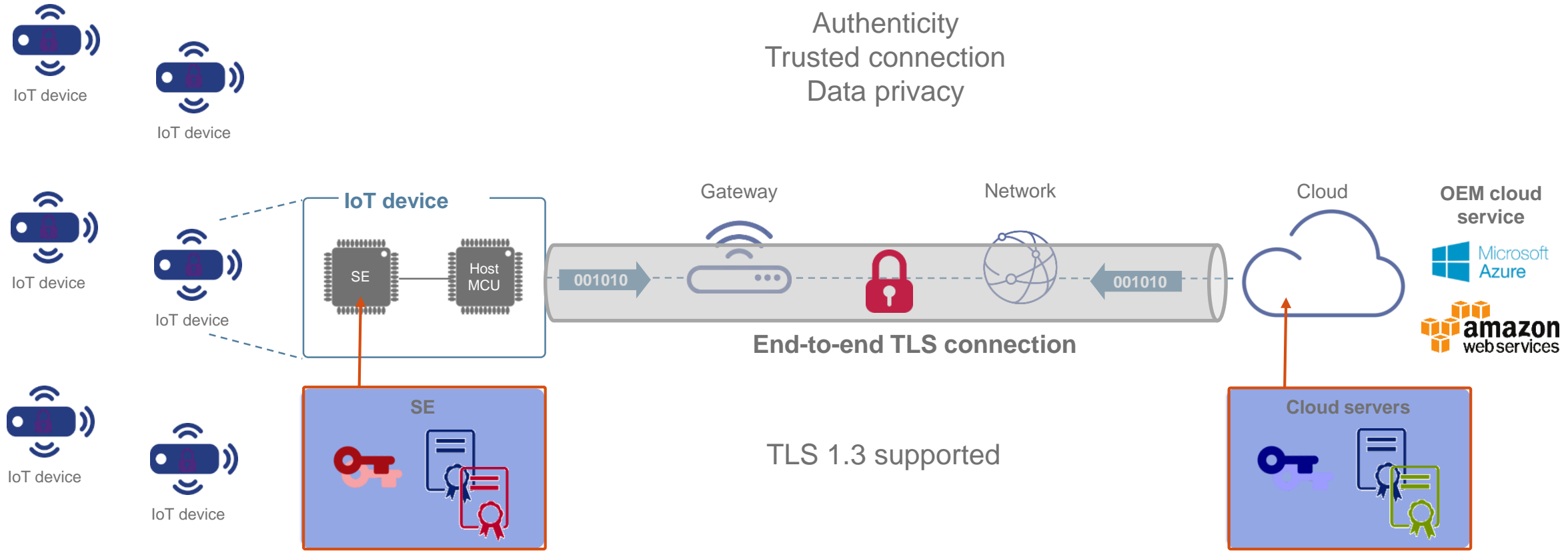
Fig. Simplified IoT device architecture



EdgeLock SE050 Plug & Trust

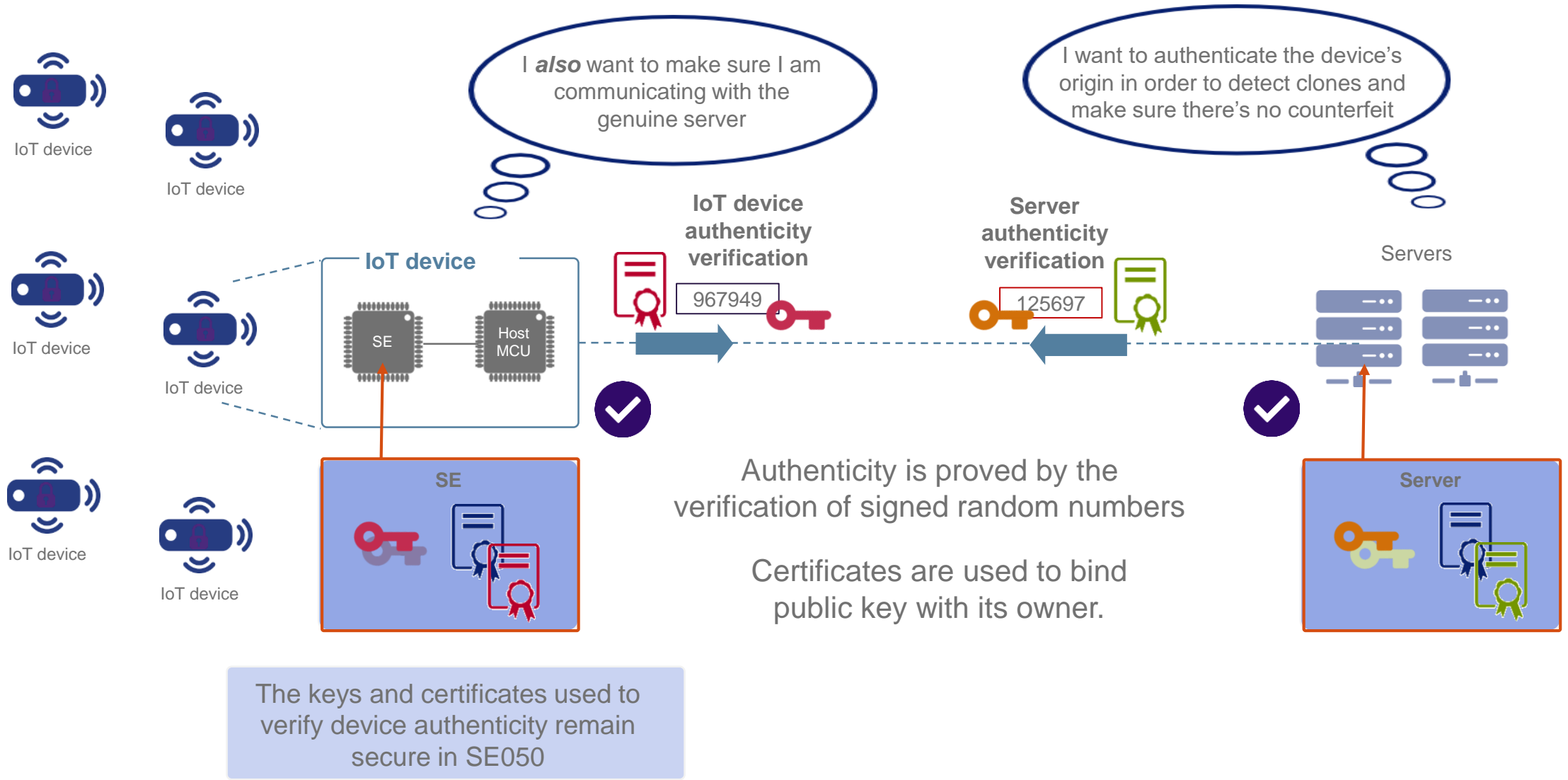
Introducing NXP's Secure Element solution for the IoT market

SE050 for secure connection to public or private clouds

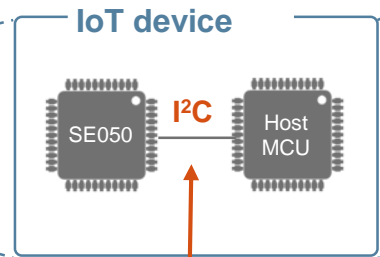
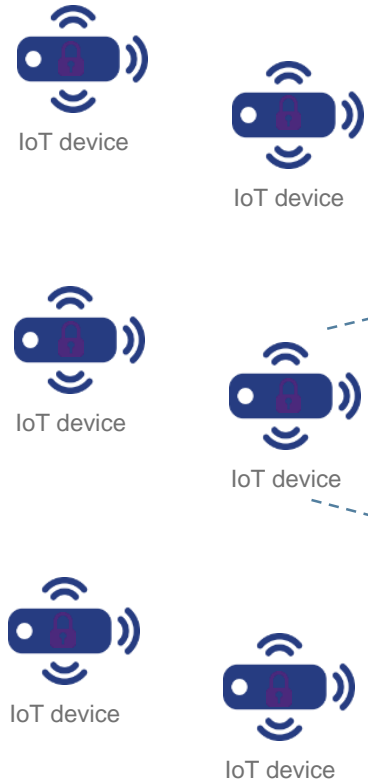


The keys and certificates used to authenticate the cloud connection remain secure in SE050

SE050 for device proof of origin / anti-counterfeit



SE050 for encrypted / authenticated interface to host processor



Host interface

SE050 provides the option to bind the Host processor to the security IC by configuring it to use an SCP03 channel. SCP03 is not mandatory in usual use cases

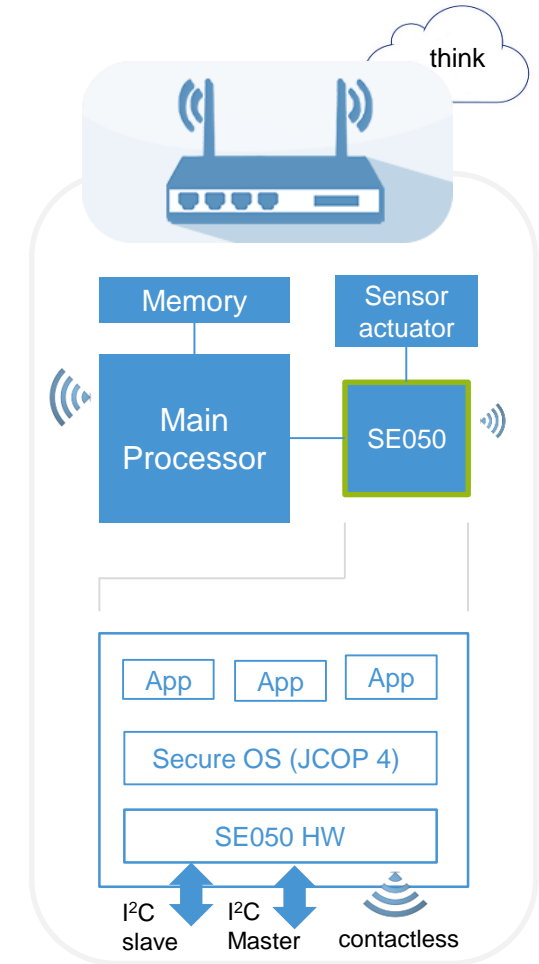
Setting up the SCP03 channel requires 3 128-bit AES keys (both on Host and SE050 side).



When using SCP03, Host processor and SE050 are mutually authenticated

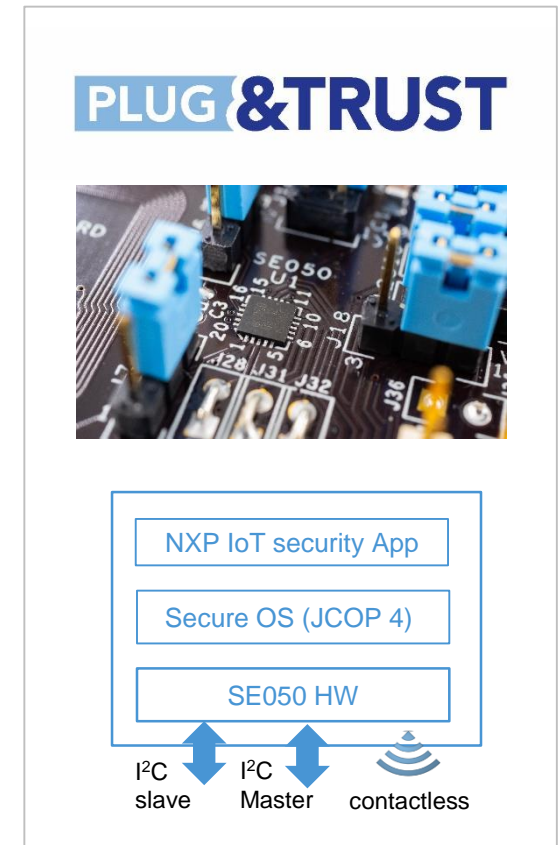
NXP introduces EdgeLock SE050, a Trust Anchor for IoT...

- 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)

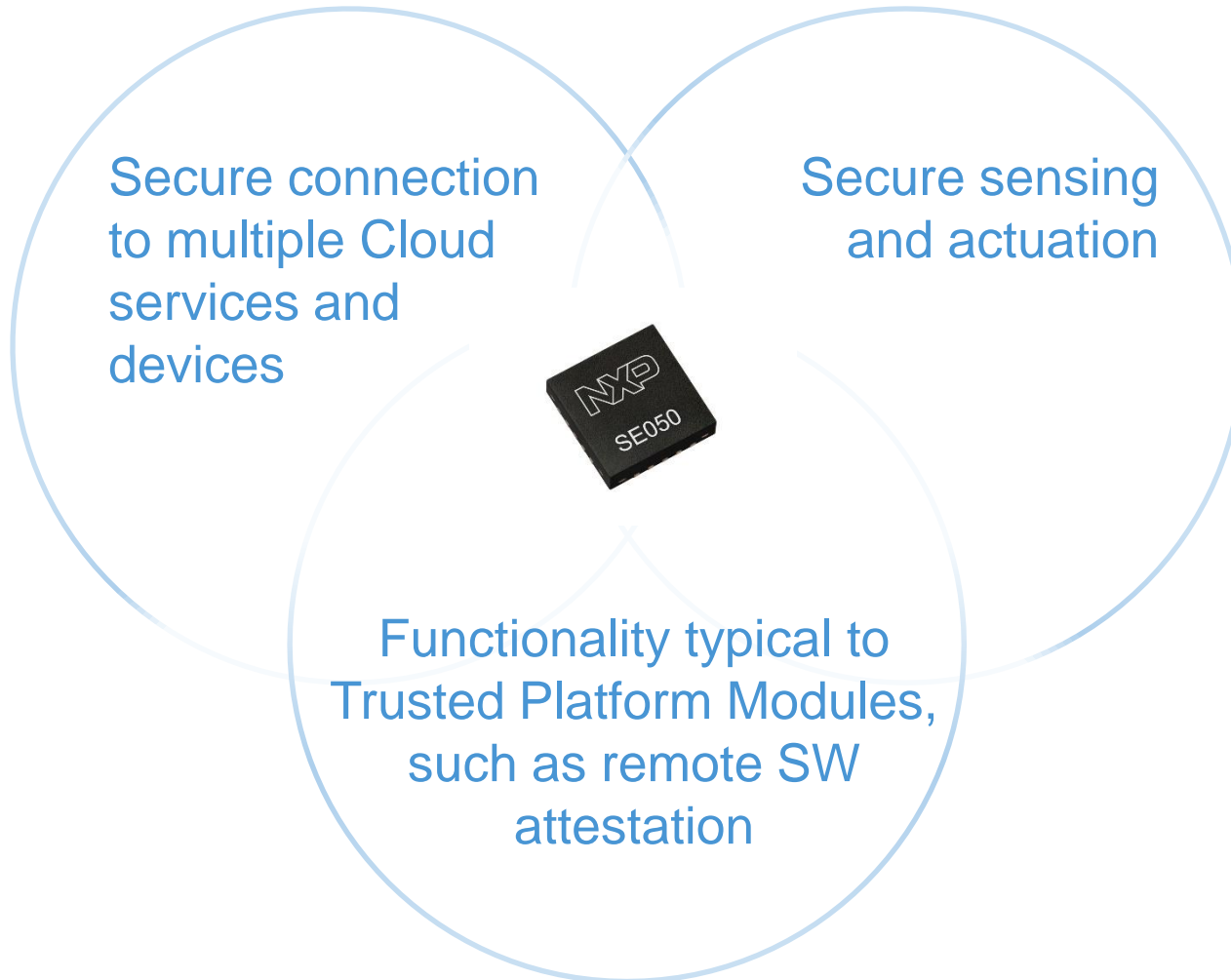


...EdgeLock SE050 Plug & Trust for out-of-the-box solutions

- 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

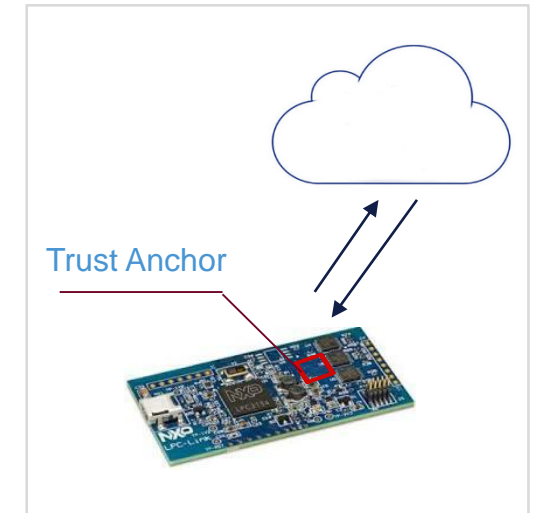


EdgeLock SE050 Plug & Trust is a convergence IoT product



EdgeLock SE050 is a certified and unique security solution

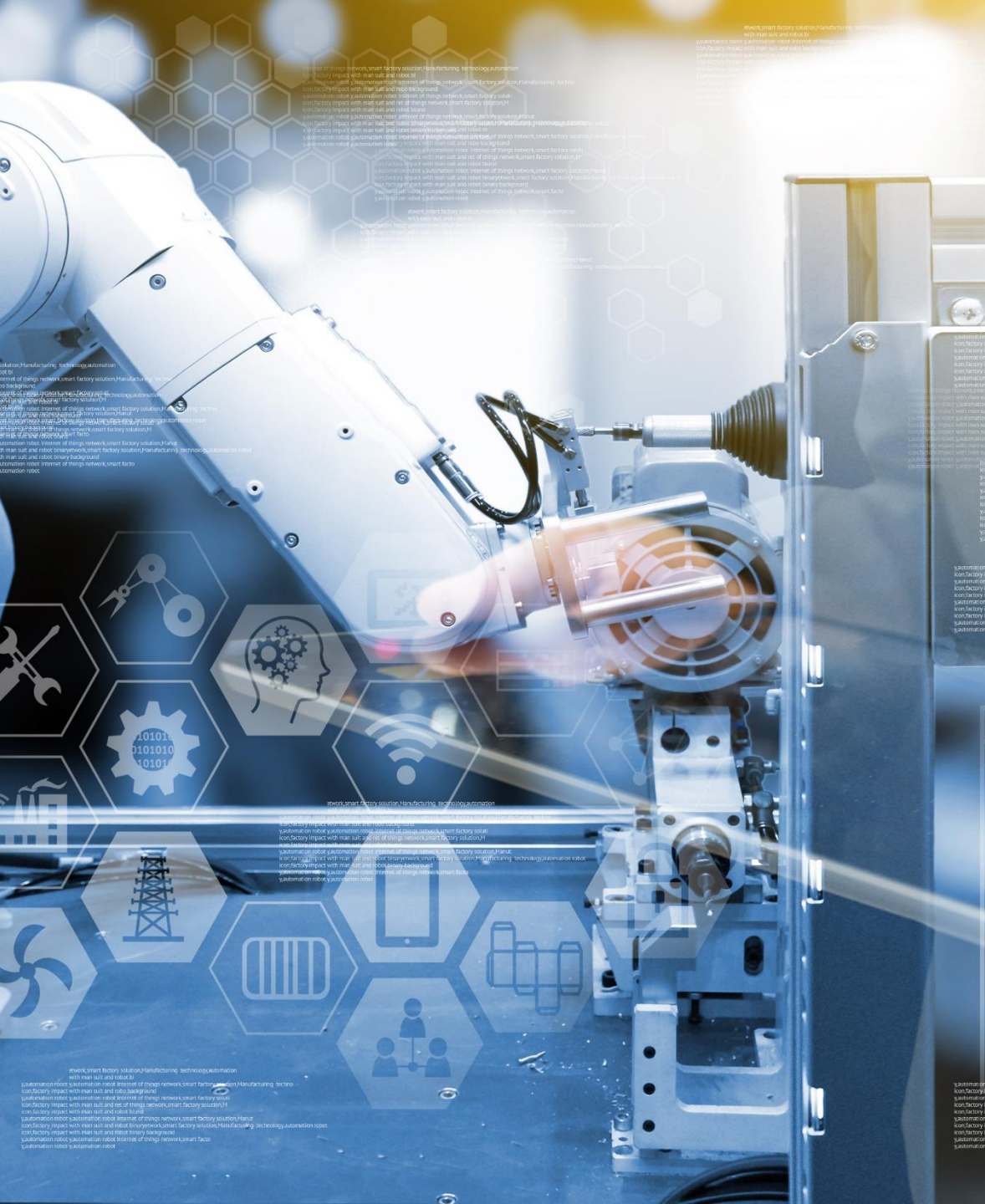
- **Security Certification**
 - Common Criteria, EAL6+ certified (HW and OS)
- **Root of Trust credentials** pre-injection in certified infrastructure
- **Flexibility** with configurable access control and large memory
- **Performance** with support of long key lengths and expanded ECC curve set
- **Easy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

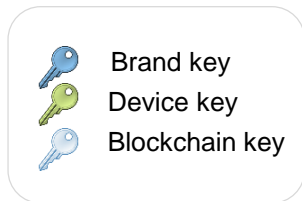


EdgeLock SE050 secures manufacturing & enable traceability

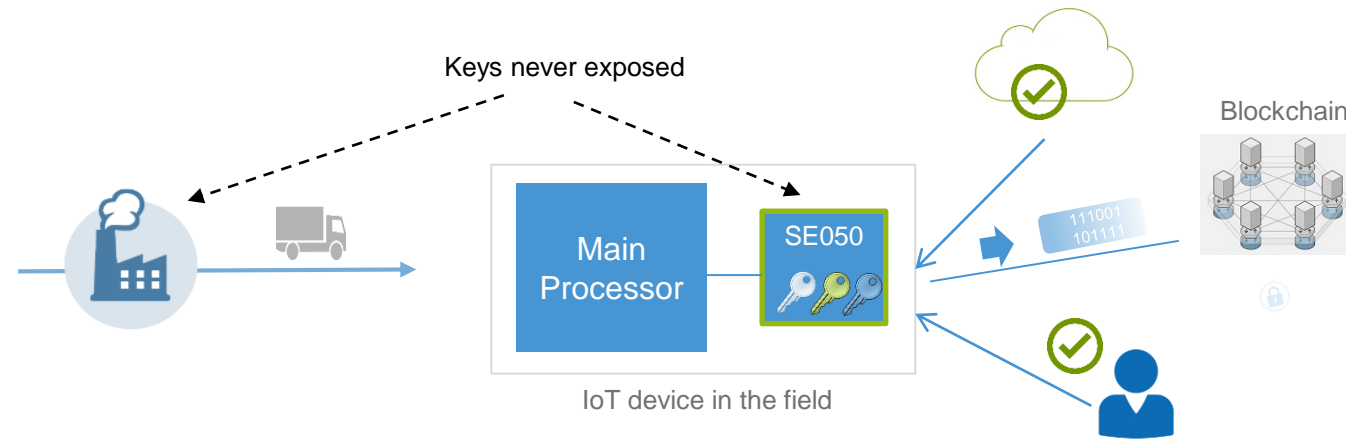


Use SE050 to

- 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 inside Blockchains for traceability

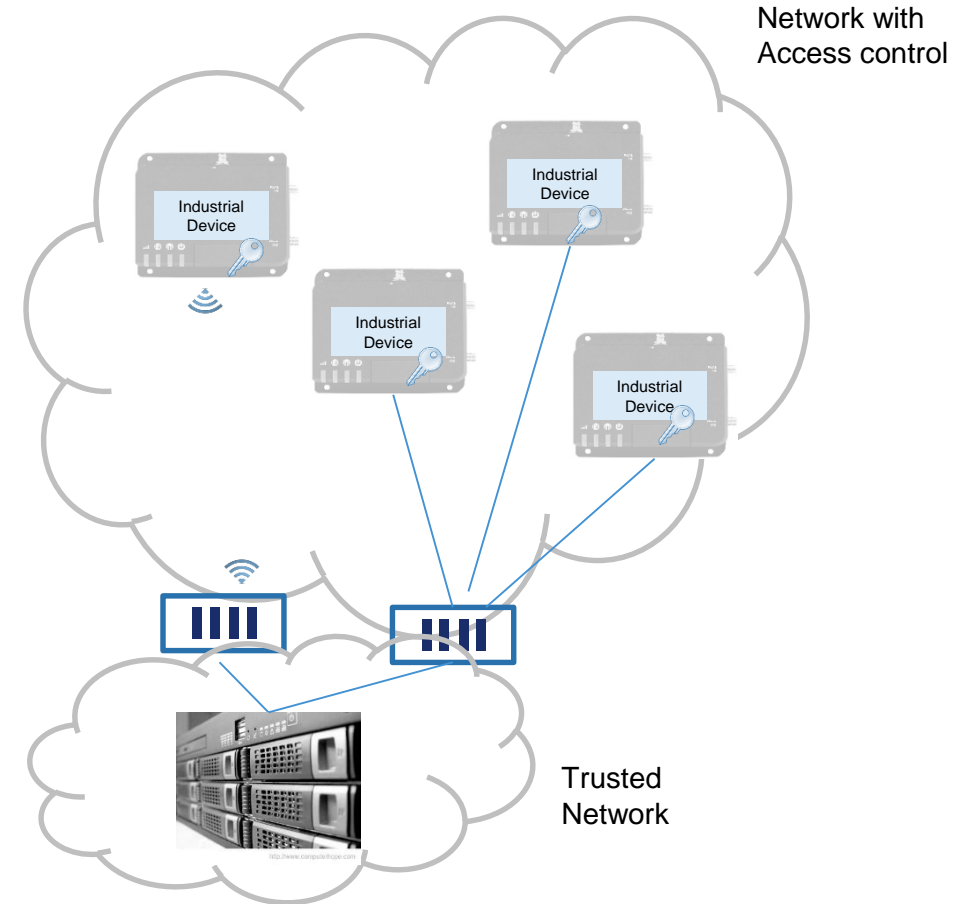


NXP Trust Provisioning Service



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

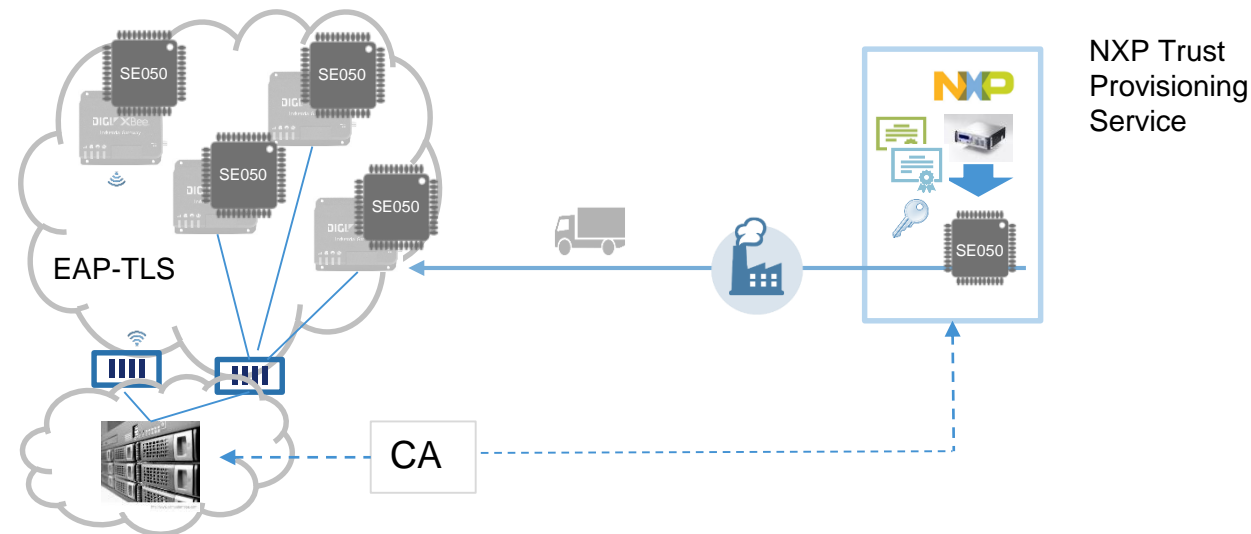


EdgeLock SE050 secures access to networks



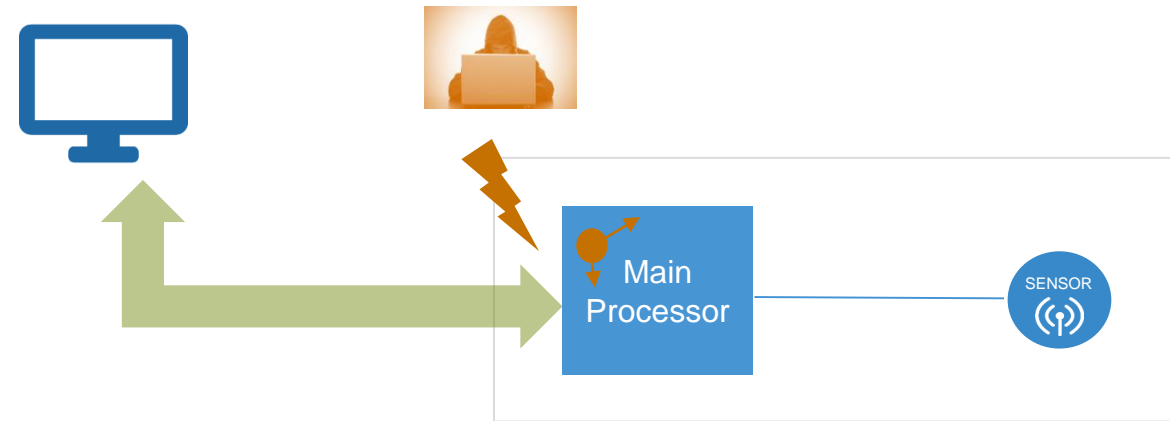
Use SE050 to

- 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

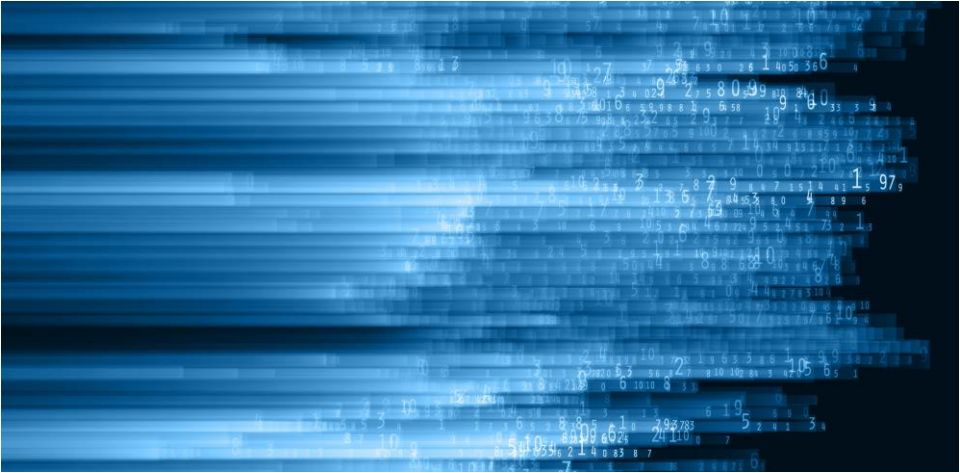


Data collection in Industrial systems is critical

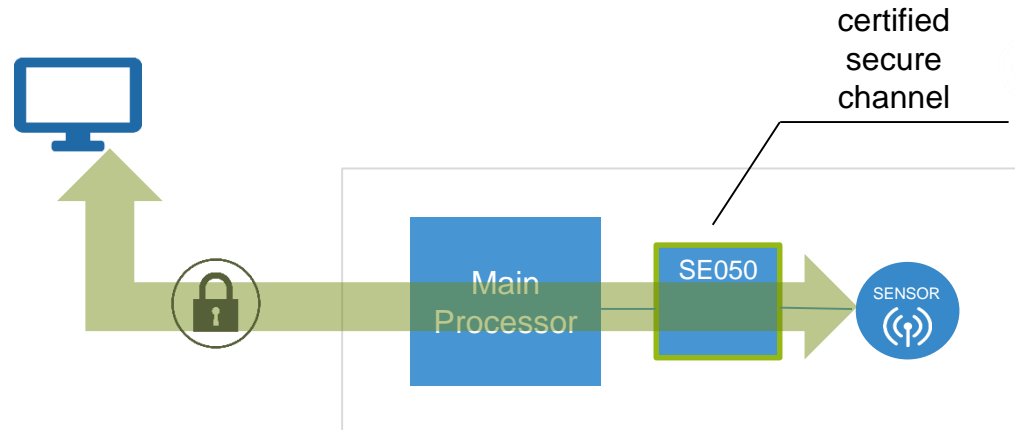
- Data from some sensors distributed across an industrial infrastructure can be extremely critical
- This data could reflect the state of actuators or monitoring a system or process
- Sensor platforms are however prone to (remote) attacks compromising integrity of their SW
- This results in possible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



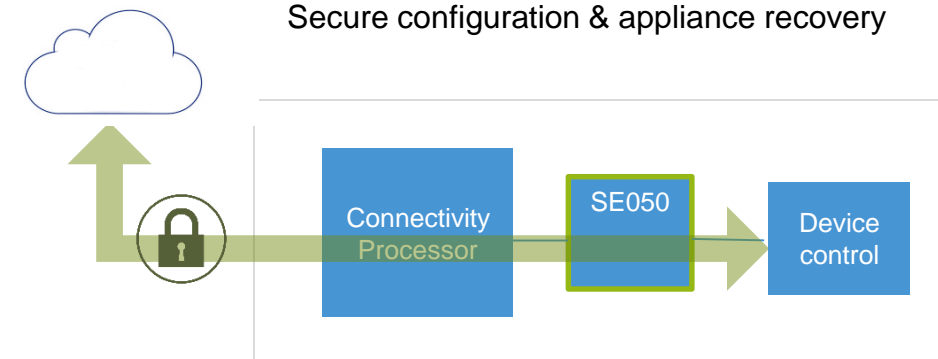
Use SE050 to

- 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

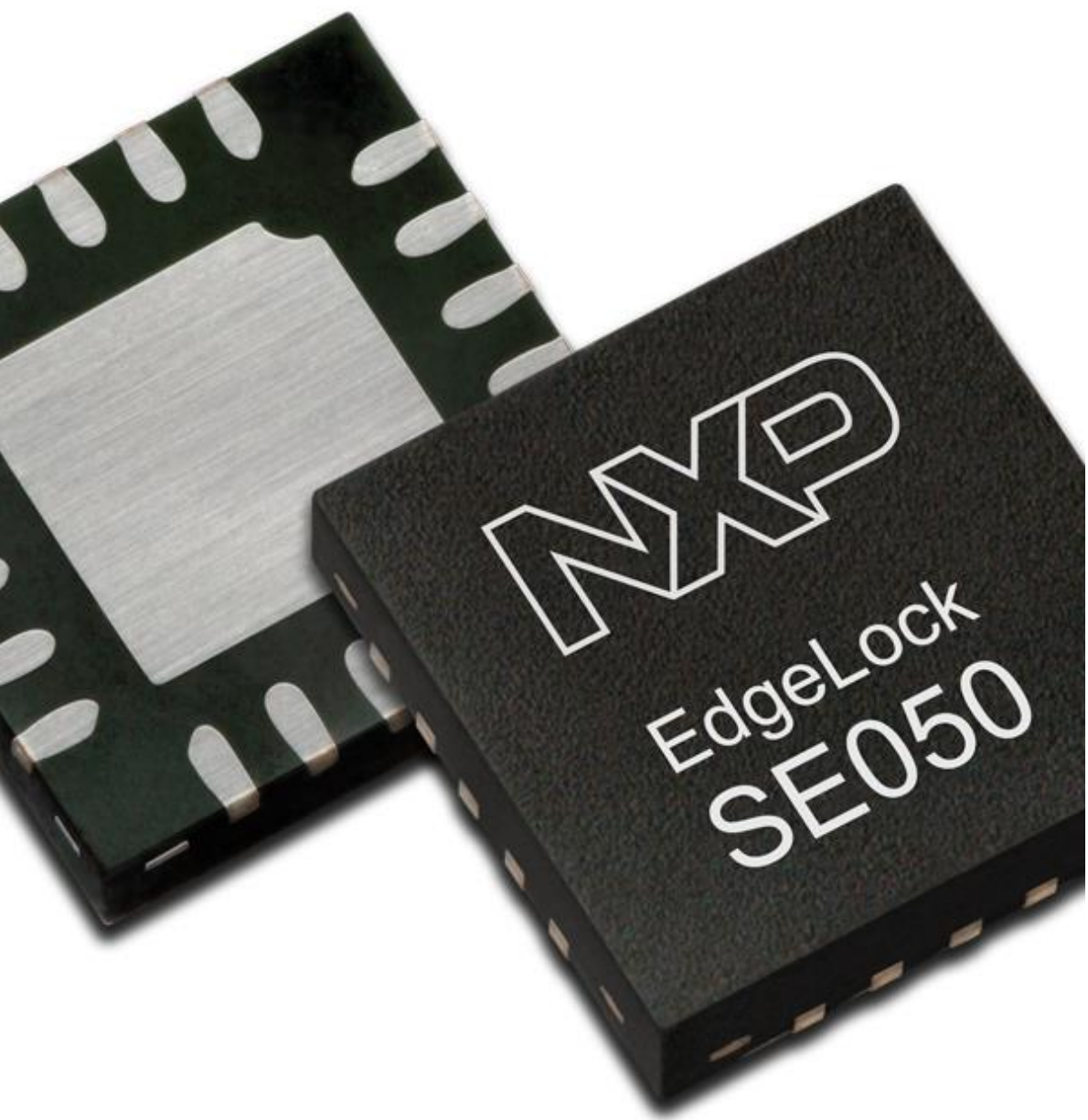
- Securely connect smart lock to Cloud services
- Securely manage user credentials
- Encrypt and decrypt lock commands





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 °C, -40...+105 °C

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



EdgeLock SE050 Plug & Trust Family



SE050A



SE050B



SE050C

Crypto support

ECC algorithms	ECDSA, ECDH(E)	-	ECDSA, ECDH(E), EDDSA, ECDA, 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 ² C plain/encrypted - 3.4Mbps	Host I ² C plain/encrypted - 3.4Mbps	Host I ² C plain/encrypted - 3.4Mbps Secondary I ² C 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
-------------------------------------	-------------------------------------	--



PLUG & TRUST

**SECURE CONNECTIONS
FOR A SMARTER WORLD**

BACKUP SLIDES



Securing the Edge – NXP landing page on security

[www.nxp.com/iotsecurity](https://www.nxp.com/applications/solutions/internet-of-things/secure-things/secure-the-edge:IoT)

Check out this page to get an overview on NXP security solutions, links to product pages and application information

Internet of Things > Secure Things > Secure The Edge

SECURE THE EDGE

Scalable solutions for IoT devices

Today's IoT devices must be designed with advanced security technology to protect the integrity and access of the device, as well as the confidentiality, authenticity and availability of their data.

IoT system developers must determine the level of protection needed in order to ensure product compliance with applicable security standards and regulations, as well as product user expectations and company risk management policies to prevent local and remote attacks.

Explore NXP's broad portfolio of scalable security solutions which provide a foundation for achieving the most effective security levels at IoT end nodes and edge nodes, while facilitating their deployment in complex, multi party IoT ecosystems.

IoT security architecture for achieving the highest security

1 Secure Element

2 External Memory

3 Security Hardening and TrustZone

4 Hardware Root of Trust

Hardware Root of Trust

Communications to back end systems for cloud services is rooted in the secure element. No secret data has to be passed between the main applications processor and the secure element as the cryptographic functions are performed in isolation.

[Next element >](#)

SE050C Smart Sensor / GW Use case

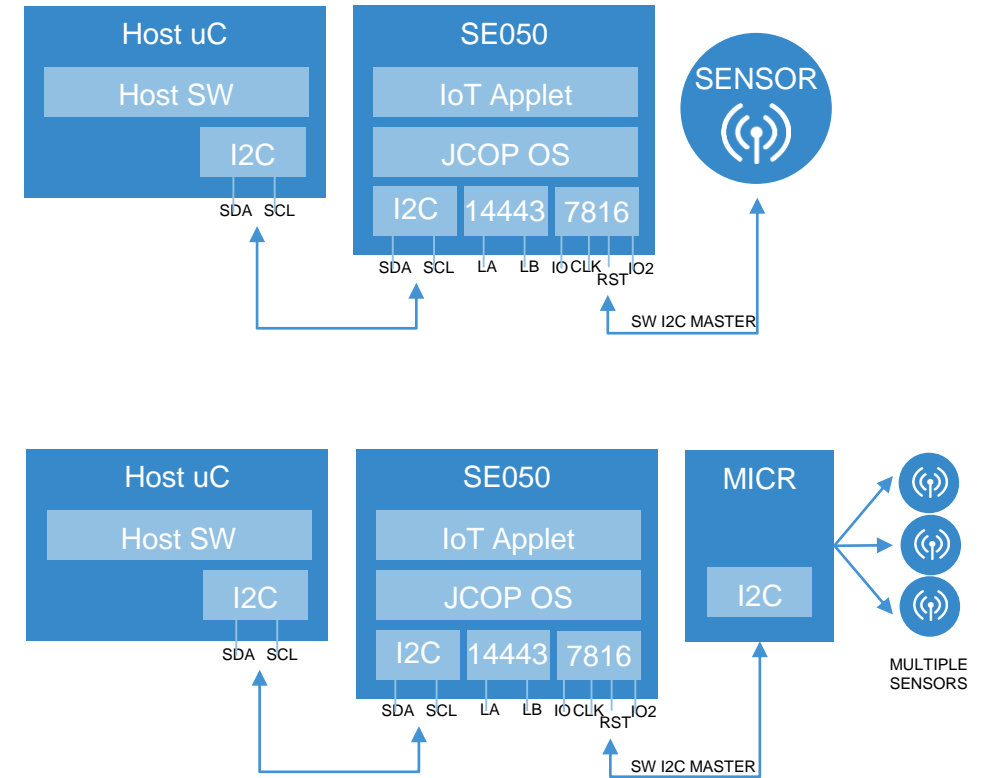
In this use case, the SE050 is connected via I2C Slave interface with a host uC and via an SW emulated I2C master interface with a trusted subsystem such as a mission critical security sensor or a low-end μ C that controls multiple sensors. Sensors will be powered by same source of Host uC or over the supply switch of SE050, depends on the wiring.

SE050 has the task to guarantee the privacy and the authenticity of the data extracted by sensor/ μ C. SE050 can sign and encrypt the data. A server can be sure that the data has been locally generated on the private I2C line to the sensor/ μ C & has full control over it via the SW emulated I2C master interface.

Data collected in the application over the SE050 private sensor can be transferred to the cloud for further treatment and analysis.

Applications

- Smart Energy e.g. Solar – sensors used to detect light
- Access to machines/robots – temperature/pressure sensor
- Sensors in a robot to force immediate stop – multiple sensors used
- User authentication via Pin Pad – temperature/pressure sensor



SE050 Block Chain Use Case

SE050 can support block chain applications with providing a unique identifier.

Unique Device identifier:

Link between the real world asset and references to this real world asset in the transactions in the blocks of the blockchain.

Unique device identifier = SE050 provisioned unique identifier

Secure device identifier:

Link between the real world asset and references to this real world asset in the transactions in the blocks of the blockchain.

Storage of the public-private key pair needed to prove ownership of transactions in blocks in blockchain.

Unique device identifier = SE050 provisioned unique identifier

Device private key \equiv SE050 provisioned private key

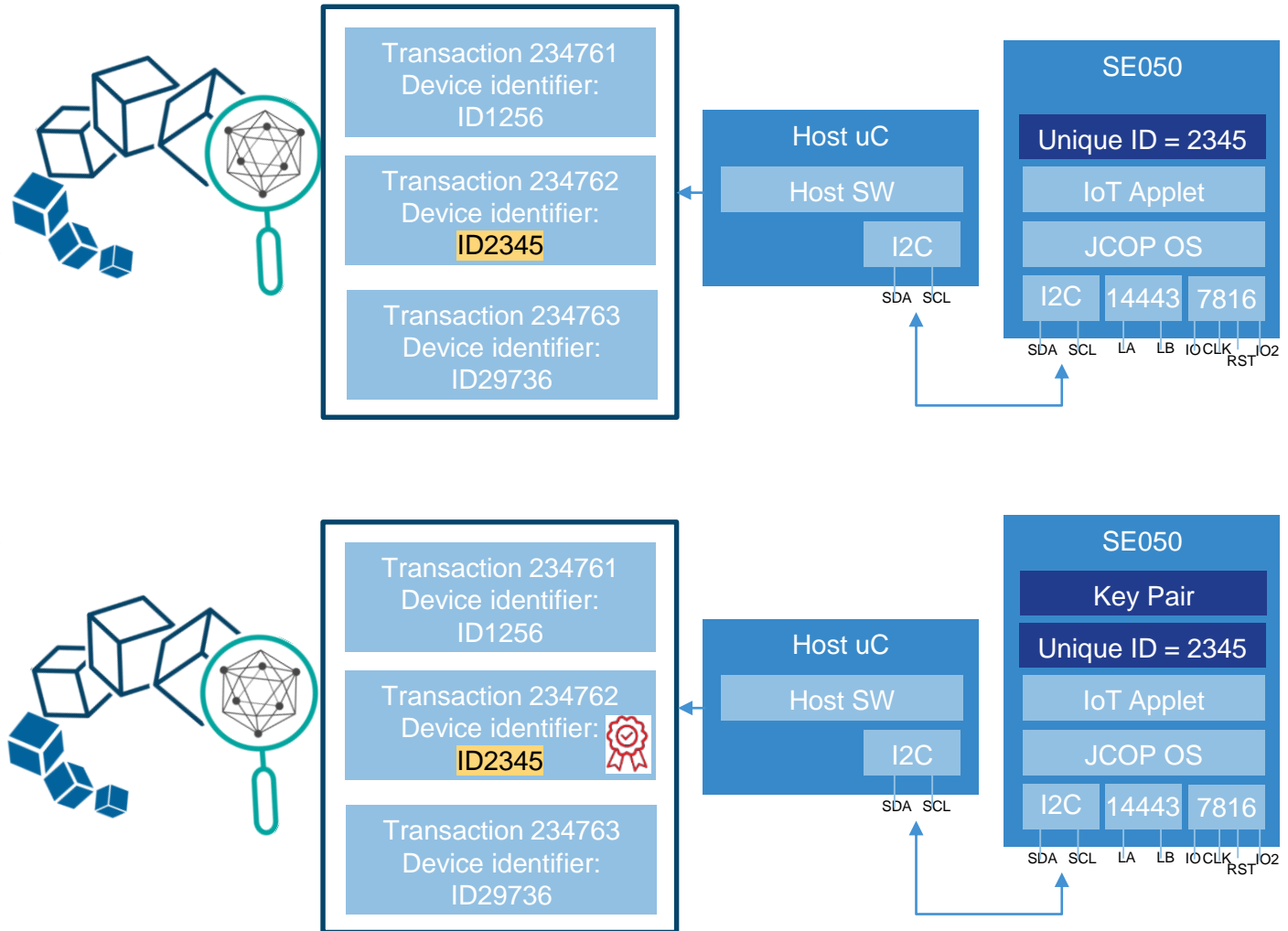
Variant 1: Host prepares transaction request, requires private key from SE050, host signs transaction request

Variant 2: Host prepares transaction record, SE050 signs transaction request using private key

Variant 3: Host presents data to SE050, SE050 prepares transaction request and signs it.

Applications

- Logistic, Smart Contract, Tags



SE050C WiFi Use case

WPA Personal (WPA-PSK):

Wifi password, WPA-PSK preshared key, to be stored secretly in the SE050. This means that the key derivation utilizing that password is fully implemented in the SE050.

SE050 can be used for WPA2 connection setup. For this SE050 supports the PBKDF2 key derivation function

For Wi-Fi, SE050 uses PBKDF2 key derivation function to generate a WiFi Key to connect to the WiFi router. This key is derived from actual WiFi Pass Phrase.

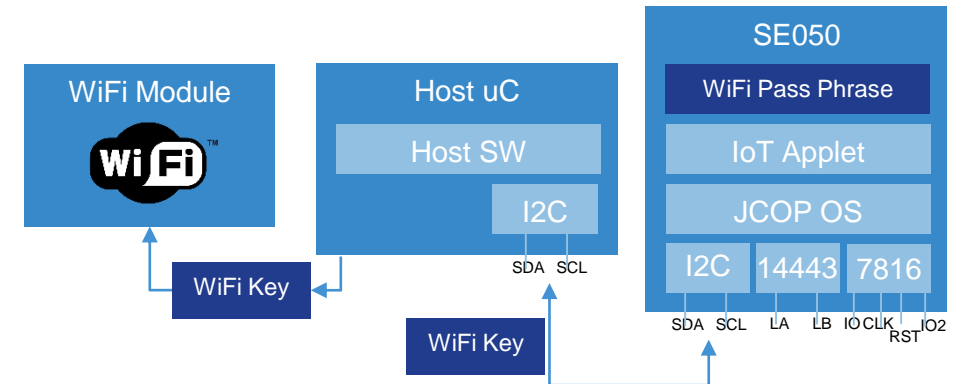
The pre injected passphrase inside the SE050 never leaves the Applet.

WPA Enterprise (EAP-TLS):

Enterprise Wi-Fi authentication is supported through

Applications

- Routers and Gateways using WPA-PSK
- All Wifi security or privacy critical IoT devices connected via Wifi



SE050C Secure Access Module (SAM) Use case

SE050 can be used for secure access together with multiple cards/devices using e.g. MIFARE DESFire protocol. For this SE050 supports the MIFARE key derivation function, DESFire EV2 authentication and session key generation.

Supported Functionality:

A MIFARE application runs on the host microcontroller, SE050 is used to store the MIFARE master key and derive the keys for different users/cards.

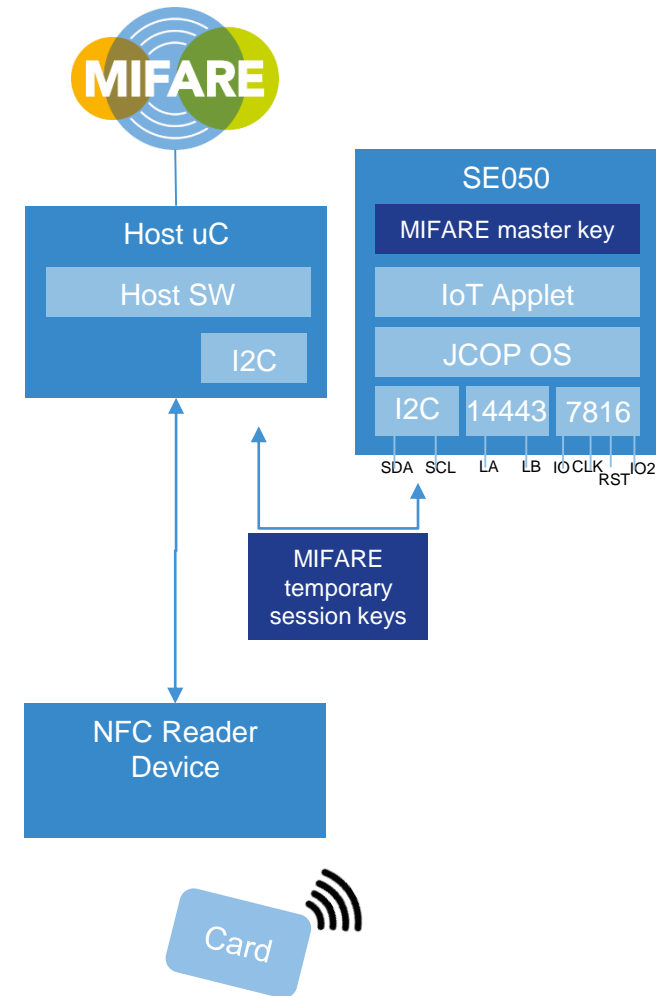
The host uses the SE050 to authenticate the MIFARE DESFIRE EV2 credential and then export the resulting session key into the host. The further standard MIFARE DESFire commands are then handled within the microcontroller knowing the session key.

In case of change key command the SE050 supports again as here knowledge of the card keys is needed.

NFC reader products are recommended for ease of design in, new installations latest DESFire (AV2 or newer).

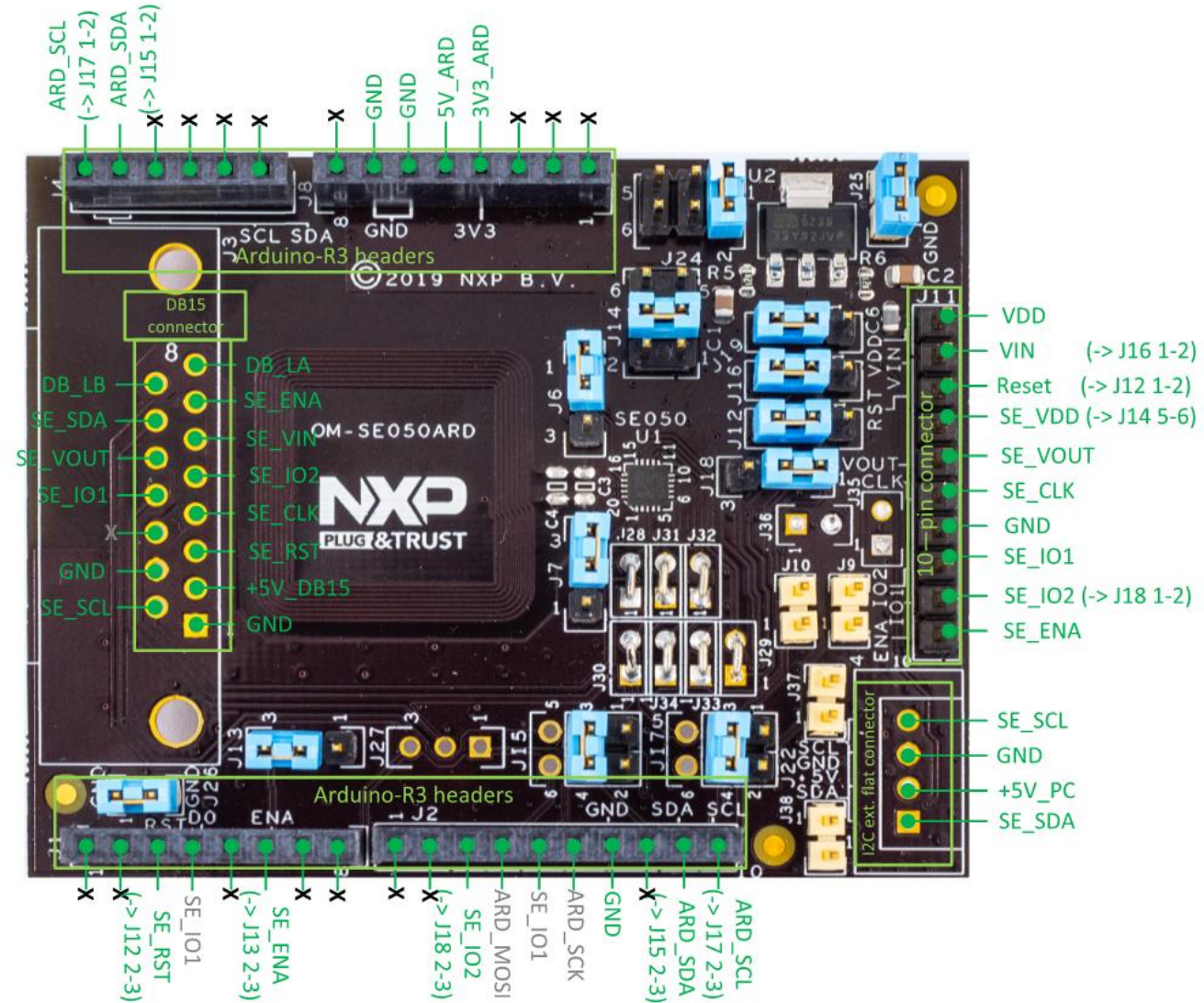
Applications

-Smart Door lock



SE050 ARD Jumper

Jumper	Description	Configuration
J6, J7	Antenna	1-2: via DB15 connector 2-3: Internal antenna -Default
J9, J10	I2C Master pull up connection	Open: not connected - Default 1-2: 3k3 Ohm
J12	Reset	1-2 RST on J11:3 2-3 RST on Arduino - Default
J13	SE050_ENA pin routing	1-2: ENA low, VOUT not connected to VIN 2-3: ENA controlled by Arduino pin J1:4 - Default
J14	SE050_VCC pin routing	1-2: Routed to VDD supply voltage (see J19) 3-4: Routed to SE050_Vout pin - Default 5-6: Routed to J11:4 pin
J15	I2C Slave SDA connection	1-2: Arduino R3 J4:5 3-4: Arduino R3 J2:9 - Default
J16	SE050_Vin supply	1-2: Supplied by J11:2 pin 2-3: Supplied by the VDD (see J19) - Default
J17	I2C Slave SCL connection	1-2: Arduino R3 J4:6 3-4: Arduino R3 J2:10 - Default
J18	SE050_IO2 routing	1-2: Routed to J11:9 - Default 2-3: Routed to J2:3
J19	VDD supply voltage	1-2: From LDO 2-3: From 3V3_ARD pin -Default
J24	VDD supply selection for LDO (if LDO is used - see J19)	1-2: From 5V_PC (USBI2C flat connector) - Default 3-4: From 5V_DB15 pin 5-6: From 5V_ARD pin

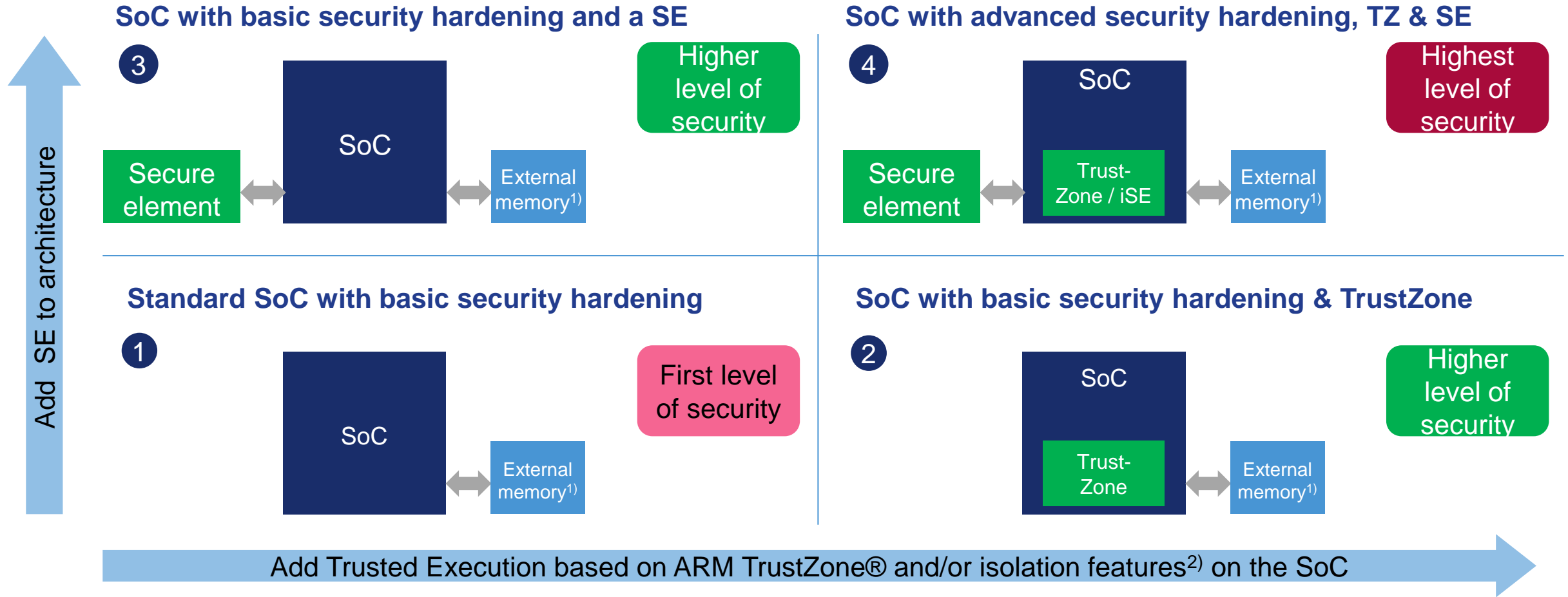


SE050 family vs. A71CH - Product comparison

	A71CH	SE050 Platform
Cryptography	ECDSA/ECDH/ECDHE 256p, HMAC, SHA256 AES Key wrapping, KDF, PRF (TLS-PSK)	ECC (ECDSA/ECDH/ECDHE/ECDA), HMAC, CMAC, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RSA (up to 4096), AES (128, 256) encryption/ decryption, DES, HKDF, MIFARE KDF, PRF (TLS-PSK)
Crypto curves	ECC NIST curve	ECC NIST (192 to 521-bit), Brainpool (160 to 512-bit), Koblitz (160 to 256 bit), Edwards (Ed25519, Curve25519)
ECDSA sign performance	~109ms	~28ms
Support ECC/RSA	Yes/No	Yes/Yes
Interfaces	I2C (400kbps)	I2C (3.4Mbps) Slave, I2C Master, (fast mode 400kbps) NFC interface
Secured IF (encryption/authentication on interface)	SCP03 (bus encryption + encrypted credential injection)	SCP03 (bus encryption + encrypted credential injection on applet and platform level)
User Memory	4 kB	50kB
Power Saving Mode	Sleep 30uA, Deep Sleep 5uA	Idle: 400uA, Deep Sleep:<5uA
Temperature/Supply voltage range	-40...+90 deg/1.62...3.6V	-40...+105 deg/1.65...3.6V
Packaging	4x4mm (HVSON-8), 2x2mm (CSP)	3x3mm (HX2QFN20)
Key Strength	Cryptographic features, secured IF, Cloud onboarding	Cryptographic features, EAL 6+ up to OS level, cloud onboarding, optimized for industrial applications, secure end-to- end channel, main TPM functions available

NXP supports architectures with scalable security features

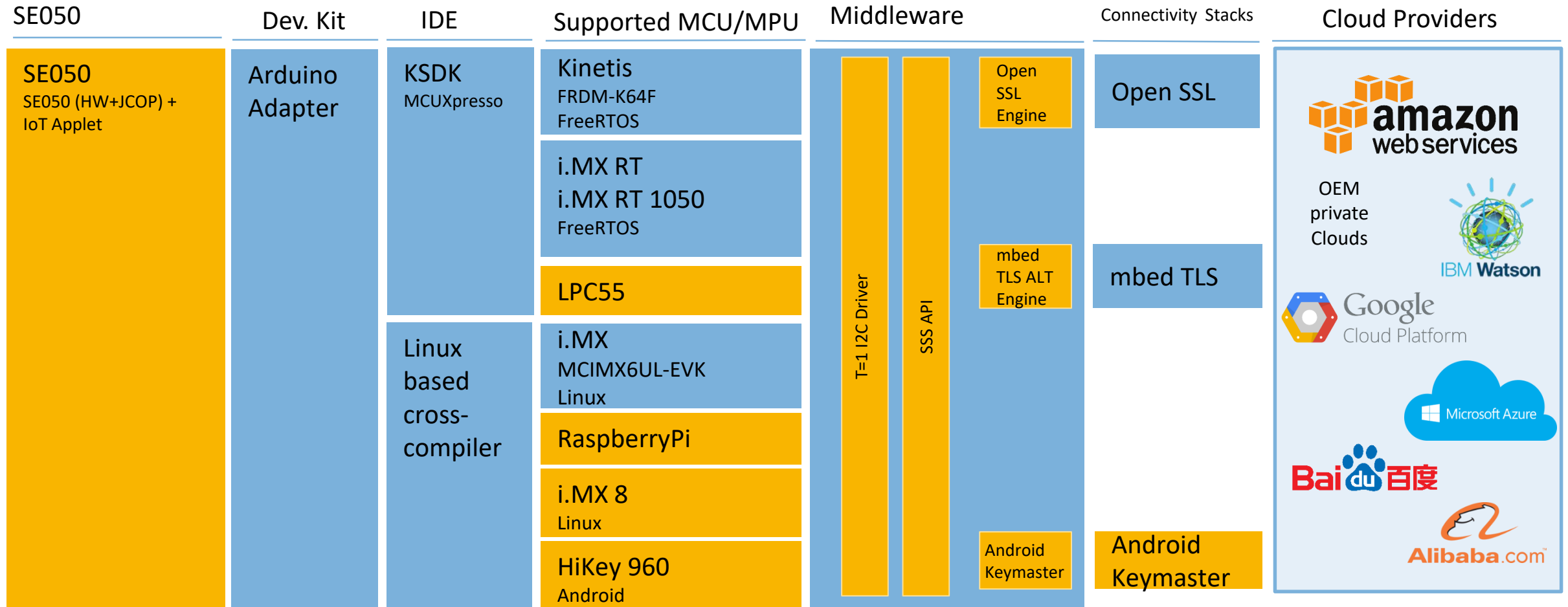
Security Architectures supported by current shipping NXP products





1) Not mandatory for MCUs/MPUs when they have embedded memory;

2) Features like RDC (Resource Domain Controller) on i.MX

SE050 Host software package



 New with SE050
 Like A71CH

SE050 IoT Applet

IoT Applet			
Life cycle management	EC key store	ECDSA, ECDH ECDHE	AES encrypt/decrypt
Object & user based access control	RSA key store	EDDSA, ECDAA	KDFs
Dynamic file system	AES/DES key store	ECC NIST , Brainpool, Koblitz	Secure hash algorithms
Context awareness	Authentication object store (PIN,admin keys etc.)	RSA encrypt/decrypt	RNG
SCP03 Secure channels	ED25519, Curve25519, ED448, Curve448	RSA signature generation/verification	Monotonic counters
I2C Master	SECP256k1		

SE050 IoT applet will support:

- Generic module management support o Lifecycle management
 - Session management
 - Timer functionality
 - Access control
 - Secure import/export of keys or files
- Applet Secure Channel management
 - SCP03
 - FastSCP
- Random number generation
- Key management (EC, RSA, AES, DES, etc.): write, read, lock, delete
- Elliptic curve cryptographical operations
- RSA cryptographical operations
- AES/DES cryptographical operations (AES ECB, CBC, CTR)
- Binary file creation and management
- Pin creation and management
- Monotonic counter creation and management
- PCR creation and management
- Hash operations
- Message authentication code generation
 - CMAC
 - HMAC
- Key derivation functionality
 - HKDF
 - PBKDF2
- Specific use case support
 - TLS PSK master secret calculation
 - MIFARE DESFire protocol support
 - I2C Master support