NXP SECURITY SOLUTIONS AND USE-CASES

PLUG &TRUST THE FAST, EASY WAY TO DEPLOY SECURE IOT CONNECTIONS

STATION F

ANNE VERNAY

JUNE 11TH 2019

PUBLIC

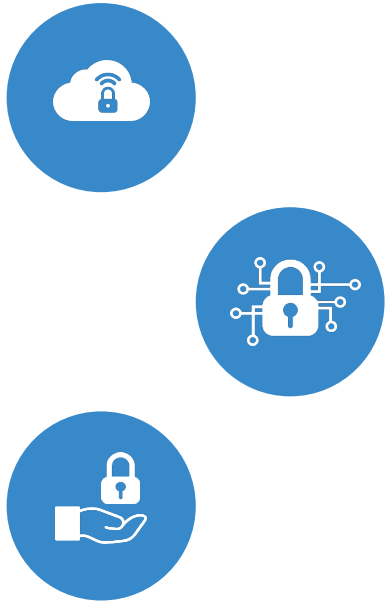
NXP PLUG &TRUST | SECURE CONNECTIONS FOR A SMARTER WORLD

SECURITY PRINCIPLES

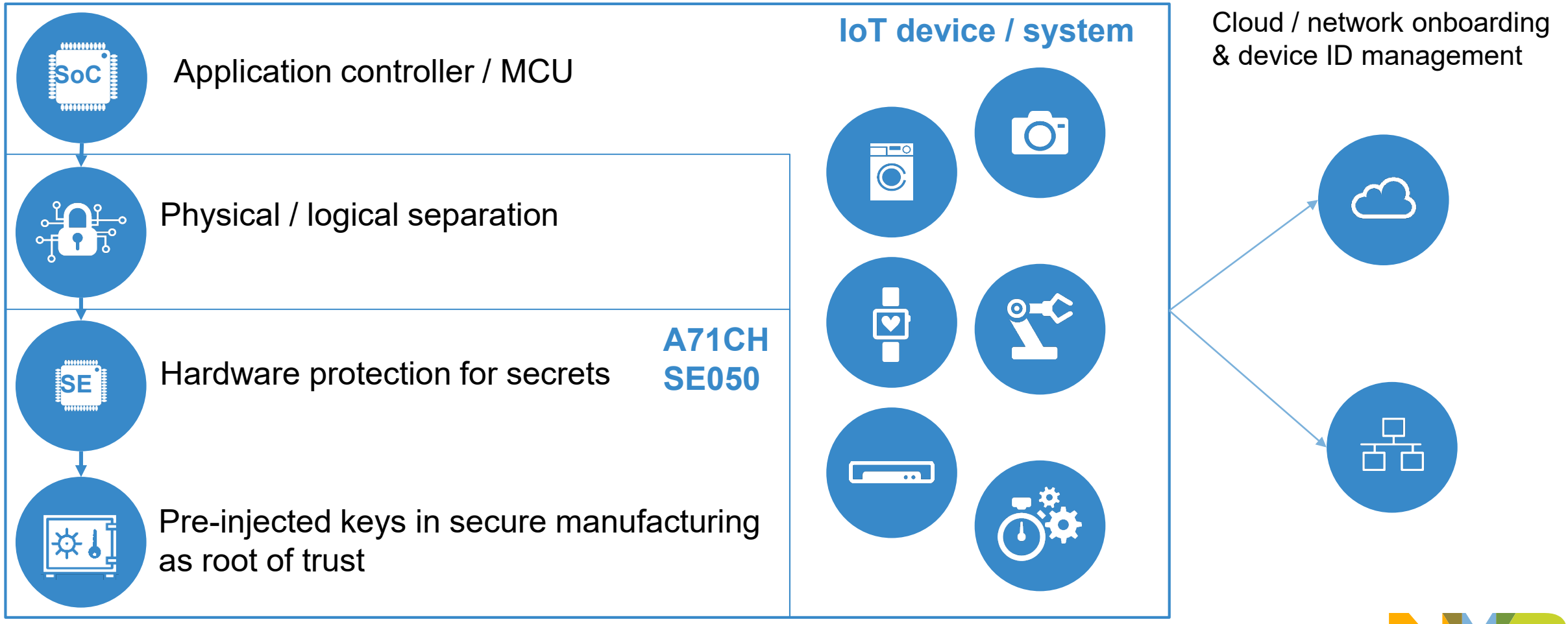
Reasons to consider a secure element in IoT devices

Why a discrete security IC in IoT devices?	
Root of trust	→ Security and key management throughout the whole value chain right from the start
Closed system	→ On Chip NV Memory with access policy → Closed system architecture to isolate memory access from host system. → NV memory only accessible via Chip OS / Applet
Out-of-the-box security	→ Scalable and ready to deploy → No need to develop secure SW

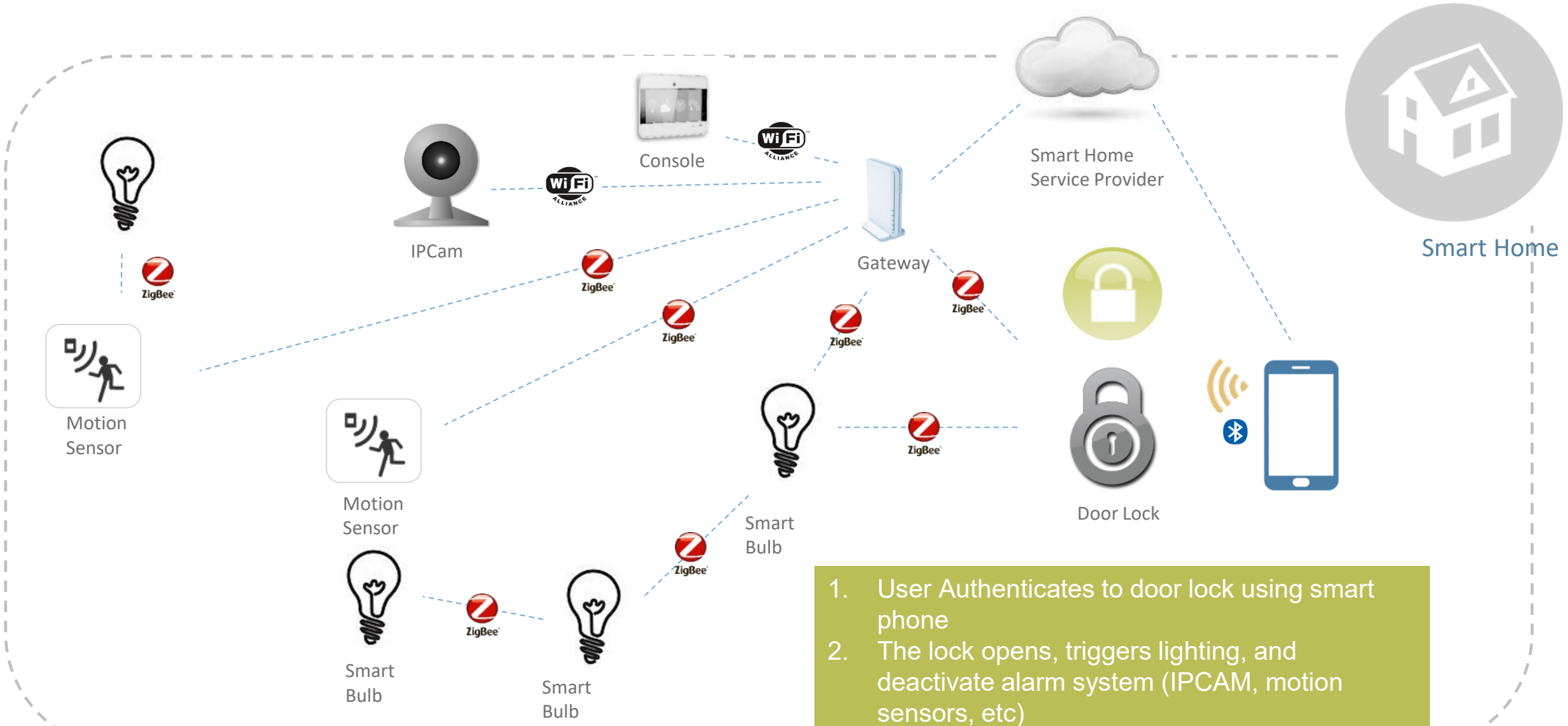
Keeping secrets secret



Layers of Security – Chain of trust based on Secure Element

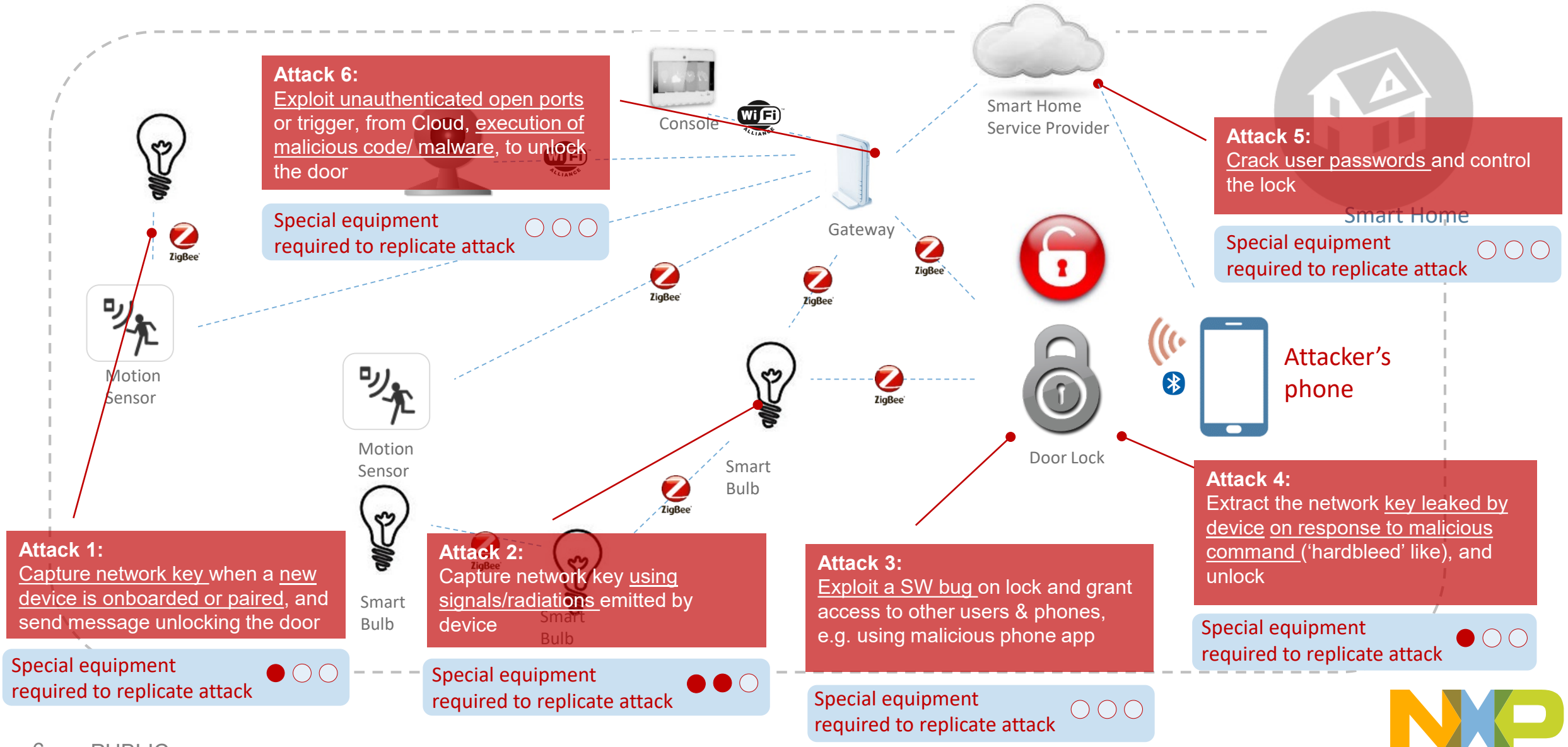


Case Study 1: Unlock the door in a Smart Home



1. User Authenticates to door lock using smart phone
2. The lock opens, triggers lighting, and deactivate alarm system (IPCAM, motion sensors, etc)
3. The lock can also be unlocked via the home gateway, controlled from WiFi consoles and phones via the Cloud

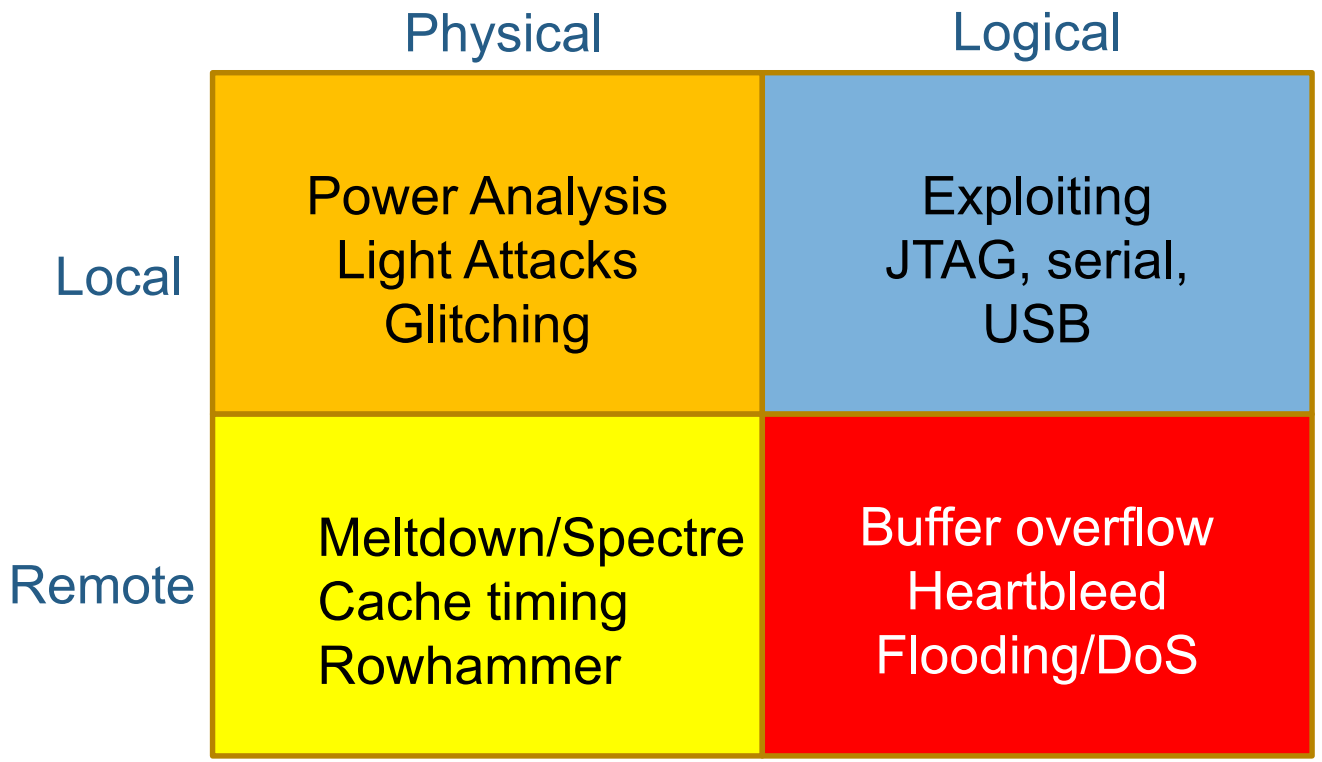
Case Study 1: Unlock the door in a Smart Home (cont'd)



Note: 'equipment required' refers typically to electronic kits including probes, signal processing board, SW based signal analyzers, etcs

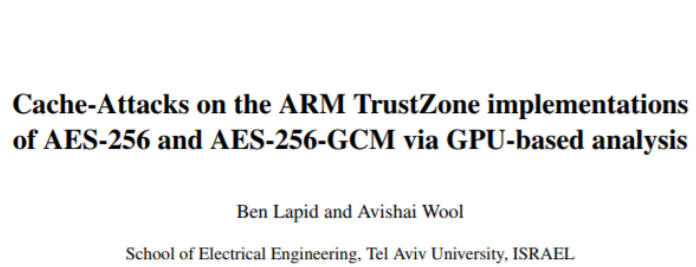
Attack Types

- ***Physical*** – making use of physical properties or deficiencies in the device.
- ***Logical*** – by sending malicious messages, the software will misbehave.
- ***Local*** – adversary must be in the proximity of the device
- ***Remote*** – adversary can be anywhere



Secure Element based security is the market trend for smart devices

Ever more sophisticated attacks


Cache-Attacks on the ARM TrustZone implementations of AES-256 and AES-256-GCM via GPU-based analysis

Ben Lapid and Avishai Wool

School of Electrical Engineering, Tel Aviv University, ISRAEL
ben.lapid@gmail.com, yash@eng.tau.ac.il

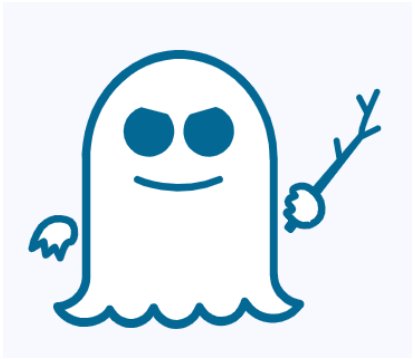

Meltdown


LILY HAY NEWMAN SECURITY 11.21.18 03:31 PM

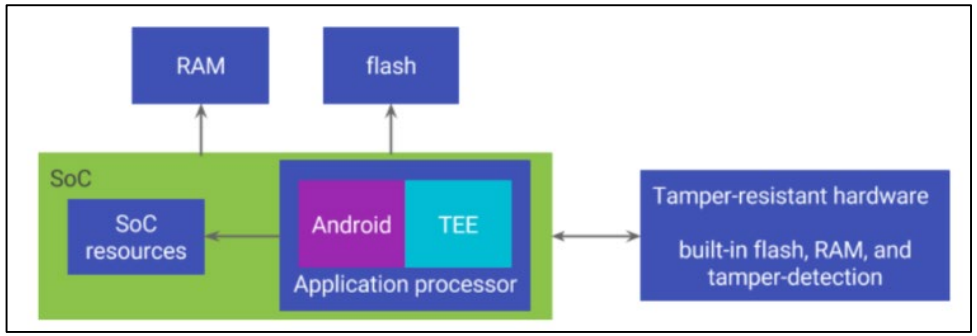
AN INGENIOUS DATA HACK IS MORE DANGEROUS THAN ANYONE FEARED

LA TIGRE

Rowhammer


Spectre

More device architectures and new use cases with Secure Element-based security

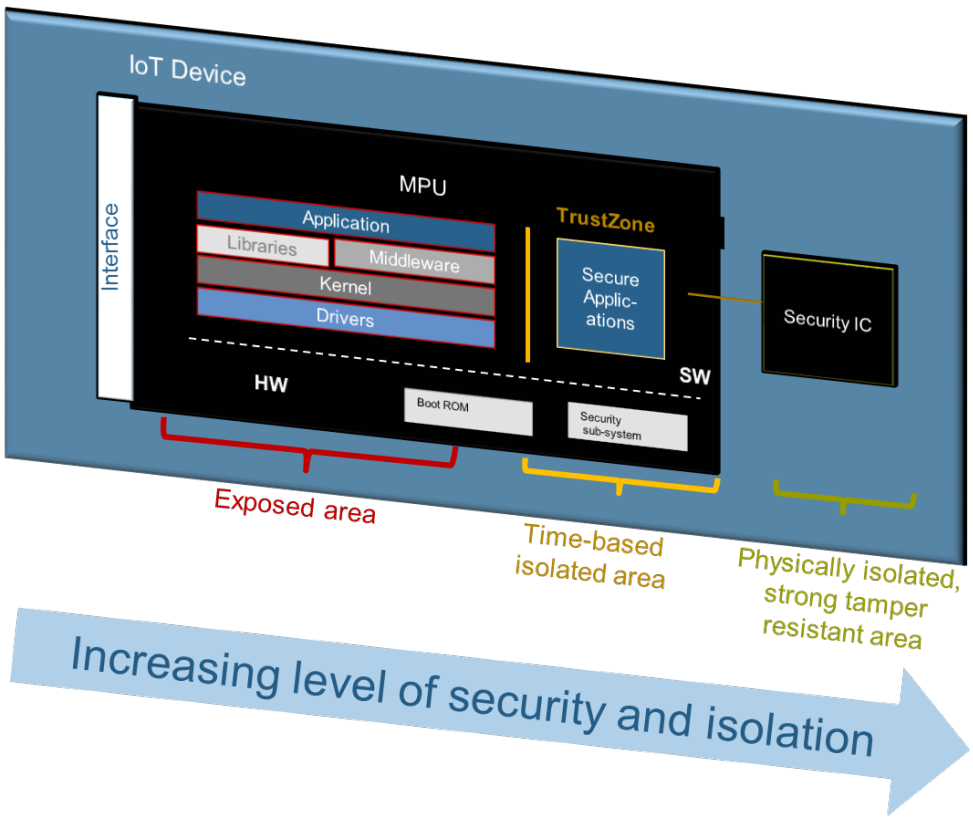


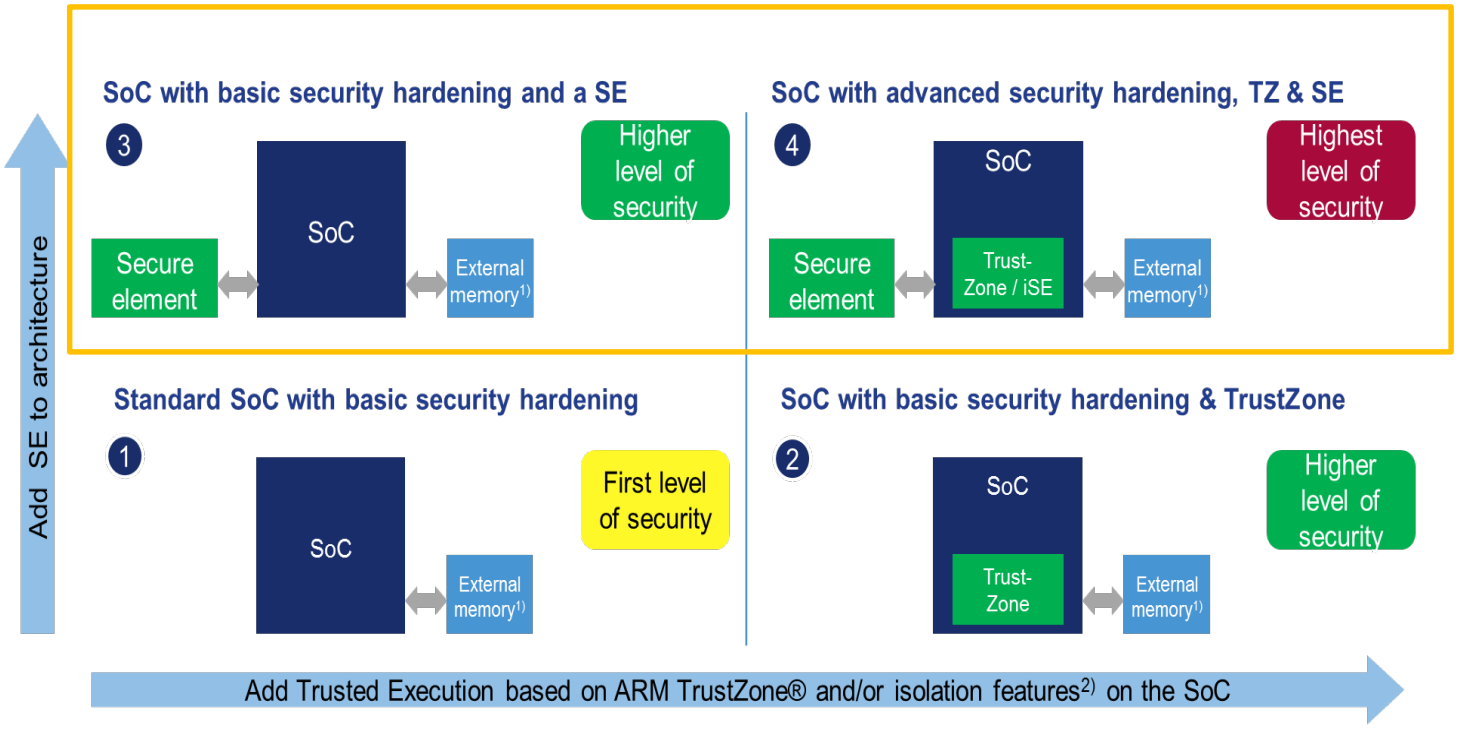
http://www.googblogs.com/how-the-pixel-2s-security-module-delivers-enterprise-grade-security/

Hardware security module

Supported devices running Android 9 (API level 28) or higher installed can have a *StrongBox Keymaster*, an implementation of the Keymaster HAL that resides in a hardware security module.

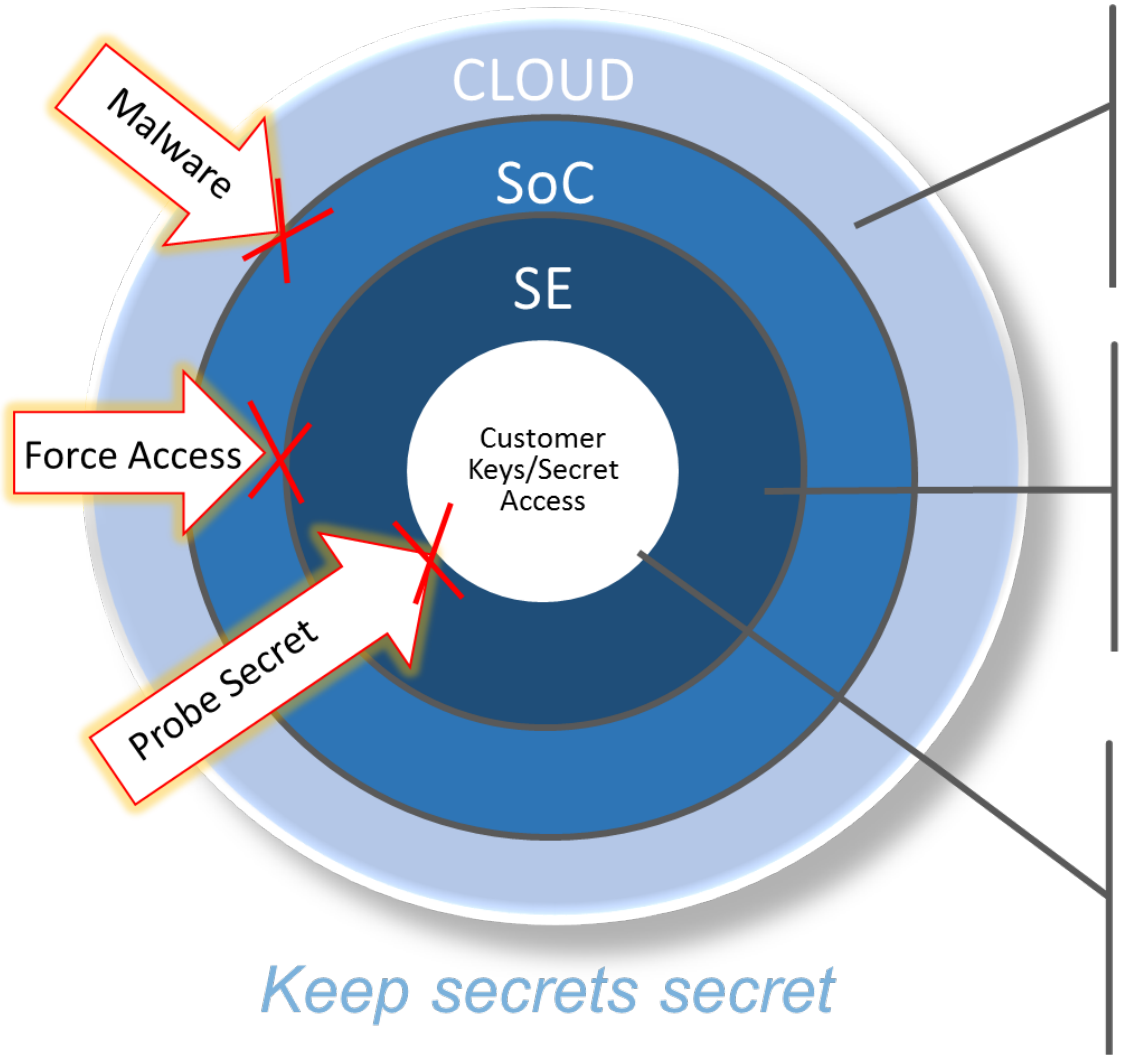
Shades of grade of security





1) Not mandatory for MCUs/MPUs when they have embedded memory;
2) Features like RDC (Resource Domain Controller) on i.MX

SE for IoT End to End Security



Network onboarding
Device ID management
Mutual authentication :
Credential stored on SE
No key/PIN handling

Out of Box
Secured Connect

Physical / Logical separation
JAVA CARD – APDU commands
Key Lifecycle Management
protects keys throughout product lifecycle from unauthorized access

Field Proven
Secured Architecture

Hardware Protection
Pre-injected keys stored in hardware
Unique ID genuine devices
HW cryptographic calculations isolated resources

Hardware Root of trust

5

EDGELOCK™ SE

NXP PLUG&TRUST

EdgeLock™SE : a new family to cover all IoT use cases

A71CH/L – Root of Trust

Security and key management throughout the whole value chain right from the start. Complete solution – ready to be used!

Plug & Trust
approach for lower time to market & easy integration

Secure Cloud Connections
AWS, IBM, Google, Alibaba, Baidu

Out-of-Box Security
system solution with secure OS & pre-programmed secure applet

SE050 – Added values

Building on top of A71CH, EdgeLock SE050 offers even more value. Flagship 40nm architecture and CC EAL 6+ certified state of the art security concepts protect strongly against most recent attack scenarios. Additional use cases to answer multiple application needs in IoT and especially industrial.

Enhanced security

- → CC EAL 6+ certified HW & OS as safe environment for IoT applets
- → RSA & ECC functionalities
- → Future proof curves & higher key length
- → Encrypted communication via SCP
- → Symmetric ciphers for en/decryption

More flexibility

- → Product family with multiple configs
- → Ease of Use pre-injected keys
- → Various new IoT Security use cases
- → Easy integration with multple MCU/MPU platforms & OS
- → Flexible applet with dynamic 50kB + MAL 1.0 for flexibility

EdgeLock™SE : SE050 family - Use Cases

Powerless configuration
TP over CL interface

Secure Access

TPM

Secure Cloud
Connection

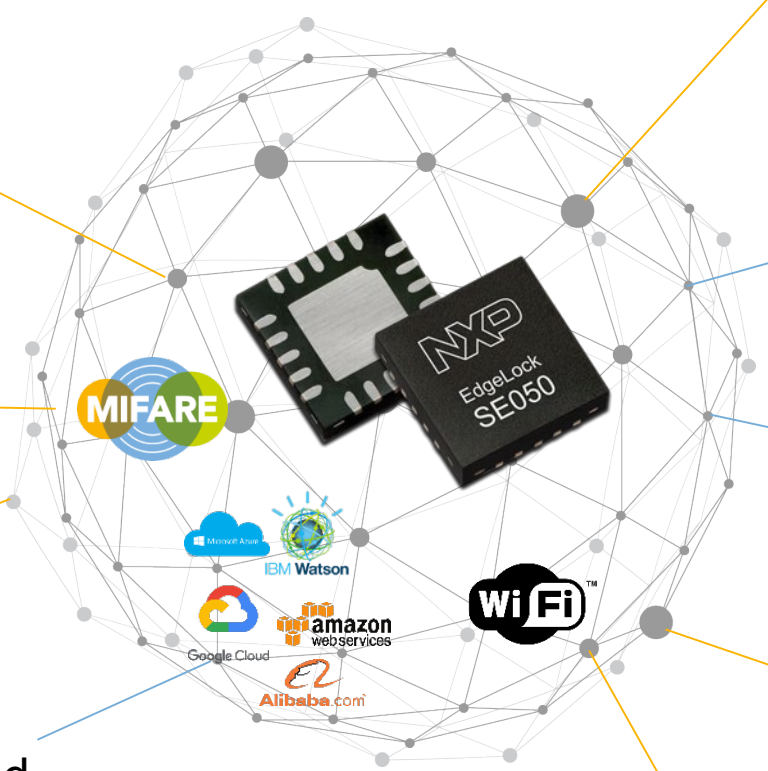
Secure Sensor / GW

Device-to-device
authentication

Attestation,
Proof of Origin

ID for
blockchain

Protection of
Wifi keys



KNOWN FROM A71CH
NEW ON SE050

EdgeLock™SE = A71CH & SE050

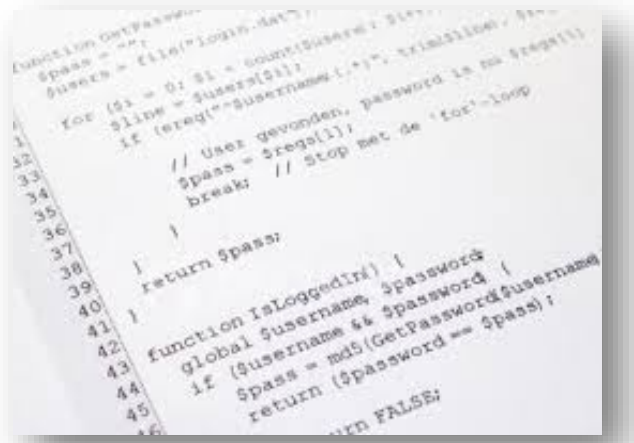
	A71CH	SE050
Cryptography	ECDSA/ECDH/ECDHE 256p, HMAC, SHA256 AES Key wrapping, KDF, PRF (TLS-PSK)	ECC (ECDSA/ECDH/ECDHE/ECDAA), HMAC, CMAC, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RSA (up to 4096), AES (128, 256) encryption/ decryption, DES, HKDF, MIFARE KDF, PRF (TLS-PSK)
Crypto curves	ECC NIST curve	ECC NIST (192 to 521-bit), Brainpool (160 to 512-bit), Koblitz (160 to 256 bit), Edward (Ed25519), Montgomery (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 applciations, secure end-to-end channel, supporting main TPM functions

A71CH product support package

A71CH development boards

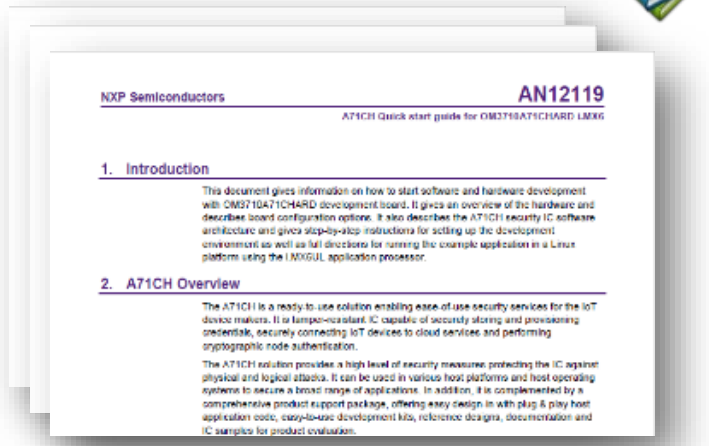
Includes an A71CH Mini PCB board and an Arduino adaptor for i.MX, Kinetis and LPC boards.

A71CH Host software package



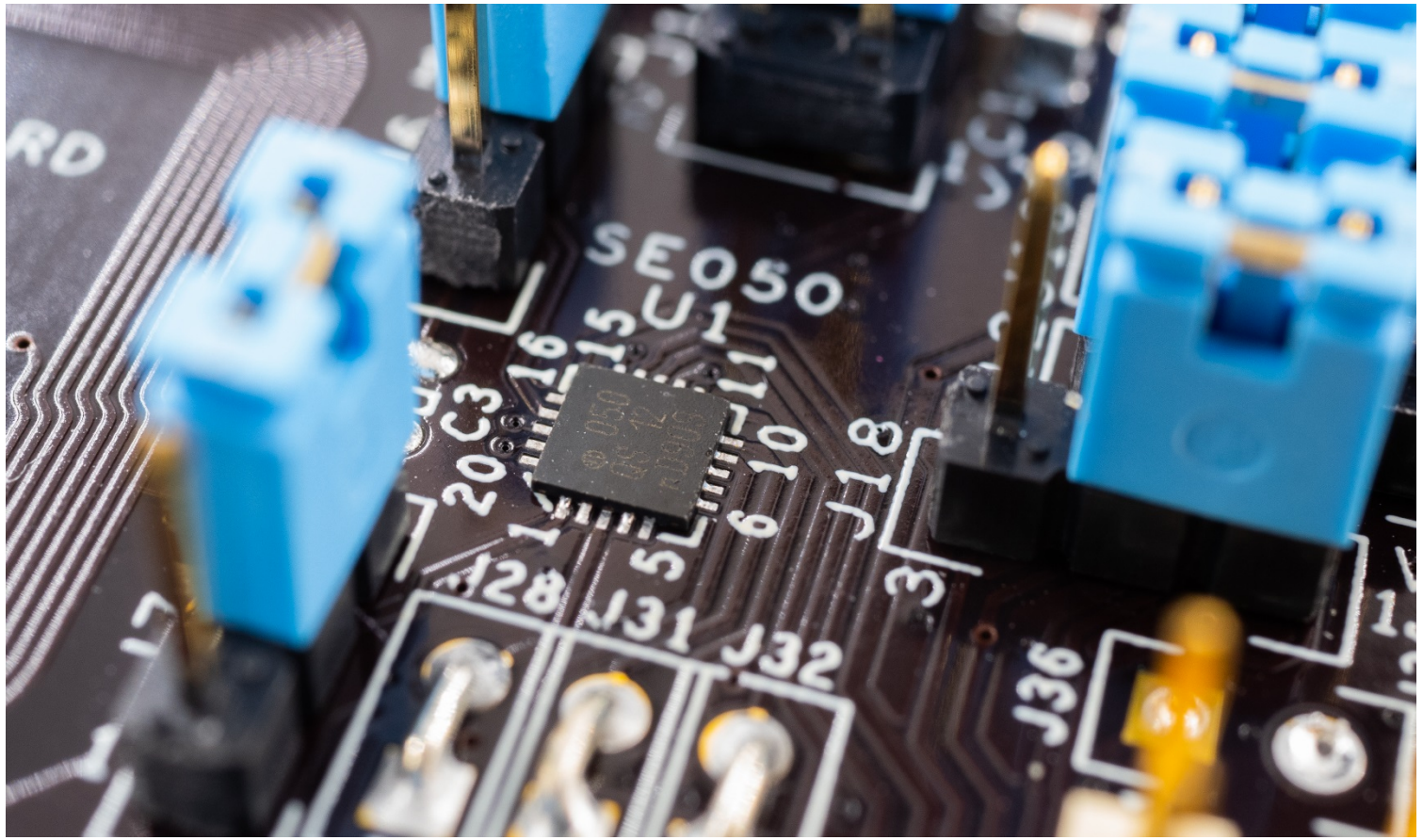
Comprehensive software package including A71CH Host SW API, sample applications, source code and API documentation

Documentation



Extensive support documentation for facilitating product evaluation and also the implementation process of the main use cases.

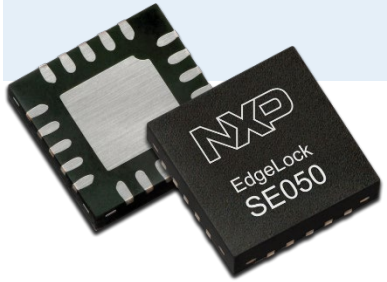
EdgeLock™ SE050 product family – Launch June 11



SE050C
ECC, RSA, AES, DES,
MIFARE KDF, CL-IF,
I2C Master

SE050B
RSA, AES, DES

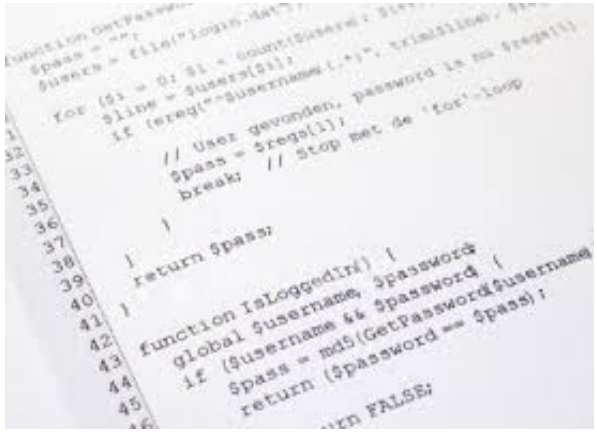
SE050A
ECC, AES, DES



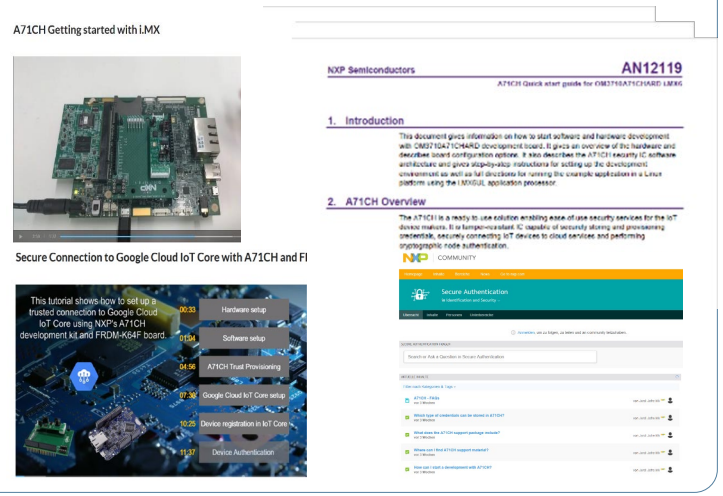
EdgeLock™SE: SE050 Plug & Trust product support package

SE050 development boards

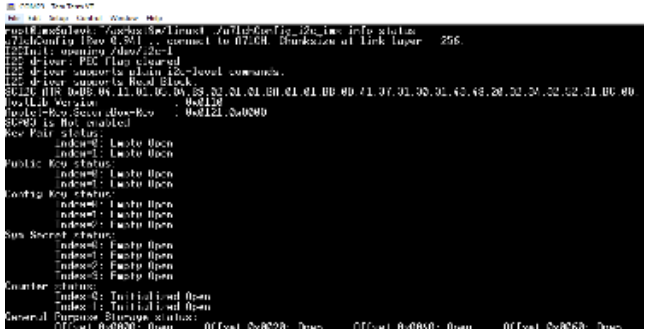
SE050 Host software package



AppNotes,Webinars,Videos,Community

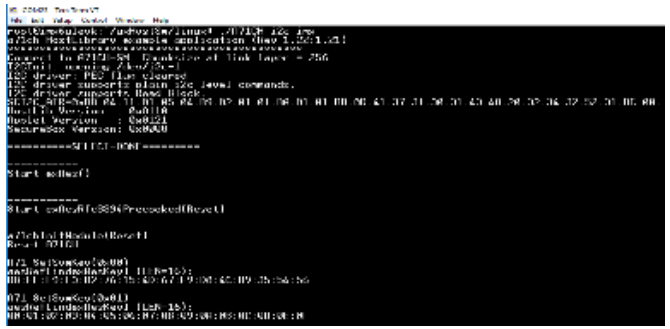


SE050 Configure tool



SE050 Demo Framework

SE050 API usage examples



Secure Provisioning

Heads-up

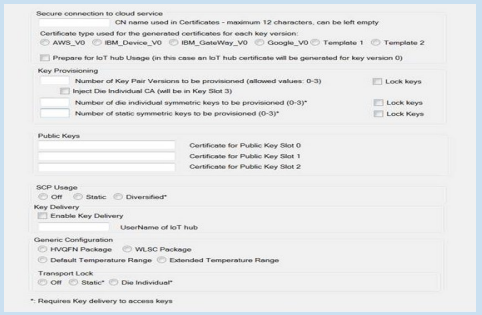
Pre-configuration

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

Enhanced TP via NXP for volumes >150k per order line

Simple TP tool enabling easier configuration of SE050

TP Tool

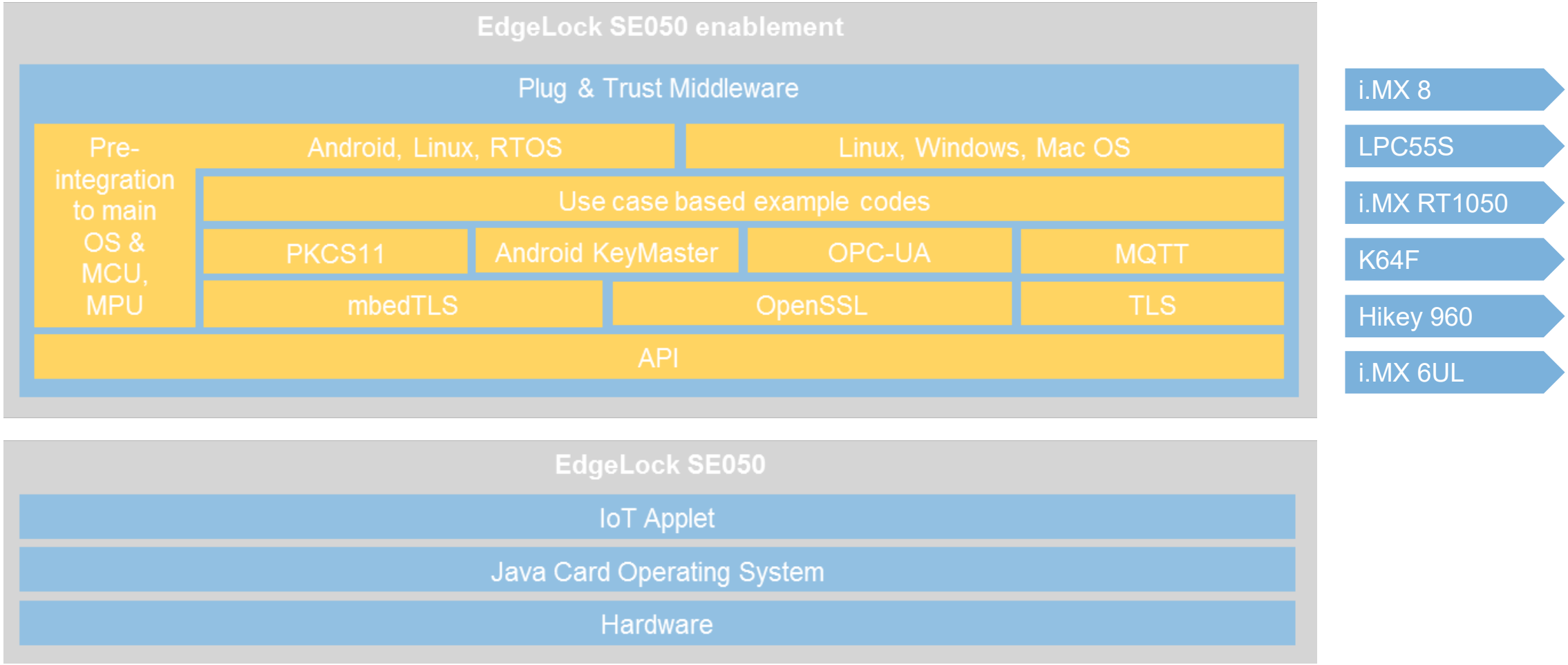


Customized provisioning for any volumes via our distributors

We enable Data I/O to upgrade the existing equipment installed at the main distributors to support SE050 provisioning

NXP PLUG&TRUST

EdgeLock™SE : SE050 Plug & Trust Middleware



CLOUD ONBOARDING WITH EDGELOCK™ SE

NXP PLUG&TRUST

Cloud onboarding with Secure Element

Secure trust provisioning with SE and secure authenticator

Onboarding flow with our Secure elements

Security use-cases features enabled

- Zero-touch onboarding on Clouds
- Secure Manufacturing, no exposure of keys at EMS and supply chain
- Ecosystem Protection

Note: Secure element and secure authenticator support more use cases

NXP products used

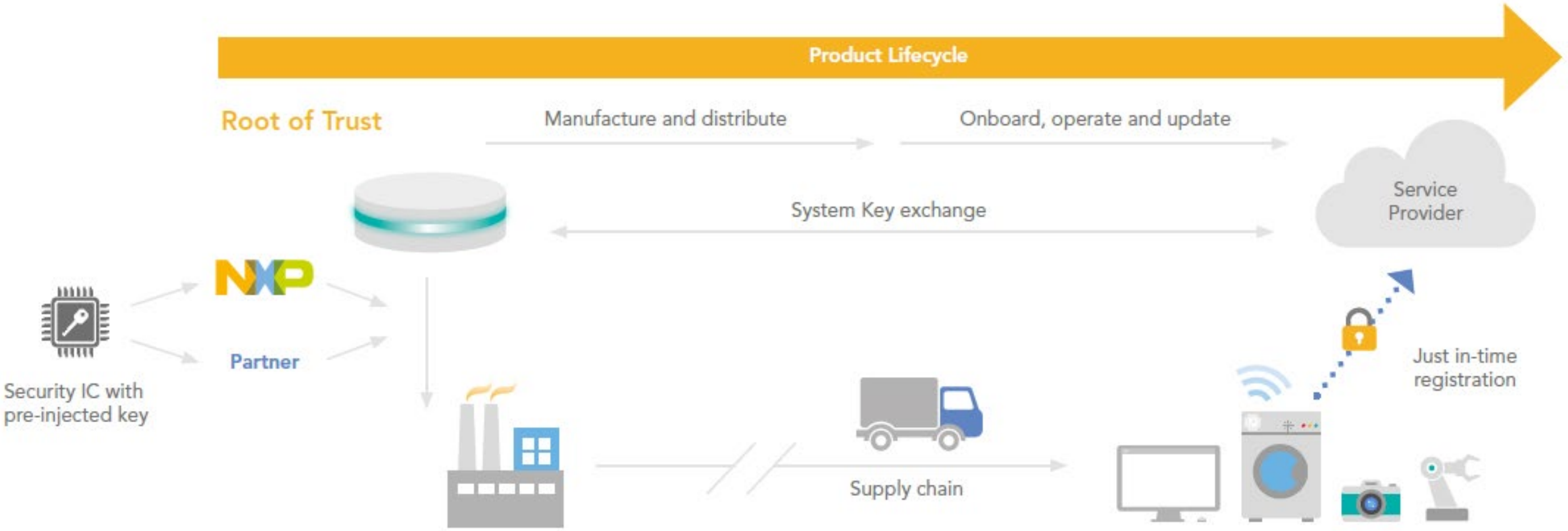
- A71 Plug & Trust Secure Elements
  - A71CH (for following clouds: AWS, GCP, WIoT)
  - A71CL (for following clouds: Alibaba, Baidu)
- SE050 EdgeLock

Security features of products used

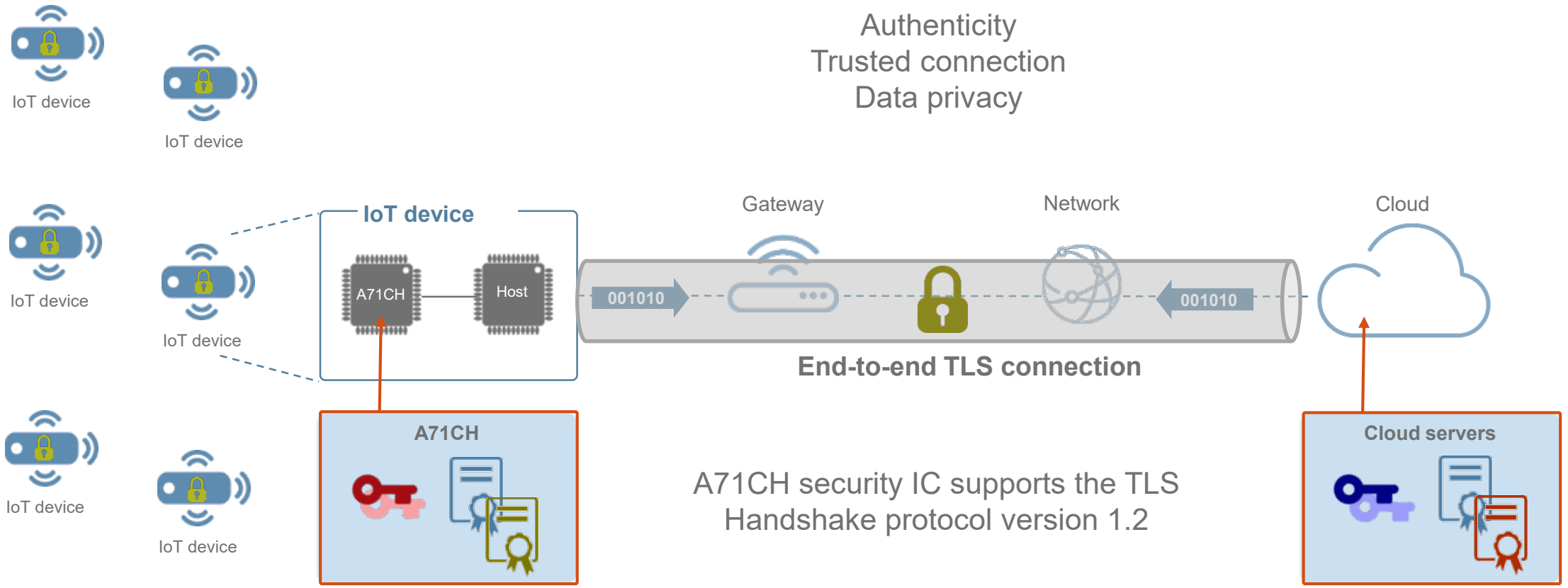
- Secure trust provisioning infrastructure (key injection)
- HW isolation and on-chip tamper resistance (credential protection at rest, at use, at update)
- Integration into SW stacks, NXP MCU/MPU, and Identity management systems of each Cloud

Onboarding flow with Secure Elements & Value Proposition

General overview & Principles



A71CH for secure connection to public or private clouds

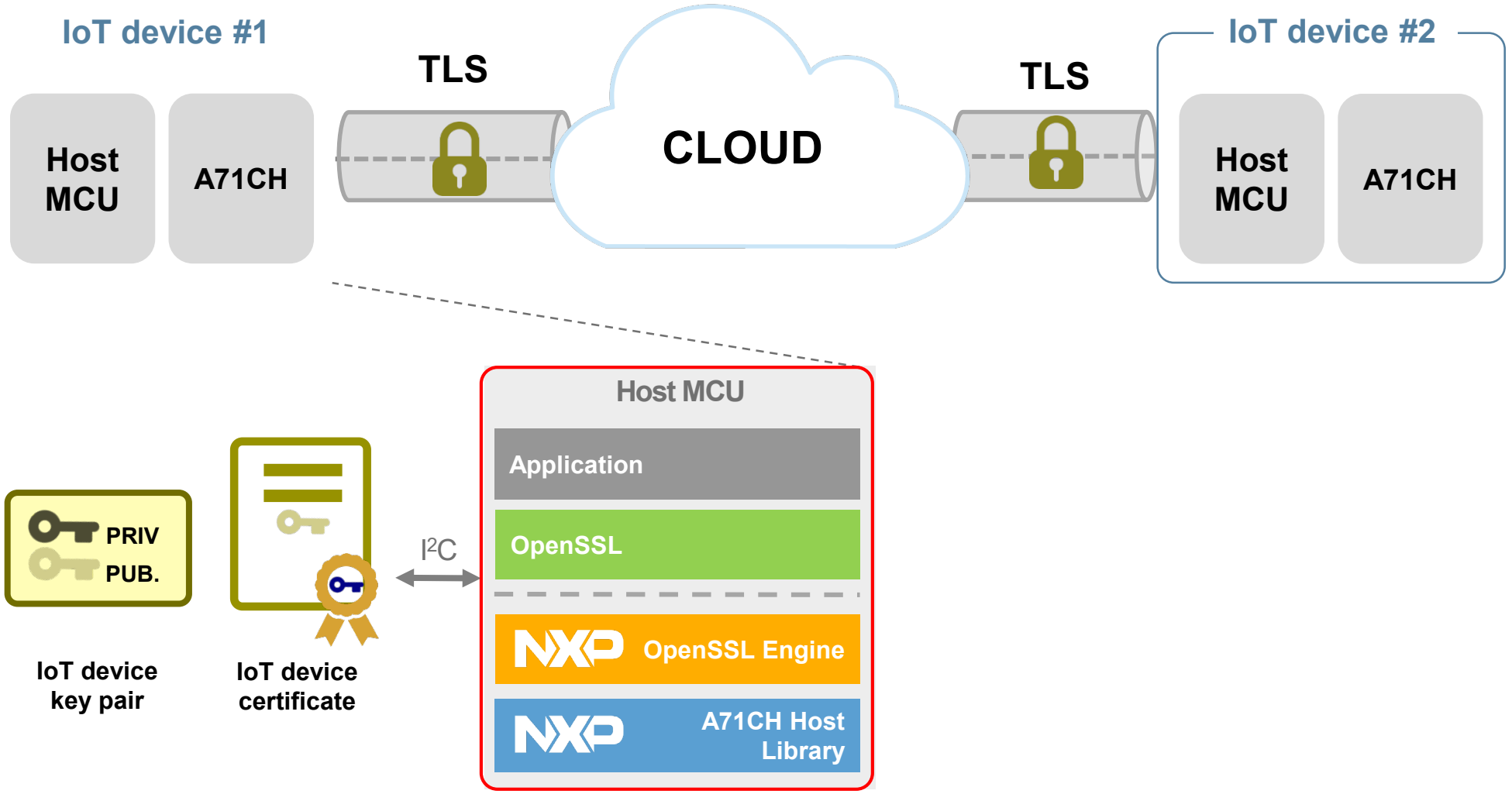


Authenticity
Trusted connection
Data privacy

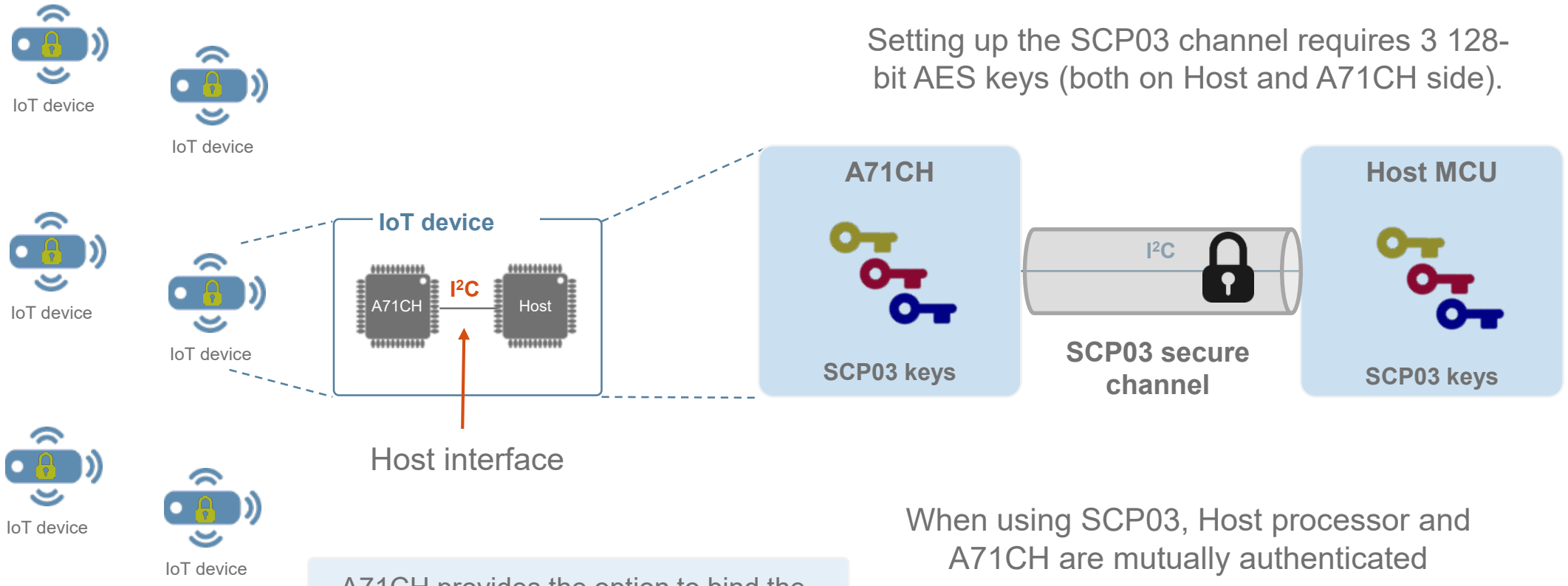
A71CH security IC supports the TLS Handshake protocol version 1.2

The keys and certificates used to authenticate the cloud connection are securely stored in A71CH
The private keys never leave the device

IoT - TLS Authentication with A71CH



A71CH for encrypted / authenticated interface to host processor



Setting up the SCP03 channel requires 3 128-bit AES keys (both on Host and A71CH side).

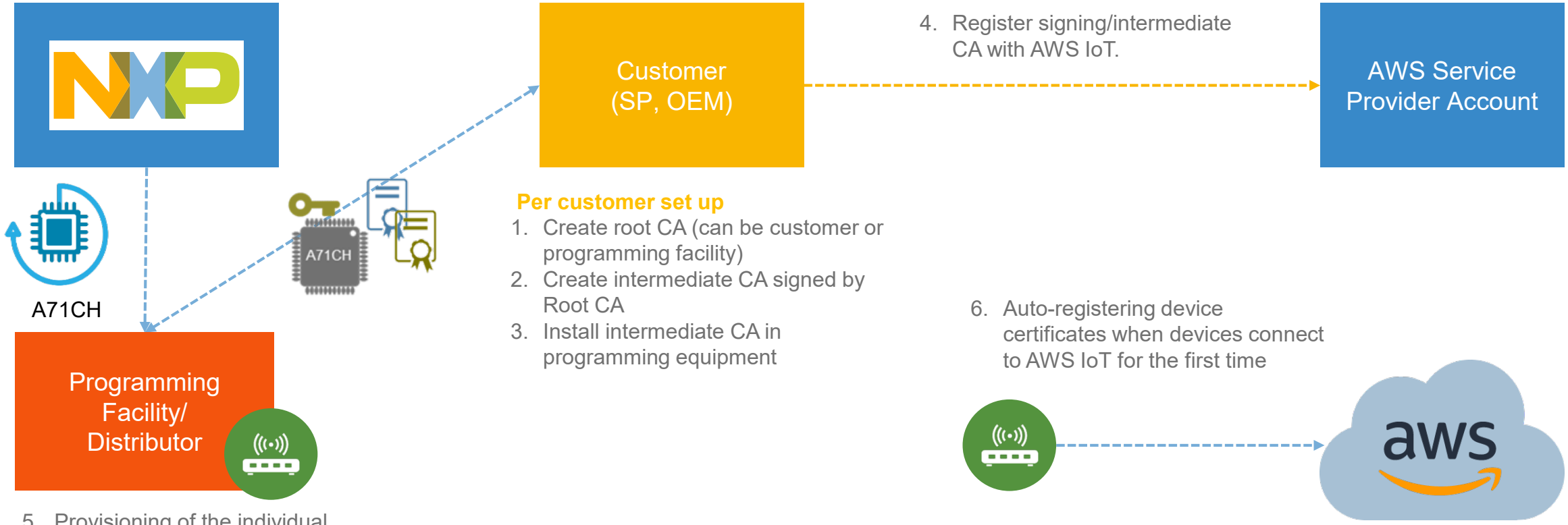
When using SCP03, Host processor and A71CH are mutually authenticated

A71CH provides the option to bind the Host processor to the security IC by configuring it to use an SCP03 channel.

Zero-touch Onboarding onto Amazon AWS

Launched in Nov 2016 – A71CH AWS

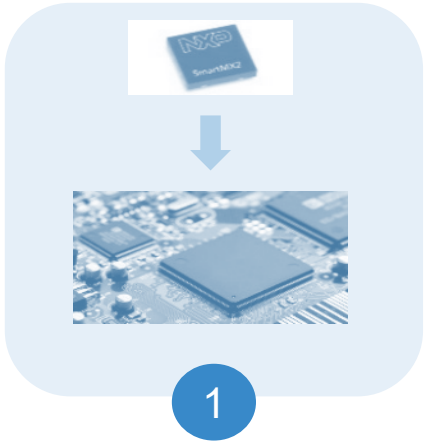
A scheme based on customer-specific X509 device certificates & Just-in-Time registration



Using A71CH for Zero-touch Secure Connections to Watson IoT

NXP products:
A7101CHTK2/T0BC2BJ
A7102CHTK2/T0BC2CJ

Include
die-Individual ECC Keys
x.509 Certificate



1

Drop NXP Security IC on the board

2

Upload Certification Authority's certificate and add devices whitelist to Watson IoT Dashboard

3

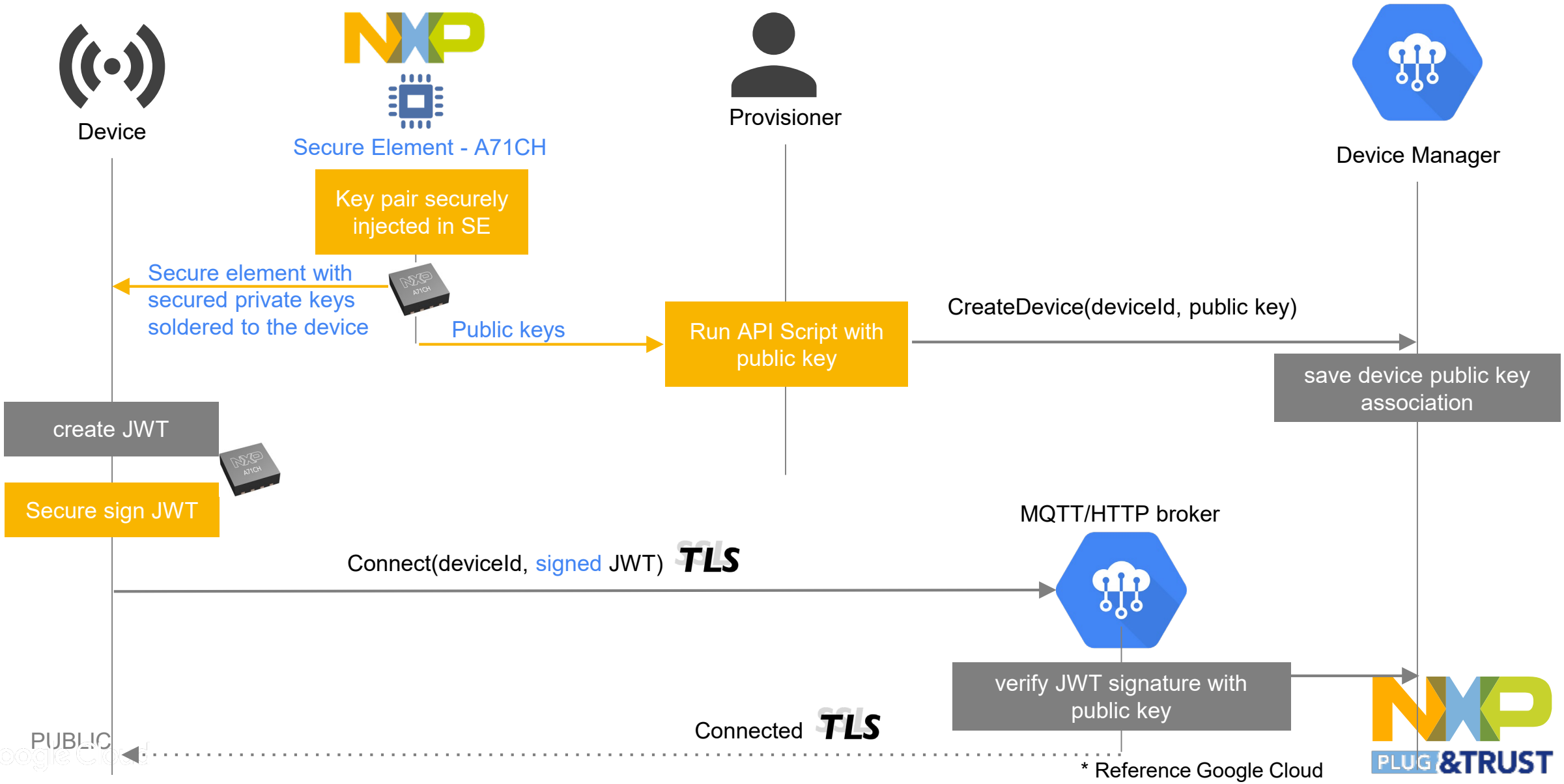
Turn on IoT Device and onboarding with Watson IoT will be automatic and secure

Key Benefits

- ✓ Secure: Private keys never leave the device, NXP root of trust (no need to manage any CA)
- ✓ Convenient: easy to deploy, enabling devices to connect securely to Watson IoT without management & exposure of keys.
- ✓ Scalable: suitable from product introduction phase (low volumes) up to mass production, no MoQ
- ✓ Cost effective: No cost of ownership for key management, no stickiness to contract manufacturers.

A71CH secure connect devices to Google Cloud*

Best in class security (hardware root of trust)



Watson IoT device authentication flow

Breakthrough solution scalable for the Mass Market

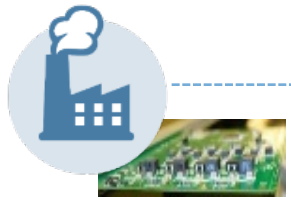
Product: A71CH provisioned and programmable

NXP is the Root CA

1 *Inject Die-Individual ECC Keys #1 and x.509 Certificate #2 signed by NXP Inter CA*

A71CH

Secure delivery of **A71CH**



2 Read of A71CH UID

OEM Customer Watson IoT Account

IBM WATSON

3 *Whitelist Devices UIDs Register NXP CA Inter CA*

4 *Device Secure Onboarding* - ***TLS over MQTT***

OEM Customer

End Customer

Device manufacturing (CM, ODM, OEM..)

Discovery questions for customer discussion

- What is the use case?
- Which host MCU/MPU controller should be supported (legacy, priority)?
- Which operating system (Linux, Windows)?
- Which connectivity stack is used (OpenSSL, mbedTLS)?
- Which cloud to connect to (priority)?
- Which crypto type (ECC)?
- What kind of keys to be stored? How many of which type?
- Is a secure provisioning of keys required or will it be done at the customer ?
- Specific security standard/qualification/certification of any kind? (e.g. extended temperature range)
- What kind of packaging (HVSON8, WLSCP)?

SECURITY AND STANDARDISATION

NXP PLUG&TRUST

Demand on Security through Standardisation and Industrial Initiatives

1 GDPR

The GDPR is ***strengthening the rights of individuals*** whose personal data is being processed through:

- the need for the individual's **clear consent** to the processing of personal data
- **easier access** by the subject to his personal data
- the **right to rectification**, to erasure and 'to be forgotten'
- the **right to object**, including to the use of personal data for the purposes of 'profiling'
- the **right to data portability** from one service provider to another

No privacy without security by design:

- Secure storage of keys
- Individual device ID
- Secure User Identities
- Secure communication channels

2 Charter of Trust

- Charter of Trust first signed at **Munich Security Conference, February 2018**
- Set the pace for **binding rules and standards** that ***build trust*** in cybersecurity and ***drive forward digitalization*** globally
- **12 partners** from different sectors signed the charter of trust, including NXP

Key principles:

- Ownership for cyber and IT security
- Responsibility throughout the digital supply chain
- Security by default
- User-centricity
- Innovation and co-creation
- Education
- Certification for critical infrastructure and solutions
- Transparency and response
- Regulatory framework
- Joint initiatives

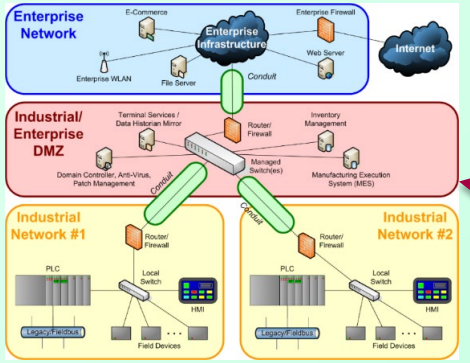
IEC 62443 : Multi-industry standard

PROCESS

DEVICE

Principal Roles

- Product Supplier (PS)
- Integration Provider (IP)
- Asset Owner (AO)
- Asset Operator (AOP)
- Maintenance Provider (MP)
- Service Provider (SP)
- System Operator (SO)
- Regulatory Authority (RA)
- Compliance Authority (CA)

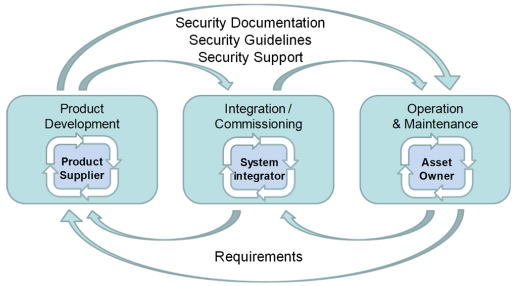


- Principal Roles
- Life Cycles
- Zones and Conduits
- Security Levels
- Maturity Assessment
- Security and Safety

Security and Safety

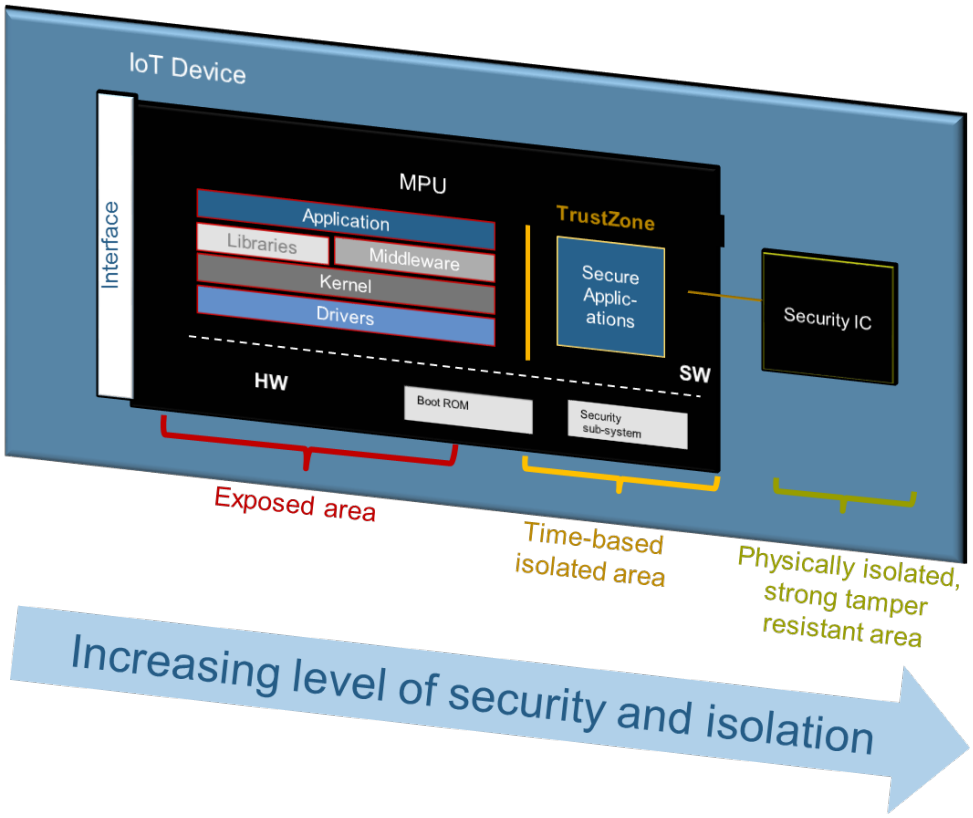
- Safety is much of the reason for security
  - Presenting consequences
- Much to be learned from the safety community
- Collaboration
  - ISA99-ISA84 joint effort
  - IEC TC65 work group 20
  - ISA Safety and Security Division

Life Cycles



Security Levels

Protect ASSET : Keys – Secrets the right Secured IoT Device



Security Levels (SL2..SL4)

Physical isolation

Logical isolation

Protection against…

4 Intentional Violation Using Sophisticated Means with Extended Resources, IACS Specific Skills & High Motivation

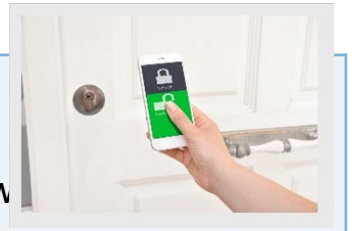
3 Intentional Violation Using Sophisticated Means with Moderate Resources, IACS Specific Skills & Moderate Motivation

2 Intentional Violation Using Simple Means with Low Resources, Generic Skills & Low Motivation

NXP PLUG&TRUST

Want to see a real example?

LOCAL NETWORK (INTRANET)



Block diagram

What does it show/solve?

provide access to IoT node with with

- Hardware secured mutual authentication w
  product DESFire light
- MCU architecture integrating SE050, CLRC663-reader board:
  - SE050 takes care DESFire light card is properly authenticated
  - SE050 ensures NDEF content is read from DESFire light and is sent to MCU to be displayed at LCD

Storyline:

- Demo shows traditional 3-step authentication with DESFire card making use of Secure element “SAM subset” functionality
- Example Use Case: traditional access control making use of strong authentication and possibly diversified encryption/decription key

NXP Components:

- Secure Element: SE050 @ SAM-like functionality applet
- Microcontroller: LPC55S69
- NFC reader: CLRC663 plus
- Contactless transponder: DESFire light card

PLUG&TRUST

SECURE CONNECTIONS
FOR A SMARTER WORLD