A71CH Technical Product Training

Roman Budek

CAS

April 2019 | AMF-SOL-T3524

SECURE CONNECTIONS FOR A SMARTER WORLD

A71CH Motivation

IoT Ecosystem

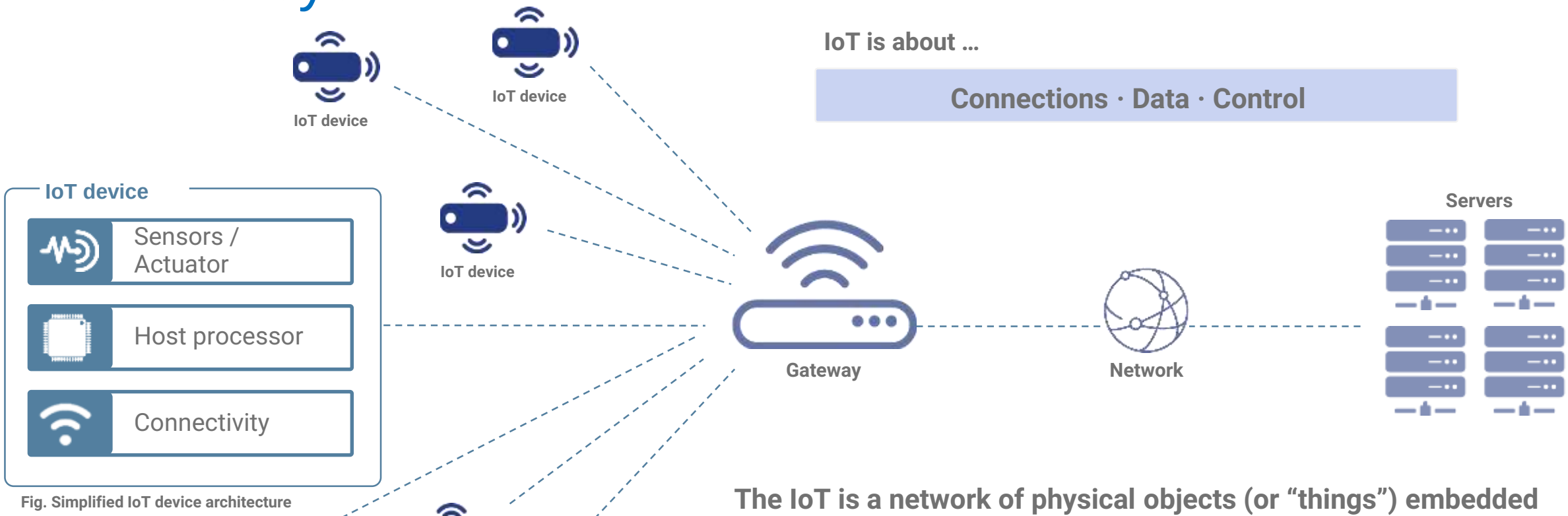


Fig. Simplified IoT device architecture

IoT is about …

Connections · Data · Control

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

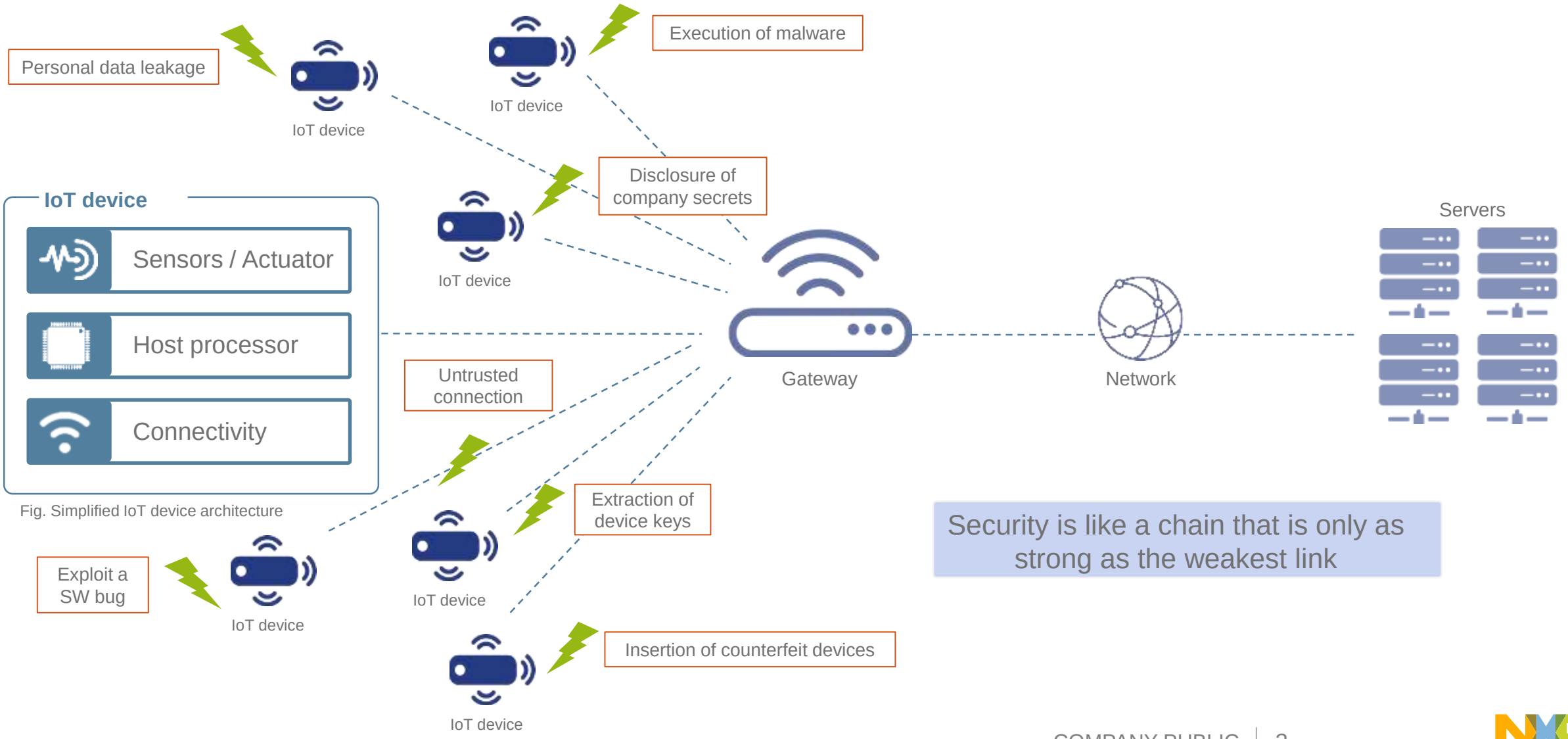
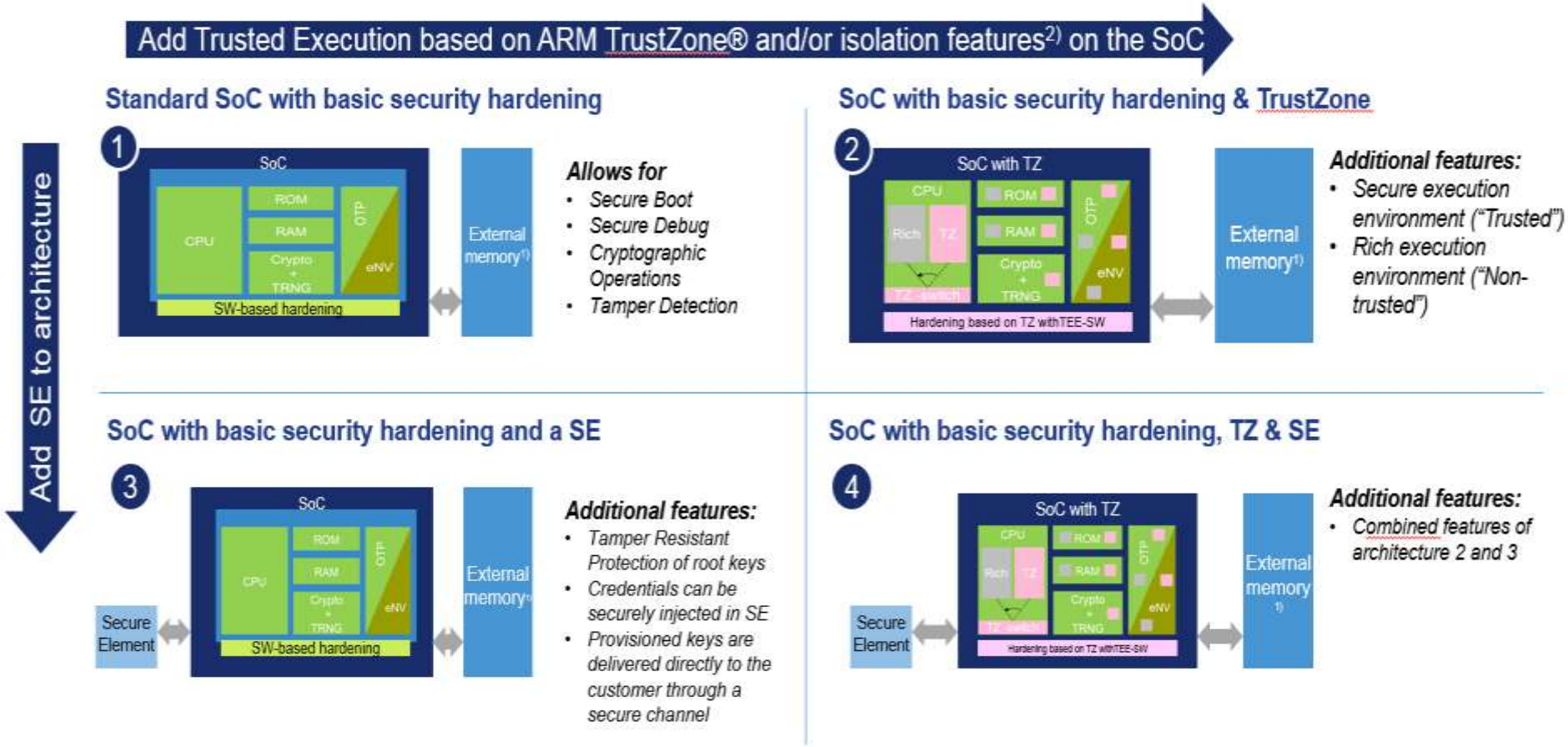


Fig. Simplified IoT device architecture

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

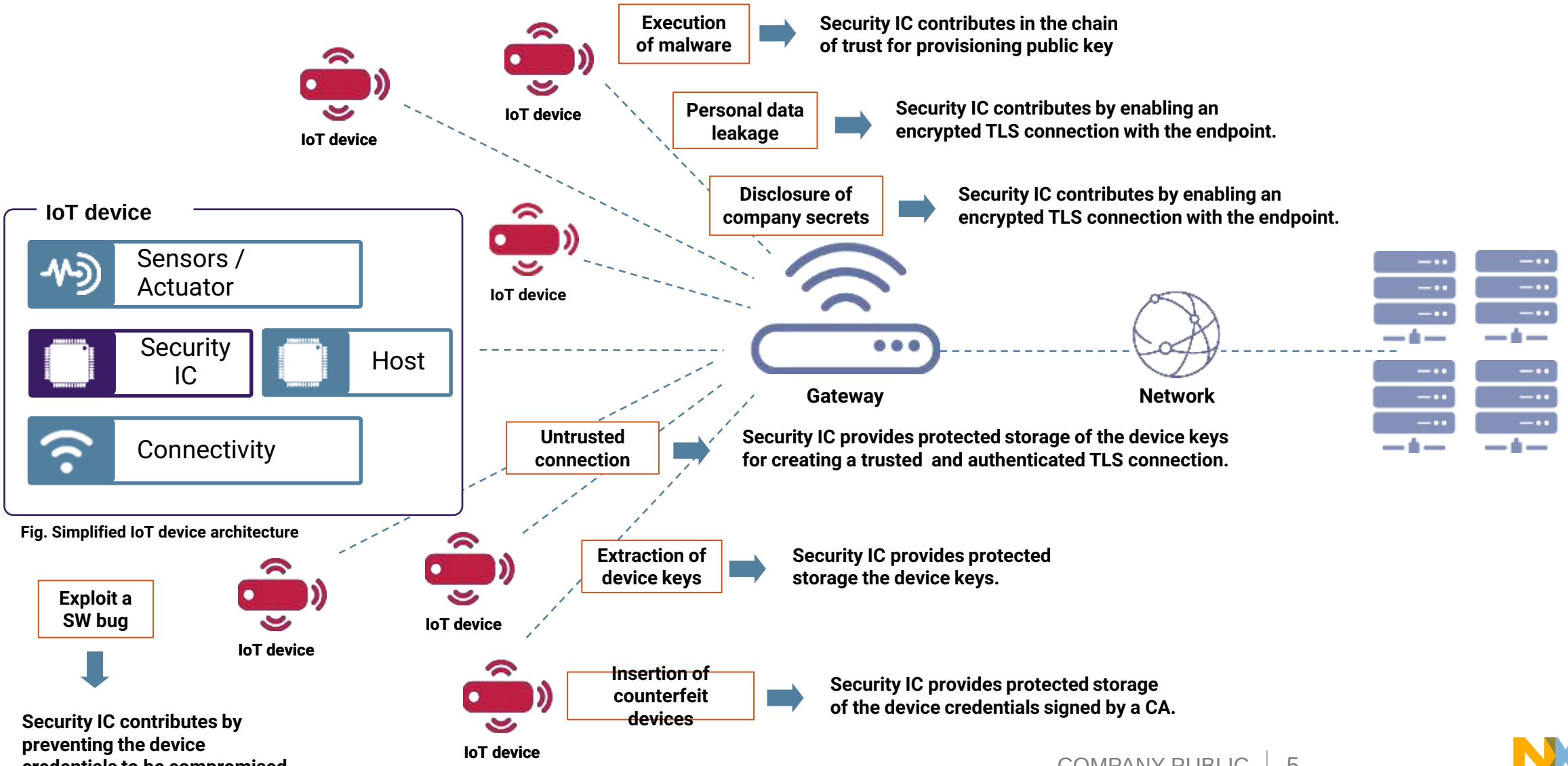
Overview of the Architectures

Security Architectures supported by current shipping NXP products

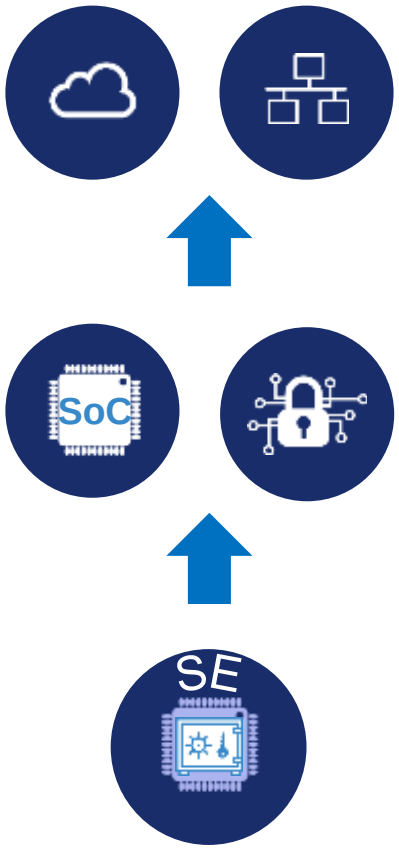


1) Not mandatory for MCUs/MPUs when they have embedded memory;
2) Features like RDC (Resource Domain Controller) on i.MX

IoT Devices Must Follow a Secure-by-design Approach



Layers of Security – Chain of Trust Based on Secure Element



Cloud / Network onboarding & device ID management

Mutual authentication based on credential stored on SE (e.g. certificate based TLS)
No key handling necessary at untrusted stages of supply chain.

Physical / Logical separation

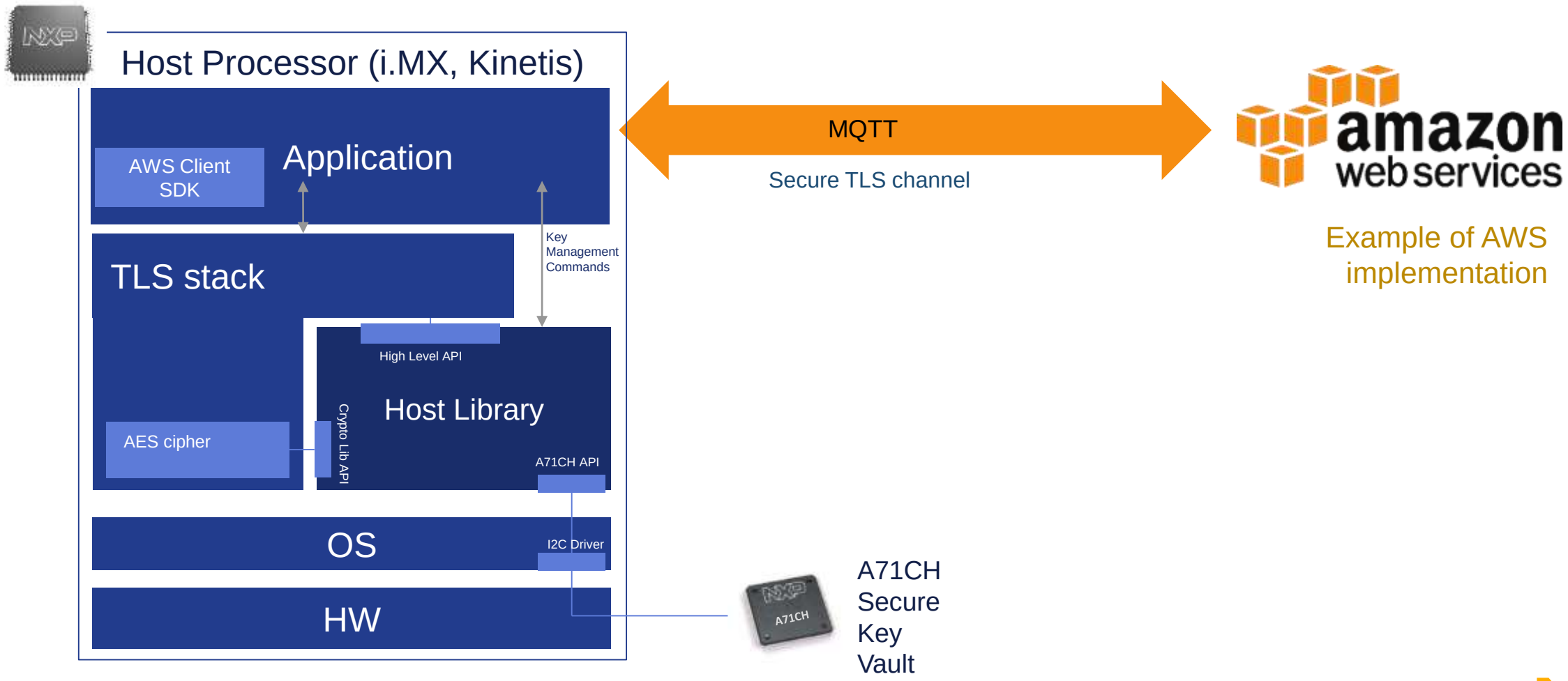
Only indirect access by the instruction set of the A71 applet, no direct memory access from SoC. Lifecycle Management protects keys throughout product lifecycle from unauthorized access (overwriting, deleting, manipulation, etc.).

Hardware Protection for the secrets

Pre-injected keys stored in hardware to identify genuine devices, all cryptographic calculations isolated in A71CH with own resources (CPU, NVM, Co-Processors, etc.), hardware design with basic measures against physical attacks, such as probing, hardware manipulation, glitches and light.

A71CH Features and Main Use Case

NXP Offers Complete Solution Including SE, Host Processor and Device SW Stack



Zero-touch Connect: Solution playing Security & Convenience factors

NXP Security IC Solution

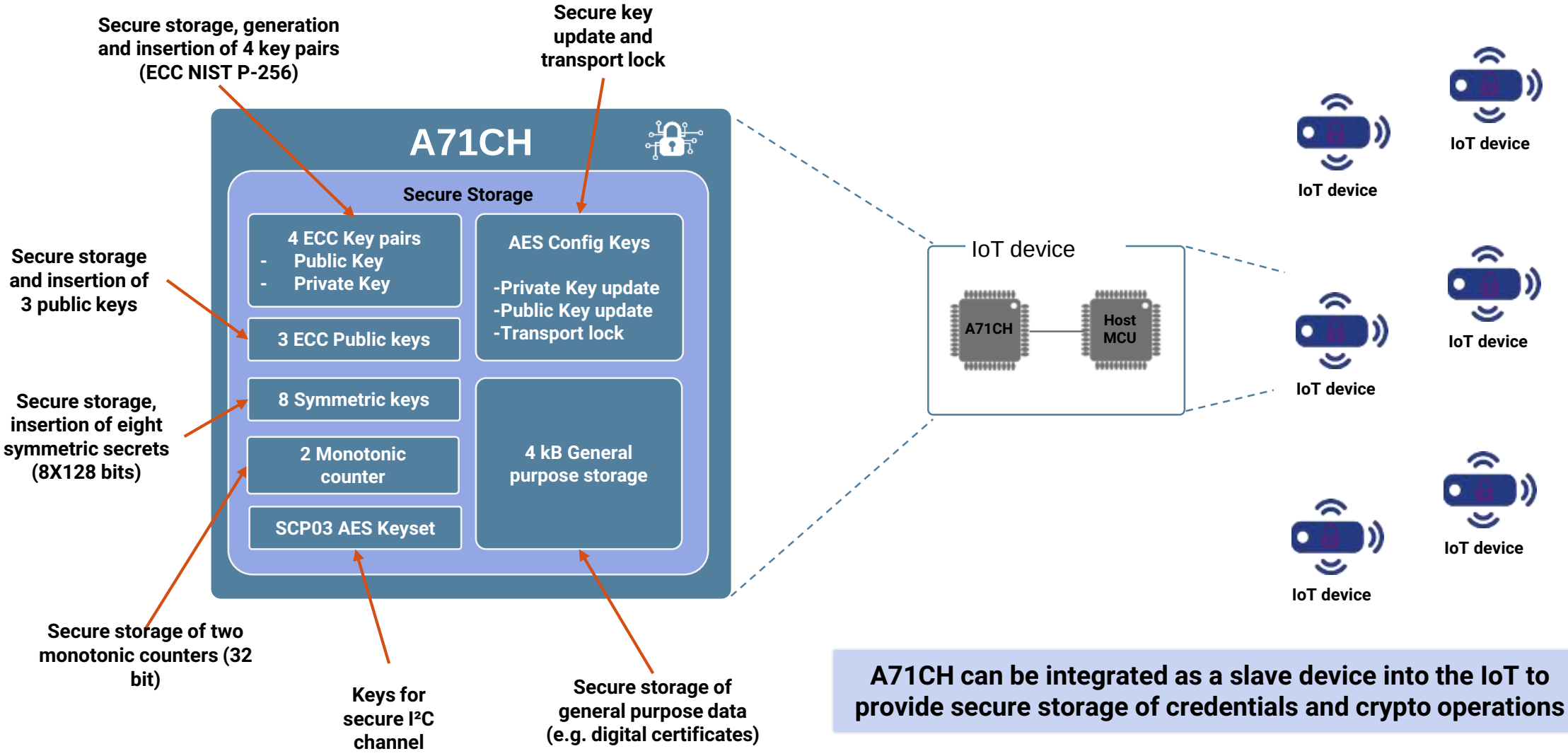
Drop NXP A71CH onto the board and integrate NXP client SW on the device.
A71CH contains all the necessary pre-injected keys for the device to connect securely to a public or private Clouds.

AWS IoT onboarding scheme

Key Benefits

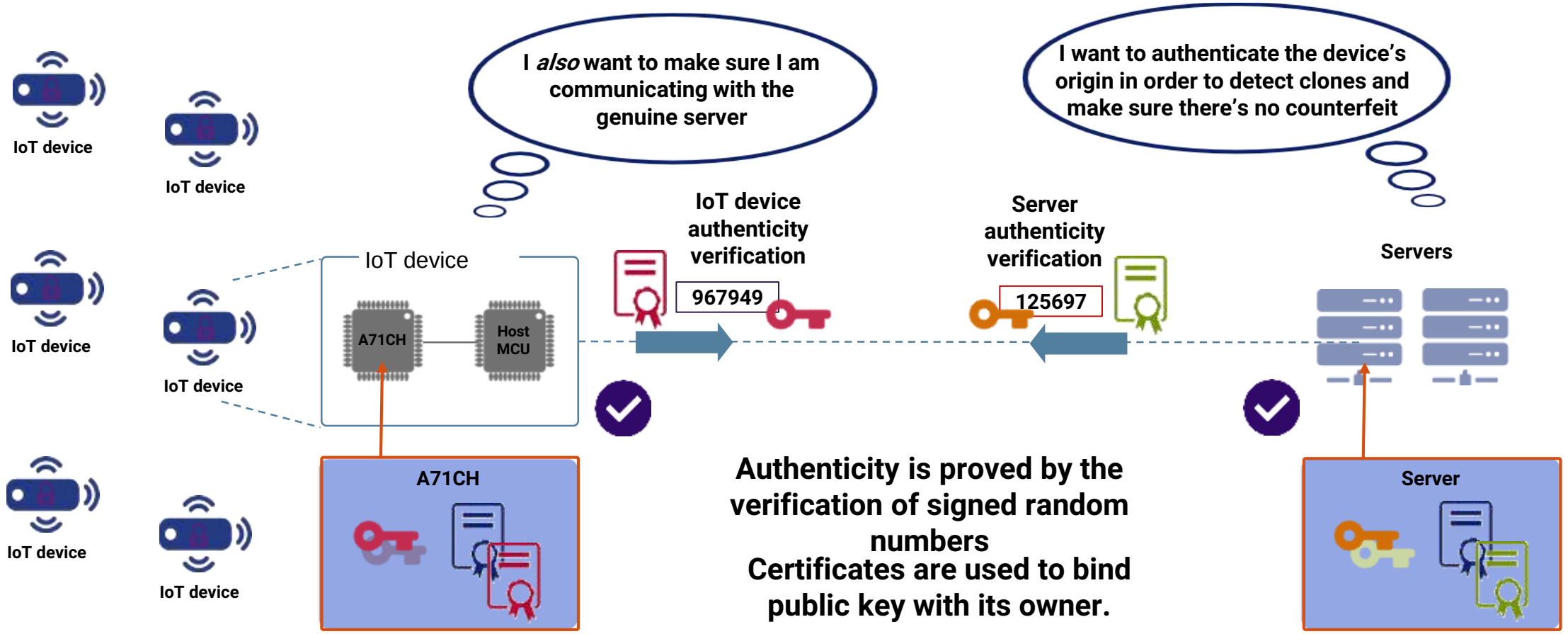
- ✓ Secure: protect back-end & data, independently from untrusted supply chain
- ✓ Convenient: easy to deploy, enabling own devices as well as 3rd party devices to connect to Public or Private Cloud.
- ✓ Scalable: suitable from product introduction phase (low volumes) up to mass production
- ✓ Cost effective: No cost of ownership for key management, no stickiness to contract manufacturers.

Protected Key Storage & Provisioning of Credentials

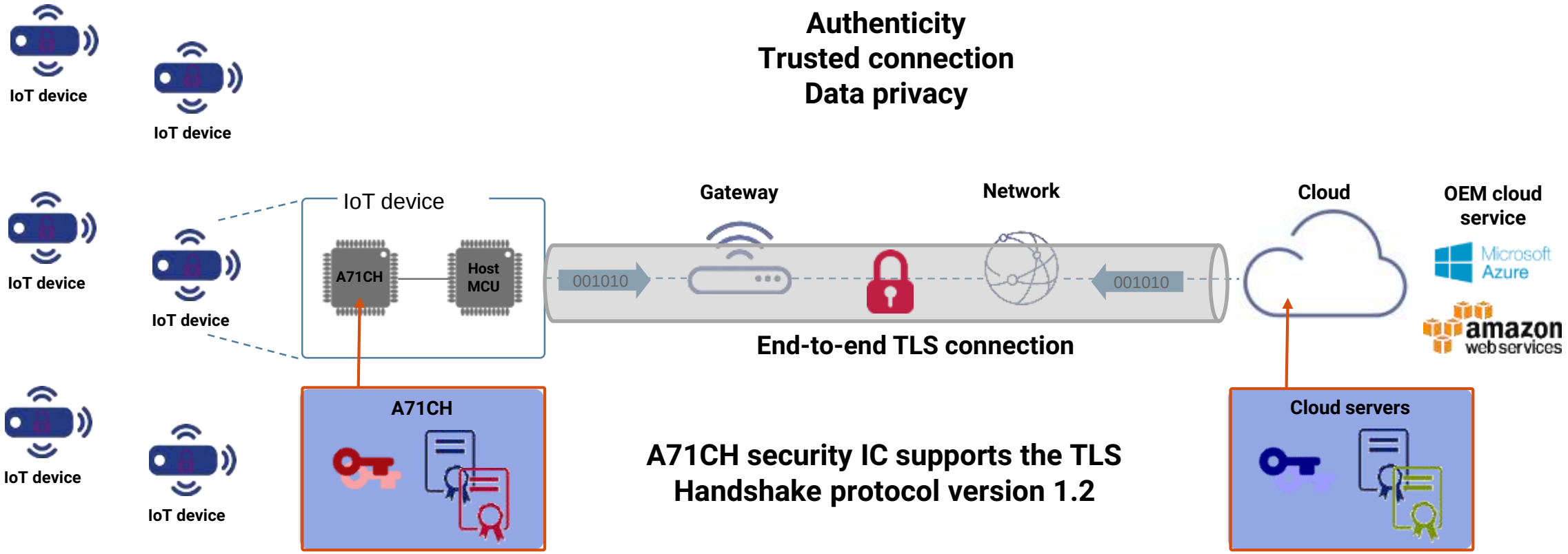


A71CH can be integrated as a slave device into the IoT to provide secure storage of credentials and crypto operations

A71CH for Device Proof of Origin / Anti-counterfeit



A71CH for Secure Connection to Public or Private Clouds



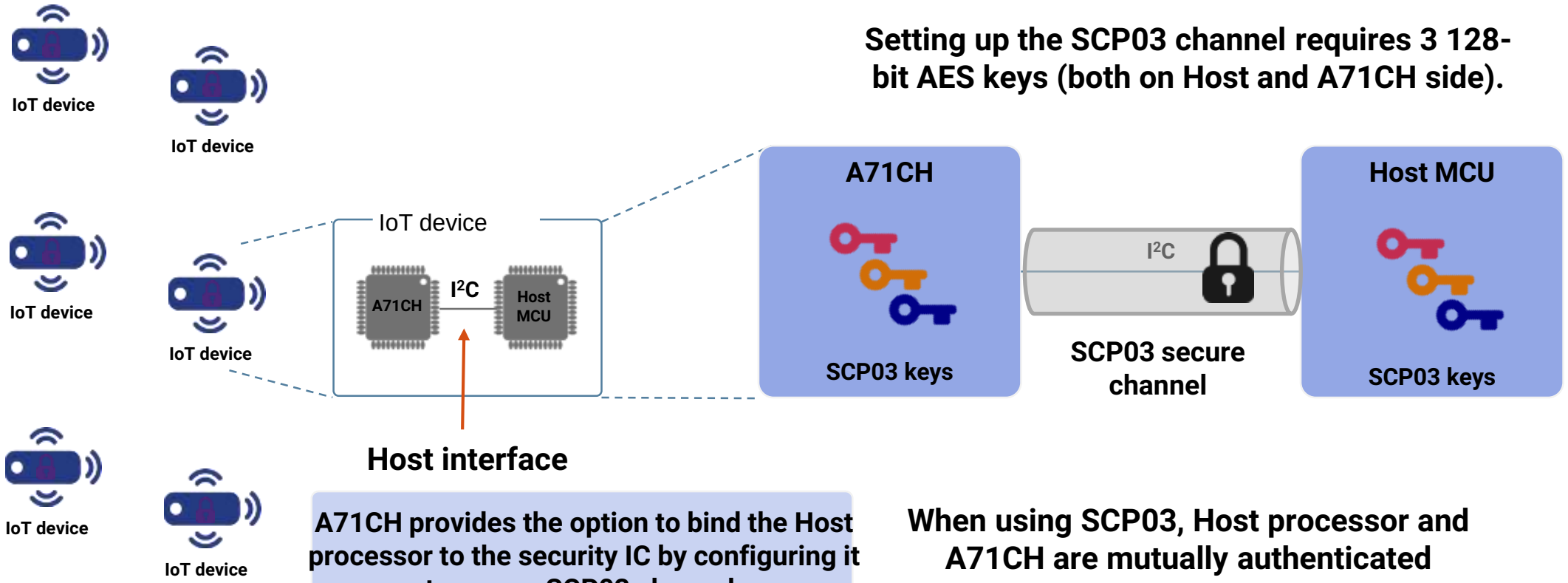
Authenticity
Trusted connection
Data privacy

End-to-end TLS connection

A71CH security IC supports the TLS Handshake protocol version 1.2

The keys and certificates used to authenticate the cloud connection remain secure in A71CH

A71CH for Encrypted / Authenticated Interface to Host Processor



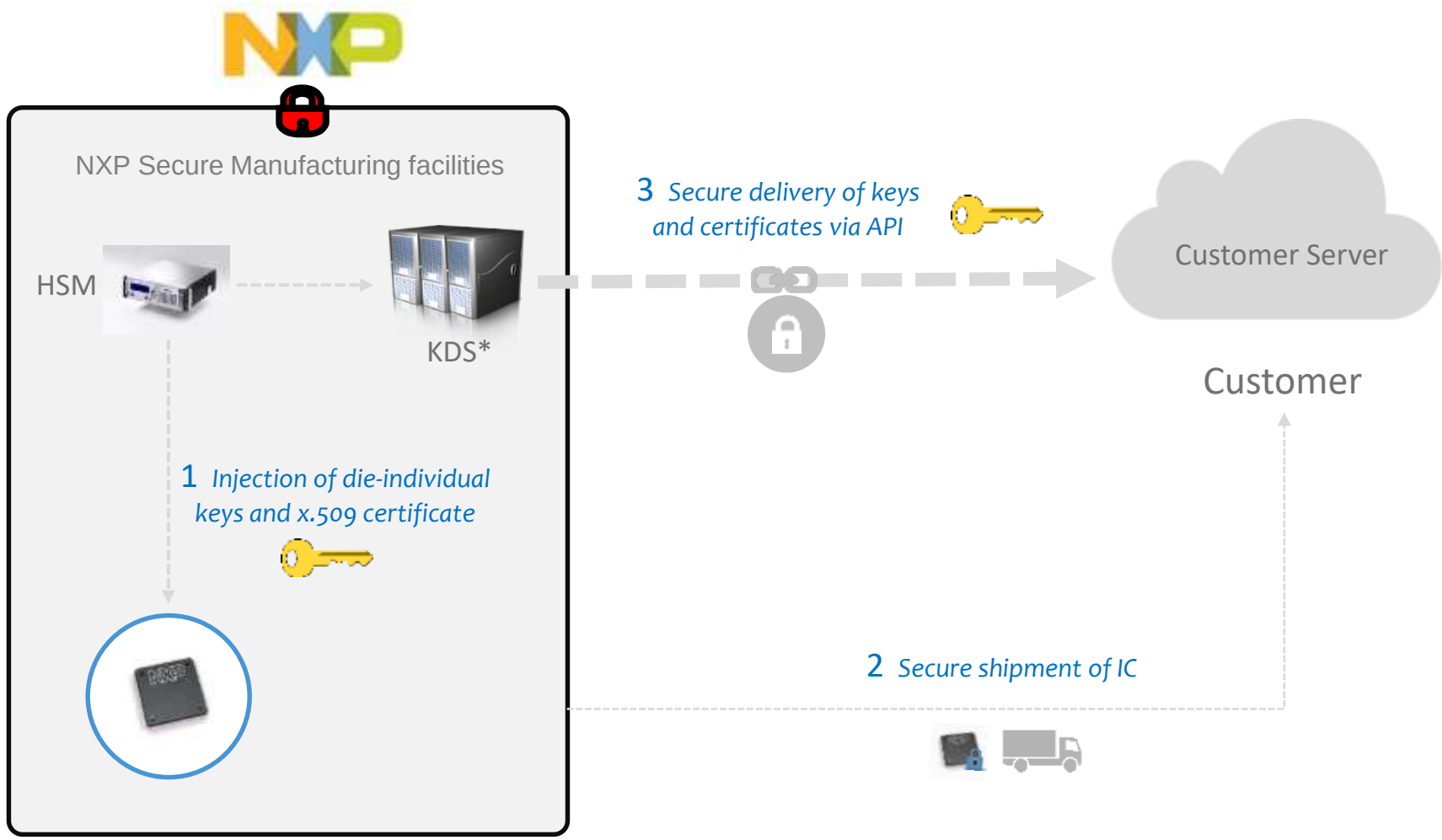
Setting up the SCP03 channel requires 3 128-bit AES keys (both on Host and A71CH side).

A71CH 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

When using SCP03, Host processor and A71CH are mutually authenticated

A71CH Trust Provisioning

NXP Secure Keys Provisioning System

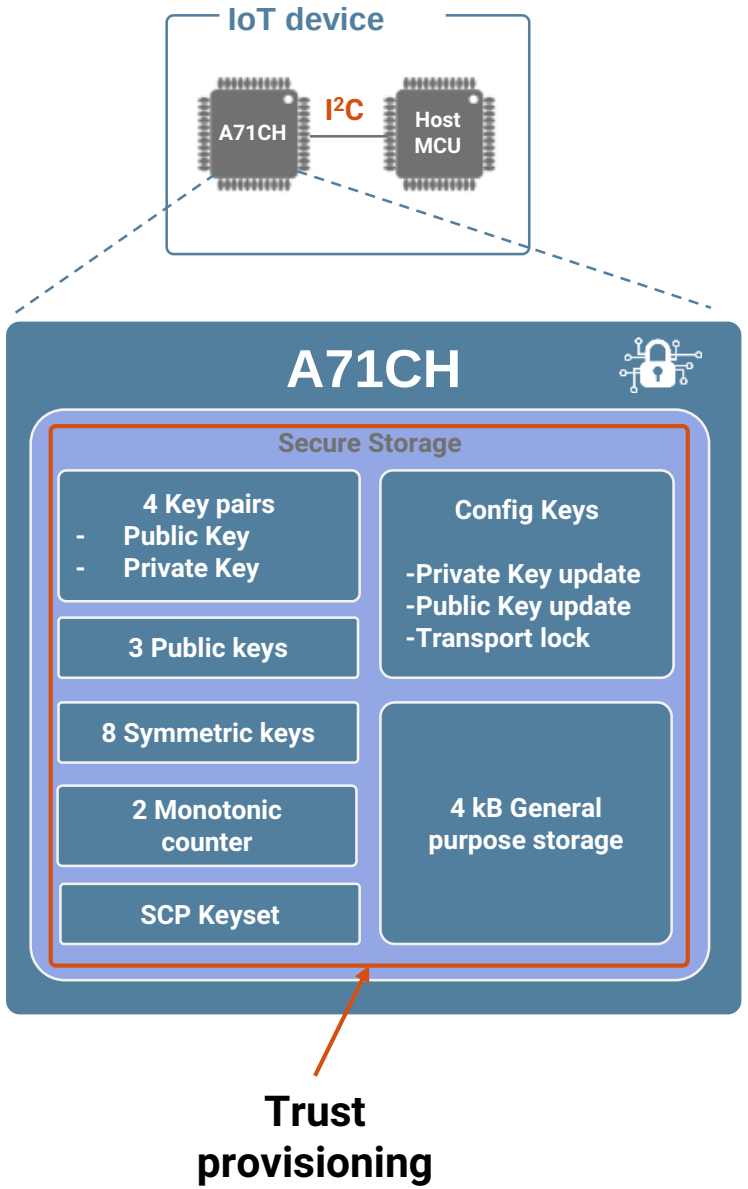


- No cost of ownership for key management
- End-to-end Security
- No reliance on EMS (easy switch)
- Less or no CAs to manage

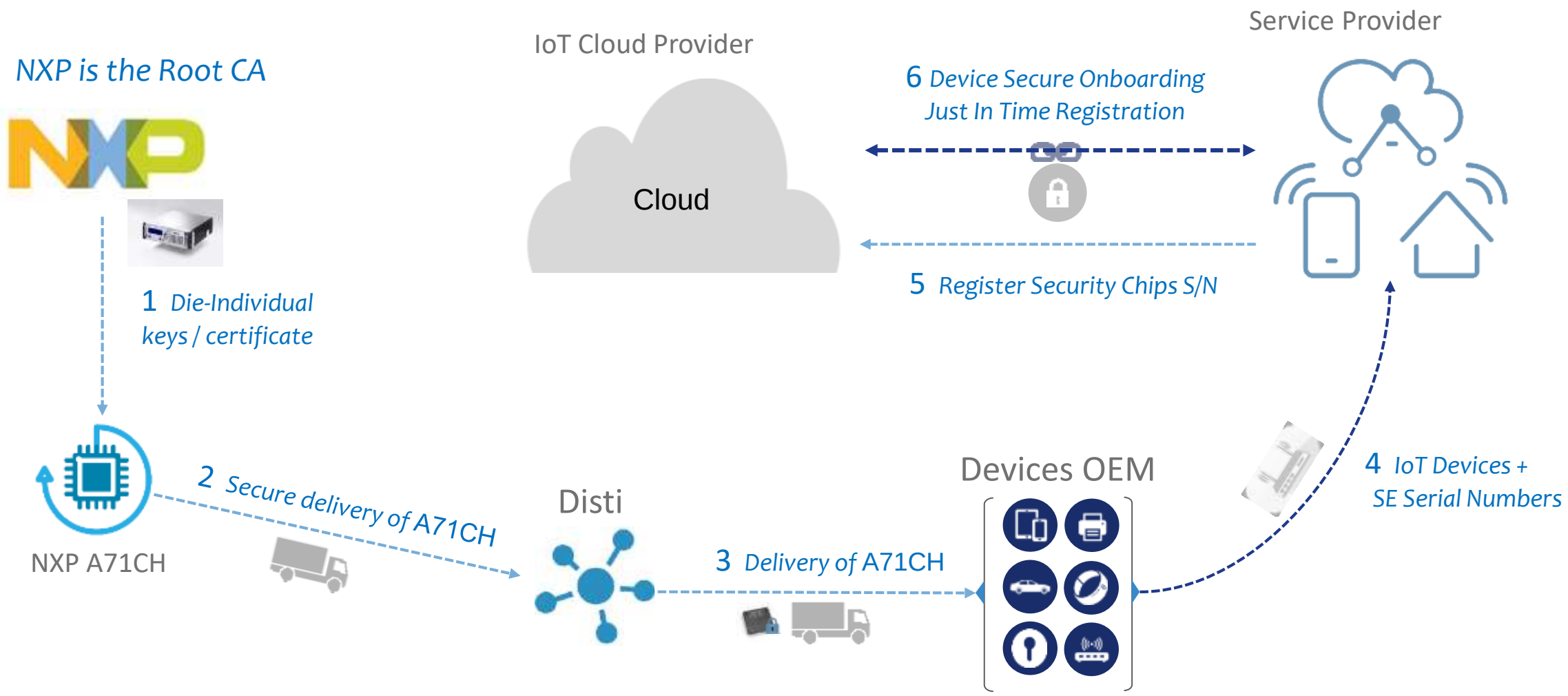
*KDS : Key Delivery Server

Trust Provisioning – What It Is

- Trust Provisioning allows to individually configure the IC content:
  - Put custom keys in device
  - Configure device
  - Readout data like UIDs
  - Key Generation / Key Injection
  - ...
- On A71CH Trust provisioning mainly means:
  - Put keys (generated or injected) inside and put certificate inside, which allow connection to Cloud systems



Enabling Trust into IoT Devices Connected to the Cloud



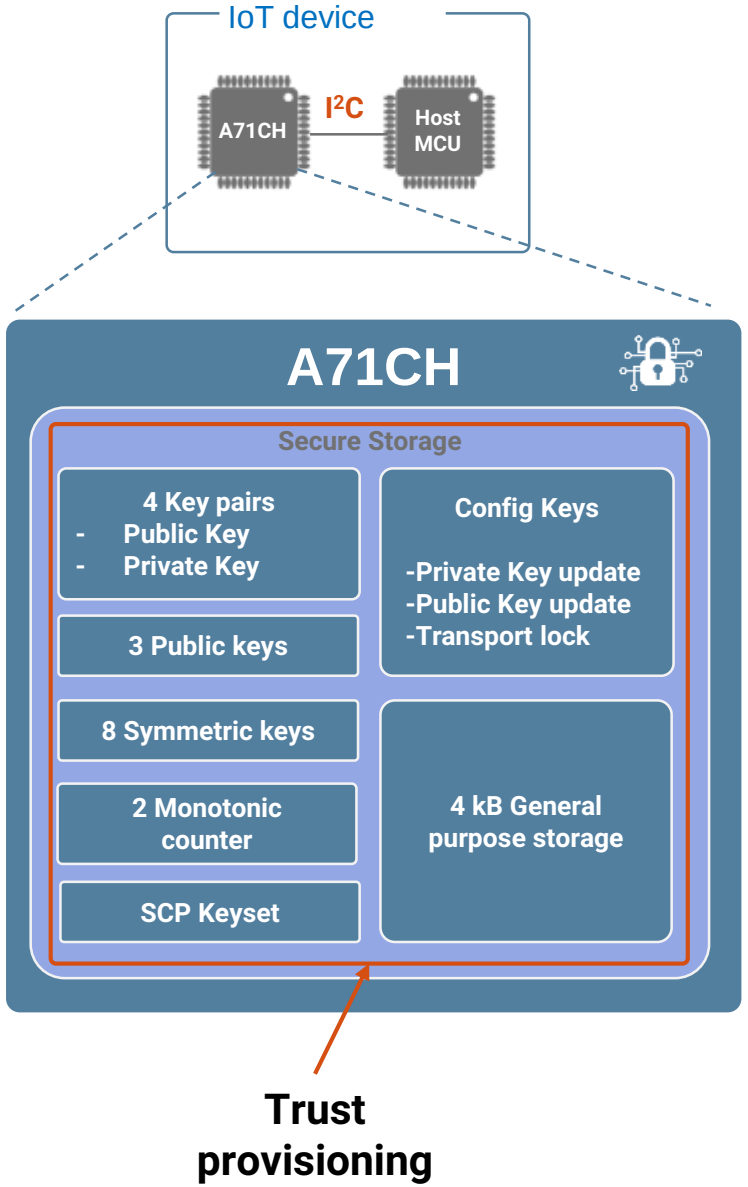
A71CH Trust Provisioning

NXP – High volume

- NXP offers this service for quantities > 150k

Distribution – Low volume

- Distributors have different business models providing the secure programming
  - In own programming centers
  - With 2nd party programming centers
  - Just programming with certificates provided by OEM
  - In partner with CAS
- To offer secure programming also for mass market, we have partnered with a company providing secure programming solutions: Data IO
- Data IO has implemented programming scripts for A71CH
- Data IO is partnering with Distributors to provide those solutions to them



A71CH Product Support Package

A71CH Arduino Compatible Development Kit

OM3710/A71CHARD

A71CH Arduino compatible dev kit

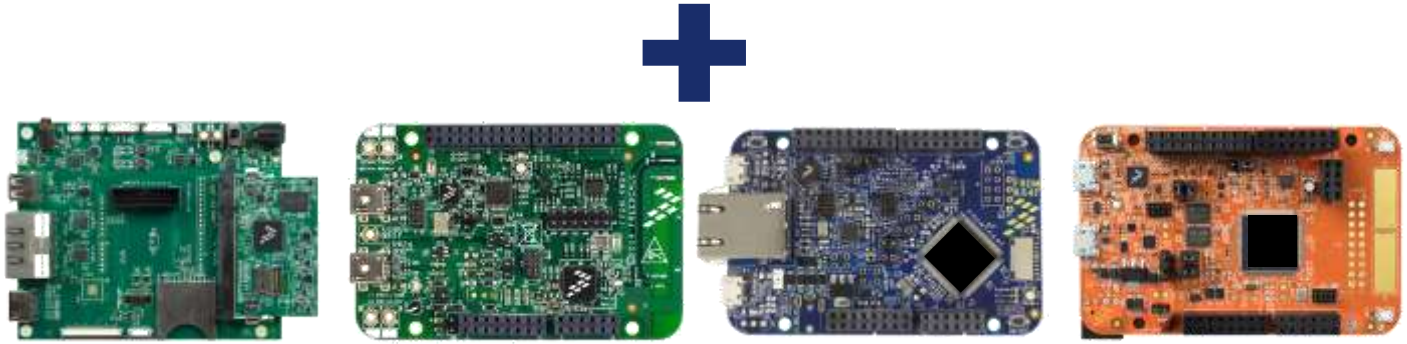
Part number complete kit: OM3710/A71CHARD
12NC: 935368997598
Ordering: eCommerce

OM3710/A71CHARD contents

- A71CH mini PCB board (OM3710/A71CHPCB)
- Arduino interface header board

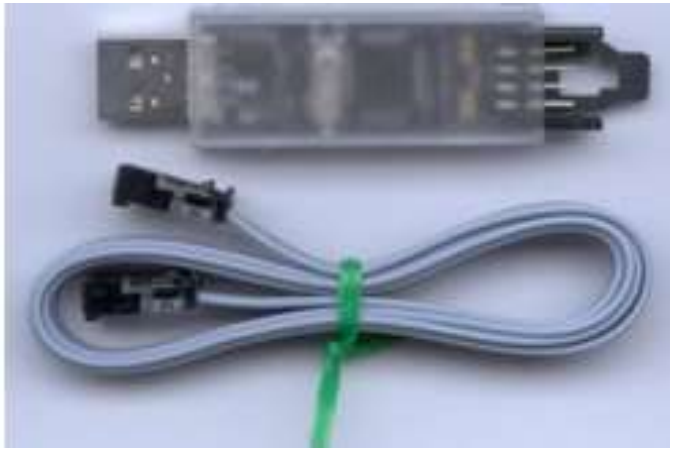
OM3710/A71CHARD features

- Arduino development kit based on Arduino adaptor board and A71CH mini PCB board.
- A71CH development kit to connect the A71CH security IC to any host featuring an Arduino compatible header.



USB / I²C Bird /Ascot Adaptor and VCOM Board to PC

USB / I²C bird (OM3710/B001)



Kinetis board as VCOM port

OM3710/B001 features

- Complete I²C/USB set enabling connection to PC.
- It shall be complemented with A71CH Mini PCB board.

OM3710/B001 contents

- I²C/USB dongle
- I²C data cable

Note: For availability please contact your NXP representative.

Features

- E.g. FRDM-K64F can be configured as VCOM boards after downloading a dedicated firmware.
- The VCOM port acts as a USB to I²C adaptor.

Part number complete kit: FRDM-K64F
12NC: 935326293598
Ordering: eCommerce

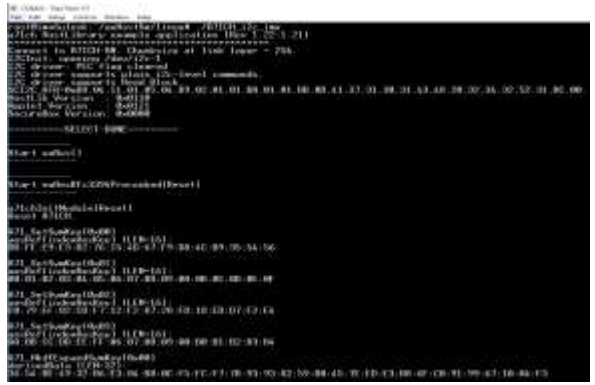
Part number complete kit: FRDM-K82F
12NC: 935327211598
Ordering: eCommerce

A71CH Host Software Package Contents

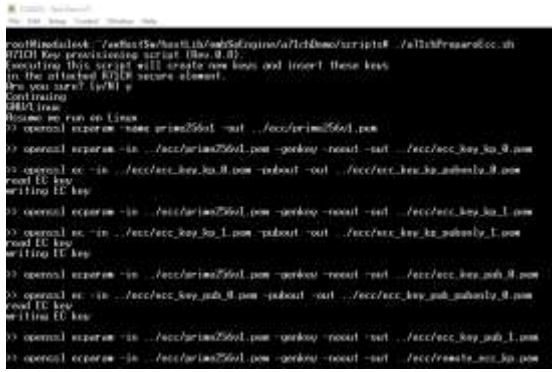
A71CH Host API source code

A71CH Host API documentation

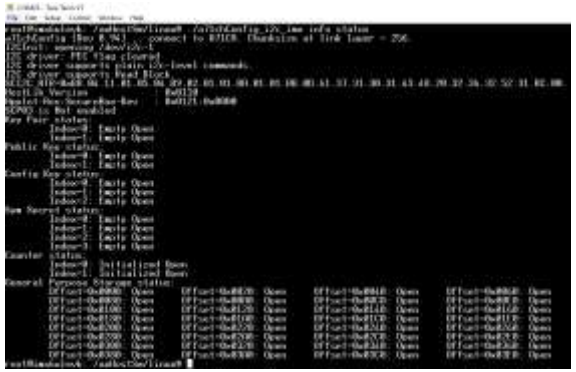
A71CH API usage examples



A71CH OpenSSL Engine examples



A71CH Configure tool



A71CH Documentation Overview 1/2

Type	Document Name	Content	Link
Datasheet	A71CH Datasheet	A71SDS 1.1 is „full“ datasheet	Link
Porting	AN12185 A71CH Porting Guidelines	Guideline on porting the hostlibrary	Link
Protocol	AN12207 - Application note SCIIC Protocol Specification	SmartCard I²C interface protocol specification	Link
	AN12211 A71CH Security Guidelines (login needed)	Security recommendations for using the A71CH security module	Link
	AN12229 A71CH APDU Specification (login needed)	APDU command specification of the A71CH	Link
Host Lib	AN12133 – A71CH Host software package documentation	Provides overview of the A71CH Host software architecture and the A71CH application examples	Link
	um4334xx - A71CH OpenSSL Engine	Included in HostLibrary Installer	

Note: xx = version of document

A71CH Documentation Overview 2/2

Type	Document Name	Content	Link
Overview	AN12121 – How to start a development with A71CH	Overview support material available for designs based on the A71CH solution.	LINK
Quick Start	AN12119 – A71CH Quick start guide for OM3710A71CHARD and i.MXUltraLite	Guide for setting up the development environment for A71CH Arduino development kit and i.MX6UltraLite	LINK
	AN12135 – A71CH Quick start guide for OM3710A71CHARD and Kinetis	Guide for setting up the development environment for A71CH Arduino development kit and Kinetis boards	Link
	AN12134 – A71CH Quick start guide for Windows	Setting up the development environment for USB I²C interface kit on Windows	Link
Use Case	AN12131 – A71CH for secure connection to AWS cloud	Detailed description on how the A71CH can be used to create a secure connection with AWS Cloud	Link
	AN12199 A71CH for secure connection to Google Cloud	How to use A71CH to secure the connection to Google Cloud	Link
	AN12132 – A71CH for secure connection to OEM cloud	Description on how the A71CH can be used to create a secure connection with the OEM Cloud	Link
	AN12120 – A7CH for electronic anticounterfeit protection	Describes how the A71CH can be used to implement a mutual authentication mechanism based on ECC crypto	Link

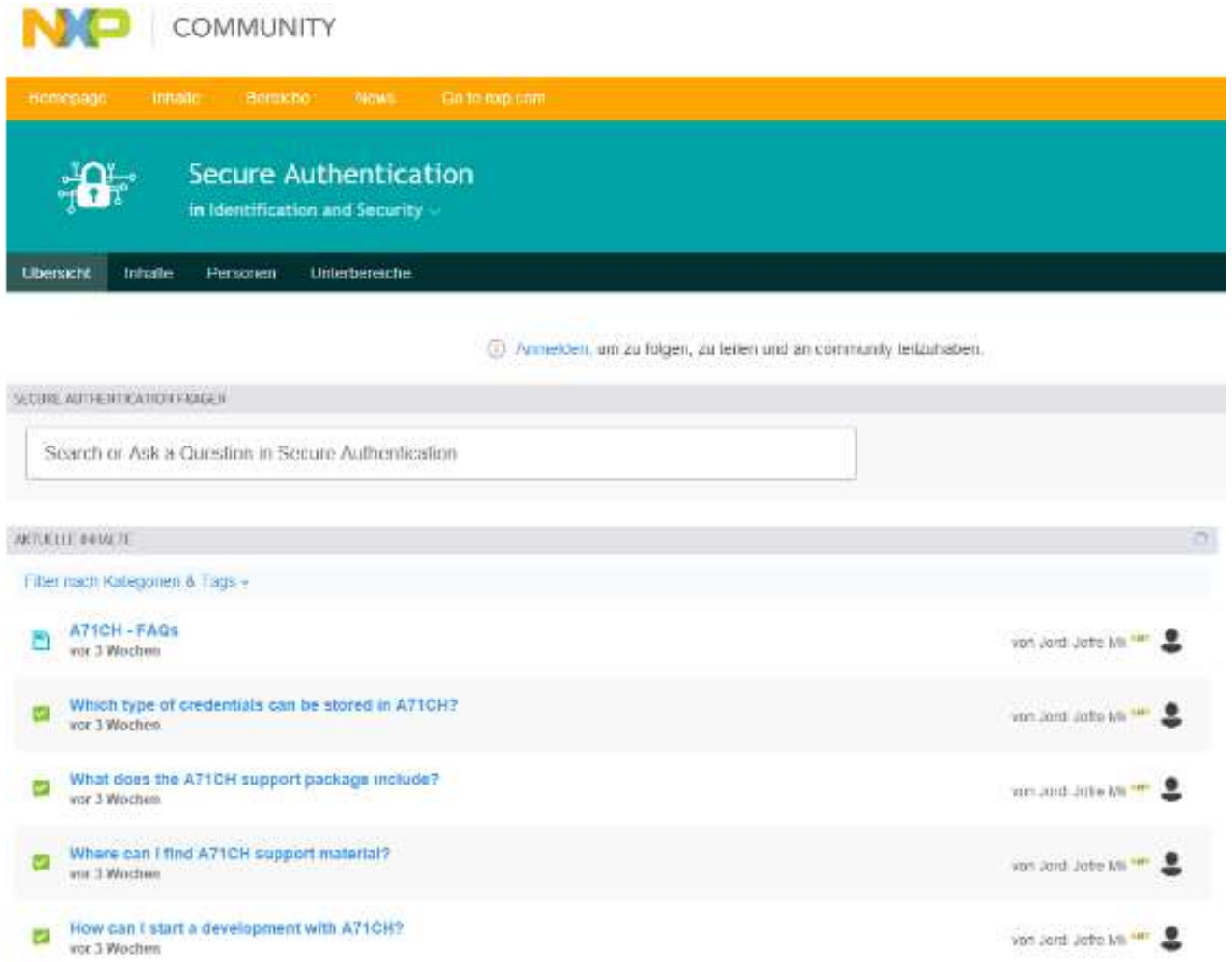
A71CH Software Overview

Login on nxp.com needed for all SW downloads

SW Name	Delivery Form	Link
Host Library Software Package – usable on Windows, Linux (i.MX)	Windows Installer (hostlib for all platforms)	Link Currently 1.4.3
	Bash Installer for e.g. Linux or Cygwin (linux hostlib)	Link
Bootable SD card image for i.MX6UL	Windows Installer (unzips image + complete hostlib)	Link Currently 1.4.0
	Bash Installer for e.g. Linux or Cygwin (unzips image)	Link

New Community Secure Authentication

https://community.nxp.com/community/identification-security/secure-authentication



A71CH Technical Implementation Details

A71CH I²C

A71CH – I²C Interface

- Standard I²C bus slave device with I²C Fast mode up to 400 kHz
- Interface Startup conditions needed at least 500µs after Power on:

Value at startup				I²C address	
IF0	IF1	I2C_SCL	I2C_SDA	Write	Read
0	x	0	0	n.a.	n.a.
1	0	1	1	0x90	0x91
1	1	1	1	0x92	0x93

- After 312ms of inactivity device goes to SLEEP and need to be woken up (any bus activity wakes device up, then send again)
- Further requirements due to next protocol layer SCI²C:
  - Repeated start needs to be possible
  - SCI²C uses SMBus Block_Read

A71CH SCI²C

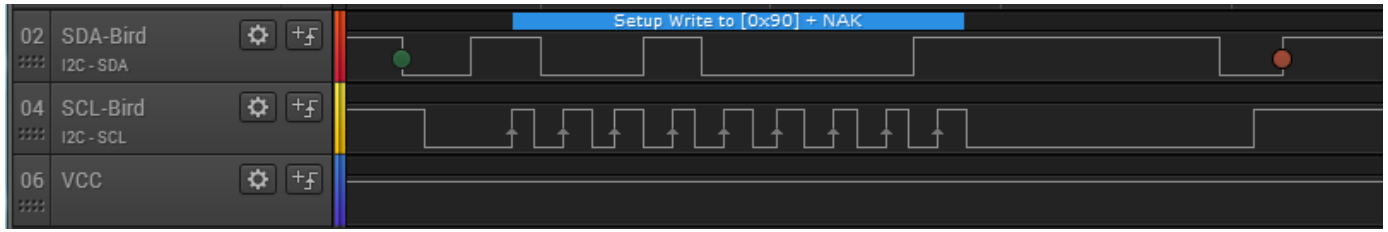
A71CH - SCI²C – What Is It

- SCI2C = **S**mart**C**ard**I²C**
- Encapsulation of Smartcard APDUs (Application Protocol Data Unit) on I²C
- Mapping of APDU commands to SMBus command
  - C-APDU (Command to device) uses BlockWrite, then polling on I²C device address until response ready
  - Waiting Time Extension like on APDU interface (device responds with request for more time until response ready)
  - R-APDU (Response from device) uses BlockRead
- Specification on nxp.com Link
  AN12207 - Application note SCIIC Protocol Specification (docNr: AN19501x)
  (Specification version has to be version 1.x, currently 1.6)
- SCI²C usage on i.MX6 explained in hostLib doxygen:
  html\page_sci2c_info.html

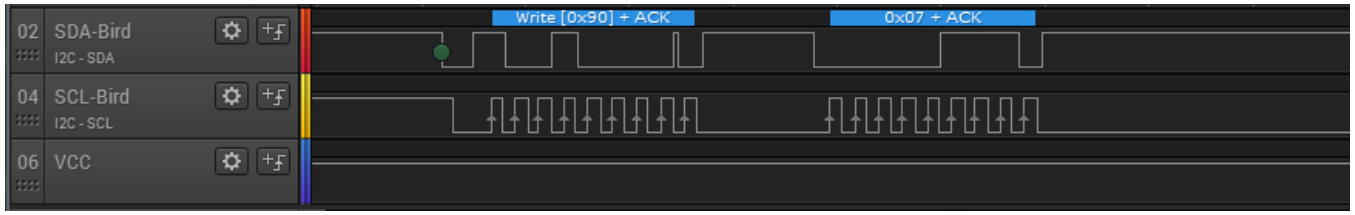
Note: Next generation IoT Secure element will use T=1 I2C instead

SCI2C – Send APDU – Wakeup Device

- To wakeup the A71 – send anything, Slave device will be NACKed



- Any edge on the I2C lines is enough to wakeup the IC
- After wakeup the IC now acknowledges the device address



- The real command needs to be sent within 312 ms

A71CH SCP03

A71CH – SCP03 – What Is It

- **S**ecure **C**hannel **P**rotocol 03, successor of SCP02
- Standard protocol to secure smartcard communication based on AES
- Specification: Global Platform: Card Technology Secure Channel Protocol '03' Card Specification v2.2 – Amendment D V1.1.1 (Link)
- Implemented in Host Library in scp.c using host cryptography

A71CH - SCP03 – Use Cases

- SCP03 can be used to bind the MCU and A71CH together
  - MCU generates random AES keys on first startup
  - Put these keys to the A71CH (most likely this first startup is in the factory)
  - After first authentication the A71CH then needs SCP03 secure channel for most functionality
  - SCP03 AES keys in MCU don‘t protect secrets, only the binding.

→ Insertion of A71CH into another device (resoldering) prevented as strong as the AES keys in the MCU are protected.

A71CH – SCP03 – Need to Know

- After keys got set and first authentication done, the SCP03 channel gets mandatory
- When no SCP03 is used, an attacker could set keys and authenticate and so create a Denial of Service situation
- → Even if no SCP03 is used, keys should get set
  - To disable SCP03 permanenty: set random keys

A71CH Features

A71CH Modes

- Some relevant states/modes (independent from each other):
  - Debug mode (on/off):
    - active on “customer programmable” type
    - allows complete reset of everything
    - Disabling debug mode is irreversible
  - PlainInjectionMode (on/off):
    - Active on “customer programmable type”
    - Allows plain injection of secrets
  - Credentials can be:
    - ABSENT or INITIALIZED
    - UNLOCKED or LOCKED (frozen)

Features and Default Values on “Customer Programmable” Type

Credential / State	Amount	Description	Default Value	Credential Freeze
Asymmetric Key Pairs	4x ECDSA NIST P-256 private + public key	Not set, not locked	CREDENTIAL_ABSENT	CREDENTIAL_ UNLOCKED
Asymmetric Public Keys	3x ECDSA NIST P-256 public keys	Not set, not locked	CREDENTIAL_ABSENT	CREDENTIAL_ UNLOCKED
Config Keys	3x AES128	Not set, cannot be locked	CREDENTIAL_ABSENT	CREDENTIAL_ UNLOCKED
Symmetric Secret	8x 128 bit key data	Not set, cannot be locked	CREDENTIAL_ABSENT	CREDENTIAL_ UNLOCKED
Monotonic Counter	2x upcounting counter with 32 bit	Counter set to 0, cannot be locked	CREDENTIAL_INITIALIZED	CREDENTIAL_ UNLOCKED
SCP channel	SCP03 keyset with 3 AES128 keys	Keys not set, SCP03 not active	SCP_NOT_REQUIRED	N/A
GP Data	128 segments of 32 bytes each	All bytes set to 0x00	CREDENTIAL_ABSENT	CREDENTIAL_ UNLOCKED
Plain Injection Mode		Plain secrets can be inserted	INJECTION_UNLOCKED	N/A
Debug Mode		Debug Mode is active	DEBUG_ON	N/A
TransportLock		Module can be set to "LOCKED"	MODULE_ALLOW_LOCK	N/A

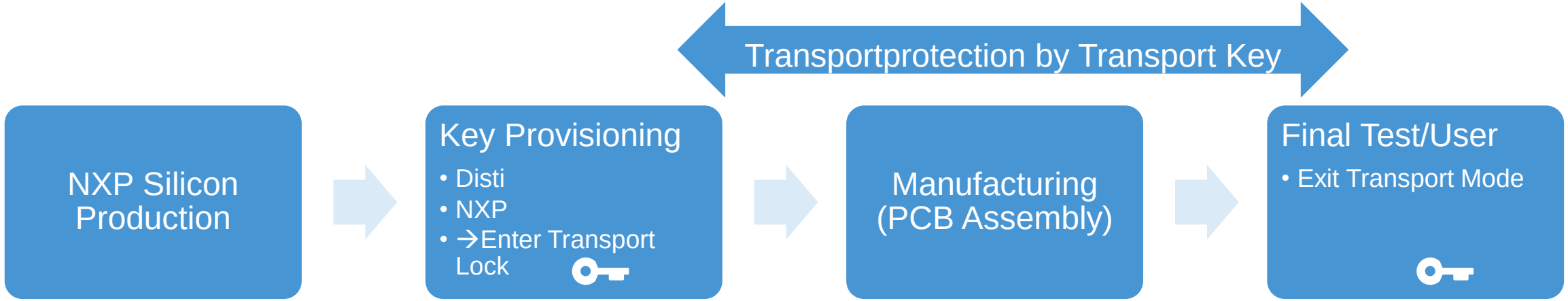
Config Keys

- A71CH contains three “config keys” (AES128)
  - 0: CFG_KEY_IDX_MODULE_LOCK – key to exit transport mode
  - 1: CFG_KEY_IDX_ PRIVATE_KEYS – key to update asymmetric keypair
  - 2: CFG_KEY_IDX_ PUBLIC_KEYS – key to update public key
- Config keys are not set by default (empty)
- Can only be used after being set
- Useful in the field to change keys (as long as they are not frozen)

Transport Lock

- In case the A71CH will be trustprovisioned by not the OEM but e.g.:
  - third party like disti
  - NXP

    To protect against misuse during transport (e.g. shipment gets lost/stolen) a transport key can be used to lock the secure element until it is used



Cloud Authentication

What Do You Need?

A71CH Arduino compatible development kit

Contents
A71CH mini PCB board
Arduino interface header board

Part number: OM3710/A71CHARD
12NC: 935368997598
URL: www.nxp.com/OM3710

FRDM-K64F board

Contents
Freedom K64F dev platform for K64, K63, and K24 MCUs.

Part number: FRDM-K64F
12NC: 935326293598
URL: www.nxp.com/FRDM-K64F

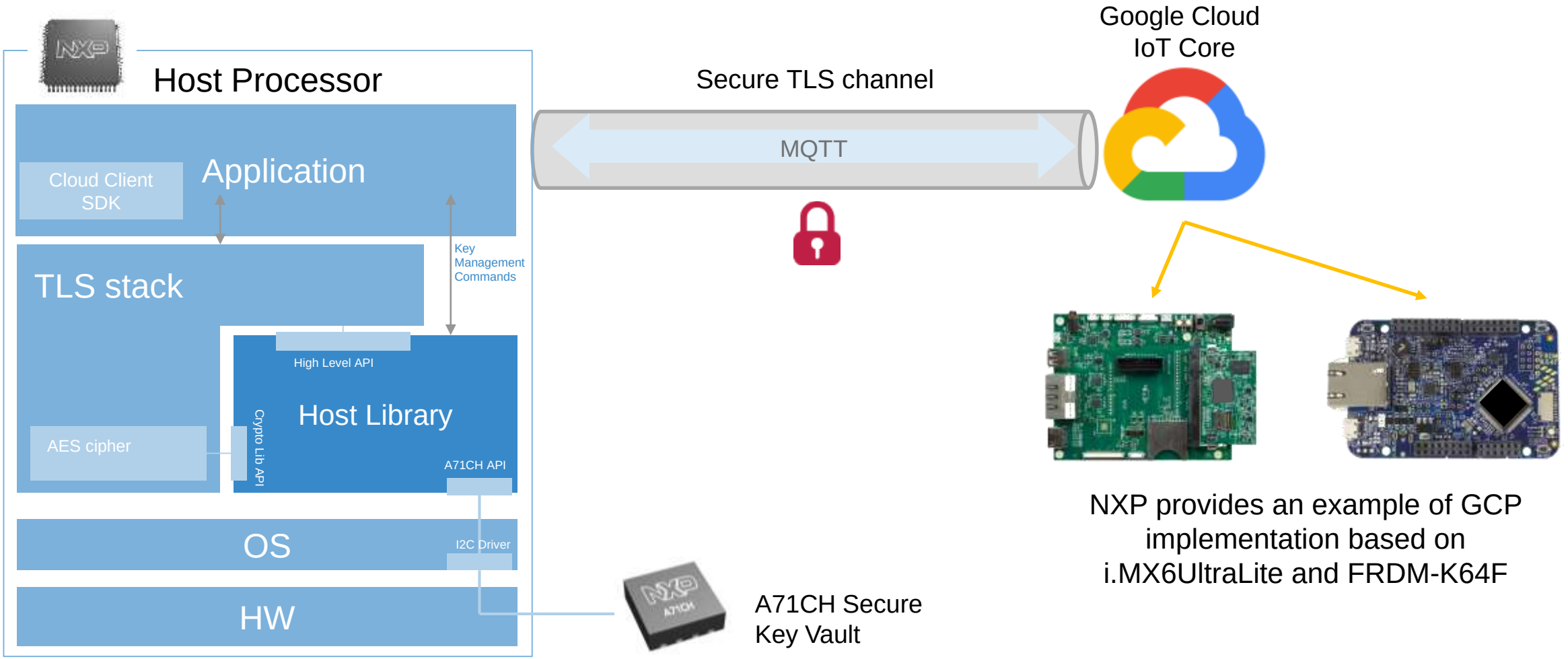
Development PC

Laptop
Standard laptop running Linux or Windows environment

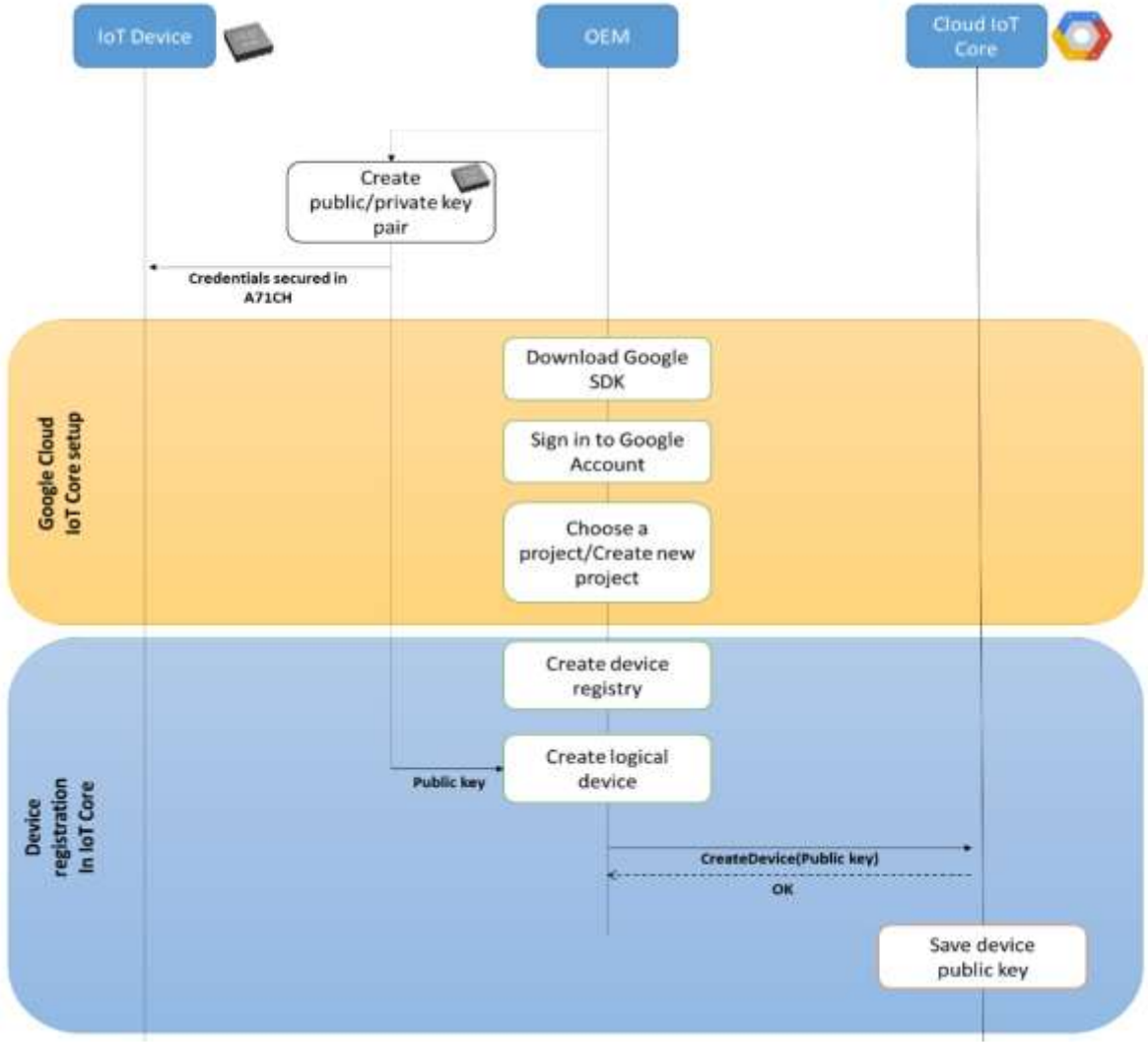
Google Cloud IoT Core account

URL:
https://cloud.google.com/iot-core/

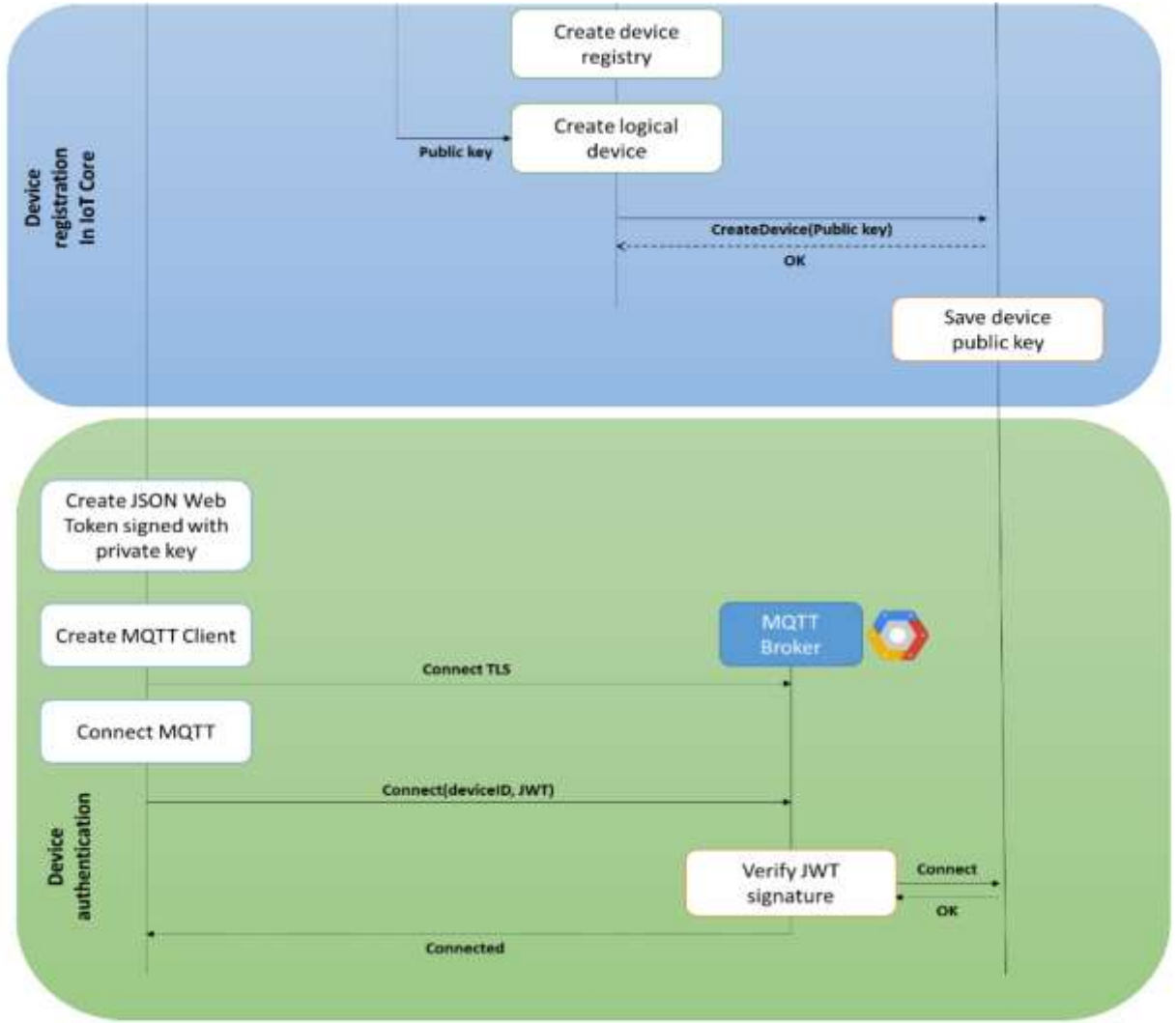
Sample Application for Google Cloud IoT Core Connection



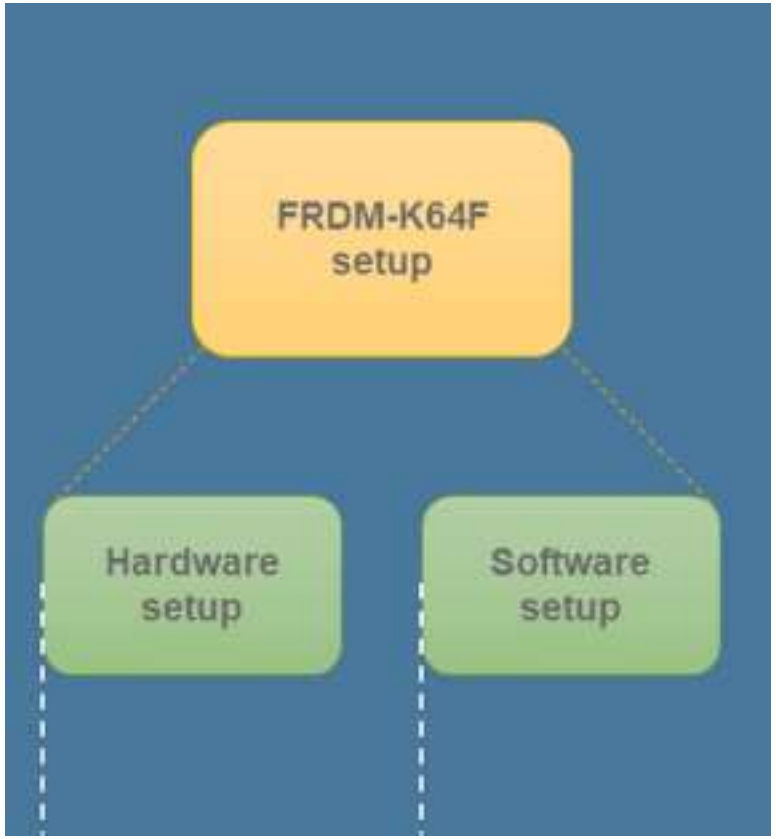
Cloud Connection Flow



Cloud Connection Flow



HW & SW Setup



https://www.nxp.com/docs/en/application-note/AN12135.pdf

Download and open AN12135

AN12135

A71CH Quick start guide for OM3710A71CHARD and Kinetis

Rev. 1.0 — 09 July 2018 Application note
458210 COMPANY PUBLIC

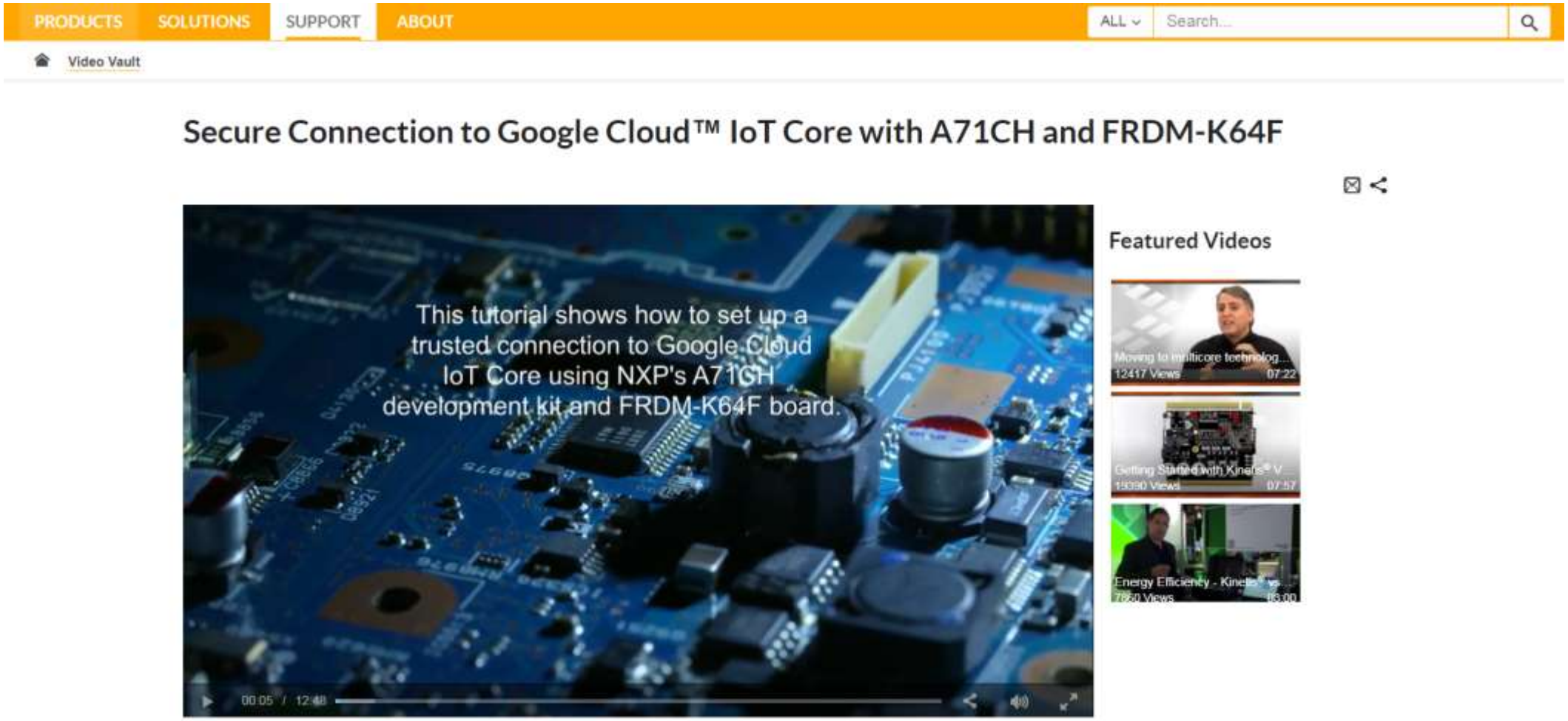
9. References

All the references contained in this document are listed in the following table:

Table 3. References

[A71CH_HOST_SW]	**A71CH Host Software Package (Bash installer for Windows)** – DocStore, document number sw4673xx[1], Version 01.04.00 (or later), available on www.nxp.com/A71CH **A71CH Host Software Package (Bash installer for Linux)** – DocStore, document number sw4672xx[1], Version 01.03.00 (or later), available on www.nxp.com/A71CH
[AN_A71CH_HOST_SW]	**AN12133 A71CH Host software package documentation** – Application note, document number 4643**[1]
[QUICK_START_WIN]	**AN12134 Quick start guide for Windows** – Application note, document number 4644**[1]
[TERA_TERM]	**Tera Term terminal** - https://osdn.net/projects/ttssh2/releases/
[MCUXPRESSO_IDE]	**MCUXpresso IDE** - https://www.nxp.com/support/developer-resources/software-development-tools/mcuxpresso-software-and-tools/mcuxpresso-integrated-development-environment-ide:MCUXpresso-IDE
[OPENSDA_FIRMWARE]	**OpenSDA / OpenSDA V2 website** - https://www.segger.com/products/debug-probes/j-link/models/other-j-links/opensda-sda-v2/
[MBED_TLS]	**mbedTLS website** - https://tls.mbed.org/
[SDKBUILDER]	**MCUXPresso SBKBuilder website** - https://mcuxpresso.nxp.com/en/select
[FRDM_K64F]	**Kinetis FRDM-K64F** - https://www.nxp.com/products/processors-and-microcontrollers/arm-based-processors-and-mcus/kinetis-cortex-m-mcus/k-seriesperformancem4/k2x-usb/freedom-development-platform-for-kinetis-k64-k63-and-k24-mcus:FRDM-K64F

Full Video Available Online



https://www.nxp.com/video/:CONNECTION-A71CH-AND-FRDM-K64F

SECURE CONNECTIONS
FOR A SMARTER WORLD