

# NXP's Portfolio for Addressing IoT Security

Donnie Garcia

Systems & Applications Engineer  
NXP IoT Solutions

June 2019 | Session #AMF-SMH-T3517



SECURE CONNECTIONS  
FOR A SMARTER WORLD

# Agenda

---

- Threat Landscape and Legislation
- IoT Security Strategies
- NXP Products: Secure Edge
- Product Functional Showcases
  - Secure Elements and Microcontrollers
  - Edge Compute Application Processors
  - Device Cloud Management Software
  - Solutions
- Conclusions

# Threat Landscape and Legislation



# The Lack of Security in IoT is Now Tangible

## THE BOTNET THAT BROKE THE INTERNET ISN'T GOING AWAY



## Mirai botnet

Disruption of major Internet services

Software bug makes Nest Cams vulnerable to hacks



## Jeep hack

Loss of control over vehicle via WiFi connection



## Nest Hack

Security camera shut down by a simple click on a phone



## Casino hack

Overview of high-rollers extracted via thermostat of a fish-aquarium in the lobby

## Target Hack

Target declared that the total cost of the data breach had been \$202M *NBC news, May 24, 2017*

SEPTEMBER 20, 2017 by Mamta Badkar in New York

Parcel delivery company **FedEx** said on Tuesday that a June **cyber attack** on its **TNT Express** unit **cost** the company **\$300m in the first quarter**, ... the **NotPetya** cyber attack, which originated from tax preparation software in Ukraine and resulted in the disruption of communications systems at TNT Express.





# Hundreds of keyless cars are vulnerable to high-tech theft, new report says


By Emily Dixon, CNN

Updated 10:27 AM ET, Mon January 28, 2019



More from CNN

 Biden camp: Giuliani's call to Ukraine

 He said his was abducted, found blood

 DOES EVERY IN STYLE.

*The vehicles can be stolen using "cheap electronic equipment" purchased online,*

*...thieves can use relay boxes to boost the fob's signal. This tricks the system into believing the fob is near the car...*

*"...say availability of relay equipment should be outlawed, and anyone found with it who is not a bona fide industry representative dealt with as if going equipped to steal."*

*manufacturers should basically not offer keyless technology which is counter to customer demand and feedback."*

*...owners of keyless cars should take extra security precautions, including storing their fobs in a "metal box or shielded pouch"*

# Consumer IoT Device Attack Trends

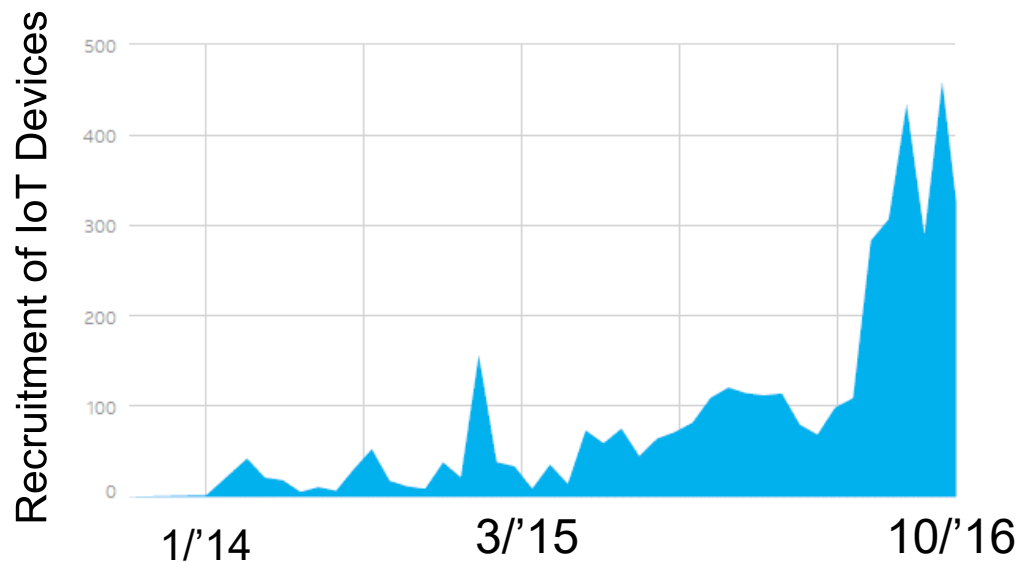
Attack method	Profitability	Comment	Trend
DDoS attacks	+	Still growing in size - simple	↑
Spam attacks	- -	Not the easiest way to spam	↓
Cryptocurrency mining	●	Depends on the coin price	→
Ransomware/locker	+	Might work on some devices	↑
Blackmail/extortion	●	Does not scale well – depends	→
Pranks/nuisance	- -	Not done by cyber criminals	→
Information stealing	●	Done because it's simple	↑
Click fraud	+	Often overlooked - profitable	↑
Premium services	+	Difficult to conduct	↓
Sniffing network traffic	●	Difficult with SSL/TLS	↓
Pivoting/attacking LAN	+	Infecting attached computers	↑
Proxy	●	Not very lucrative, but useful	→

- Profitability motivates the IoT attacker
- DDoS attacks are enabled by dark web store fronts
- As the value of devices and the data they handle increases, Ransomware or device lock out attacks will rise
- IoT devices with weak cybersecurity allow attackers entry into protected networks

[https://www.rsaconference.com/writable/presentations/file\\_upload/sem-m03d-profiting-from-hacked-iot-devices-coin-mining-ransomware-something-else.pdf](https://www.rsaconference.com/writable/presentations/file_upload/sem-m03d-profiting-from-hacked-iot-devices-coin-mining-ransomware-something-else.pdf)

# These Attacks Are Not Incidents – It is Structural

Botnet activity rises as the IoT becomes a target – AT&T study



AT&T study on Botnet activity across its global network. Spikes indicate recruitment of new bots into the network before a massive attack was launched

BotNet attacks for sale

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ lifetime
1 Concurrent *	1 Concurrent *	1 Concurrent *	1 Concurrent *	1 Concurrent *
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>

Screenshot of study into the cost of launching a DDOS attack – Actual Service offering available on the Web

Source: Kaspersky lab on Securlist.com

# Legislation

Government is noticing/acting...



- Convergence on IoT security guidelines from many angles (foreign and domestic)
- OWASP (Open Web Application Security Project) has a nice [list](#)

<https://www.youtube.com/watch?v=YxC1kcZDMyc&feature=youtu.be>





# California just became the first state with an Internet of Things cybersecurity law

3

By [Adi Robertson](#) | [@thedextriarchy](#) | Sep 28, 2018, 6:07pm EDT

[f](#) [t](#) [SHARE](#)



MOST READ

# IoT Device Security Regulation is on the Way



## Congress Introduces Bill to Improve IoT Security

The Internet of Things Cybersecurity Improvement Act aims to establish a bare minimum of security standards for IoT devices used by the federal government.

By Jessica Davis | Mar 13, 2019



CYBERSECURITY

## FDA Releases Draft Premarket Cybersecurity Guidance for Medical Device Manufacturers

The Food and Drug Administration (FDA) has released draft guidance to the healthcare industry that updates cybersecurity recommendations for medical device manufacturers with the aim of addressing vulnerabilities and evolving cybersecurity threats.

BY HEATHER LANDI, ASSOCIATE EDITOR — OCTOBER 19, 2018



## Japan to Probe IoT Devices and Then Prod Users to Smarten Up

A government project begins testing millions of Internet-connected devices to see how safe they are from cyberattacks

By John Boyd



# IEC62443

## Security requirements for Industrial Automation Control Systems

- IEC: International Electrotechnical Commission
- ISA: International Society of Automation
- ANSI: American National Standards Institute
- ISO: International Standardization Organization

### Collaborative Development

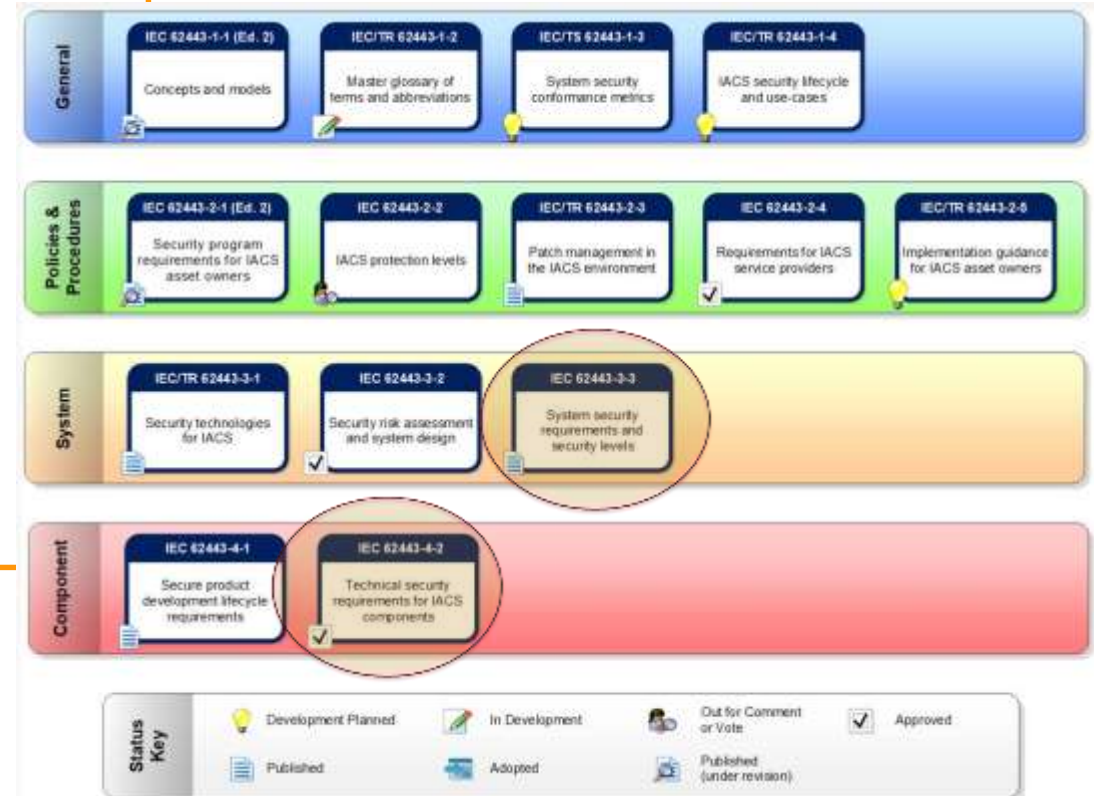


- ISA-62443 (and IEC 62443) is a series of standards being developed by two groups:
  - ISA99 → ANSI/ISA-62443
  - IEC TC65/WG10 → IEC 62443
- In consultation with:
  - ISO/IEC JTC1/SC27 → ISO/IEC 2700x



May 2018

Copyright © ISA – All Rights Reserved



### References:

- <https://www.isa.org/isa99/>
- <https://isaorg.sharepoint.com/sites/Standards/ISA99>



# Requirements

## Foundational Requirements

- FR 1 – Identification & authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

## Security Levels

### Protection against...



Comment: Most industrial customers focus on SL2 and SL3.  
SL4 for nation state type security

Copyright © ISA – All Rights Reserved



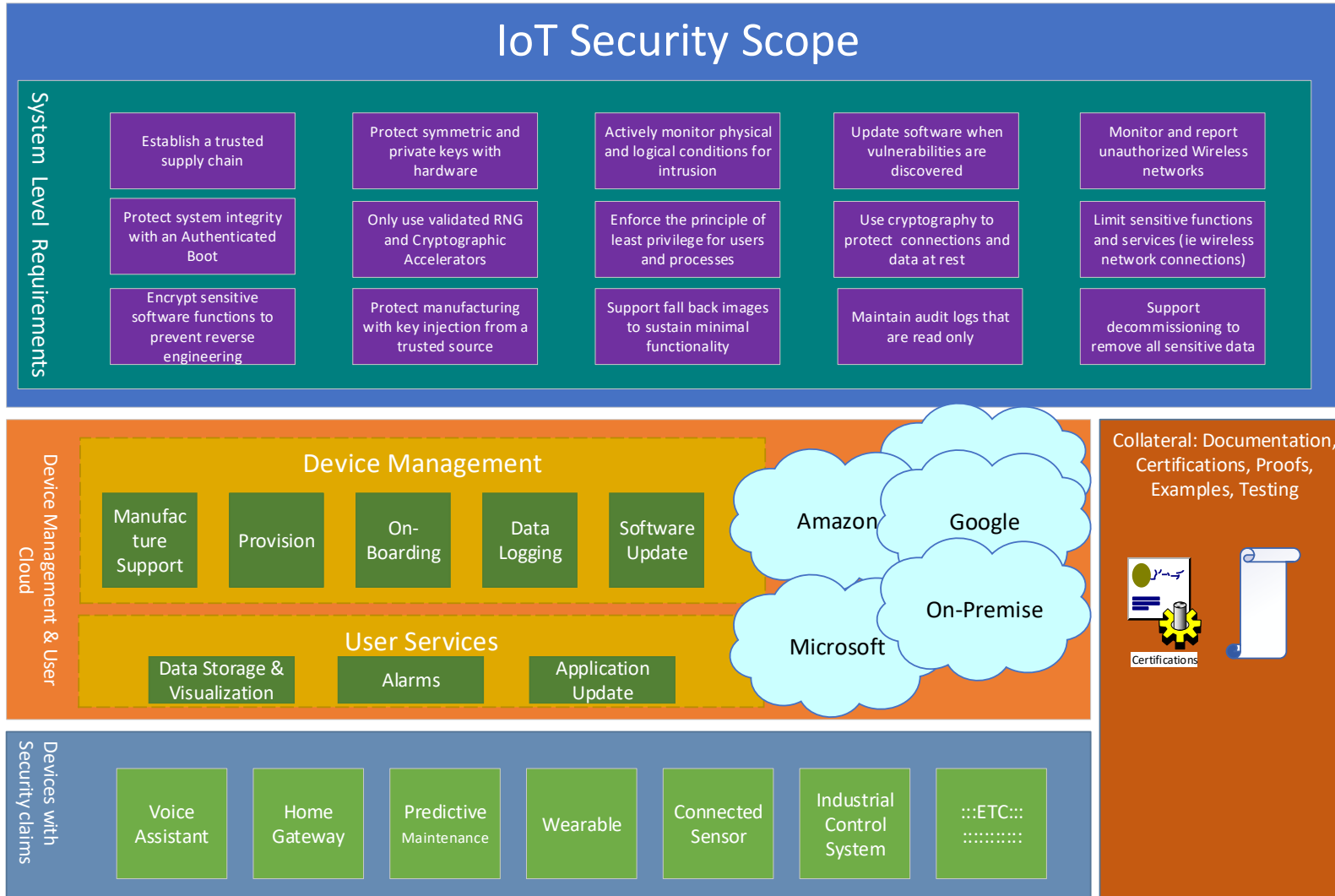
# IoT Security Strategy



# Design Challenges Across Device Lifecycle



# IoT Security System Level Diagram



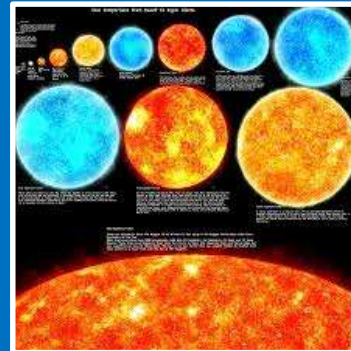
- Security scope spans across multiple domains
  - Numerous device form factors and services
  - Cloud User services and Device Management
  - Certifications, regional standards and other proof points

# IoT Security Strategies



## Address the entire device lifecycle

- Once deployed MCU/MPU capabilities & Cloud based monitoring ensure device lifetime integrity with hardware protected keys and secure boot for every device power up



## Scale to align to end product needs

- Security technology is rooted in MCU/MPU hardware capabilities at many processor integration and performance points (NXP: i.MX, Layerscape, Kinetis, LPC, JN)



## Be easy to deploy and easy use

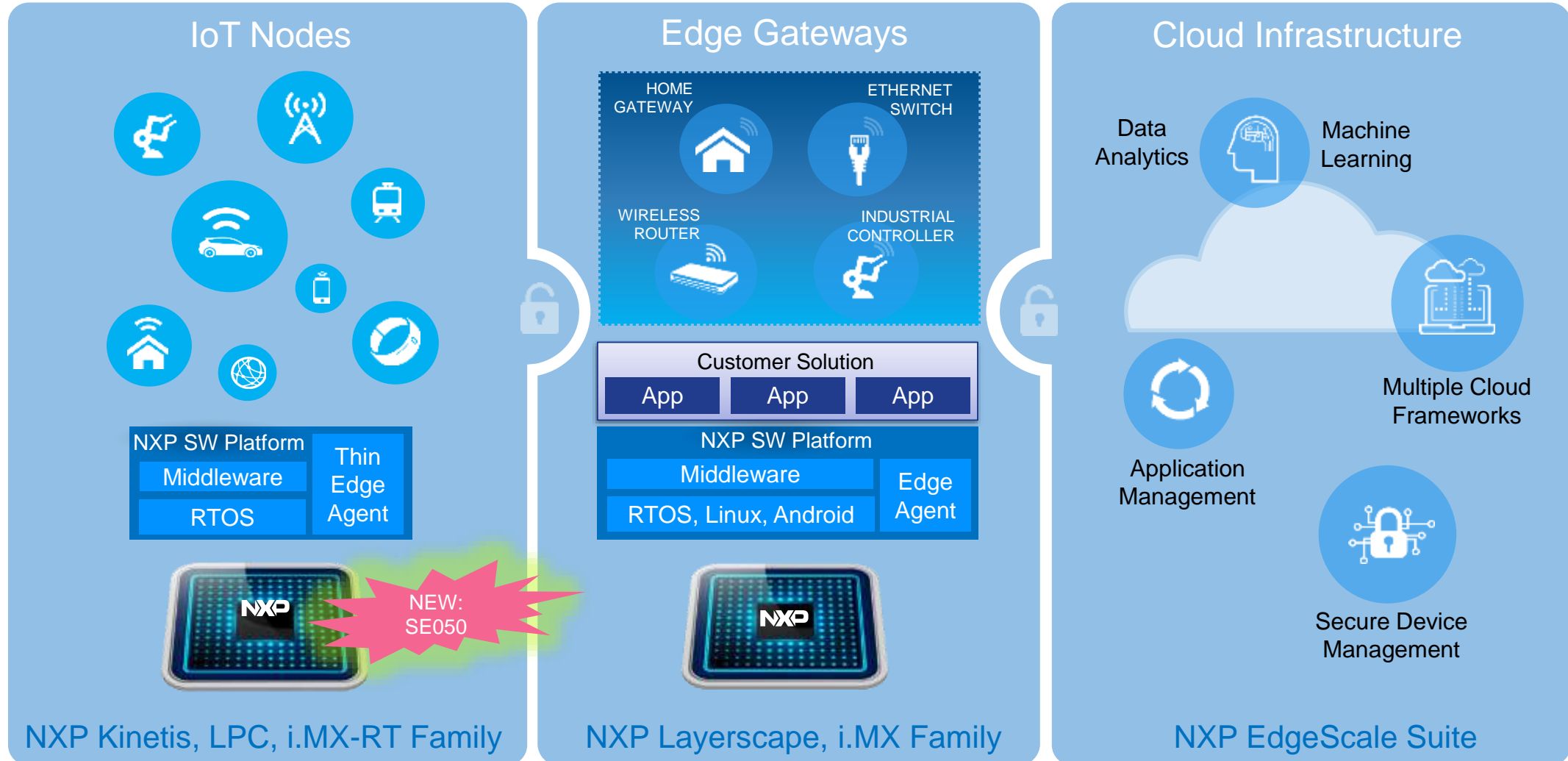
- Fully Documented steps and procedures from installing bootstrap through decommissioning stage (NXP: Edgescale documentation)



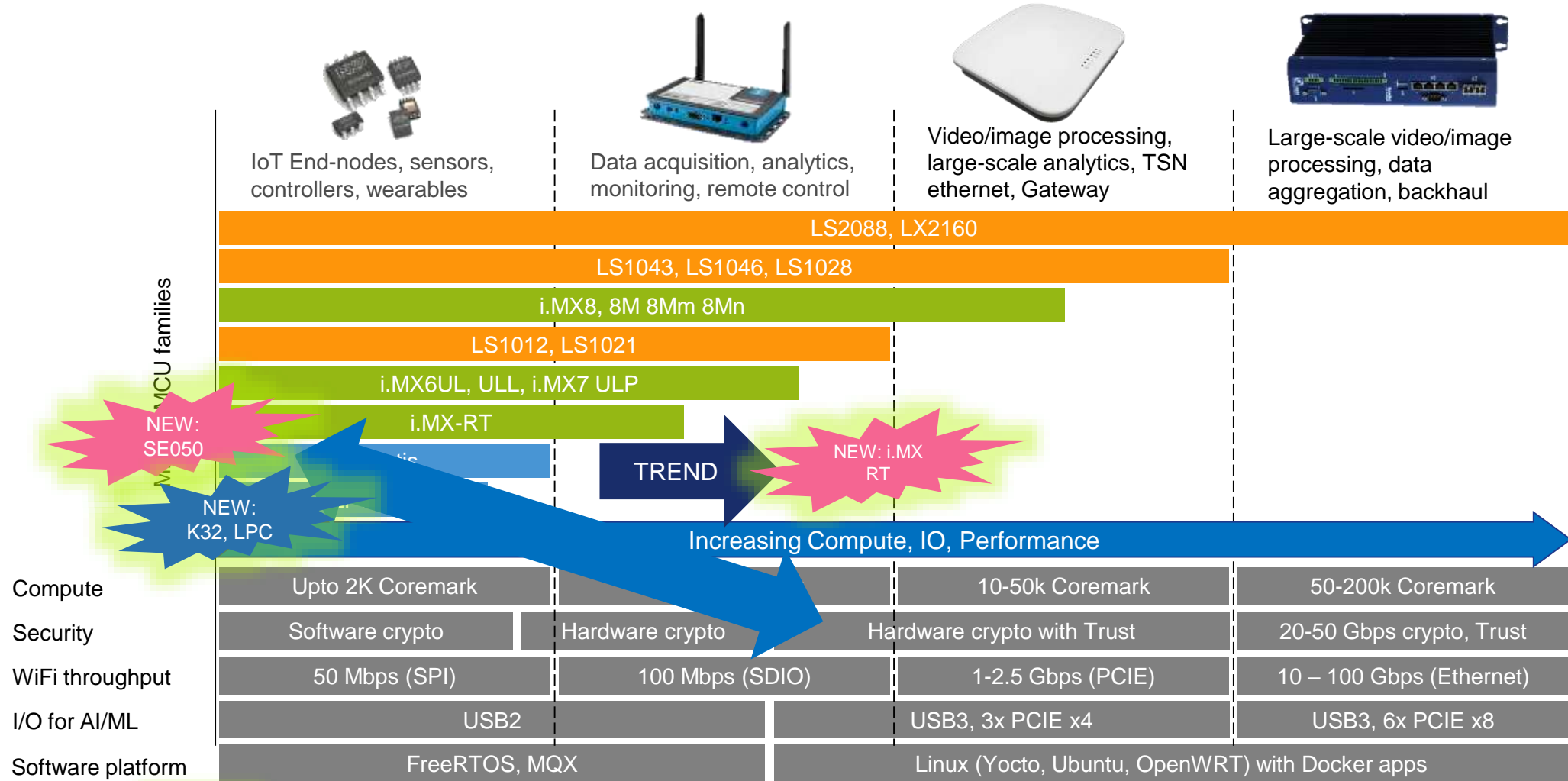
# NXP Product Portfolio



# NXP Solutions for Edge Computing



# IoT & Edge Compute Selection Chart

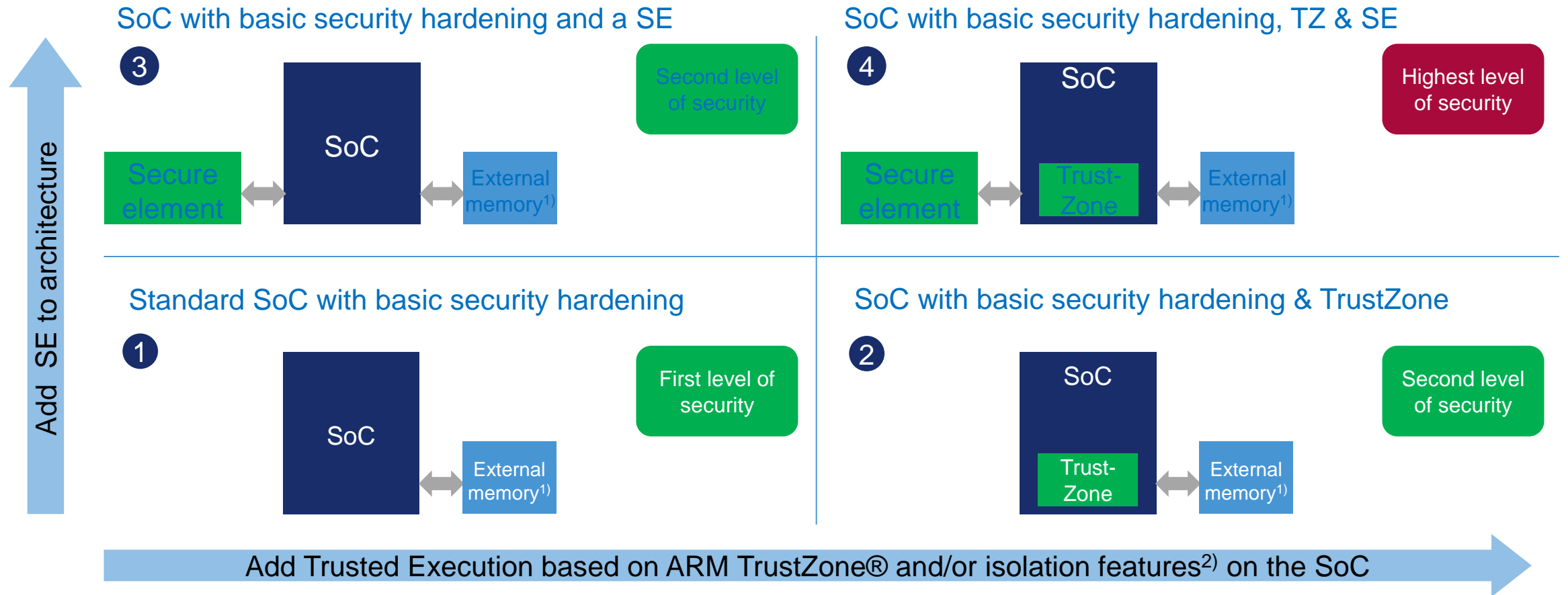


JCOP



# Secure Edge Architectures

Security Architectures supported by current shipping NXP products

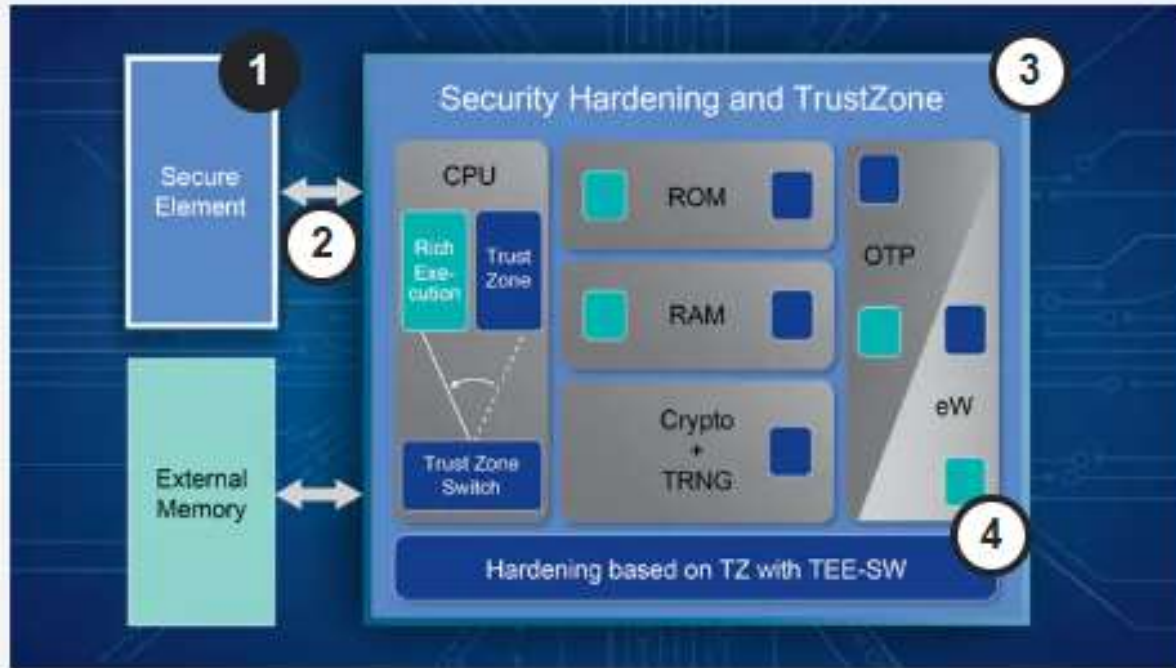


1) Not mandatory for MCUs/MPUs when they have embedded memory;

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



# IoT Security Architecture for Achieving the Highest Security

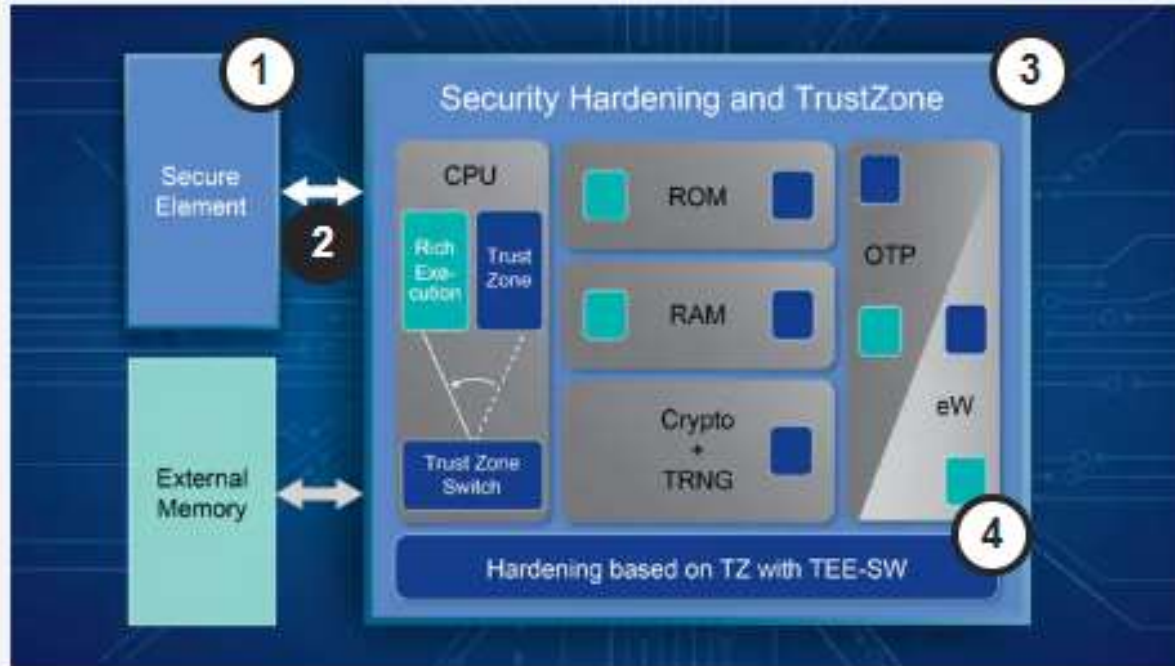


## 1 Secure Element

With the highest tamper resistance against local physical attacks, secure elements provide strong anti-counterfeiting protection. In addition, the reduced attack surface due to logical separation, allows secure functions, such as attested logs to be supported. For our secure elements such as [SE050](#), [A71CH](#) and [A1006](#), we offer scalable provisioning processes that reduce effort and complexity to achieve a trusted supply chain.

[Next element >](#)

# IoT Security Architecture for Achieving the Highest Security

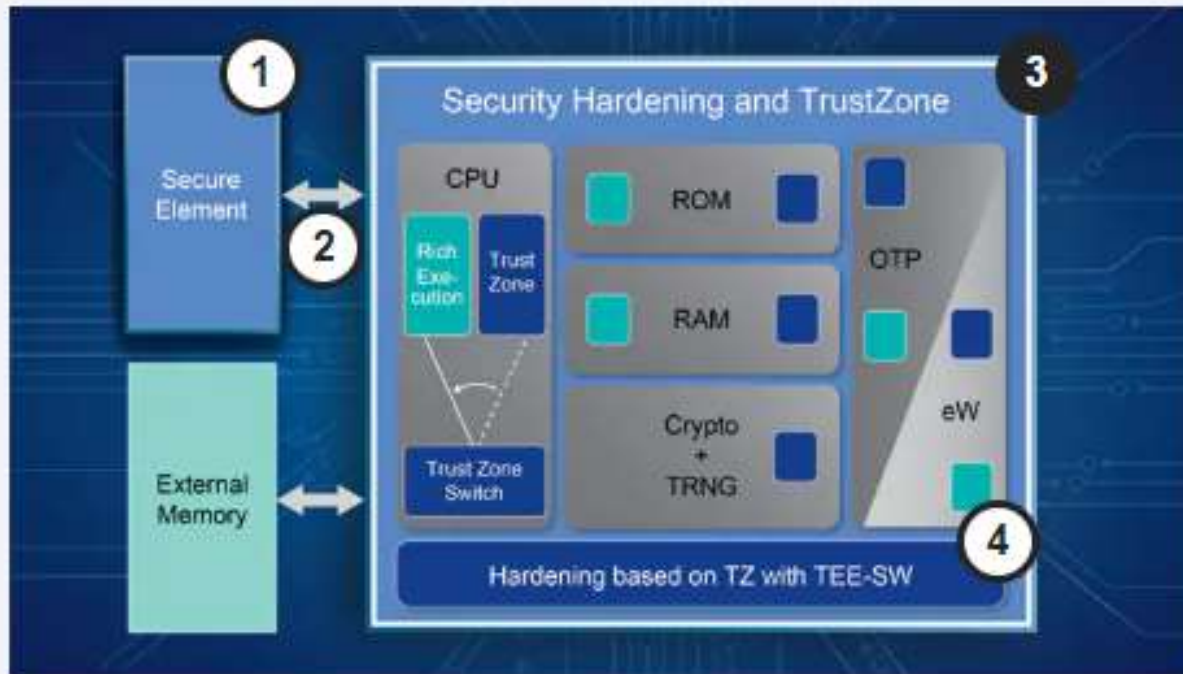


## 2 Hardware Root of Trust

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 >](#)

# IoT Security Architecture for Achieving the Highest Security



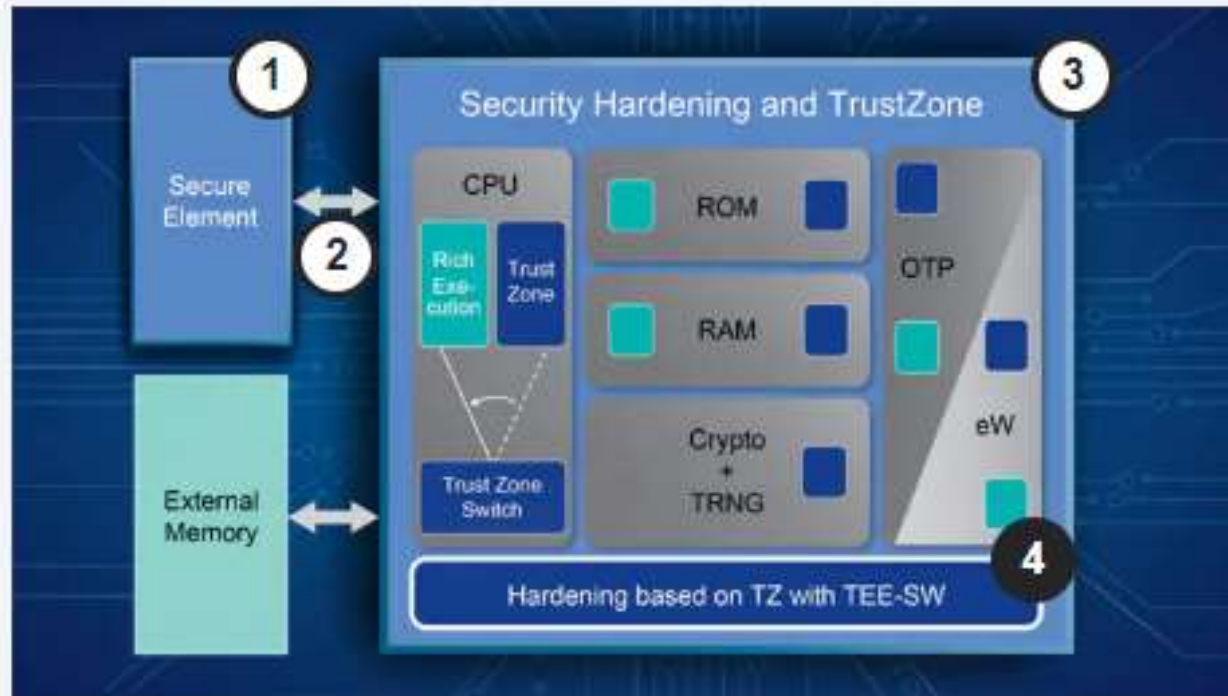
### 3 Processor with security hardening

To maintain the integrity of the application during operation, **NXP processors** provide the technology to support the product life cycle. Secure boot ensures that only authenticated software will be run. Interfaces for debugging and flash storage are protected. Tamper cases are monitored and device operation is restricted if system tamper is detected.

[Next element >](#)



# IoT Security Architecture for Achieving the Highest Security



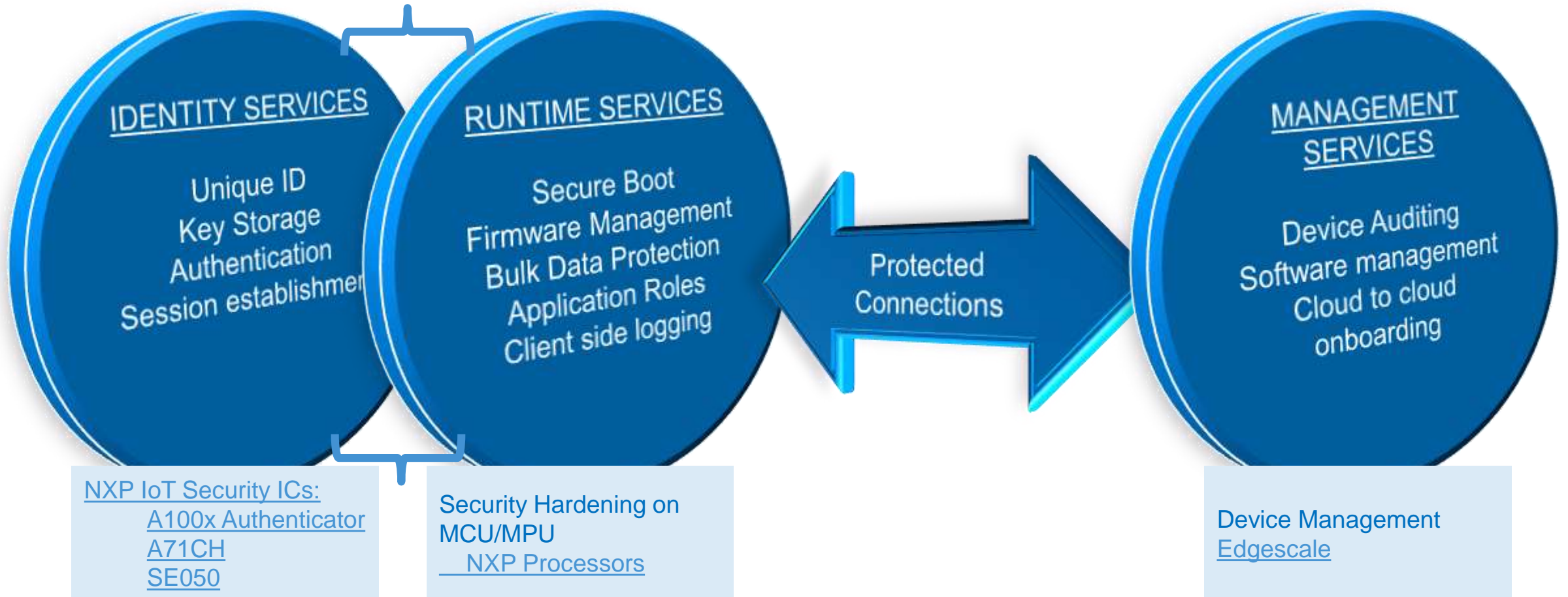
## 4 Arm® Trustzone®

Processors with Arm Trustzone provide a level of isolation within the chip to logically separate trusted operations. This protection is the basis for protecting firmware updates, logging, and remote testing of the IoT End and Edge node devices.

[Next element >](#)

# NXP for Secure Deployment from Edge to Cloud

May Functionally Overlap





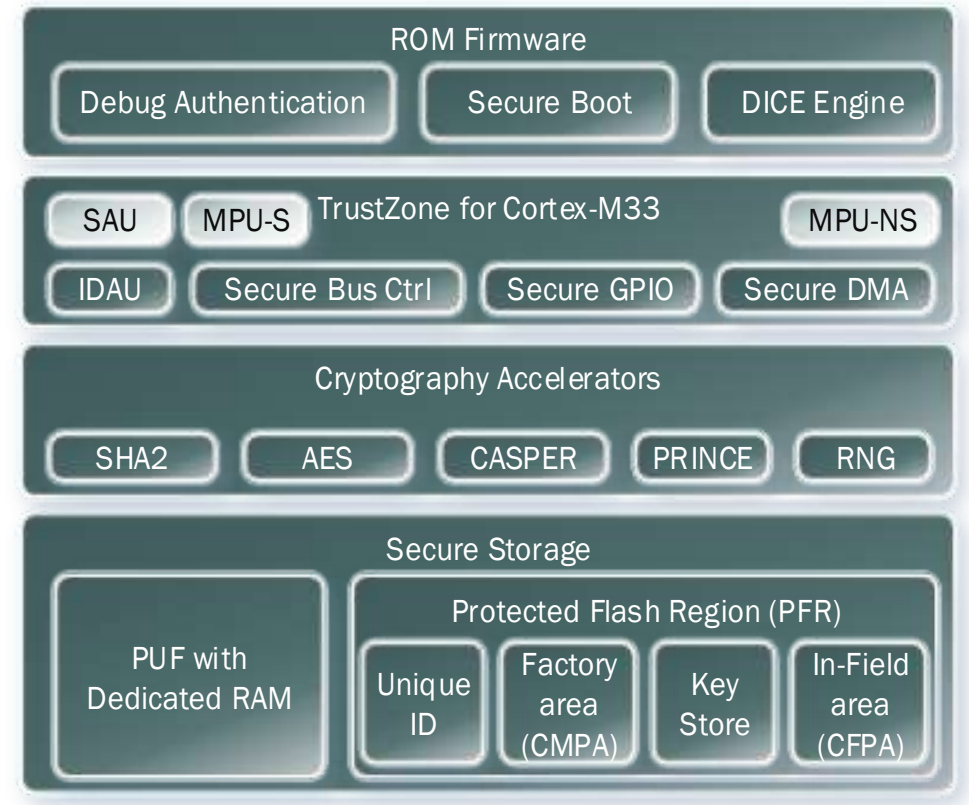
# Secure Elements and End Nodes

A71xx, A100x, SE050, LPC, Kinetis, i.MX RT



# NXP LPC5500 MCU Series: Security Subsystem Overview

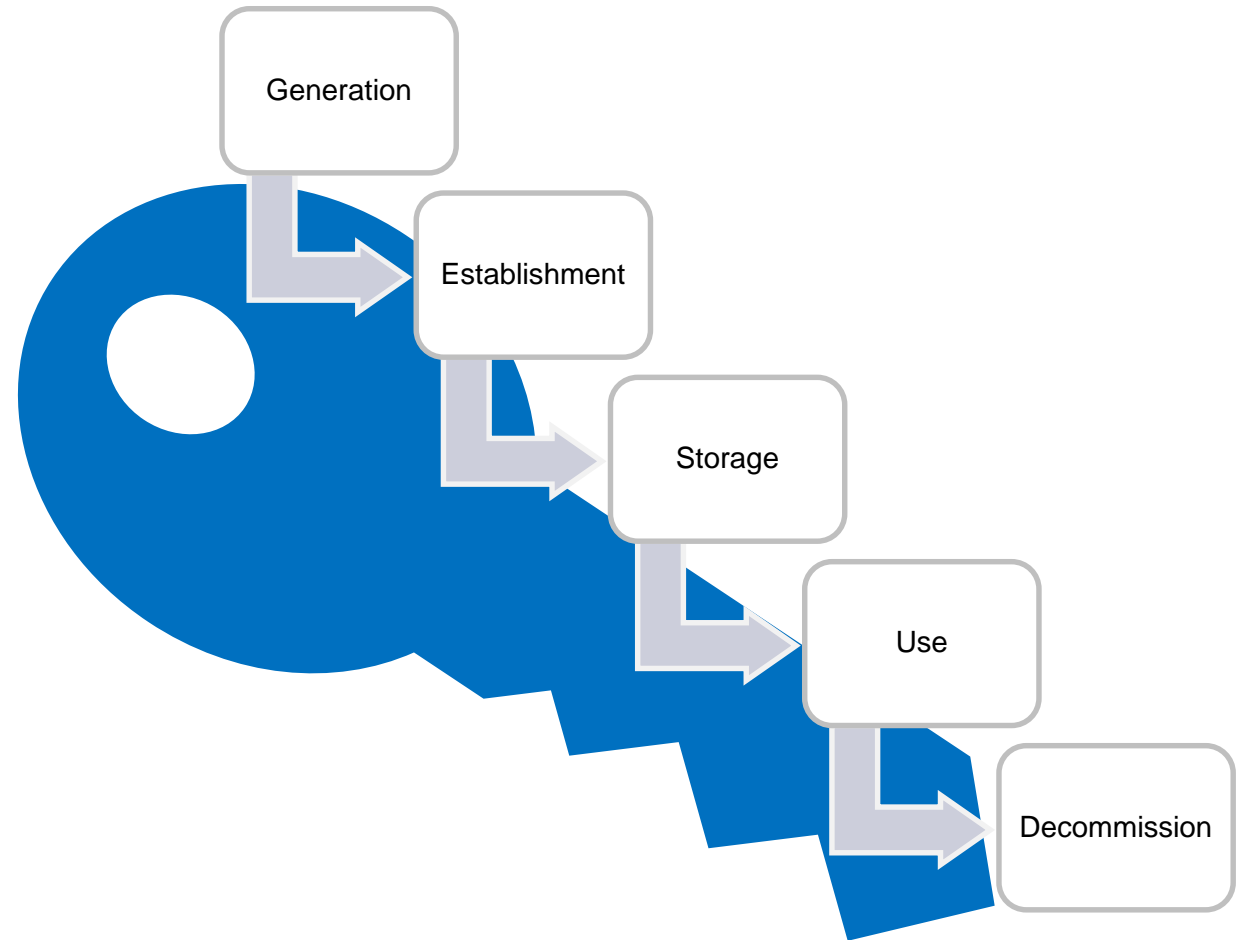
- **ROM Supporting**
  - Secure Boot, Debug Authentication & DICE Engine
- **TrustZone for Cortex-M33**
  - Arm's Security Attribution Unit (SAU)
  - Arm's Memory Protection Unit (MPU): Secure & Non-Secure
  - NXP's (implementation) Defined Attribution Unit (using IDAU interface)
  - NXP's Secure Bus, Secure GPIO & Secure DMA Controllers
- **Cryptography Accelerators**
  - Symmetric (AES-256) & Hashing (SHA2) engine
  - On-the-fly flash encryption/decryption engine (PRINCE)
  - Asymmetric engine for RSA and ECC (CASPER)
  - Random Number Generator (RNG)
- **Secure Storage**
  - Physically Unclonable Function (PUF)
    - Device unique root key (256 bit strength), 64-4096 bit key size
  - Protected Flash Region
    - RFC4122 compliant 128-bit UUID per device
    - Customer Manufacturing Programable Area (Boot Configuration, RoT key table hash, Debug configuration, Prince configuration)
      - PUF Key Store (Activation code, Prince region key codes, FW update key encryption key, Unique Device Secret)
    - Customer Field Programable Area (Monotonic counter, Prince IV codes)



# Protected Over the Lifecycle\* of the Cryptographic Keys

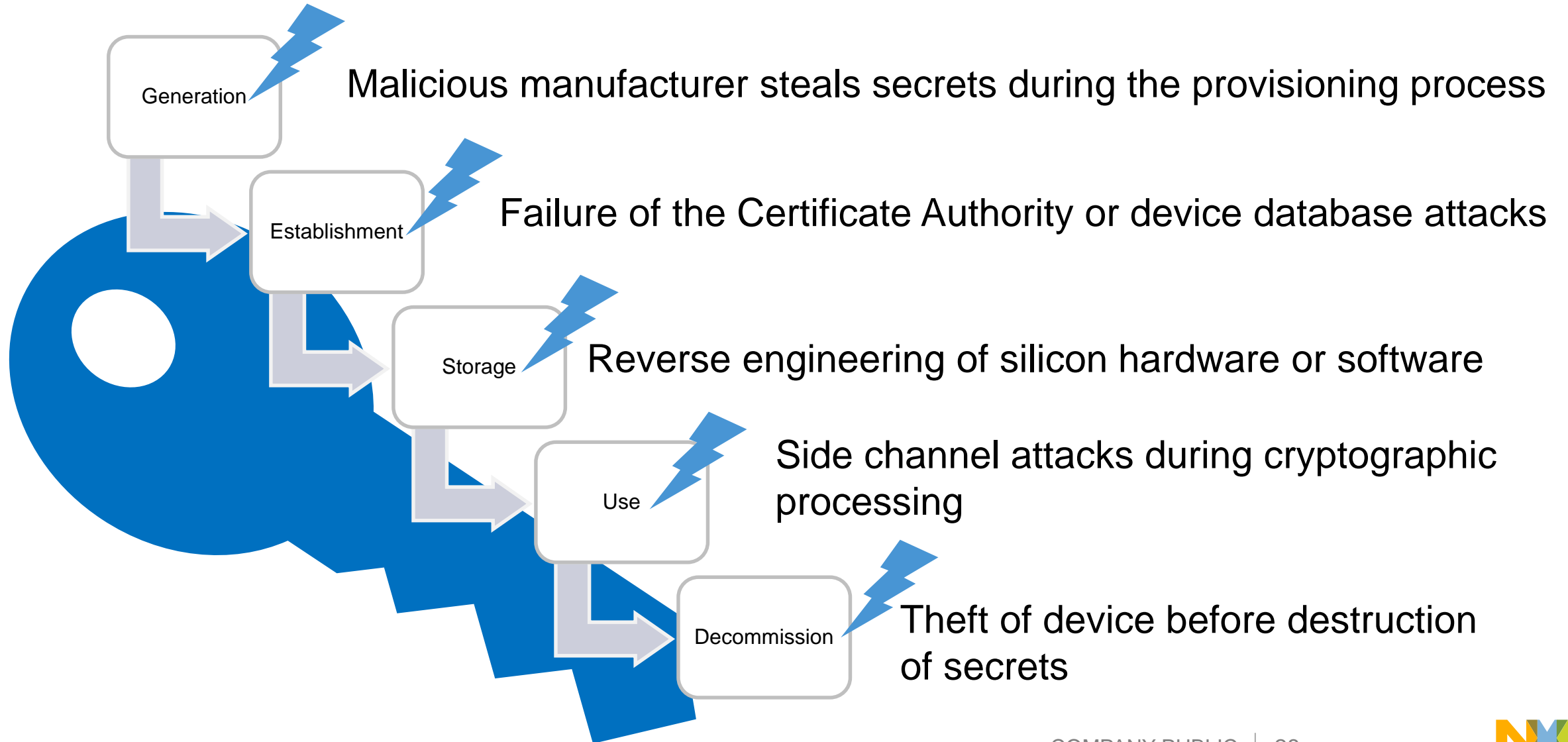
## Key Lifecycle

- **Generation**
  - Who/what creates the key material
- **Establishment**
  - How the key material is shared or signed between entities
- **Storage**
  - Where the key material is placed for future access
- **Use**
  - How the key is utilized during the cryptographic processing
- **Decommission**
  - Revocation and destruction of key material



\*Key Lifecycle <https://community.nxp.com/docs/DOC-333095>

# Protected From Attacks



# HW Protected Keys Example: Dedicated Security ICs

- NXP IoT Security ICs:
  - A71CH
  - A100x Secure Authenticator
  - SE050
- Premier example of a Hardware Protected Key integrated circuit
- Derived from CC certified solutions
  - Protects key generation and establishment with optional provisioning provided by NXP or qualified partners
  - Protected storage with bank grade tamper resistance in the design of the IC
  - Resistance to side channel attacks to protect the use of the keys

## A71CH Overview

### KEY BENEFITS

- ▶ Secure, zero-touch connectivity
- ▶ End-to-end security, from chip to edge to cloud
- ▶ Secure credential injection for root of trust at IC level
- ▶ Fast design-in with complete product support package
- ▶ Easy to integrate with different MCU and MPU platforms

### KEY SECURITY FEATURES

- ▶ Protected access to credentials
- ▶ Encrypted/authenticated interface to host processor
- ▶ Certificate-based TLS set-up (ECC NIST P-256)
- ▶ TLS set-up using pre-shared secret (TLS-PSK)
- ▶ Connectionless message authentication (HMAC)
- ▶ ECC key generation & signature verification
- ▶ Symmetric key derivation
- ▶ Secure vault for product master secrets (key wrapping, derivation, locking)
- ▶ Encrypted key injection
- ▶ Optional trust provisioning by NXP and qualified partners



# HW Protected Keys Example: MCU/MPU Security Hardening

- Devices such as NXP [i.MX products](#) integrate security technology for protecting keys
  - Fuse locations for keys with read out protection for protected storage of key material
  - Keys are passed to hardware accelerators without software interaction for protected use
  - Access to keys is restricted by security state machine requiring authenticated boot
  - Zero-izable keys with tamper monitors for decommissioning

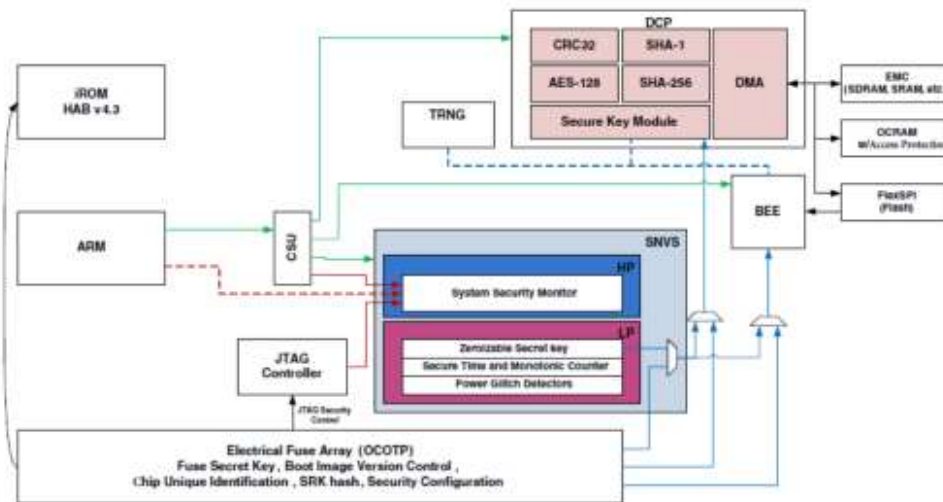


Figure 1-1. Security subsystem (simplified)



# HW Protected Keys Example: Hardware PUF

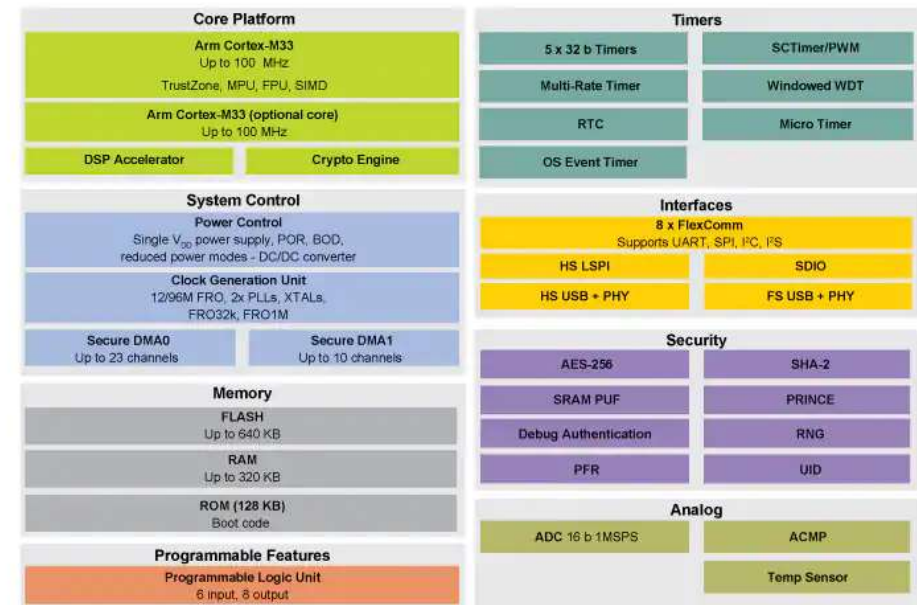
Recently launched LPC5500 family also makes use of PUF technology on the microcontroller in addition to other security capabilities

## Unique Security Enhancements

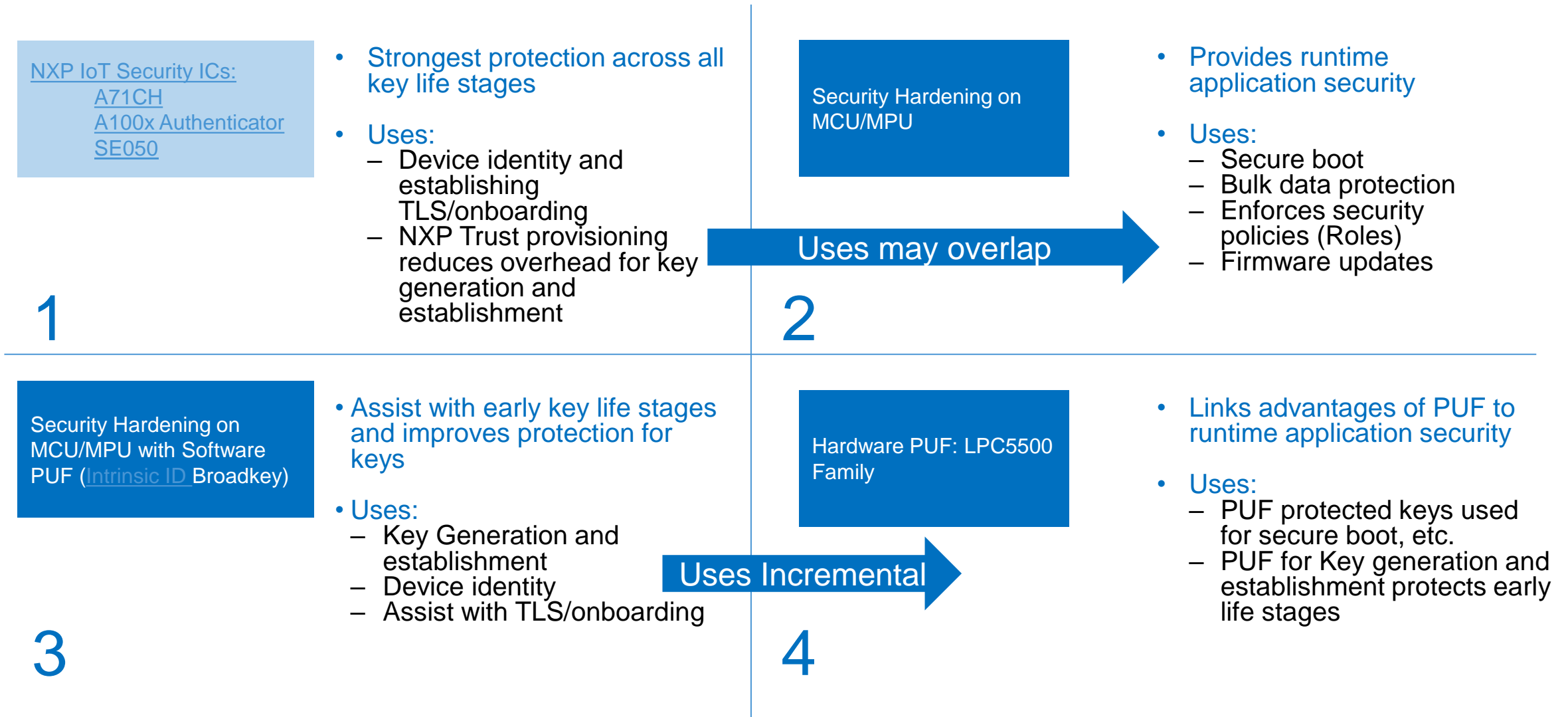
A cornerstone to establishing device trustworthiness is NXP's ROM-based secure boot process that utilizes device-unique keys to create an immutable hardware 'root-of-trust'. The keys can now be locally generated on-demand by an SRAM-based Physically Unclonable Function (PUF) that uses natural variations intrinsic to the SRAM bitcells. This permits closed loop transactions between the end-user and the original equipment manufacturer (OEM), thus allowing the elimination of third-party key handling in potentially insecure environments. Optionally, keys can be injected through a traditional fuse-based methodology.

Furthermore, NXP's SEE improves the symmetric and asymmetric cryptography for edge-to-edge and cloud-to-edge communication by generating device-unique secret keys through innovative usage of the SRAM PUF. The security for public key infrastructure (PKI) or asymmetric encryption is enhanced through the Device Identity Composition Engine (DICE) security standard as defined by the Trusted Computing Group (TCG). SRAM PUF ensures confidentiality of the Unique Device Secret (UDS) as required by DICE. The newly announced solutions support acceleration for asymmetric cryptography (RSA 1024 to 4096-bit lengths, ECC), plus up to 256-bit symmetric encryption and hashing (AES-256 and SHA2-256) with MbedTLS optimized library.

"Maintaining the explosive growth of connected devices requires increased user trust in those devices," said John Ronco, vice president and general manager, Embedded & Automotive Line of Business, Arm. "NXP's commitment to securing connected devices is evident in its new Cortex-M33 based products built on the proven secure foundation of TrustZone technology, while incorporating design principles from Arm's Platform Security Architecture (PSA) and pushing the boundaries of Cortex-M performance efficiency."

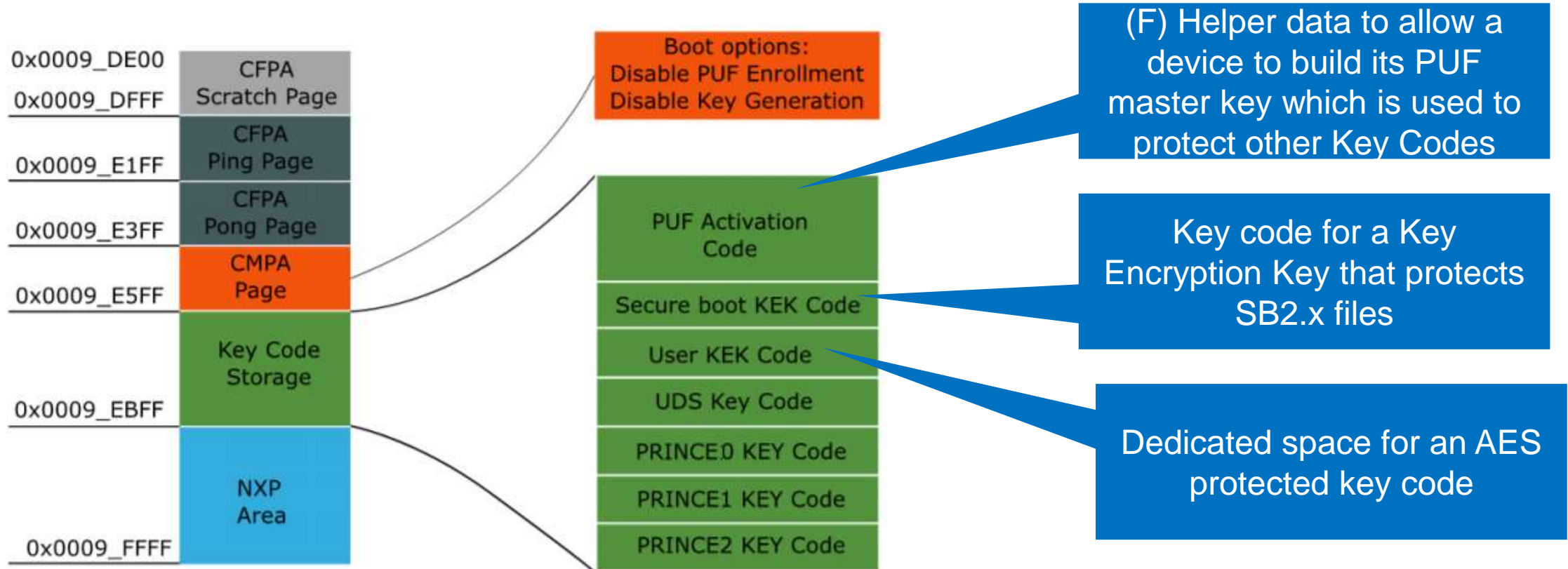


# Exploring Protected Key Options



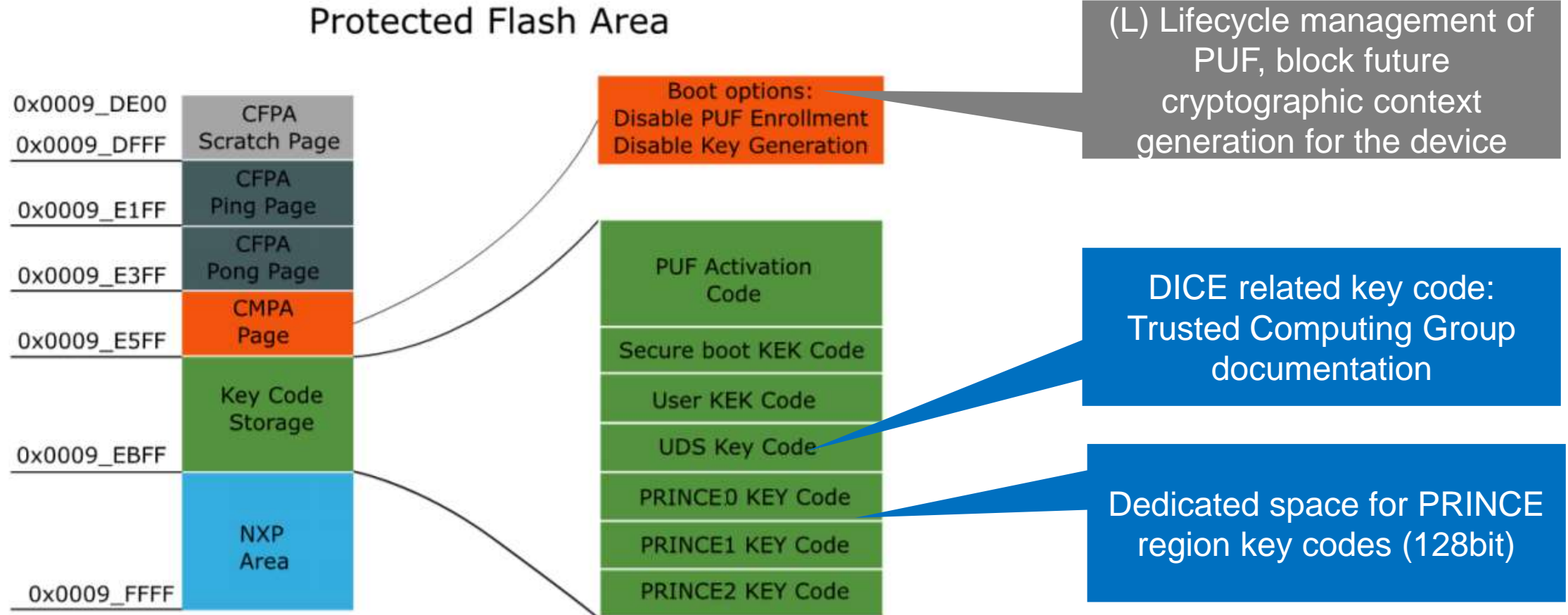
# PUF Based Key Management on LPC5500 Series

## Protected Flash Area



CFPA Customer Field Programmable Area  
CMPA Customer Manufacturing floor Programmable Area

# PUF Based Key Management on LPC5500 Series



CFPA Customer Field Programmable Area  
 CMPA Customer Manufacturing floor Programmable Area



# Command Line or GUI Options for PUF Provisioning

The screenshot displays the 'elftosb-gui' application window. On the left, the 'Device configuration' panel is visible, showing 'LPC55xx' as the target device. Under 'Key Store Security', the 'SRAM PUF Enroll' section is active, with 'Enroll' checked. Below this, several key types are listed: 'SBKEK', 'PRINCE region 0 key', 'PRINCE region 1 key', 'PRINCE region 2 key', and 'UDS'. The 'Export' section is also visible, with 'To nonvolatile device memory' checked and 'Memory ID' set to '0'. On the right, the 'Process output' window shows the execution of 'blhostwinblhost.exe' with various command-line options. Red boxes highlight specific command-line arguments: '-- key-provisioning enroll', '-- key-provisioning set\_user\_key 3 ".temp\tempSbkek.bin"', and '-- key-provisioning write\_key\_nonvolatile 0'. A list of key codes is shown in green boxes: 'PUF Activation code', 'Secure boot KEK Code', 'User KEK code', 'UDS Key Code', 'PRINCE0 KEY Code', 'PRINCE1 KEY Code', and 'PRINCE2 KEY Code'. Red arrows point from the GUI options to their corresponding command-line arguments and key codes.

```
(2018-11-16 13:55:23) >> blhostwinblhost.exe -V -p COM32,57600 -- key-provisioning enroll
Ping responded in 1 attempt(s)
Framing protocol version = 0x50010300, options = 0x0
Inject command 'key-provisioning'
Successful generic response to command 'key-provisioning'
- took 0.009 seconds
Response status = 0 (0x0) Success.

(2018-11-16 13:55:23) >> blhostwinblhost.exe -V -p COM32,57600 -- key-provisioning set_user_key 3 ".temp\tempSbkek.bin"
Ping responded in 1 attempt(s)
Framing protocol version = 0x50010300, options = 0x0
Inject command 'key-provisioning'
Successful generic response to command 'key-provisioning'
- took 0.009 seconds
Response status = 0 (0x0) Success.

(2018-11-16 13:55:23) >> blhostwinblhost.exe -V -p COM32,57600 -- key-provisioning write_key_nonvolatile 0
Ping responded in 1 attempt(s)
Framing protocol version = 0x50010300, options = 0x0
Inject command 'key-provisioning'
Successful generic response to command 'key-provisioning'
- took 0.009 seconds
Response status = 0 (0x0) Success.
```

Scalable methods for instantiating device unique keys which are protected by PUF technology

# Secure Debug

## Debug Protection Mechanism

### Challenges

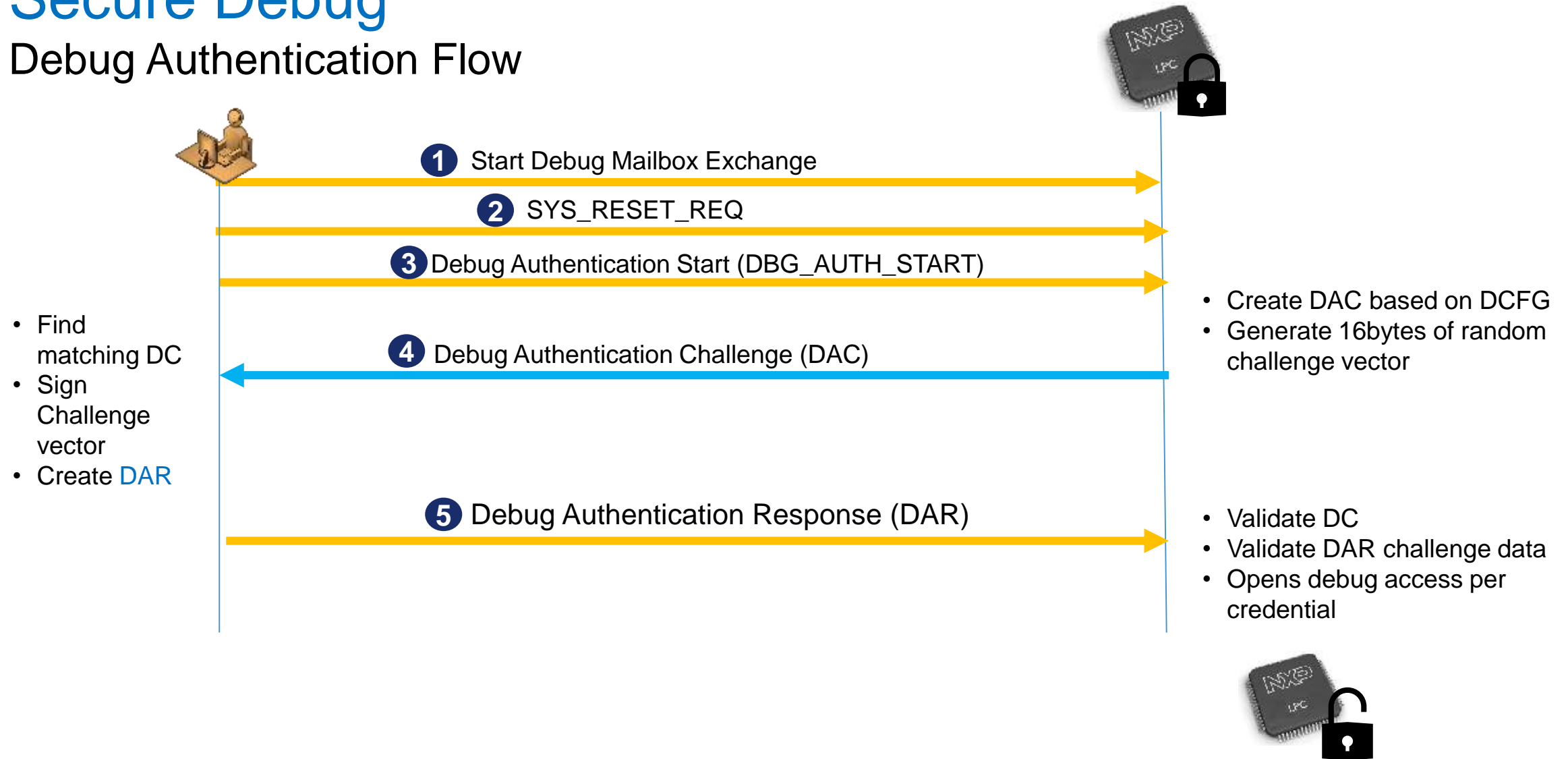
- Only authorized external entity allowed to debug
- Permit access only to allowed assets
- Support Return Material Analysis (RMA) flow without compromising security

### LPC55S69 Solution

- Supports RSA-2048/RSA-4096 signed certificate based challenge response authentication to open debug access
- Provides individual debug access control over partitioned assets
- Provides flexible security policing
  - Enforce UUID check
  - Certificate revocations
  - OEM customizable attribution check (model number, department ID etc)
- Security policy fixed at manufacturing

# Secure Debug

## Debug Authentication Flow



# Secure Debug

## Debug Protection Mechanism

### Debug Credential (DC) Certificate

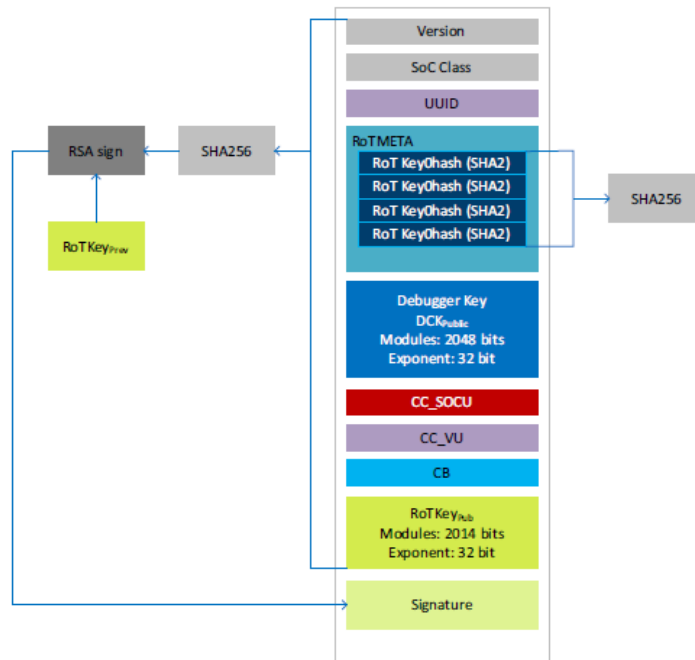


Fig 190. Debug Credential certificate fields

### PKI for Secure boot and Debug

- Same Root of Trust Private keys are used to create the DC signature
- Options for HW and SW constraints
  - Device Unique ID bound
  - Level of Debug access
  - Mass erase enable

# Secure Debug

## LPC55Sxx Debug Domains – SoC Credential Constraints

### DC HW Credential Constraints

NIDEN - Non-secure non-invasive debug.

DBGEN - Non-secure invasive debug

SPNIDEN - Secure non-invasive debug

SPIDEN - Secure invasive debug

TAPEN - TAP (Test Access Point) controller

uDBGEN - Micro-CM33 invasive debug

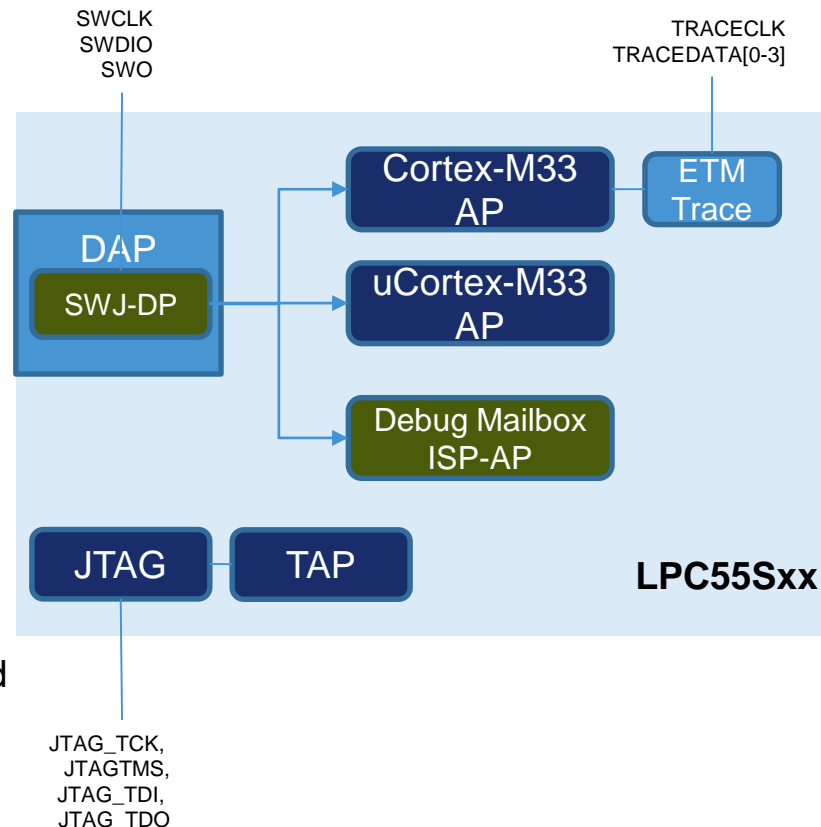
uNIDEN - Micro-CM33 non-invasive debug

### DC SW Credential Constraints

ISPEN - ISP boot command

FAEN - Field Return Analysis mode command

MEEN- Flash mass erase command



### Configuration Control

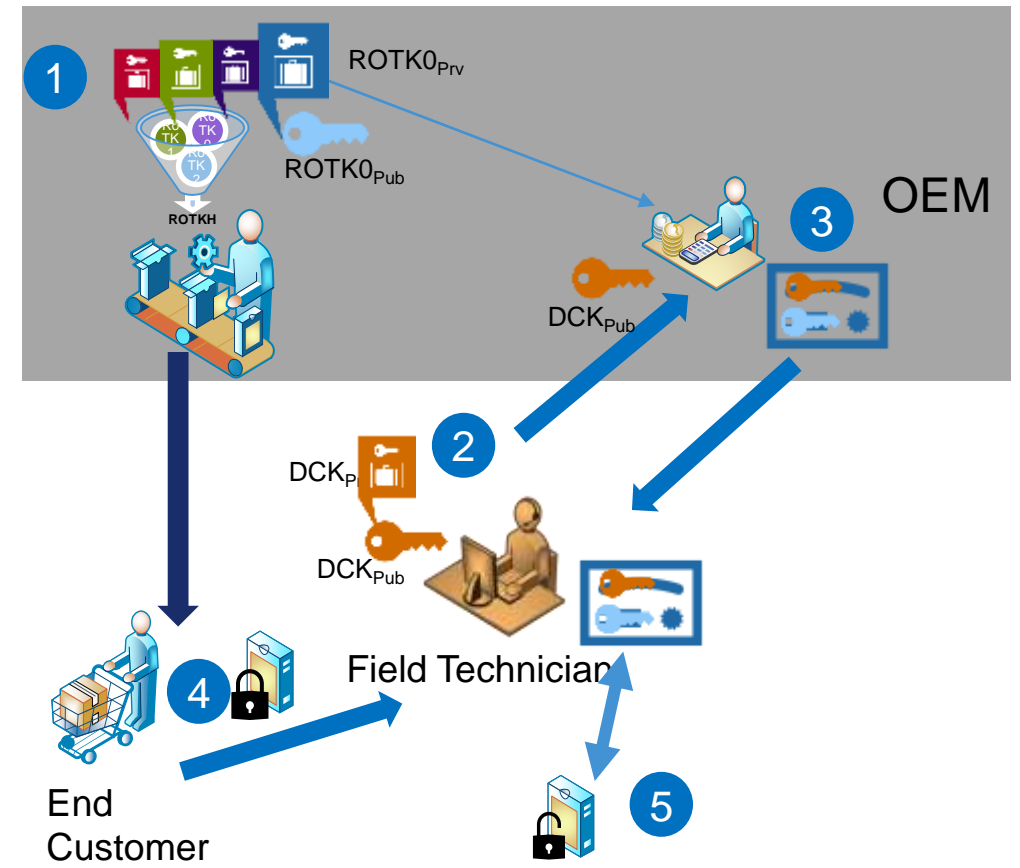
- Fields in Customer Programmed Protect Flash Region provide control of the sub-domains
  - Disabled permanently
  - Enabled after debug authentication
  - Enabled permanently
- Other controls
  - Enforce UUID checking
  - Revoke debug keys



# Secure Debug

## Debug Authentication for RMA Use Case

- 1 OEM generates RoT key pairs and programs the device before shipping.
  - SHA256 hash of RoT public key hashes
- 2 Field Technician generates his own key pair and provides public key to OEM for authorization.
- 3 OEM attests the Field Technician's public key. In the debug credential certificate he assigns the access rights.
- 4 End customer having issues with a locked product takes it to Field technician.
- 5 Field technician uses his credentials to authenticate with device and un-locks the product for debugging.

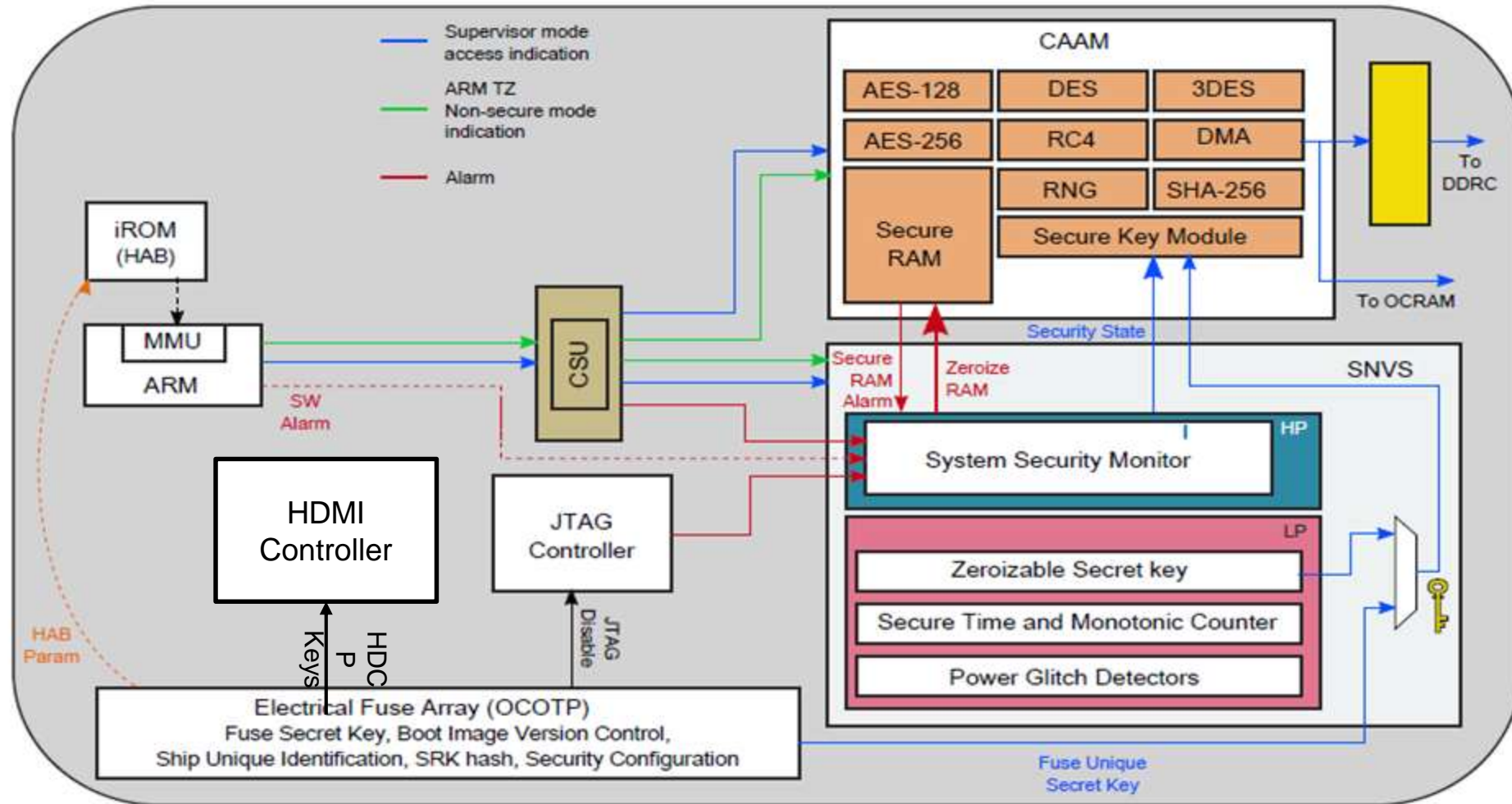


# Higher Performance Edge Devices

i.MX, Layerscape



# i.MX 8M Security Sub-System



# i.MX Product Security Features Overview

Feature	i.MX 6Q/D/S	i.MX 6SoloX	i.MX 6UL	i.MX 7S/D	i.MX 8MQuad	i.MX 8MMini	i.MX 8QuadMax	i.MX 8QuadXPlus
CAAM (HW Crypto)							✓(SECO)	✓(SECO)
AES128/192/256, SHA1/224/256, DES/3DES	✓	✓	✓	✓	✓	✓	✓ + SHA 384/512	✓ + SHA 384/512
Elliptic Curve (modulus up to 1024) RSA (up to 4096)			✓	✓	✓	✓	✓ High performance	✓ High performance
Crypto Accelerator Unit (CAU) (DES, AES co-processor instruction)							✓	✓
Certifiable RNG	✓	✓	✓	✓	✓	✓	✓	✓
Run Time Integrity Protection			✓	✓	✓	✓	✓	✓
Isolated security applications (eg SHE)							✓	✓
Boot								
High Assurance Boot (RSA/ECDSA)	✓ RSA	✓ RSA	✓ RSA	✓ RSA	✓ RSA	✓ RSA	✓	✓
Encrypted Boot	✓	✓	✓	✓	✓	✓	✓	✓
Always ON domain	✓	✓	✓	✓	✓	✓	✓	✓
Secure Storage (non-volatile)	✓	✓	✓	✓	✓	✓	✓	✓
Tamper Detection Signal	✓	✓	✓ Active	✓ Active			✓ Active	✓ Active
Volt/Temp/Freq Detect			✓	✓			✓	✓
Inline Encryption			✓ BEE				✓ IEE	✓ IEE
Manufacturing/Debug								
Secure Debug	✓	✓	✓	✓	✓	✓	✓ Domains	✓ Domains
Manufacturing Protection				✓	✓	✓	✓	✓
Resource Domain Isolation		✓		✓	✓	✓	✓	✓
Content Protection	✓ 6Q 1.x only					✓ HDCP 1.x/2.x	✓ HDCP 1.x/2.x, DTCP	✓ DTCP

# SoC Requirements for Manufacturing Protection Feature

- SoC with built-in Manufacturing Protection Hardware which includes:
  - CAAM with Public Key accelerator module (PKHA) and Manufacturing Protection protocol registers
  - Dedicated fuses (approx. 256)
  - HAB (secure boot) support
- All i.MX 7/8 SoCs with CAAM's PKHA support Manufacturing Protection. This includes i.MX 7D and i.MX 8, Layerscape
  - Popular feature included in many upcoming chips



# Manufacturing Protection (MP) Goals and Example Usage

## MP Goals

- Help prevent Contract Manufacturer from accessing Primary Manufacturer's secrets
- Allow Primary Manufacturer to detect "over-production" of devices
- Provide method to authenticate NXP chips

## MP Implements

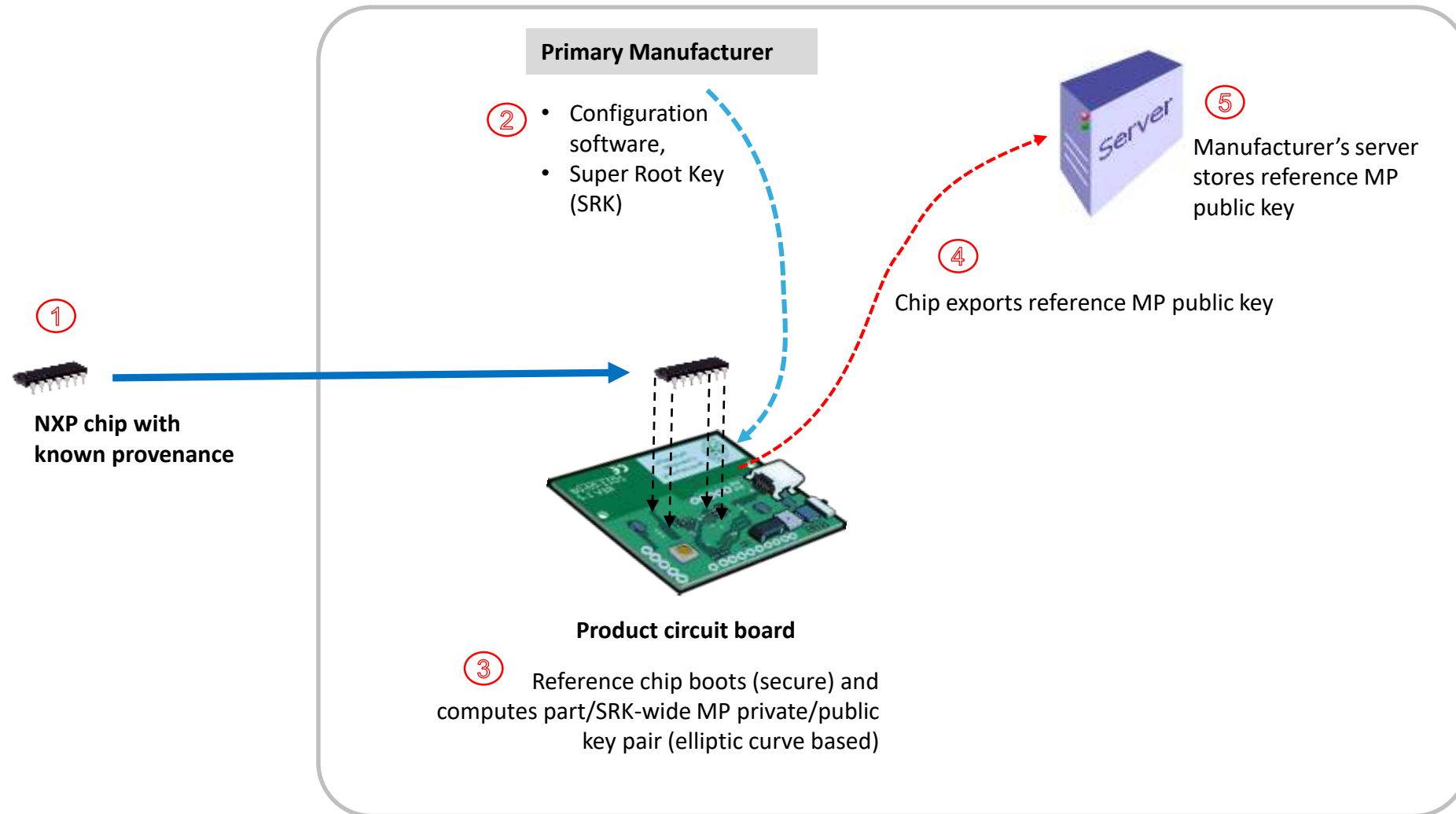
- MP asymmetric key pair generation, derived from part number-specific secret and Primary Manufacturer's public super root key (SRK)
- Protection of MP private signing key, buried in security hardware only available for use when chip is in a trustworthy state
- Method to sign messages using MP private signing key

## MP Example

During manufacturing,

- Primary Manufacturer server verifies the authenticity of an NXP chip before installing secrets
- Primary Manufacturer establishes a secure connection to a secure environment within the chip
- Primary Manufacturer server installs secrets in chip secure environment

# Primary Manufacturer Registration




# Chip Distribution with Manufacturing Protection



**Primary Manufacturer**

- Signed configuration software,
- Primary Manufacturer SRK (to be fused on the chip)

Authenticated channel used to download keys, proprietary software and data (that is then BLOB'ed)




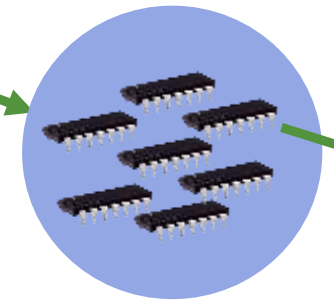
See Manufacturer Registration details on next slide

MP root secret(s)




Chip unique ID

Chip Fabrication

Chip distributor

Chip Distribution







Contract manufacturer

Product

Chip information signed with MP private key, derived from chip and Primary Manufacturer's SRK

Device Manufacture

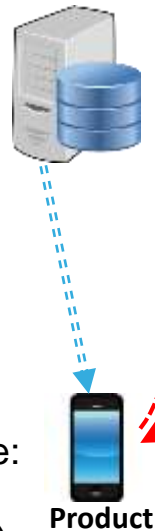
Provisioned Product

Device Distributor

Device Distribution

# Secrets Insertion and Auditing

1. Contract Manufacturer burns fuses:
  - Hash of Primary Manufacturer's Super Root Key (SRKH)
  - Other device-specific configuration bits
2. Contract Manufacturer downloads Primary Manufacturer-signed MP software e.g.:
  - Authentication software
  - Secrets Provisioning software
3. NXP chip boots securely (CLOSED)
  - Verifies signature of MP software (note: the actual SRK is authenticated by comparison to its hash stored in fuses)
4. MP software prepares chip message (signed by HW-embedded MP private key)
  - Msg optionally includes e.g. chip unique ID, fuse values, etc...



5. MP signed message sent to primary manufacturer's server

6. Primary Manufacturer's server verifies signature over MP message using reference MP public key
7. Server logs/audits chip serial number
8. Server and chip's MP software establish a secure channel
9. Server downloads proprietary production software and secret keys (perhaps chip specific)
10. (note: MP software may encrypt and cryptographically bind downloaded secrets to the specific chip)

Primary Manufacturer



Contract Manufacturer

# Advantages

- Each chip authenticated and uniquely identified via server
  - The product can therefore be provisioned securely and uniquely
  - Product secrets kept from Contract Manufacturer and NXP
- No special security provisions (environments) needed on factory floor
- Isolation of Primary Manufacturers (competitors) from each other
- Prevents illicit production by Contract Manufacturers
- Allows for detection of counterfeited chips



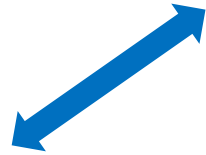
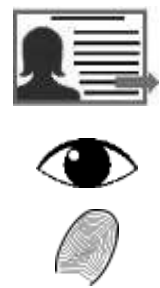
# Edgescale



# Management and Security Challenges

## Traditional PC, Mobile devices

- Multiple authentication mechanisms
- Cloud based security and application management



*EdgeScale*

## Edge computing devices

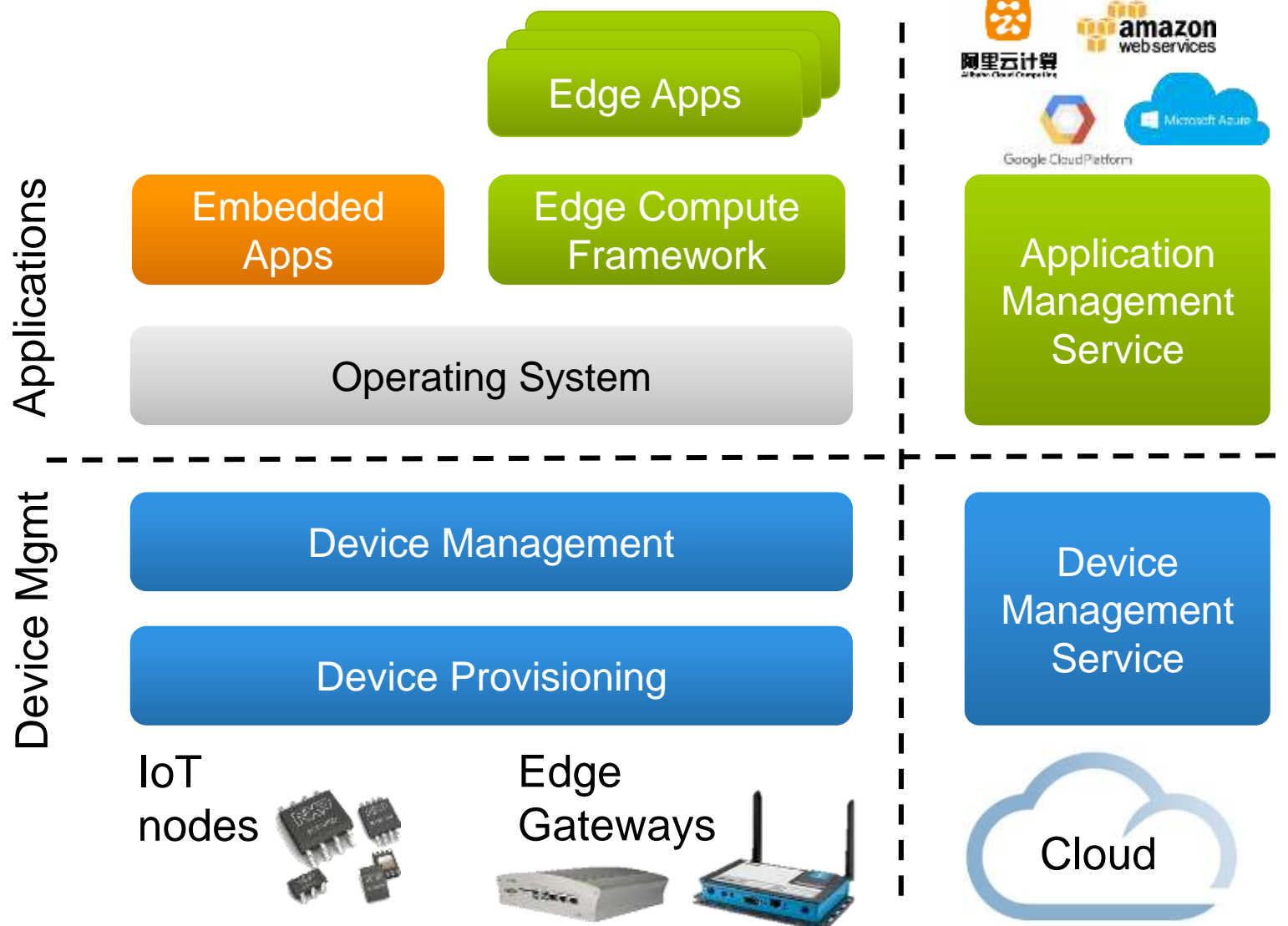
- Traditionally embedded devices
- No physical access/lack display
- Many (10s, 100s, 1000s) per user



## Solution: Cloud based Management & Security for Edge

- Manage devices, apps remotely
- Secure provisioning, upgrades

# EdgeScale for Device Management



Customer have choice for Application Management

- AWS, Azure, Aliyun, Google
- Home-grown or 3<sup>rd</sup> Party
- Optionally, use Edgescale for Docker application mgmt.

EdgeScale provides

- Device Management
- Security via Hardware Root of Trust

# NXP Partner Edge-Box Solutions



Imago LS2088  
Vision-Box



Scalus LS1012  
Grapeboard

Powered  
By  
EdgeScale



DNI LS1046  
Enterprise Whitebox

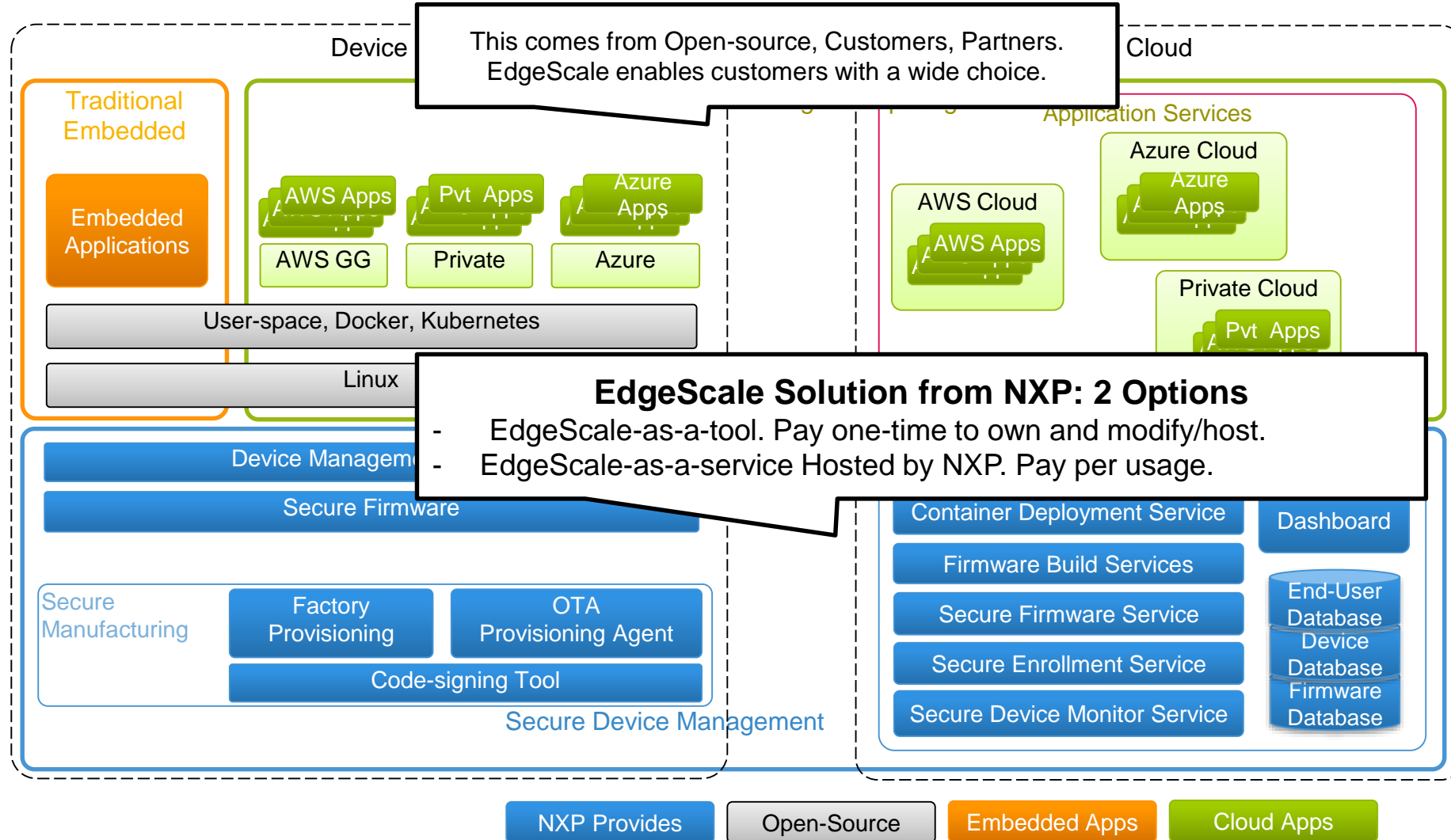


Nexcom LS104x  
Edge Gateway



Accton LS1043  
IoT Gateway

# EdgeScale Business Model





# EdgeScale – What You Get

## EdgeScale-as-a-Tool

- Complete access to all EdgeScale features.
- Jump-start your Edge/IoT management solution.
- Flexibility to host on your own infrastructure.
- Freedom to modify and integrate with your own framework.
- Professional support and customization services

Each service builds on top of the former.

or

## Secure Device Manufacturing Service

- Inject Unique-ID and credentials/keys to the device.
- Securely boot device with signed firmware

## Secure Device Management Service

- Securely enroll, validate device from cloud
- Securely download, update and manage firmware
- Monitor device health, diagnostics, usage

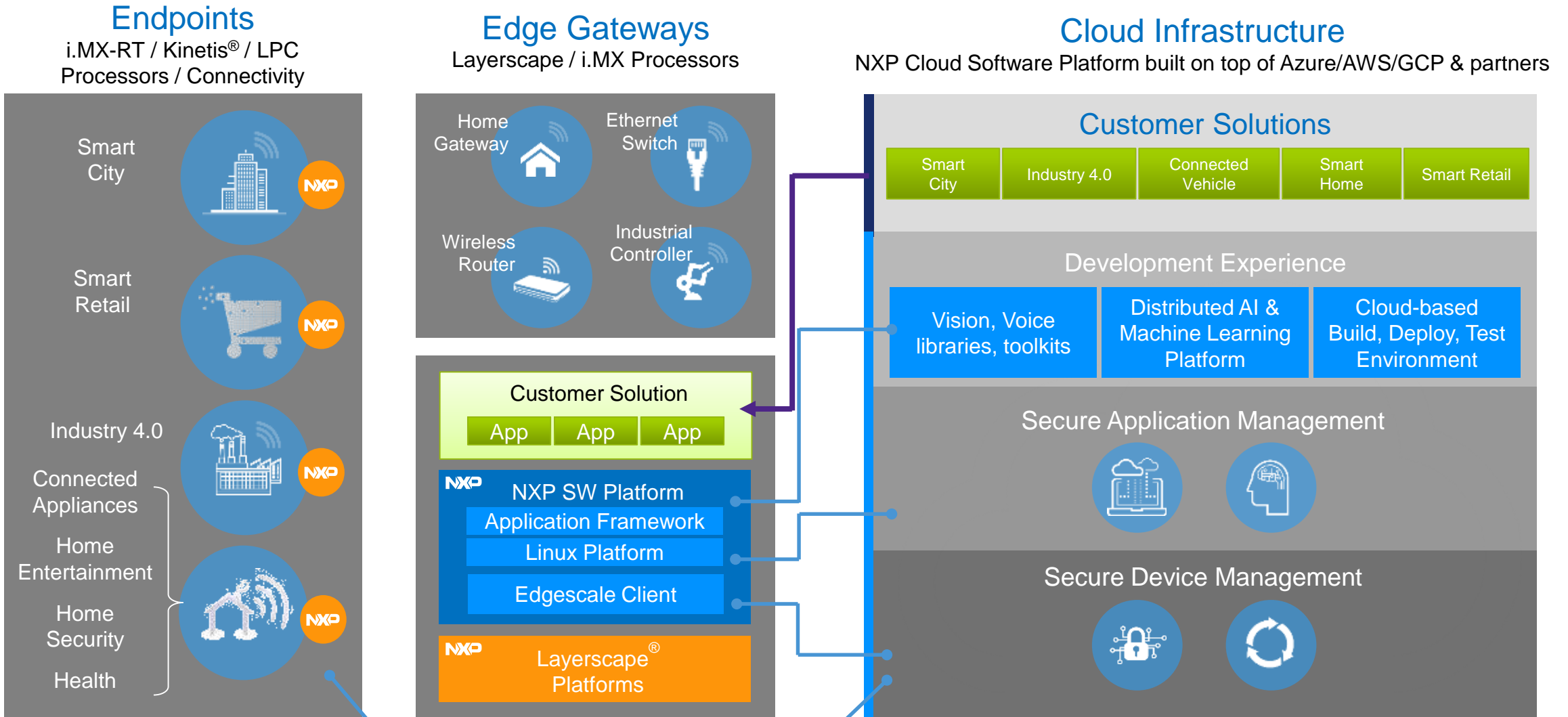
## Secure Application Management Service

- Securely deploy applications from the cloud.
- Manage your own app-store, develop and build on the cloud.

## Secure AI & Data Management Service

- Optimize, convert and deploy AI models from cloud to edge.
- Store, stream and manage data securely.

# NXP – Improving the Edge Experience

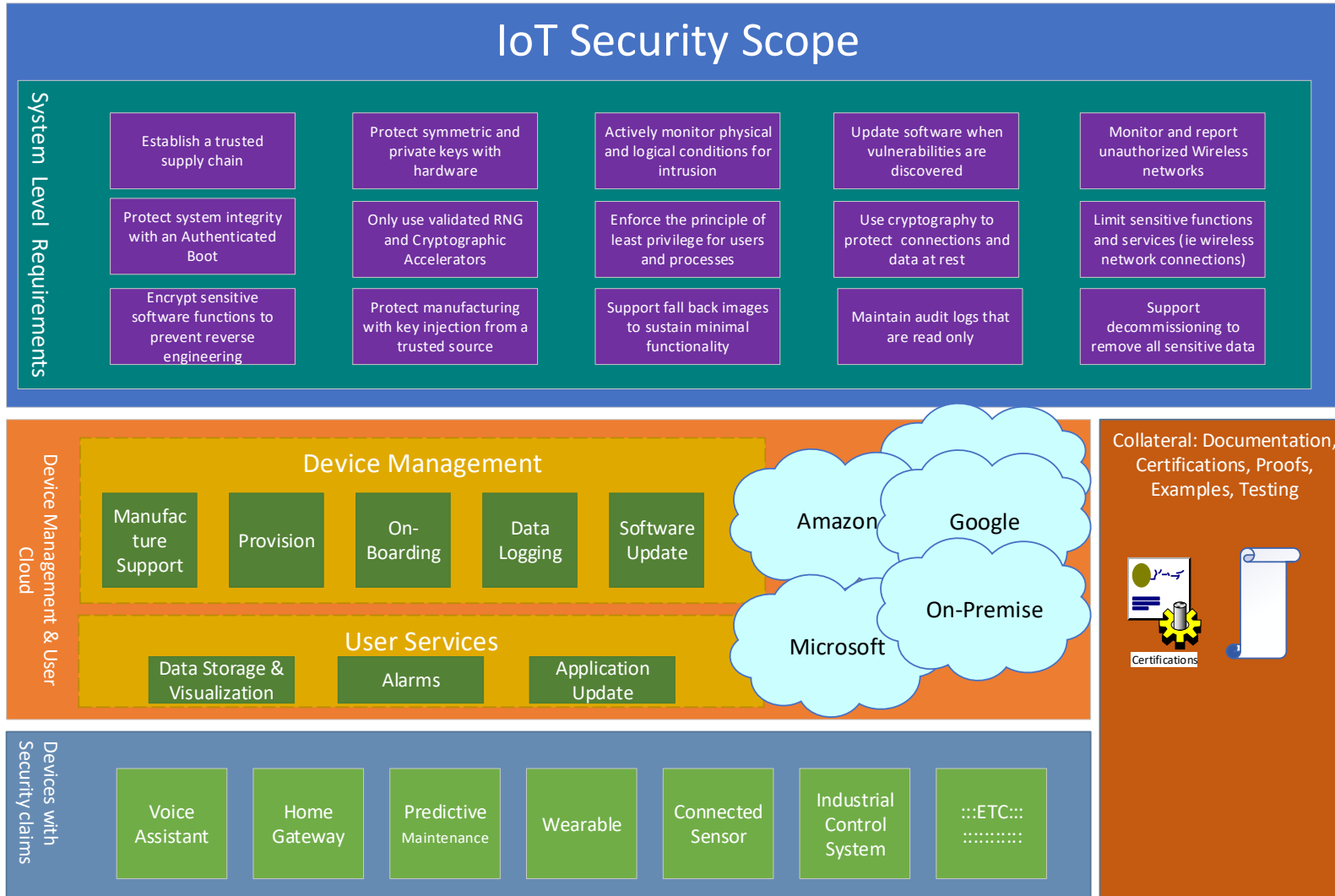


# Solutions

NXP Designs



# IoT Security System Level Diagram



- Security scope spans across multiple domains
  - Numerous device form factors and services
  - Cloud User services and Device Management
  - Certifications, regional standards and other proof points

# Voice Solution – System Level Security Capabilities

Capability	Sys. Level Security Goal
Authenticated Boot	Protect System integrity with Secure Boot
Arm mBed TLS for transport layer security	Use cryptography to protect connections and data at rest Protect symmetric and private keys with hardware
encrypted firmware and on-the-fly decryption with hardware protected key	Encrypt sensitive software services to protect against reverse engineering
over-the-air updates based on Amazon FreeRTOS OTA middleware	Update software when vulnerabilities are discovered
fallback and golden application image support	Support fall back image to protect minimal functionality
data storage based on hardware protected keys	Use cryptography to protect connections and data at rest



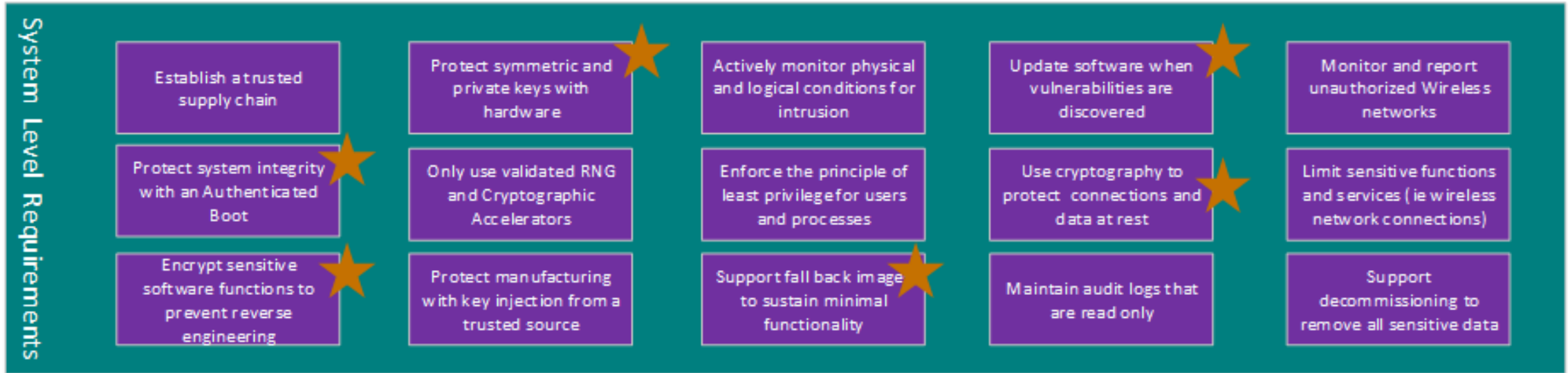
MCU solution for Alexa Built-in™ products

## MCU-Based Solution for Alexa™ Voice Service

NXP's MCU-based solution for Amazon's Alexa Voice Service (AVS) leverages the i.MX RT106A audio crossover processor, enabling developers to quickly and easily add Alexa voice assistant capabilities to their products. This turnkey design with ultra-small form factor comes completely integrated with Amazon-qualified software for an out-of-the-box AVS experience.



# System Level Security Goals



★ Addressed by Voice Solution

# MCU/MPU Security Hardening: OTPMK Protection

- Devices such as NXP [i.MX products](#) integrate security technology for protecting keys
  - Fuse locations for OTPMK key material with read out protection for protected storage of key or key material
  - Keys/key material are passed to hardware accelerators without software interaction for protected use
  - Access to the use of keys is restricted by security state machine requiring authenticated boot
  - **Zero-izable keys with tamper monitors for decommissioning**

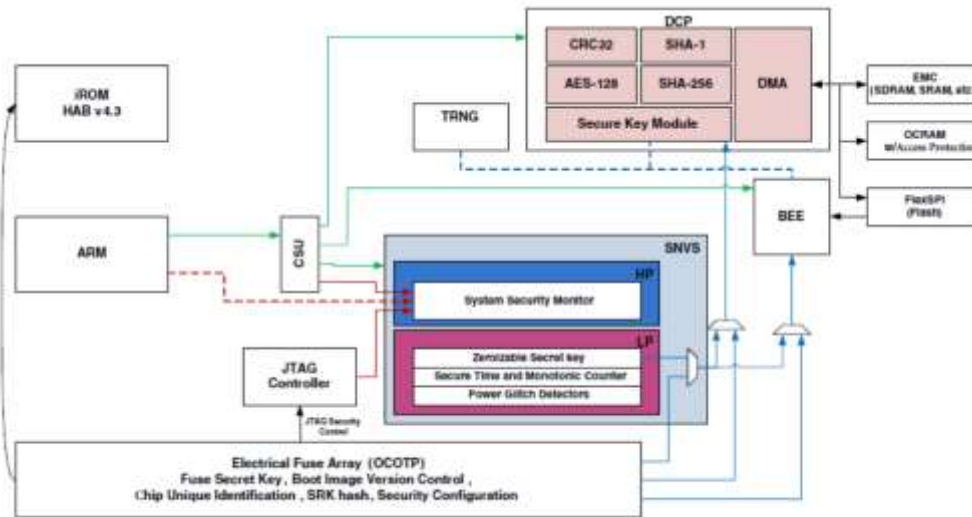
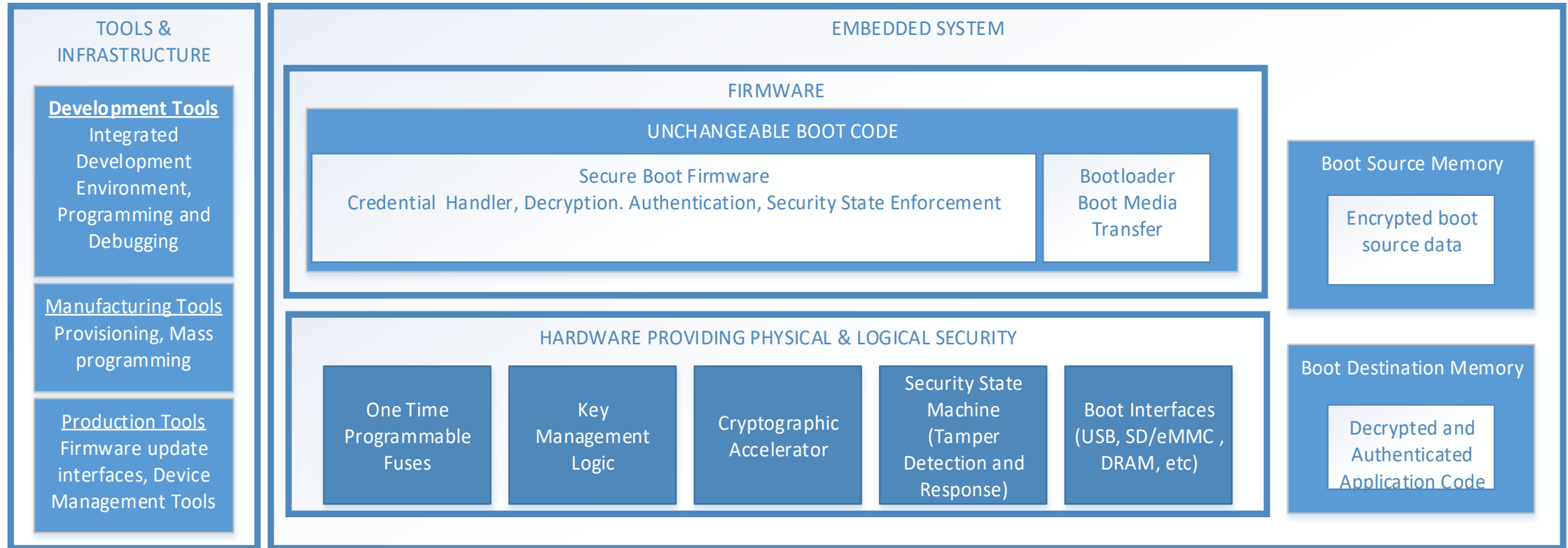


Figure 1-1. Security subsystem (simplified)

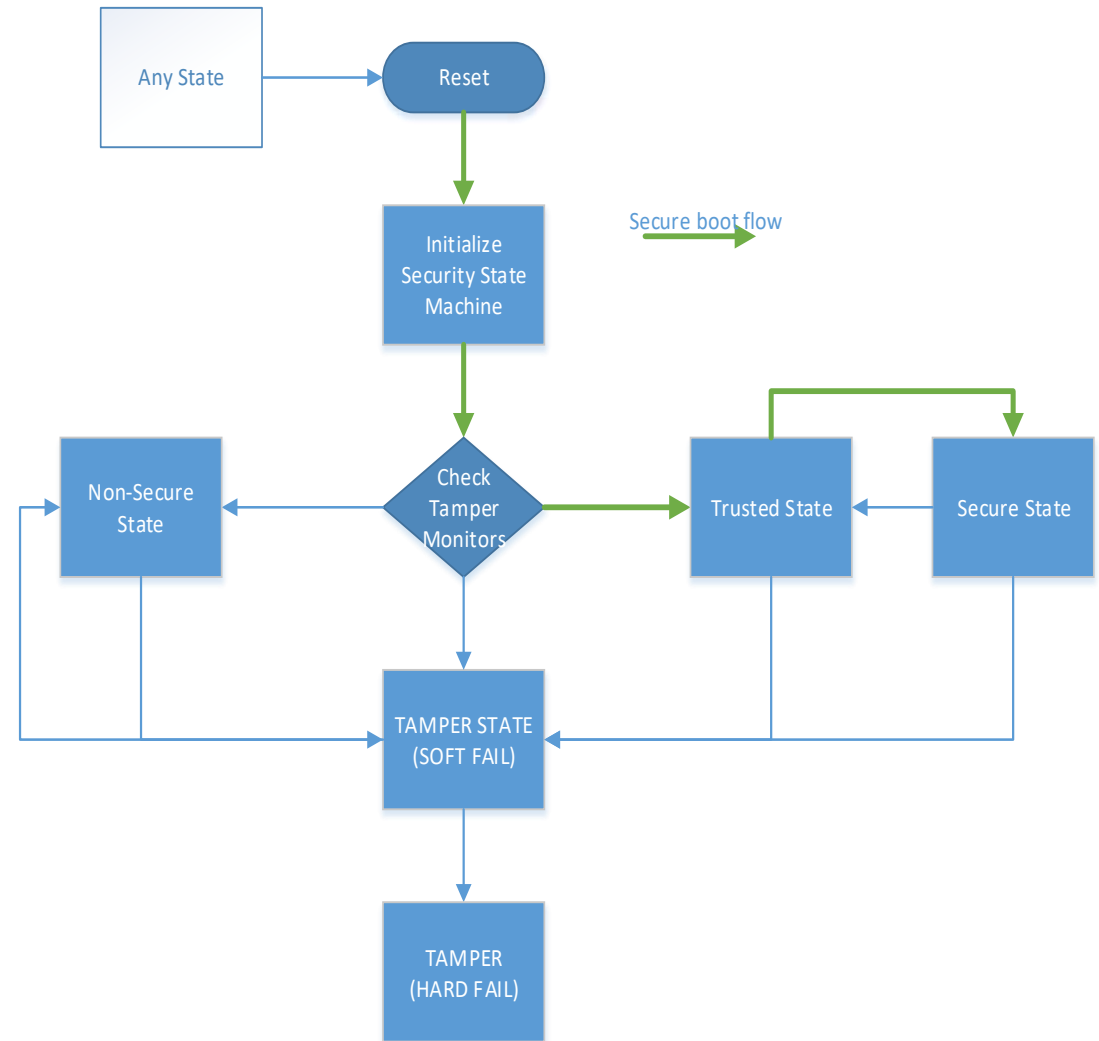


# i.MXRT Secure Boot Architecture Diagram



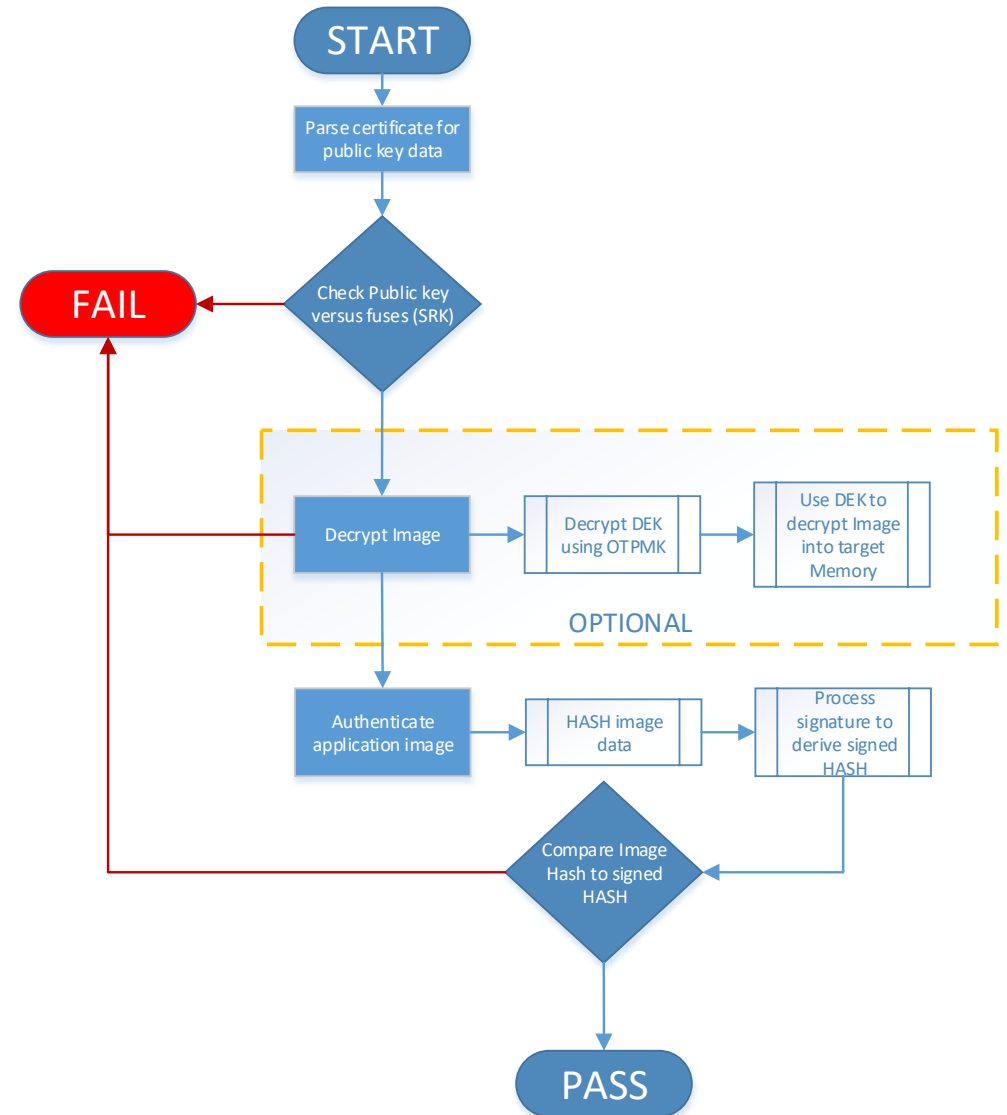
# Security State Machine

- Monitoring the process of booting and enforcing security protections is a block in the i.MX RT named the Secure Non-Volatile Storage (SNVS).
- Security state machine separated into an independent power domain on the chip.
- Power domain isolation allows tamper monitoring to be extended into a device state where a backup battery, such as a coin cell, is used for protection.
- SNVS serves as the SOC's central reporting point for security-relevant events such as the success or failure of boot software validation and the detection of security threat events.



# HAB Runtime Operation

- Option for Authenticated and encrypted handling of boot data
- Decryption (Optional) always occurs first on the data
- SRK hash checks integrity
- Hardware (SNVS/Security state machine) dictates what operations are performed



# Encrypted XiP – BEE Features

- Provides an on-the-fly decryption engine, which is used for decrypting ciphertext of FlexSPI (only)
- Standard AXI interconnection
- On-the-fly AES-128 decryption, supporting ECB and CTR mode
- Aliased memory space support. Address remapping for up to two individual regions
- Independent AES Key management for those two individual regions
- Bus access pattern optimization with the aid of local store and forward buffer
- Non-secured access filtering based on security label of the access
- Illegal access check and filtering



# Encrypted XIP on Serial NOR via FlexSPI Interface

- BEE supports two separate encrypted regions using two separate AES Keys
- Flashloader will only configure one region and only supports using the OTPMK
- To use encrypted XIP the ROM needs the following information configure the BEE controller:
  - Protection Region Descriptor Block (PRDB)
  - Key Information Block
- **PRDB and KIB are both stored encrypted in external memory**
  - BEE\_KEY0\_SEL and BEE\_KEY1\_SEL determine the key used to decrypt KIBs:
    - OTPMK derived key used with flashloader
    - Other key options could be used with an offline encryption tool
  - KIB -> encrypted by BEE\_KEYn\_SEL -> Encrypted KIB (EKIB)
  - PRDB -> encrypted by AES key in the KIB -> Encrypted PRDB (EPRDB)

# Conclusions



# Wrap-up

- In today's threat landscape, all IoT devices must address security
  - Legislation
  - Common IoT Attacks
- Security integration involves people, processes and technology
  - Address the entire lifecycle of devices
  - Scale to meet device threats
  - Easy to use and deploy
- NXP portfolio includes processing options for Secure End Nodes and Secure Gateways
- NXP Edgescale Cloud Software and Services leverages NXP chip level expertise to satisfy device lifecycle management security requirements



**SECURE CONNECTIONS  
FOR A SMARTER WORLD**