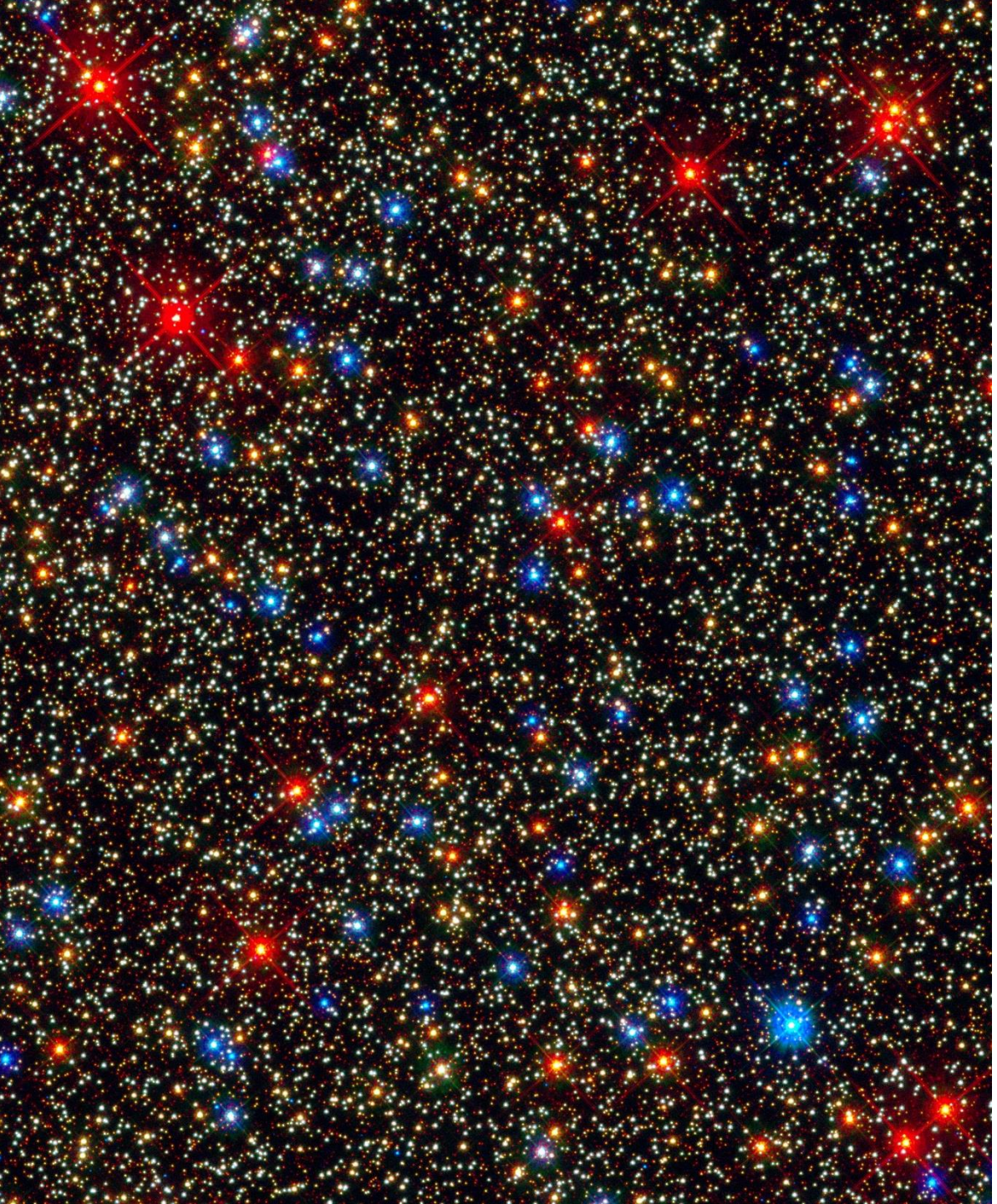
ADVANCE YOUR IoT SECURITY LEVERAGING HARDWARE PROTECTED KEYS

DONNIE GARCIA
NXP IoT SECURITY SOLUTIONS
APRIL 2019

SECURE CONNECTIONS FOR A SMARTER WORLD

Abstract

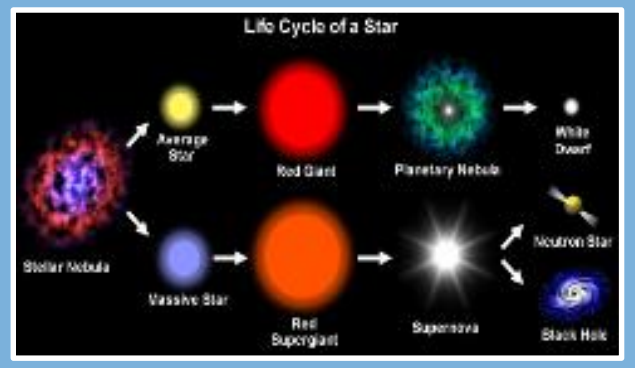
- *Cryptography is the basis for protecting the confidentiality, integrity and authenticity of the data within the Internet of Things ecosystem. For the IoT Edge device, the cryptographic keys used to perform the services such as encrypted boot, onboarding, and over the air updates are critical components that must be protected. Chip level hardware protected keys are the standard for achieving strong security protection for embedded designs. This session will define what a hardware protected key is and show several examples of how these keys are realized on NXP processors. Then it will dive deeper into Physical Unclonable Function (PUF) based keys that can be deployed on the vast majority of MCUs and the advantages of PUF technology. The i.MX RT 1050 family of devices will be used as a real world example of how Intrinsic ID BroadKey® SRAM based PUF can advance your IoT Security.*



Agenda

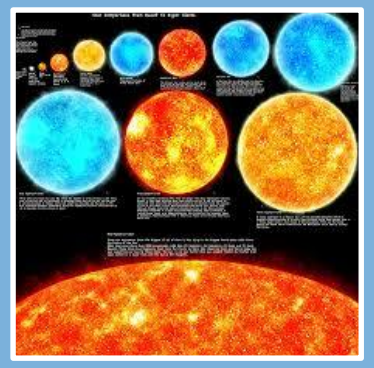
- System level view of addressing IoT Security
- Hardware Protected Keys
- SRAM PUF Technology
- Implementing SRAM PUF on the i.MX RT1050 EVK
- Conclusions

IoT Security Strategies



Address the entire **device lifecycle**

- Once deployed processor 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

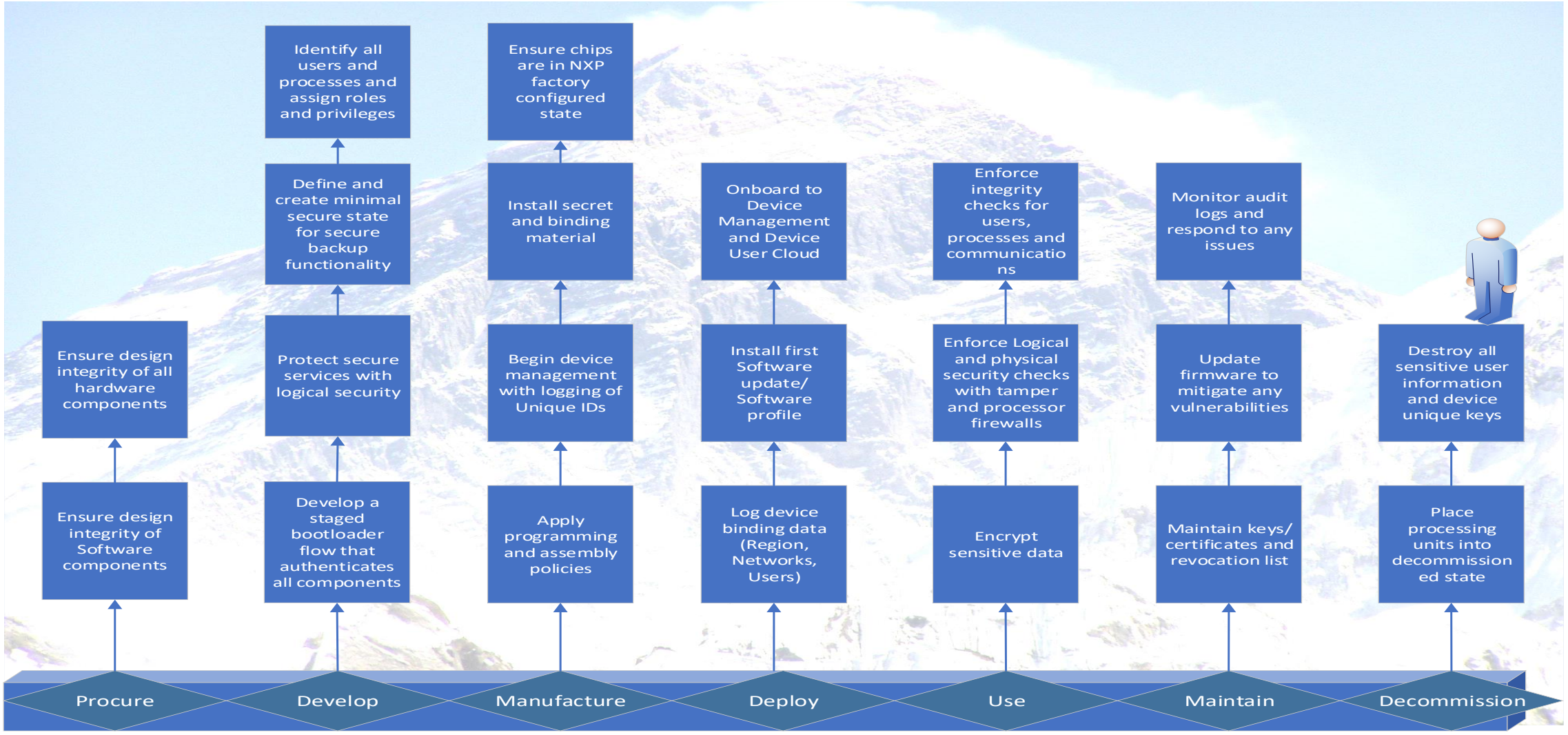
- Security technology is rooted in MCU/MPU hardware capabilities at many processor integration and performance points (NXP: A71xx, SE050, i.MX, Layerscape, Kinetis, LPC, JN)

Be **easy** to deploy and **easy** use

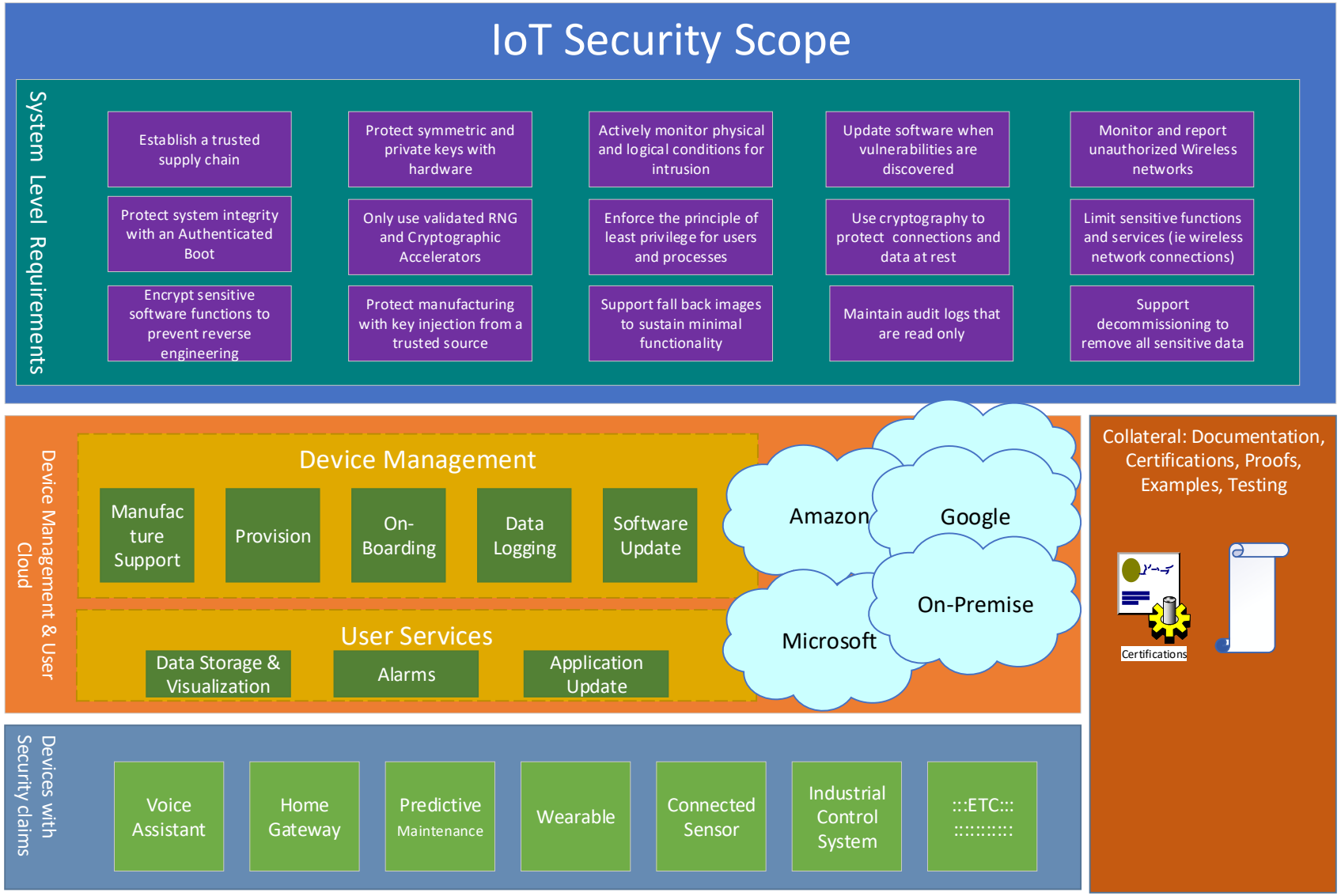
- Fully Documented steps and procedures from installing bootstrap through decommissioning stage (NXP: Edgescale documentation)

SYSTEM LEVEL VIEW OF ADDRESSING IoT SECURITY

Design Challenges across device lifecycle

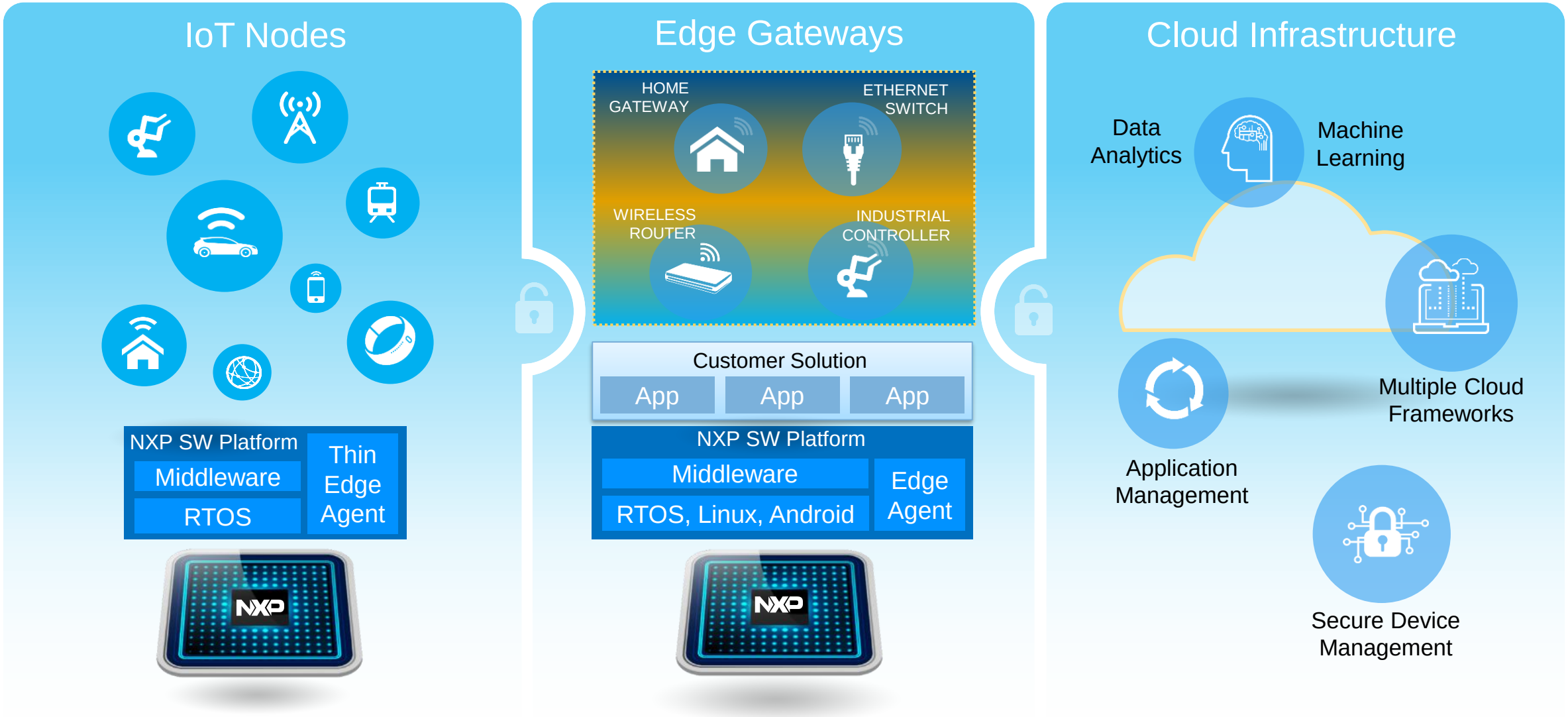


IoT Security System Level Diagram



- 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

NXP Solutions for Edge Computing



NXP: SE050, LPC, Kinetis, i.MX-RT

NXP Layerscape, i.MX Family

NXP EdgeScale Suite

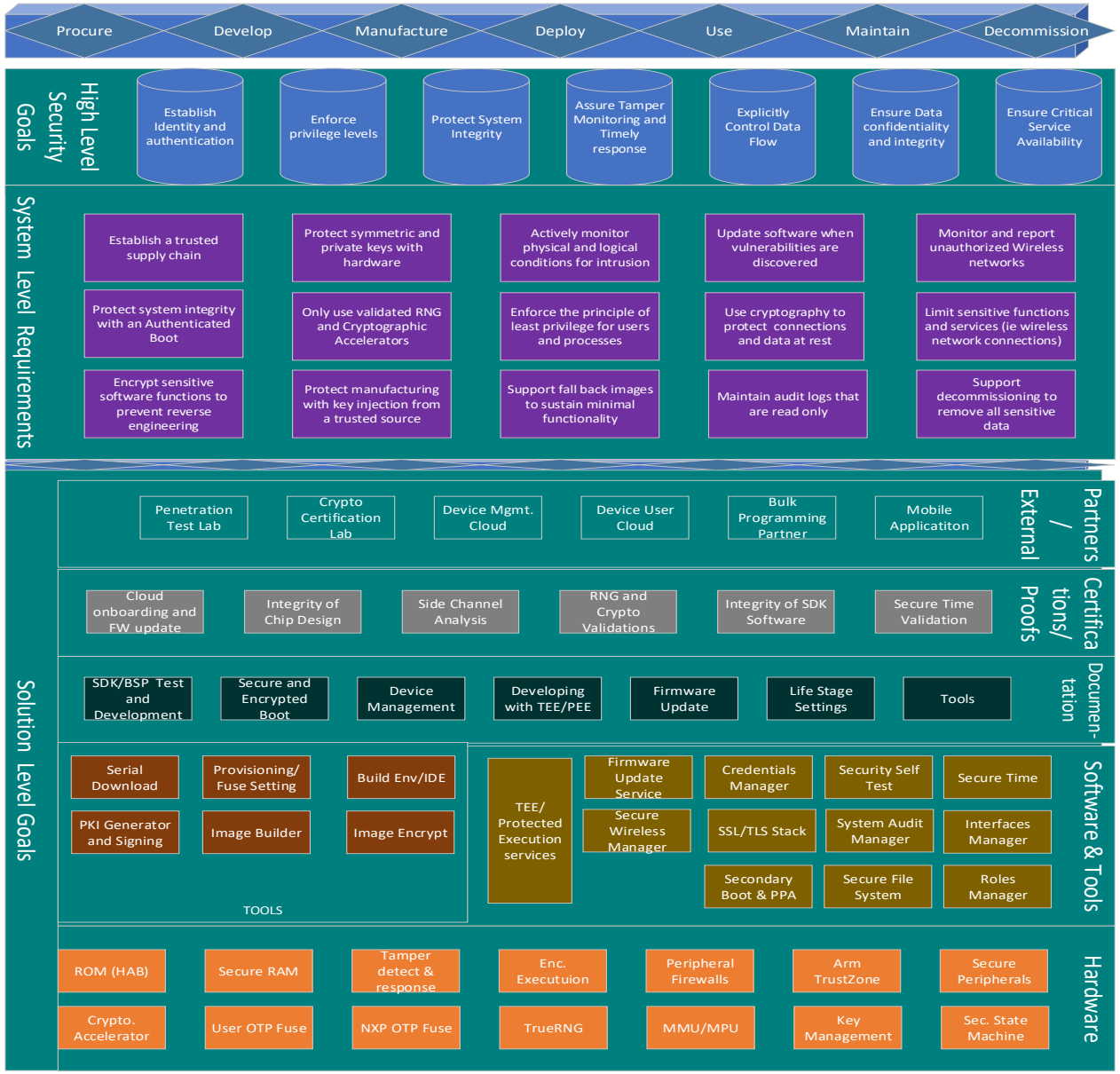
NXP for Secure deployment from Edge to Cloud

Can functionally overlap in runtime*

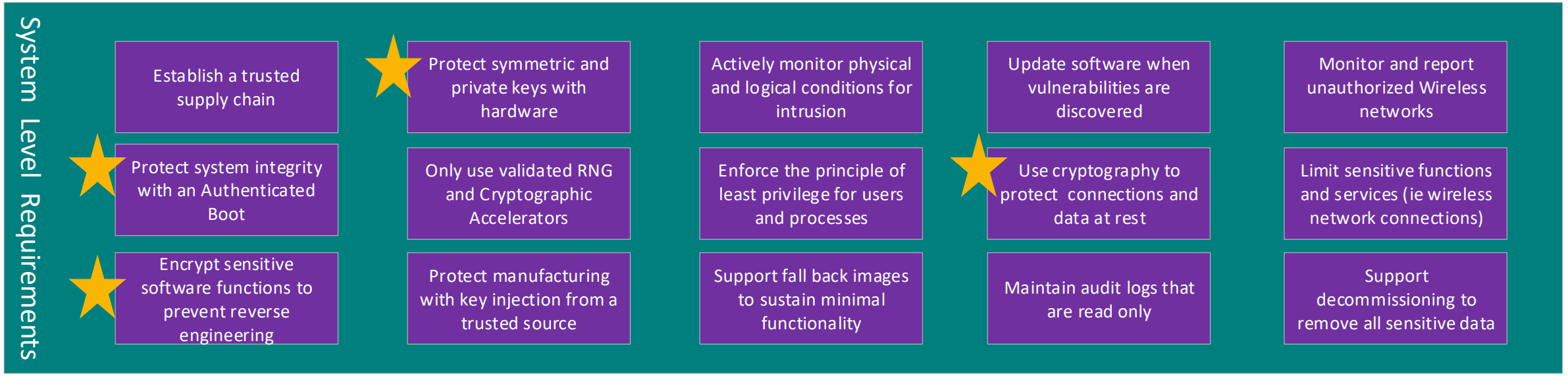
*With secure provisioning identity can be established in a processor

Device Level Security Solution

- Security scope at the device level
  - Hardware
    - SoC specific security technology
  - Software and Tools
    - Logical Security implementation
    - Trusted Execution Environment
  - Documentation
    - Security Policies
    - Internal/External Documentation
  - Certifications
    - Third-Party analysis
  - Partner/External
    - Cloud services



System Level Security Goals Depend on Cryptography

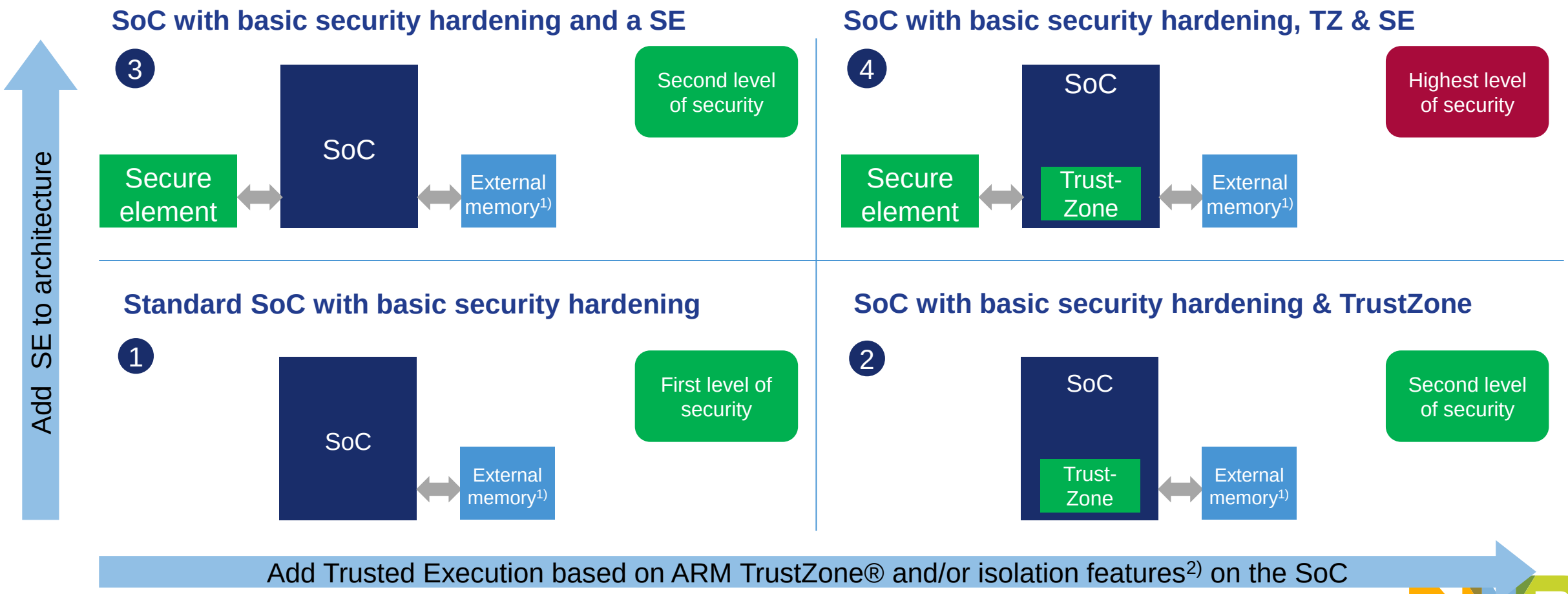


- **Cryptography is a fundamental capability needed to address edge device security**
  - Basis for protecting data at rest and in transit
  - Provides robust identity for the end device by cryptographic authentication
- **The key material used for cryptographic operations must be protected by hardware**
  - Attacks against Confidentiality/Integrity/Authenticity are aimed at attaining the Cryptographic Key

Requirements which depend on Cryptography

Secure Edge Architectures

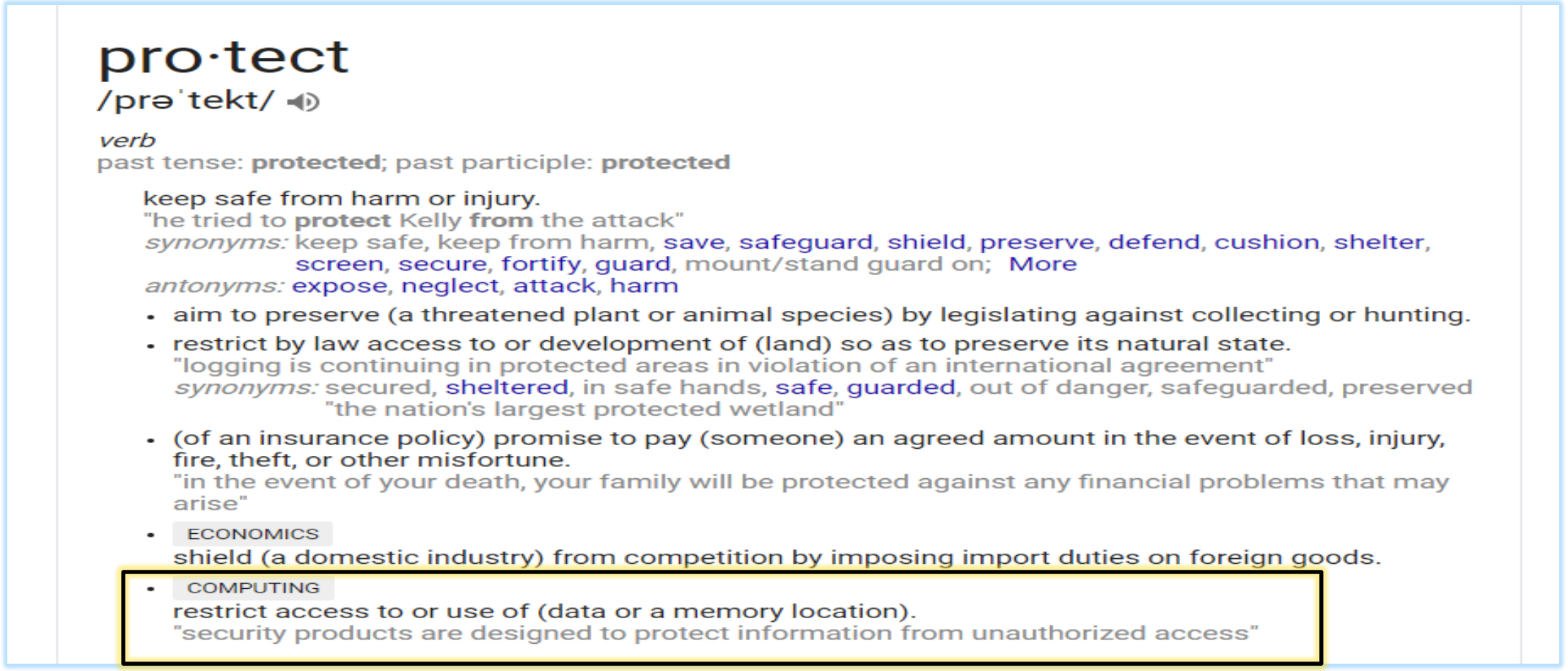
Security Architectures supported by current shipping NXP products



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

HARDWARE PROTECTED KEYS

Defining Hardware Protected Keys



pro·tect

/prəˈtekt/

verb

past tense: **protected**; past participle: **protected**

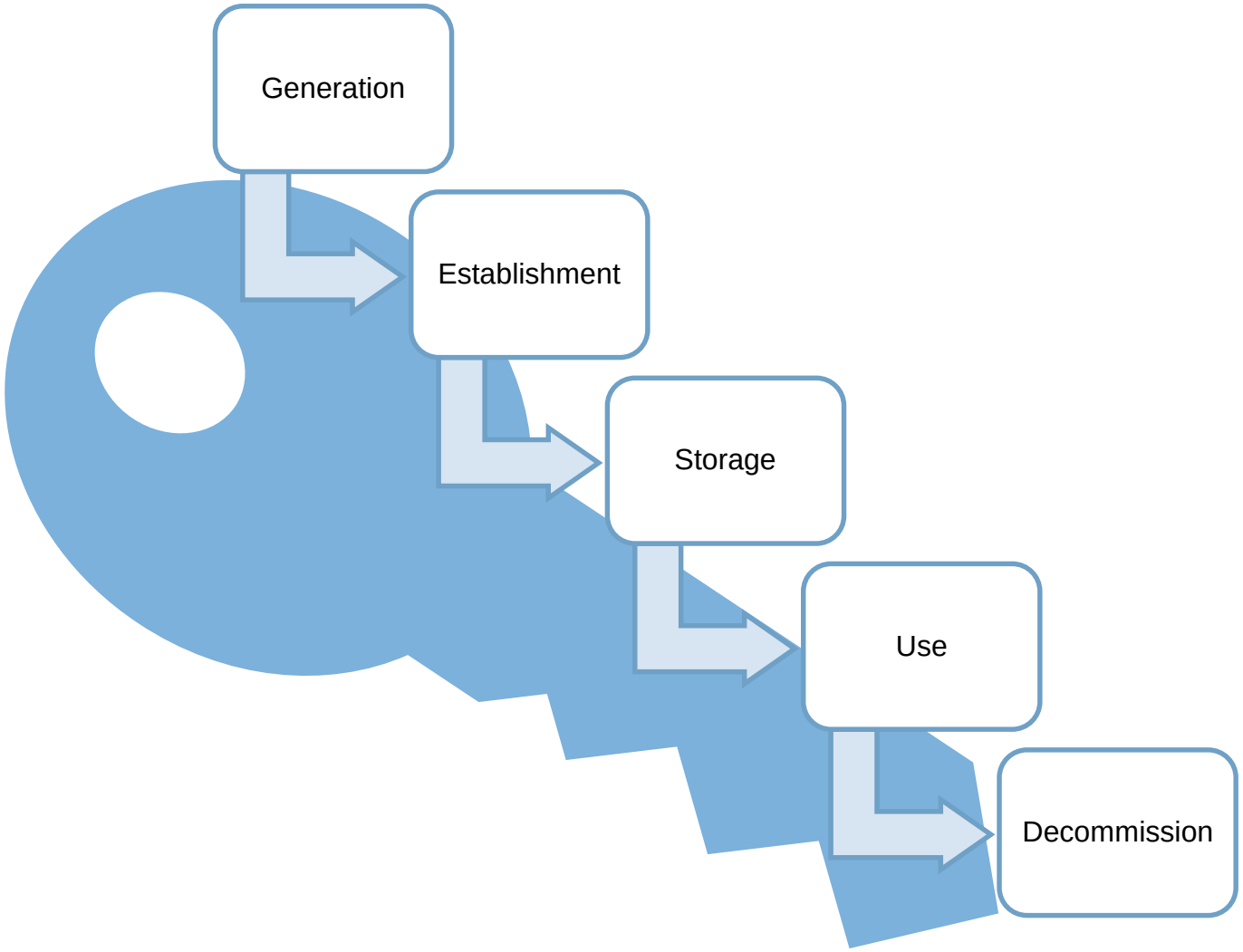
keep safe from harm or injury.
"he tried to **protect** Kelly **from** the attack"
synonyms: keep safe, keep from harm, save, safeguard, shield, preserve, defend, cushion, shelter, screen, secure, fortify, guard, mount/stand guard on; More
antonyms: expose, neglect, attack, harm

- aim to preserve (a threatened plant or animal species) by legislating against collecting or hunting.
- restrict by law access to or development of (land) so as to preserve its natural state.
  "logging is continuing in protected areas in violation of an international agreement"
  synonyms: secured, sheltered, in safe hands, safe, guarded, out of danger, safeguarded, preserved
  "the nation's largest protected wetland"
- (of an insurance policy) promise to pay (someone) an agreed amount in the event of loss, injury, fire, theft, or other misfortune.
  "in the event of your death, your family will be protected against any financial problems that may arise"
- ECONOMICS
  shield (a domestic industry) from competition by imposing import duties on foreign goods.
- COMPUTING
  restrict access to or use of (data or a memory location).
  "security products are designed to protect information from unauthorized access"

Protected over the lifecycle* of the Cryptographic keys

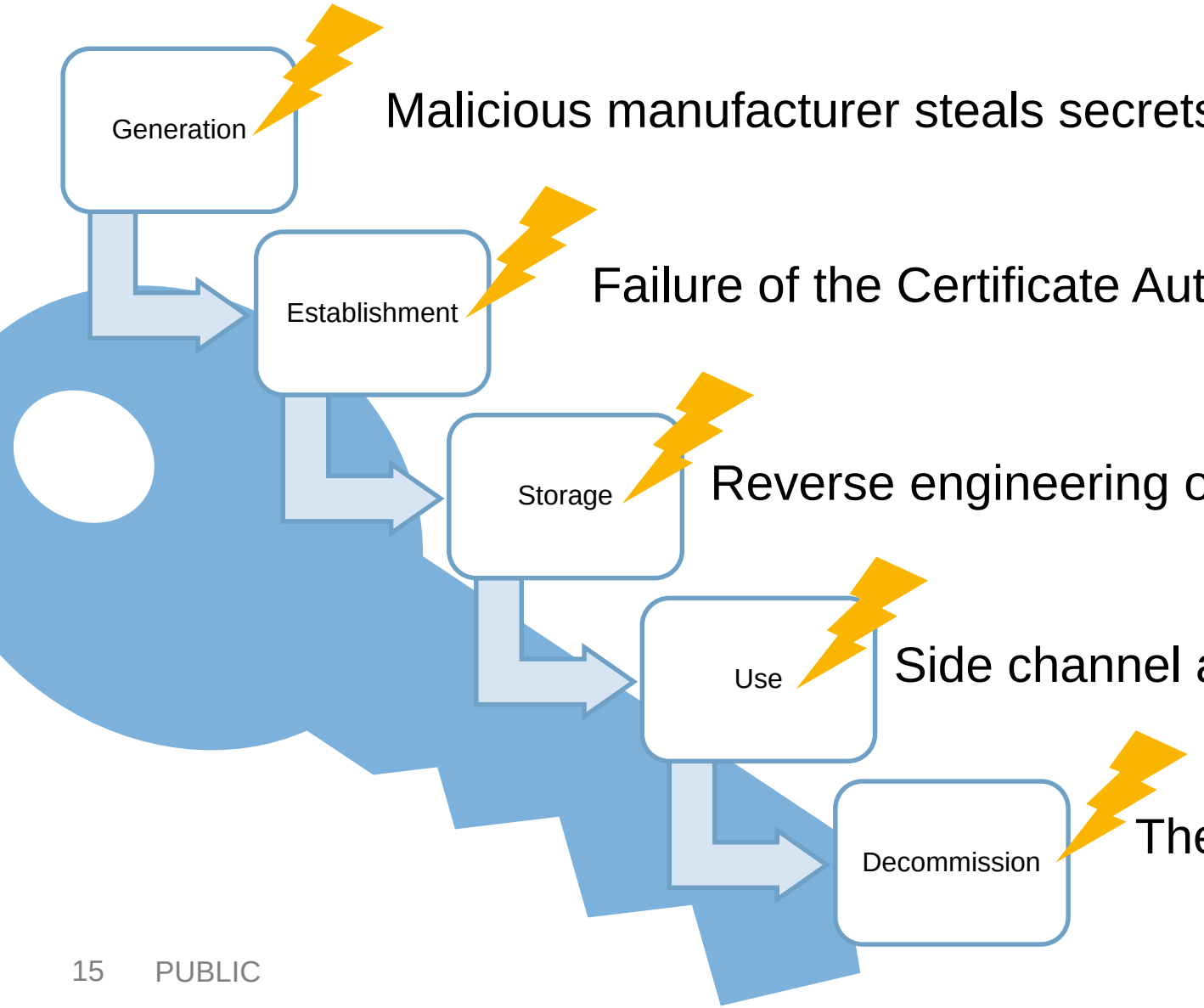
PROTECTED

- 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



Malicious manufacturer steals secrets during the provisioning process

Failure of the Certificate Authority or device database attacks

Reverse engineering of silicon hardware or software

Side channel attacks during cryptographic processing

Theft of device before destruction of secrets

HW Protected Keys Example 1: 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 2: MCU/MPU Security hardening

- Devices such as NXP i.MX products integrate security technology for protecting keys
  - Fuse locations for 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

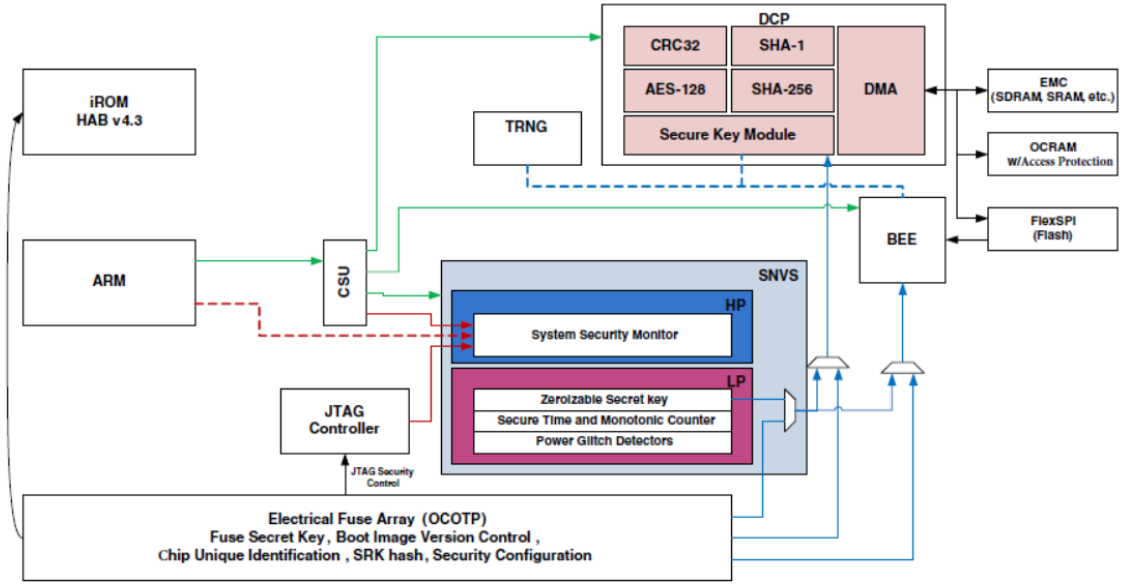
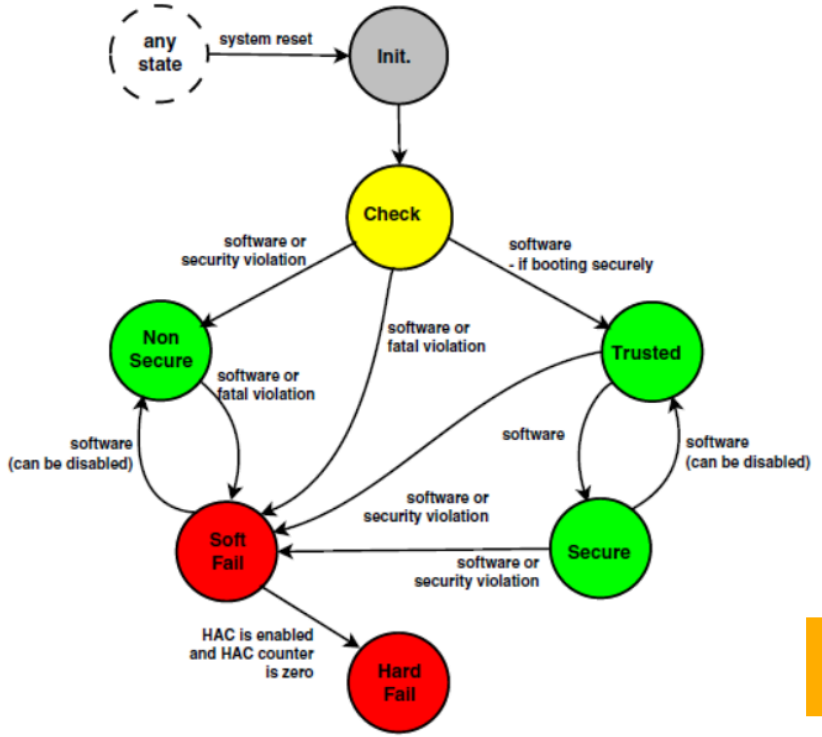


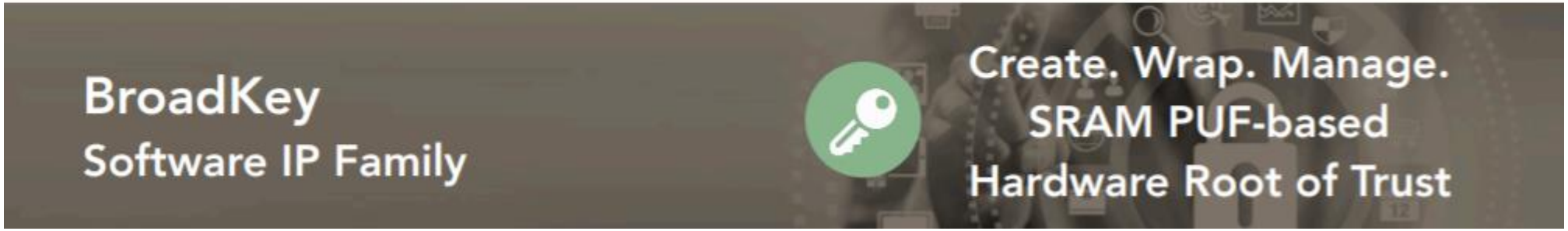
Figure 1-1. Security subsystem (simplified)



HW Protected Keys Example 3: Software PUF

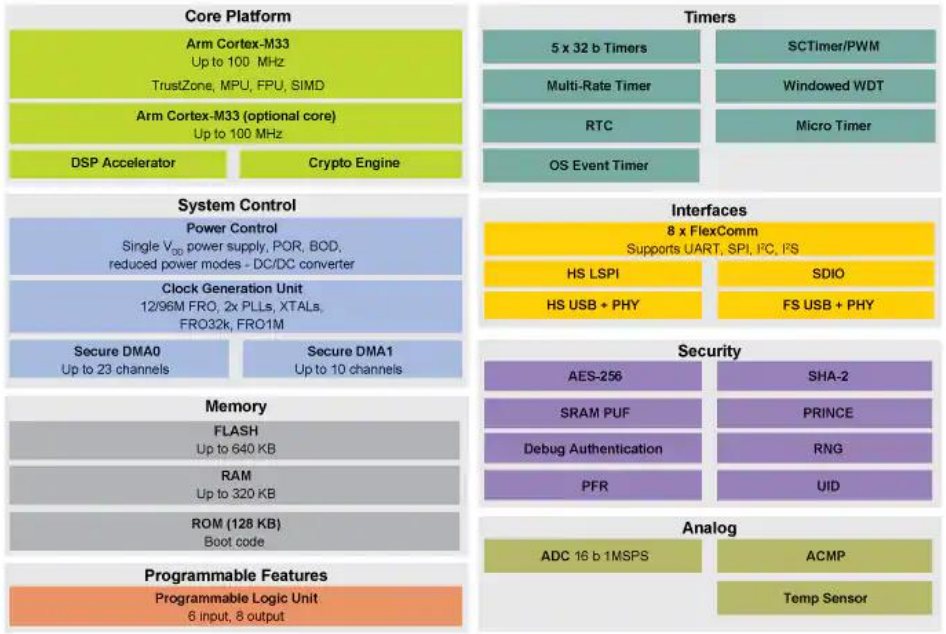
- Intrinsic ID has a software based implementation of a cryptography library based on a cryptographic key derived from a patented SRAM Physical Unclonable Function
  - Key generation is device unique and unclonable based on the SRAM PUF technology
  - Key is ephemeral and not stored so is protected from physical attacks
  - BroadKey SW is developed to meet FIPS 140-2 Appendix B and applies countermeasures for side channel attacks
  - Destroying the activation code decommissions the key and protected key material

INTRINSIC ID



HW Protected Keys Example 4: Hardware PUF

- Recently launched LPC5500 family also makes use of Intrinsic ID SRAM PUF technology in the design of 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

NXP IoT Security ICs:
A71CH
A100x Authenticator
SE050

- **Strongest protection across all key life stages**
- **Uses:**
  - Device identity and establishing TLS/onboarding
  - NXP Trust provisioning reduces overhead for key generation and establishment

1 External Security IC

Security Hardening on MCU/MPU

- **Provides runtime application security**
- **Uses:**
  - Secure boot
  - Bulk data protection
  - Enforces security policies (Roles)
  - Firmware updates

2 Security with OTP Keys

Uses may overlap

Security Hardening on MCU/MPU with Software PUF (Intrinsic ID BroadKey)

- **Assist with early key life stages and improves protection for keys**
- **Uses:**
  - Key Generation and establishment
  - Device identity
  - Assist with TLS/onboarding

3 Software SRAM PUF

Hardware PUF (Intrinsic ID QuiddiKey): LPC5500 Family

- **Links advantages of PUF to runtime application security**
- **Uses:**
  - PUF protected keys used for secure boot, etc.
  - PUF for Key generation and establishment protects early life stages

Uses Incremental

4 Security w/SRAM PUF

PUF TECHNOLOGY

SRAM PUF Overview

Leverages the intrinsic entropy of the silicon manufacturing process

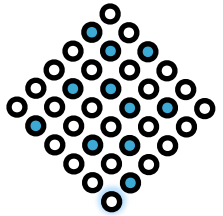
Device unique, unclonable fingerprint derived on every activation of the PUF

PUF master key is used to protect other secrets

1 

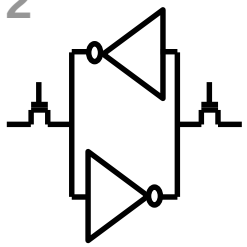
Process Variation

Naturally occurring **variations** in the attributes of transistors when chips are fabricated (length, width, thickness)



3 Silicon Fingerprint

The start-up values create a **random** and repeatable pattern that is unique to each chip

2 

SRAM Start-up Values

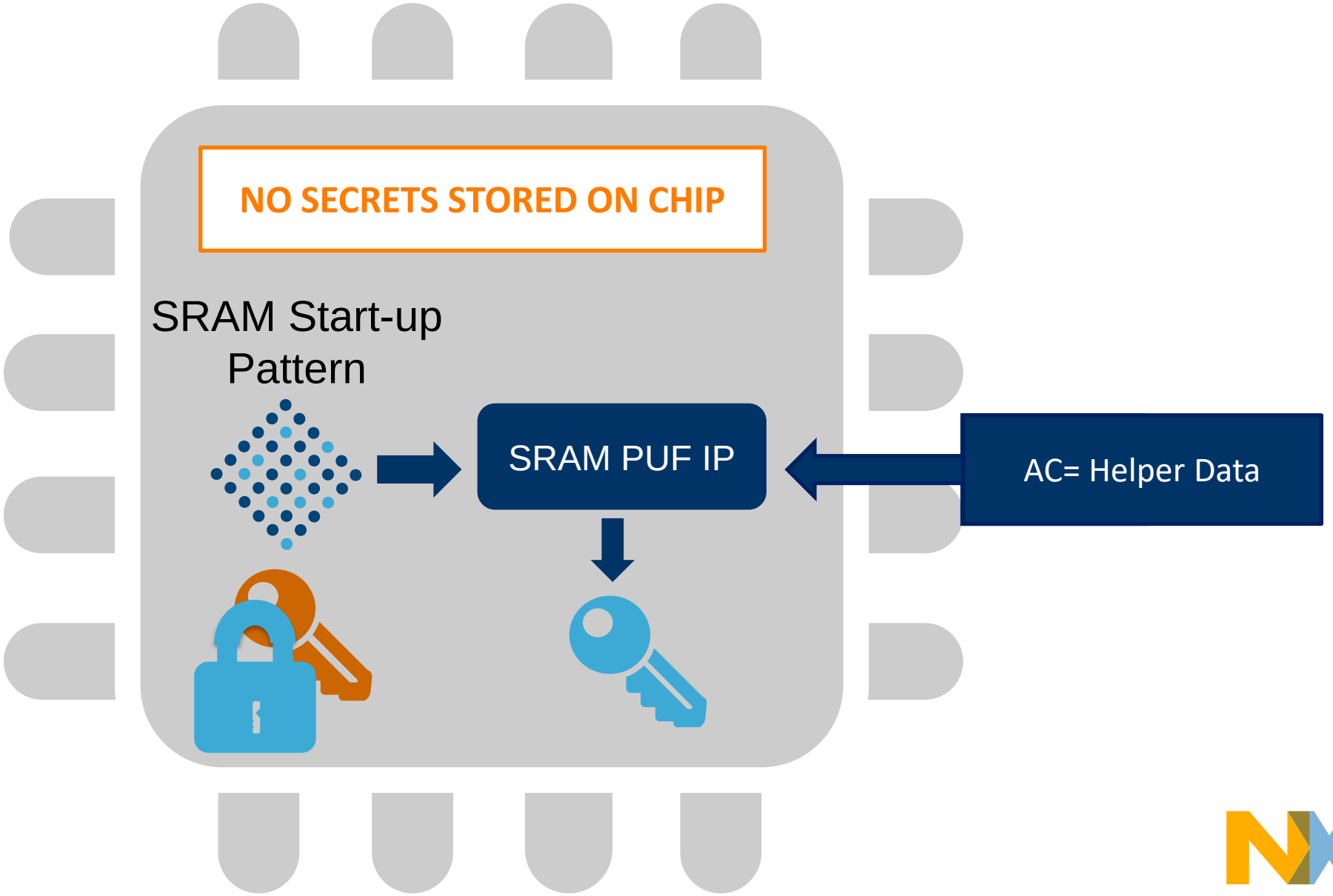
Each time an **SRAM block** powers on the cells come up as either a 1 or a 0

4 

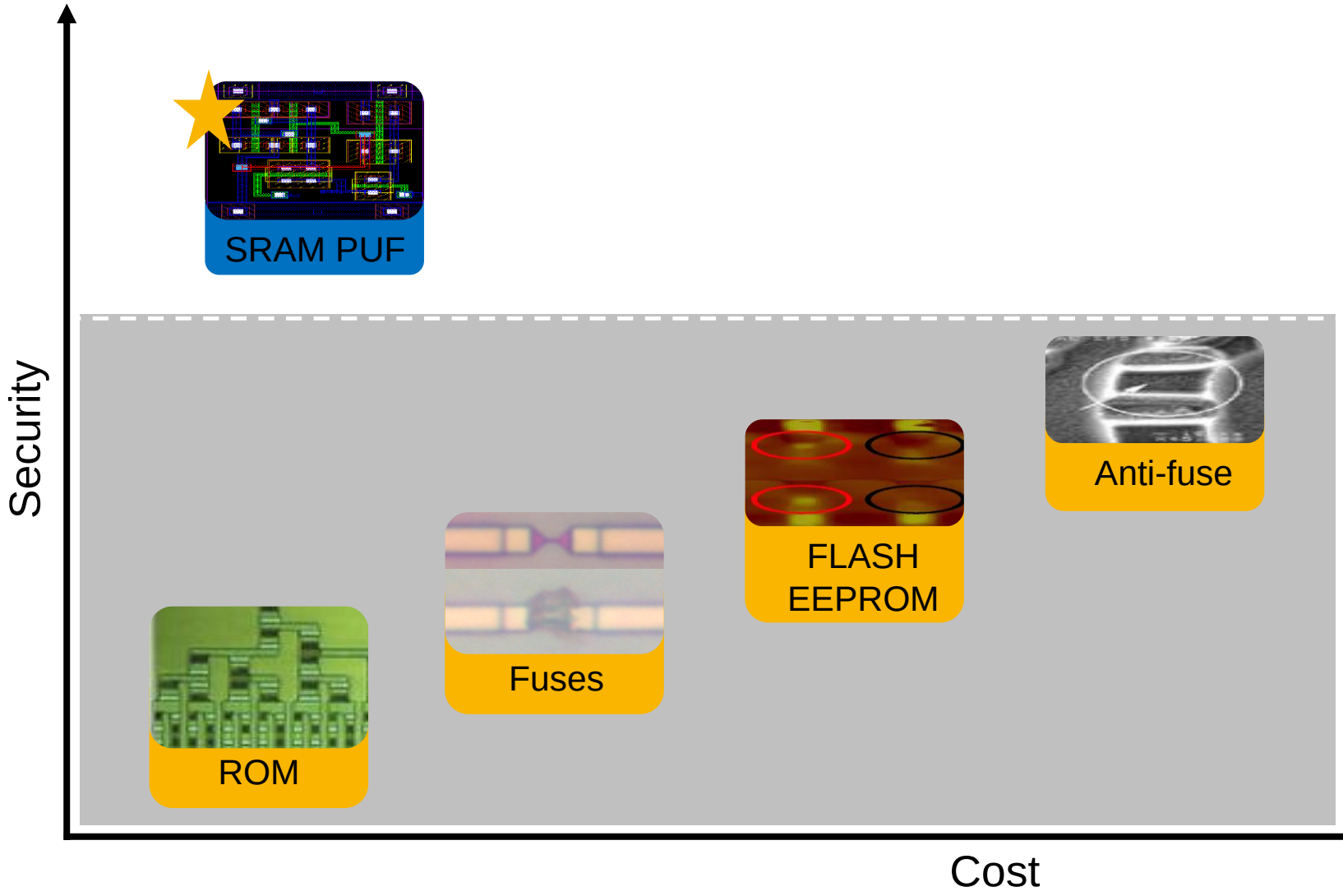
SRAM PUF Key

The silicon fingerprint is turned into a **secret key** that builds the foundation of a security subsystem

Using PUF Technology



SRAM PUF Disruptive Physical protection



SRAM PUF Technology

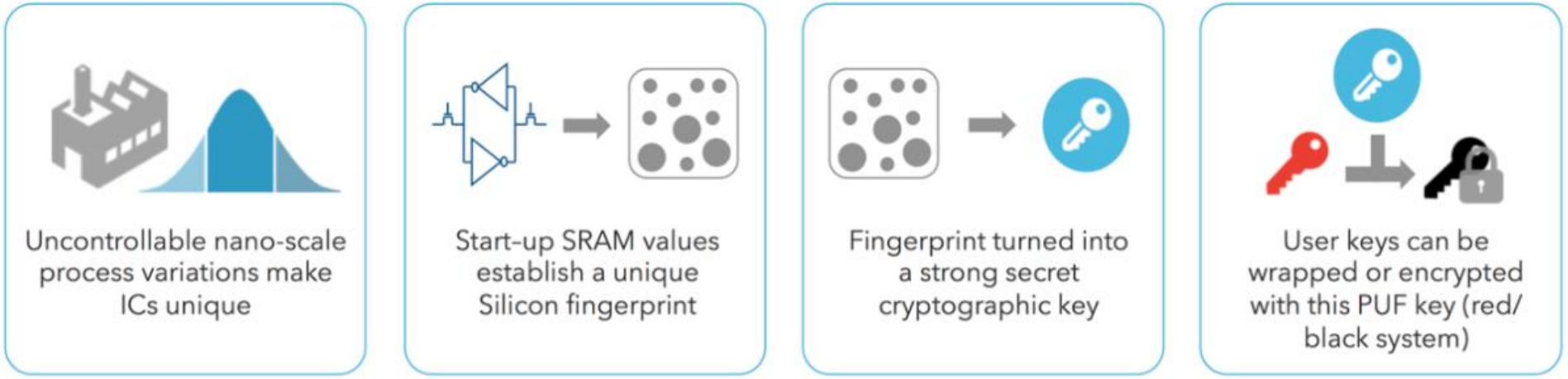
- Key generated by device entropy
- No traces of sensitive data in the embedded system

Other Solutions

- Key programmed externally
- Permanent physical alteration
- Key visible in structure

Intrinsic ID BroadKey

- **BroadKey-Pro** (most feature complete offering)
  - Device-unique key derivation
  - Random number generation
  - Wrapping and management, including elliptic curve private key generation and storage, importing and exporting of public keys, signature generation and verification
  - Key agreement functionality and public key encryption and decryption



BroadKey-Pro API summary and Uses

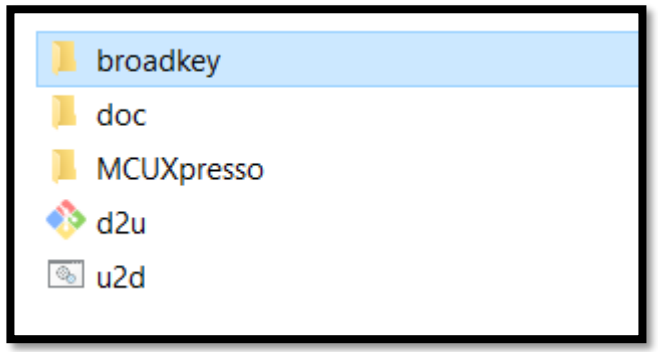
- **API Summary**
  - BASE
    - Init, Enroll, Start, Stop
  - Key and RNG Generation
    - Symmetric and Asymmetric keys, Random numbers
  - Wrap/Unrap
    - Handle key material
  - Public Key Management
    - Derive, import, export for public keys
    - Create private key code
    - ECDSA, ECDH

- **USES**
  - Key provisioning
    - At manufacturing or at deployment
  - Transport Layer Security
    - Integrated with TLS library
  - Securing data at rest
    - Linked to specific device
    - Binding SW
  - OTA Firmware update
    - Secure operation with confidentiality, authenticity and integrity

Getting BroadKey

- BroadKey Software IP is delivered as a library compiled for a specific target chip, along with interface specifications and user manual.
  - NXP Request from Intrinsic ID based BroadKey for a specific platform
    - (ie. i.MX RT) and IDE (MCUXpresso IDE)

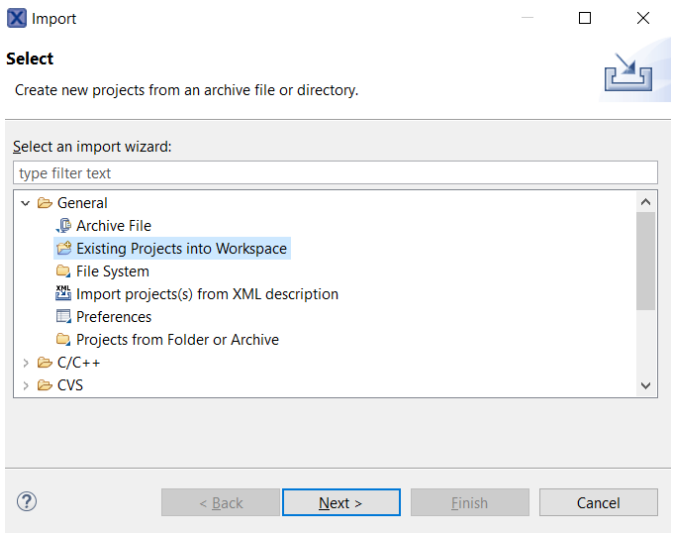
INTRINSIC ID

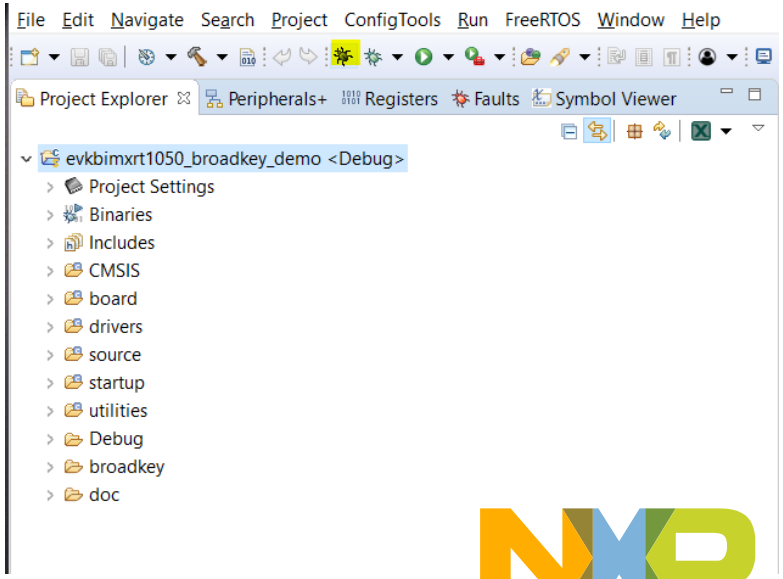


UTILIZING PUF ON THE i.MX RT1050 EVALUATION KIT

Using BroadKey: MCUXpresso Demo Application

- Steps needed to use the BroadKey delivery from Intrinsic ID
  - Install MCUXpresso IDE
  - Import the demonstration project
  - Connect the iMX RT EVK board
  - Run the demo from the debugger
  - See Output on the debug Terminal



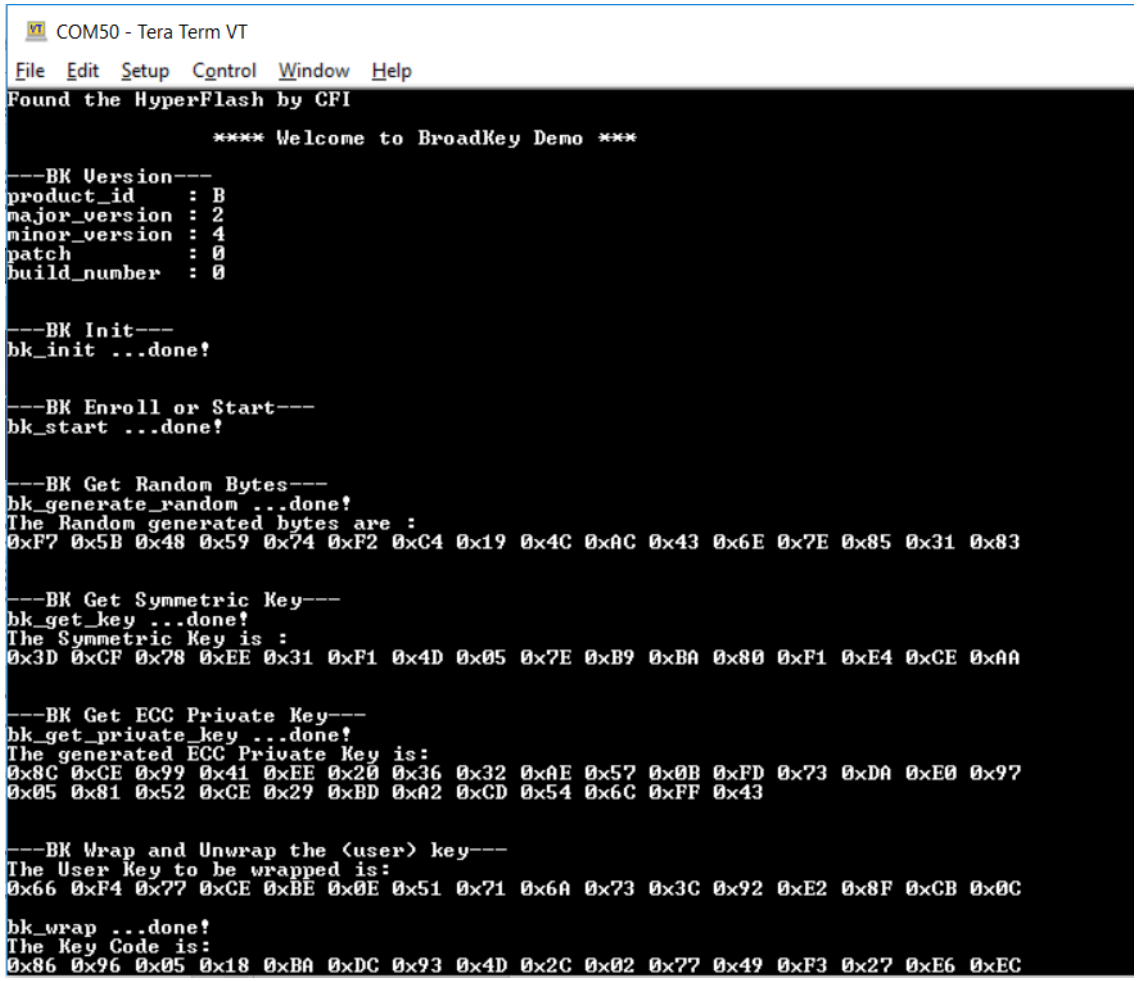


BroadKey Demo

Readme included in the demo

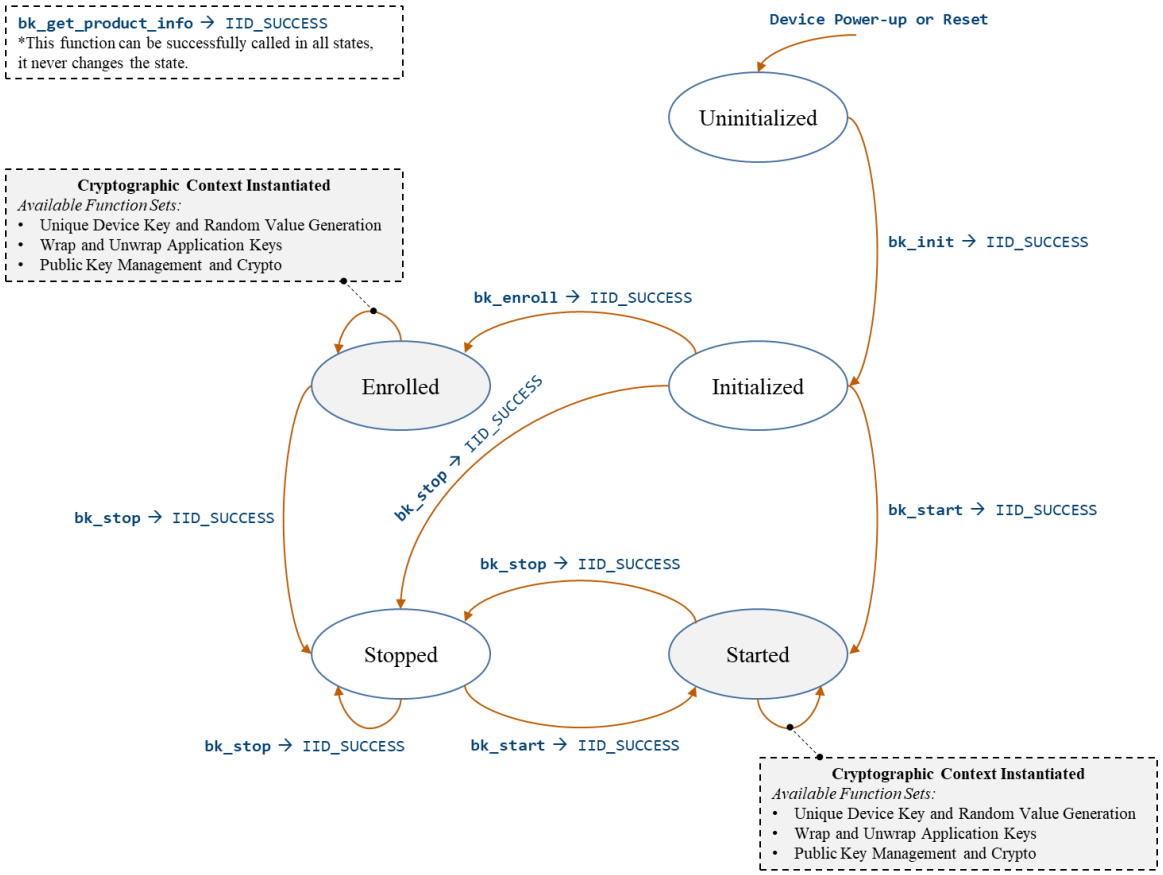
```
==================
- GCC ARM Embedded 7-2017-q4-major
- MCUXpresso10.2.0

Hardware requirements
=====================
- Mini/micro USB cable
- EVKB-IMXRT1050 board
- Personal Computer

Board settings
==============

Prepare the Demo
================
1.  Connect a USB cable between the host PC and the OpenSDA USB port on the target board.
2.  Open a serial terminal with the following settings:
    - 115200 baud rate
    - 8 data bits
    - No parity
    - One stop bit
    - No flow control
3.  Download the program to the target board.
4.  Launch the debugger in your IDE to begin running the demo.

```

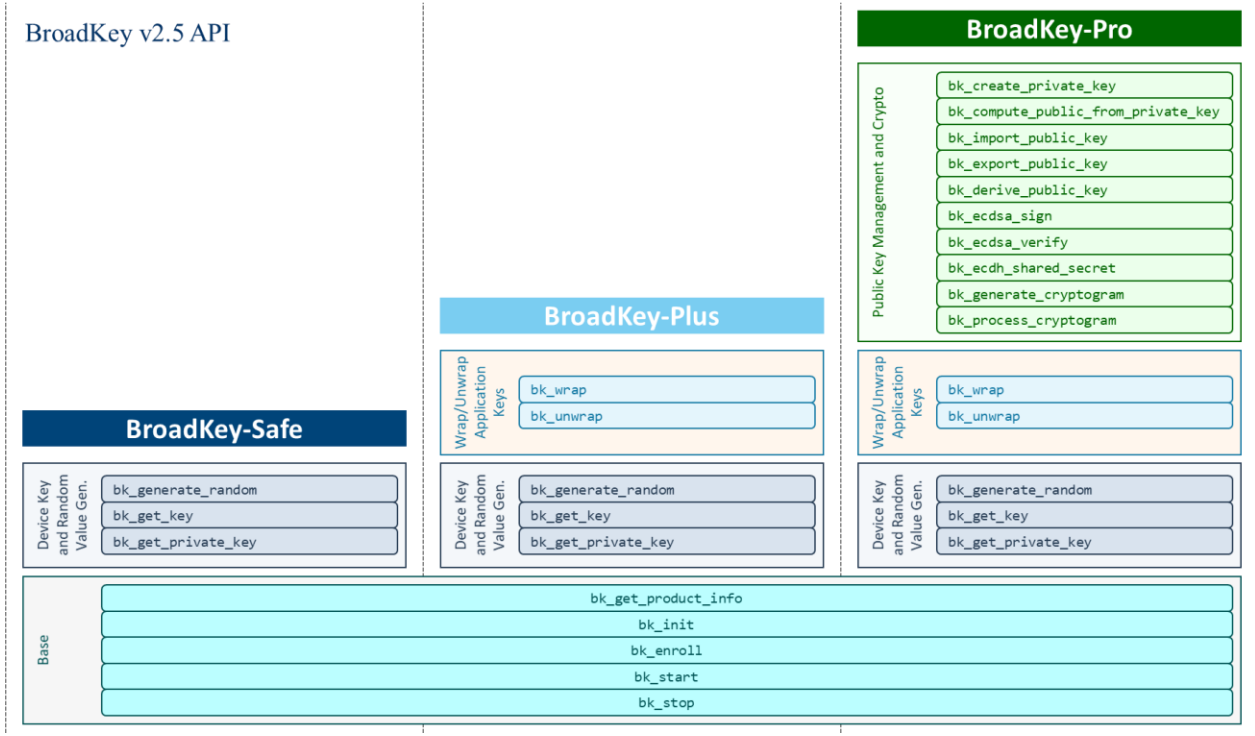
Terminal output



BroadKey Documentation

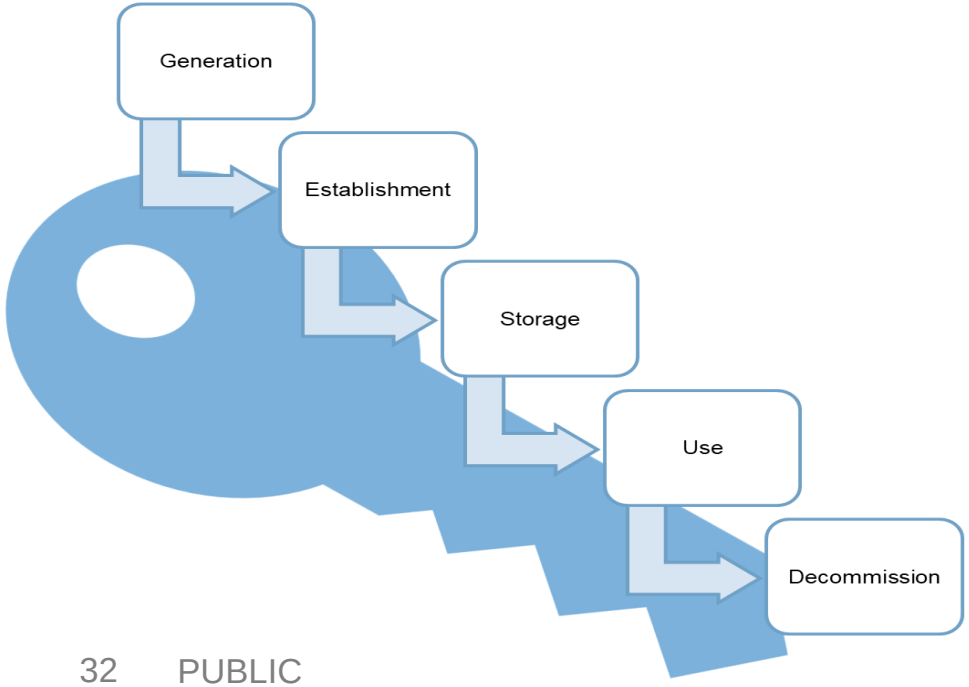
- Robust and detailed documentation covering all APIs
  - Great for understanding the life stages of PUF keys
  - Includes performance benchmarking for Arm Cortex-M devices
  - Must read document





BroadKey Demo Summary

- Demo utilizes External Flash Memory to store the PUF activation code and has linker file configuration aligned to BroadKey requirements
- Demo is executed from internal SRAM
- Demo provides the base functionality to see BroadKey across the key life cycle
  - BroadKey is initialized, enrolled to generate AC (if needed), then used
- Demonstration of key wrap and unwrap functions showing protected key storage
- Demo allows erasure of the AC (Activation Code) to Decommission the Cryptographic Context




```
Memory region         Used Size  Region Size  %age Used
        SRAM_DTC:       89908 B       128 KB     68.59%
        SRAM_ITC:          0 GB       128 KB      0.00%
         SRAM_OC:          0 GB       128 KB      0.00%
        SRAM_PUF:          1 KB         1 KB    100.00%
        SRAM_OC2:          0 GB       127 KB      0.00%
    BOARD_SDRAM:          0 GB        32 MB      0.00%
Finished building target: evkbimxrt1050_broadkey_demo.axf
```

BroadKey Demo (API Example Only)

- Currently the demo resides in SRAM, but the predominant use case for i.MX RT series is Execute in Place (XiP)
  - Performing XiP and writing an Activation Code (AC) to the external flash needs special care at the application level
  - Intrinsic ID has 2 versions of Broadkey, one for provisioning and one for OEM application use
- Currently the demo completely shows the BroadKey API
  - Application cases such as OTA and Cloud connection to AWS IoT/Google/MS Azure core are future work
- i.MX RT security features add security protections to the system using BroadKey
  - Secure Boot, Encrypted Boot, and encrypted XIP ensure the integrity and confidentiality of Broadkey
  - Hardware firewalls could establish trusted execution of BroadKey

CONCLUSION

Why Intrinsic ID BroadKey?

- Breakthrough technology aligned to IoT Security Strategies for scalability and ease of use
  - Protection of keys throughout the key lifecycle
  - APIs to support a broad range of uses
- Alignment to strategic needs when addressing IoT
  - Portable to many MCU/MPU types
  - Scalable key strength and functionality
  - Easy to deploy and use

BroadKey Configurations	Safe	Plus	Pro
Security Strength (bits)	128/256	128/256	128/256
PUF (KB) related to Security Strength	0.7/1	0.7/1	0.7/1
Code Size (KB)	8	10	21
Generate Device Keys and Random Values	Y	Y	Y
Wrap and Unwrap Application Keys		Y	Y
Public Key Management and Crypto Operations			Y

Why NXP i.MX RT Series?

High Performance
Real-Time Processing

- Cortex-M7 up to 600MHz (50% faster than current existing M7 products)
- 20ns interrupt latency
- Up to 1MB Tightly Couple Memory

High level of Integration

- High Security enabled by AES-128, HAB and On-the-fly QSPI Flash Decryption
- 2D graphics acceleration engine
- Parallel camera sensor interface
- LCD display controller up to WXGA (1366x768)
- Audio interface with three I2S for multichannel high performance audio

Low BOM Cost

- Competitive pricing starting @ $1.48 10k RSL
- Fully integrated PMIC with DC-DC
- Low cost package, 10x10 BGA, enabling 4 Layer PCB design
- SDRAM interface

Easy to Use

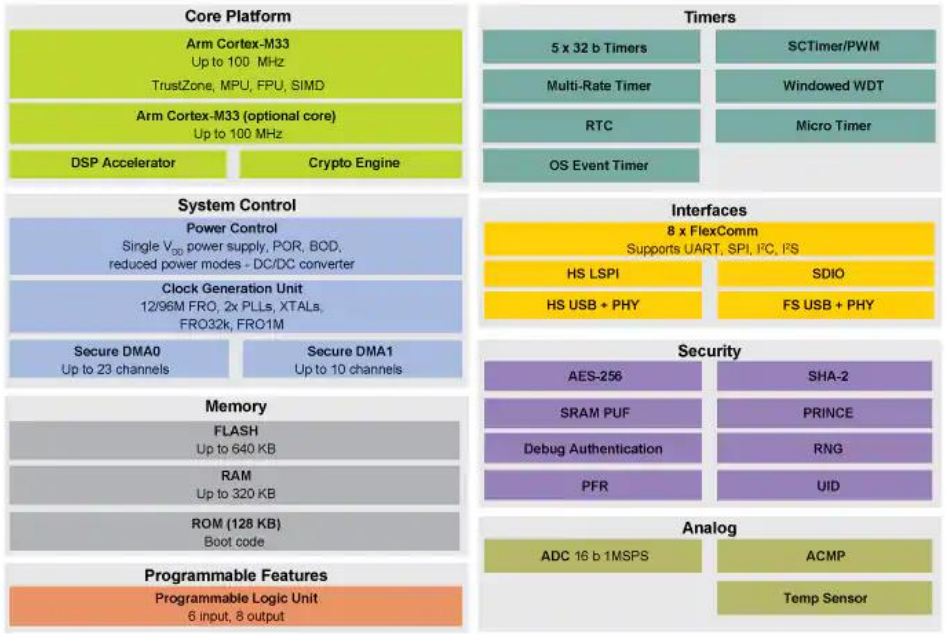
- MCU customers can leveraging their current toolchain (MCUXpresso, IAR, Keil)
- Rapid and easy prototyping and development with NXP FreeRTOS, SDK, ARM mbed and the global ARM ecosystem
- Single voltage input simplifies power circuit design
- Scalability to Kinetis & i.MX products

ECDSA P256 Sign and Verify Times on i.MX RT

- For 256 bit curve strength ECDSA sign and verify complete in less than 4 million CPU cycles
  - For 600MHz CPU clock that results in sign and verify times <7milliseconds

HW Protected Keys Example 4: Hardware PUF

- Recently launched LPC5500 family also makes use of Intrinsic ID SRAM PUF technology in the design of the microcontroller in addition to other security capabilities



This webinar meets 3 times.

Tue, Apr 16, 2019 10:00 AM - 11:00 AM CDT
Tue, May 21, 2019 10:00 AM - 11:00 AM CDT
Tue, Jun 18, 2019 10:00 AM - 11:00 AM CDT

Show in My Time Zone

Part 1: Utilizing hardware protected keys on broad market Microcontrollers

For the IoT Edge device, the cryptographic keys used to perform the services such as encrypted boot, onboarding, and over the air updates are critical components that must be protected. Chip level hardware protected keys are the standard for achieving strong security protection for embedded designs. This session will define what a hardware protected key is and show several examples of how these keys are realized on NXP processors. The i.MX RT 1050 family of devices will be used as a real world example of how Intrinsic ID Broadkey® SRAM based PUF can advance your IoT Security.

Part 2: Using hardware protected keys on state of the art Microcontrollers

For the latest microcontrollers addressing IoT applications, hardware protected keys address critical security functions to protect application integrity, software confidentiality and encrypt data at rest. This session will explore the ability of the recently launched NXP IoT microcontroller, LPC5500 series. This family of devices will work as the main processing unit for a broad range of IoT applications and integrates breakthrough capabilities with regards to security. Along with Arm TrustZone technology the SRAM PUF based key management makes security easy to use and easy to deploy.

Part 3: Advanced IoT application key management based on hardware protected keys

The recently launched NXP IoT microcontroller, LPC5500 series, works as the main processing unit for a broad range of IoT applications. Along with Arm TrustZone® technology the chip supports SRAM PUF based key management. The product includes a software development kit (MCUXpresso SDK) that contains prebuilt applications to demonstrate edge to cloud connections out of the box. With the integrated security technology and software enablement, the LPC5500 makes security easy to use and easy to deploy. Join this session for a quick run through the demo applications available to kickstart your next IoT designs.Less

Conclusions

- In today's threat landscape, all IoT devices must address security
- Cryptography is a common component in securing IoT Designs
- NXP device options exist to protect the cryptographic keys for embedded designs
- Intrinsic ID BroadKey on the i.MX RT working together combine to create a solution aligned to the need for addressing lifecycle, scalability and ease of use

Thanks!

Conclusions

- In today's threat landscape, all IoT devices must address security
- Cryptography is a common component in securing IoT Designs
- NXP device options exist to protect the cryptographic keys for embedded designs
- Intrinsic ID BroadKey on the i.MX RT working together combine to create a solution aligned to the need for addressing lifecycle, scalability and ease of use

Questions & Answers Session

SECURE CONNECTIONS
FOR A SMARTER WORLD