NXP與IAR建構的微處理器安全防護解決方案

AUGUST, 2021

SECURE CONNECTIONS
FOR A SMARTER WORLD

AGENDA

- IoT市場的安全趨勢與NXP微處理器簡介
  IoT security market trend and NXP MCU introduction

- 恩智浦微處理器的安全架構與功能
  NXP MCU security architecture and functions

- IAR Systems 安全解決方案搭配 NXP MCU，實現最佳IP 保護
  Maximize your IP protection with IAR Security Solution & NXP's MCU

IoT市場的安全趨勢與NXP 微處理器簡介

IoT security market trend and NXP MCU introduction

JAMES HUANG

SR REGIONAL MARKETING MANAGER, BL EP GC

SECURE CONNECTIONS
FOR A SMARTER WORLD

AIOT TREND FOR EDGE COMPUTING

Smart Nodes
NXP I.MX Family
(Machine-learning)

Smart-nodes can run targeted Edge applications

Data Nodes
NXP LPC/Kinetis/
JN/QN/K32W
Families

Customer Solution

AWS App	Azure App	Aliyun App

NXP SW Platform

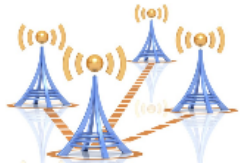
- Application Framework
- Linux Platform
- Secure Firmware

Edge Gateway
NXP Layerscape, i.MX
(Control, Analytics, Machine-Learning)

Gateways are a natural host for Edge computing.

Edge computing is the application of cloud technology outside a large data center.

Network



Cloud

Google Cloud Platform

阿里云计算
Alibaba Cloud Computing

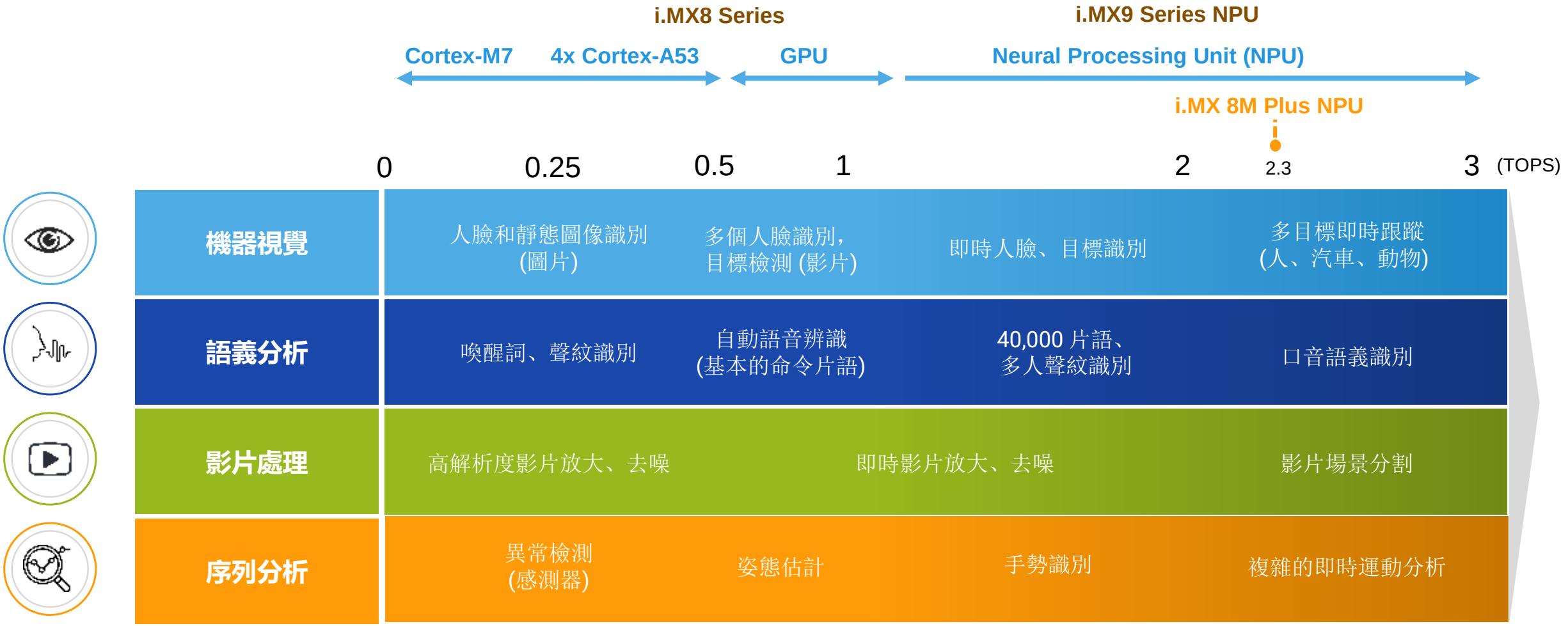
Microsoft Azure

amazon web services

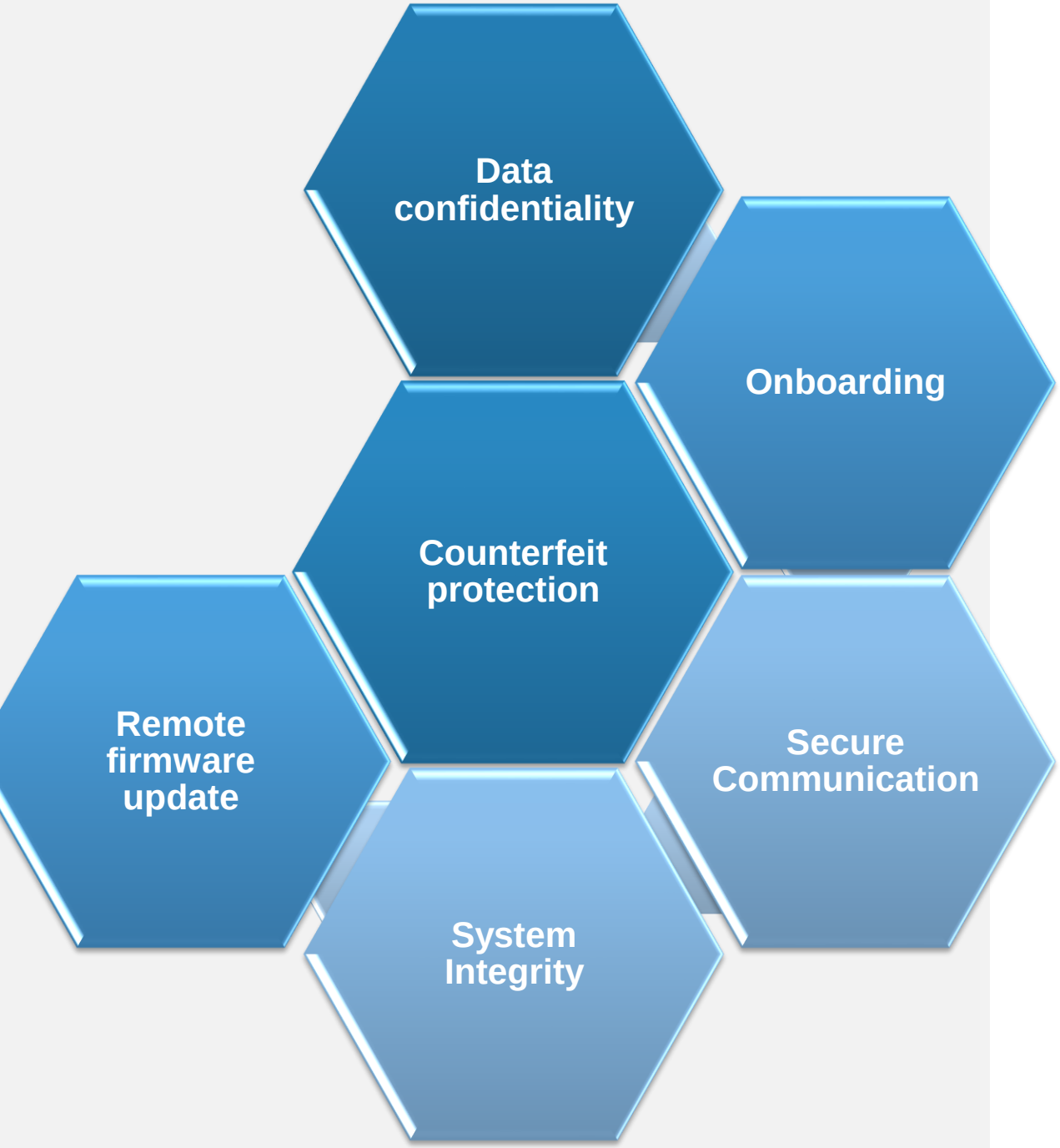
中国移动 China Mobile

Edge applications can also run on access – e.g. Base-stations, Central Office – costlier pipe, higher latency.

深度學習應用實例和AI加速器



AI/ML部分和其他模組都最終要服務於整個系統的目標應用，達到系統的最優性價比。



ESSENTIAL SECURITY GOALS

- **Counterfeit protection**
  - Every device has a unique identity that can not be reproduced by an attacker
- **Onboarding**
  - Shared credentials between the end device and the back end system
- **System integrity**
  - Trust in the functionality provided by the end device
- **Secure communication**
  - Cryptography applied to the communications for the device
- **Data confidentiality**
  - Protection of data in the device
- **Remote firmware update**
  - Safe updating of the software on the end device

OVERVIEW OF THE ARCHITECTURES

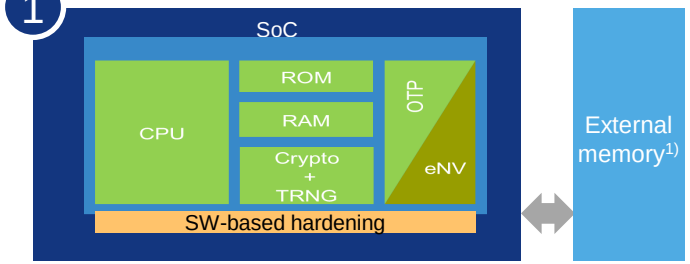
Security Architectures supported by current shipping NXP products

Add Trusted Execution based on ARM TrustZone® and/or isolation features[2] on the SoC

Add SE to architecture

Standard SoC with basic security hardening

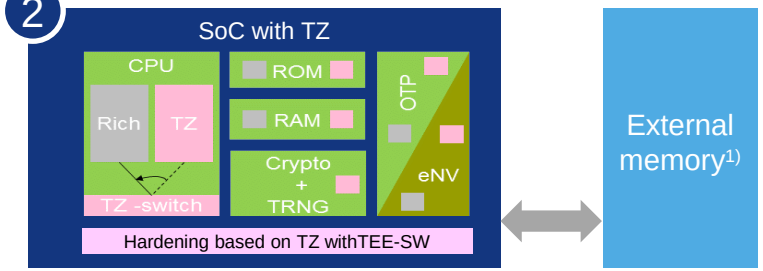
1



Allows for
- *Secure Boot*
- *Secure Debug*
- *Cryptographic Operations*
- *Tamper Detection*

SoC with basic security hardening & TrustZone

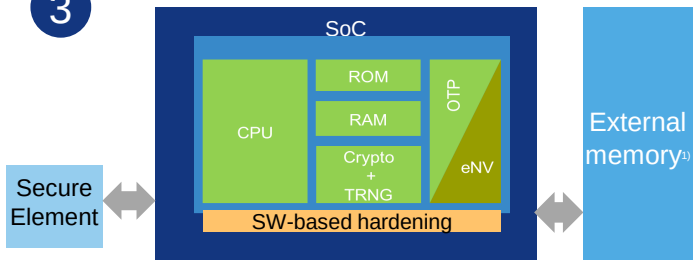
2



Additional features:
- *Secure execution environment (“Trusted”)*
- *Rich execution environment (“Non-trusted”)*

SoC with basic security hardening and a SE

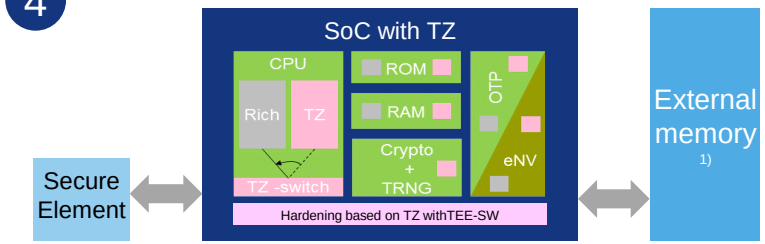
3



Additional features:
- *Tamper Resistant Protection of root keys*
- *Credentials can be securely injected in SE*
- *Provisioned keys are delivered directly to the customer through a secure channel*

SoC with basic security hardening, TZ & SE

4

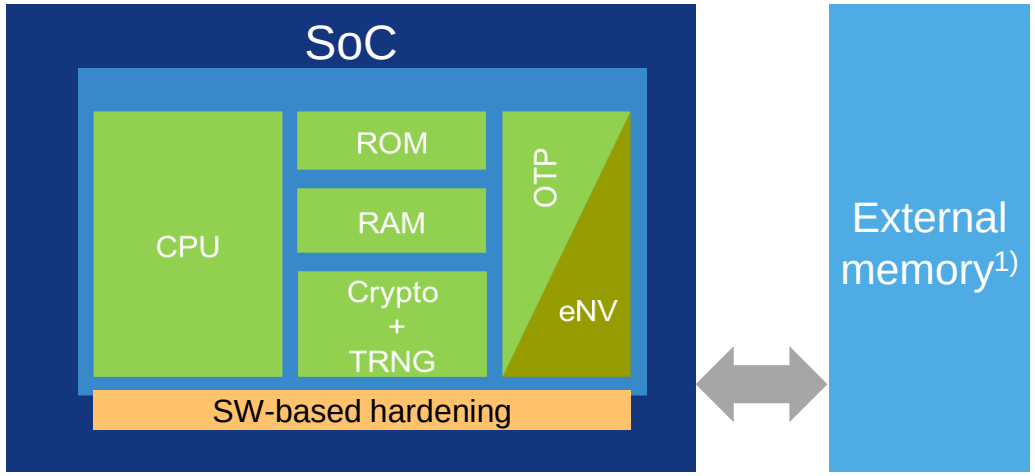


Additional features:
- *Combined features of architecture 2 and 3*

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

1. STANDARD SOC WITH BASIC SECURITY HARDENING

Standard SoC with basic security hardening



NXP products that have this architecture

Examples of products
Kinetis KL8x (M0+); K8x (M4), etc. LPC LPC54S01x (M4), i.MXRT10xx, i.MXRT11xx (M7) All i.MX (MPU)
All Layerscape & QoriQ Processor
Secure Element SE050, etc.

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

Brief description

- Architecture with basic security hardening allows for
  - Secure Boot
  - Protected/Secure Debug
  - Cryptographic Operations
  - Tamper Detection

For i.MX and Layerscape products:

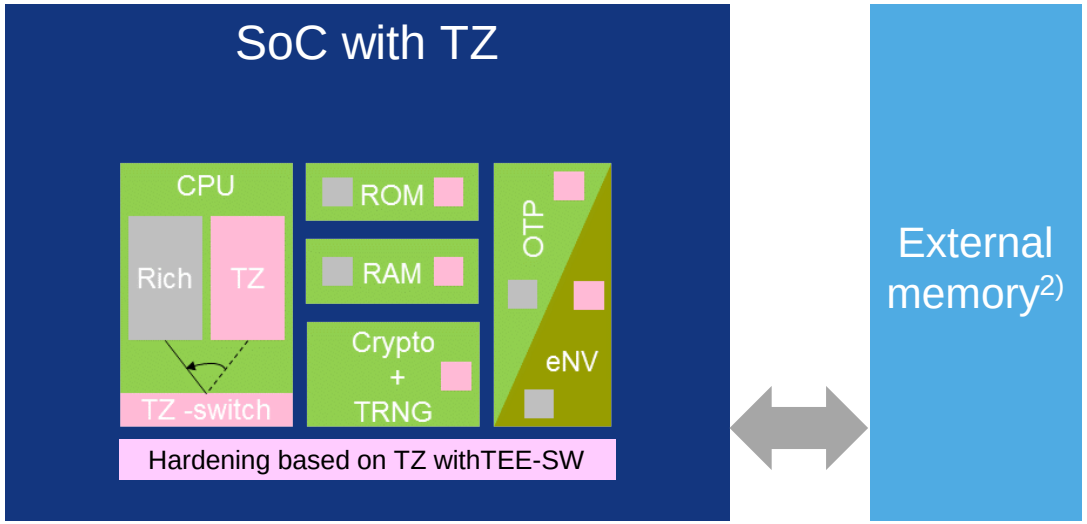
- Hash of root keys can be burned into fuses on-chip accessible only by a dedicated crypto subsystem for authentication of the boot image

Key benefits

- When comparing to an SoC without basic security, this architecture provides improved security at multiple points in the products Life Cycle

2. SOC WITH BASIC SECURITY HARDENING AND TRUSTZONE (TZ)

SoC with basic security hardening & TrustZone



NXP products that have this architecture

Examples of products
All i.MX (MPU) LPC55Sxx (M33), iMXRT600 (M33), iMXRT500 (M33)
All Layerscape processor
Secure Element SE050, etc.

Brief description of additional features introduced by ARM TrustZone

- A level of isolation within the SoC, creating
  - Trusted execution environment (“Secure world”) with full access to the system memory map
  - Rich execution environment (“Non-trusted”) with no access to security critical registers and data

Key benefits (compared to architecture 1: Basic security hardening)

+ Enhanced secure attestation
+ Enhanced secure firmware OTA updates
+ Enhanced secure logging in TZ environment
+ Better protection against roll back attacks
+ More secure communication to the backend[1)] if end point is in TrustZone
+ Industry Standards Trusted OS providing Global Platform API[3)] can be run in TrustZone

1) *Note: does not hold for denial of service, 2) not mandatory for MCUs/MPUs when they have embedded memory. 3) As it has a Protection Profile available the customer can certify the product*

EDGEVerse 全方位軟體和支援

目標市場

工業邊緣	IoT邊緣	網路邊緣

整合支援雲端平台

雲端平台範例

aws · Microsoft Azure · Alibaba Cloud · Google Cloud · Baidu 百度 · salesforce · PREDIX · IBM Cloud

軟體支援與服務

NXP eIQ™ 機器學習	音訊解決方案	密鑰注入 EdgeLock-2-Go	統包式解決方案和軟體服務	合作夥伴

邊緣智慧　　安全與配置　　裝置管理

中介軟體和應用程式碼範例

安全	連結	圖像	音訊/影音	網路

作業系統

ubuntu · yocto PROJECT · CentOS · Open Industrial Linux

MCUXpresso

Android	Common Linux Platform	Zephyr	FreeRTOS	Azure RTOS

SoC

i.MX	MPUs	Crossover	MCUs

EDGELOCK™ SECURE ENCLAVE

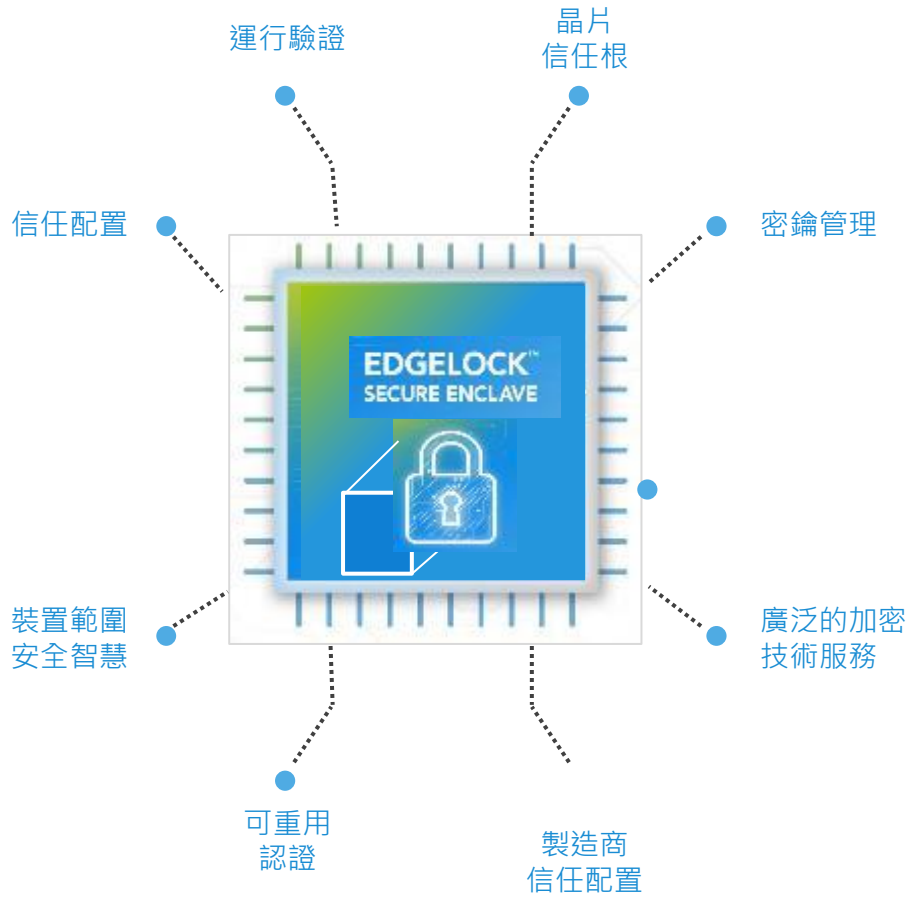
不僅是加密
更先進的內建（on-die）安全技術，透過廣泛的加密服務和更簡單的安全認證路徑增強運行驗證、晶片信任根、信任配置、細密式（fine-grained）金鑰管理

安全HQ
管理安全功能的系統——該內建堡壘監督安全功能，以保護系統免受攻擊

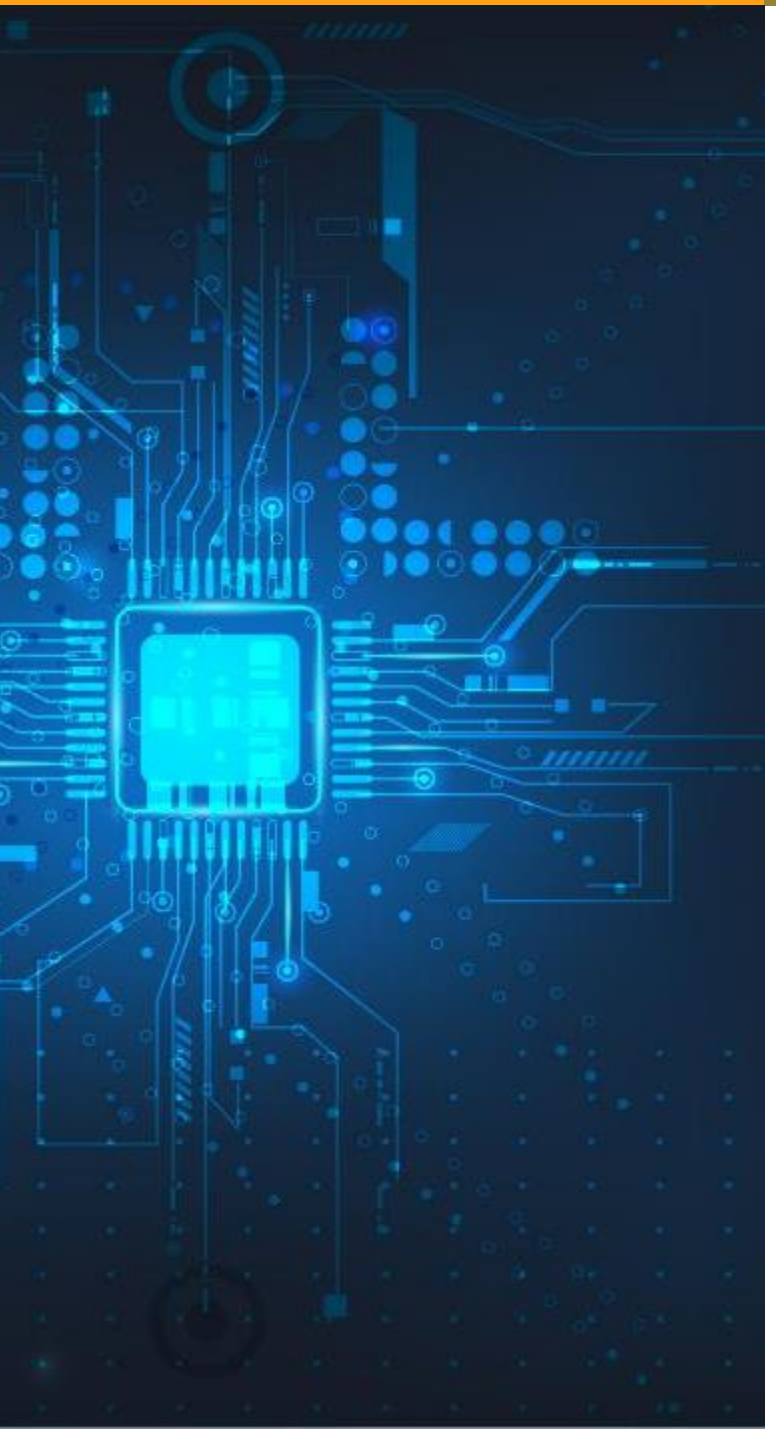
託管代理
代理將安全性擴展到晶片（分佈在中央HQ外），以建立並維持安全能力的可信度

智慧
追蹤和管理電源轉換，以防止異構多核心裝置中出現全新攻擊表面

立即可用
預先配置的安全性原則可降低複雜性，並有助於避免代價高昂的錯誤，進而加快產品上市

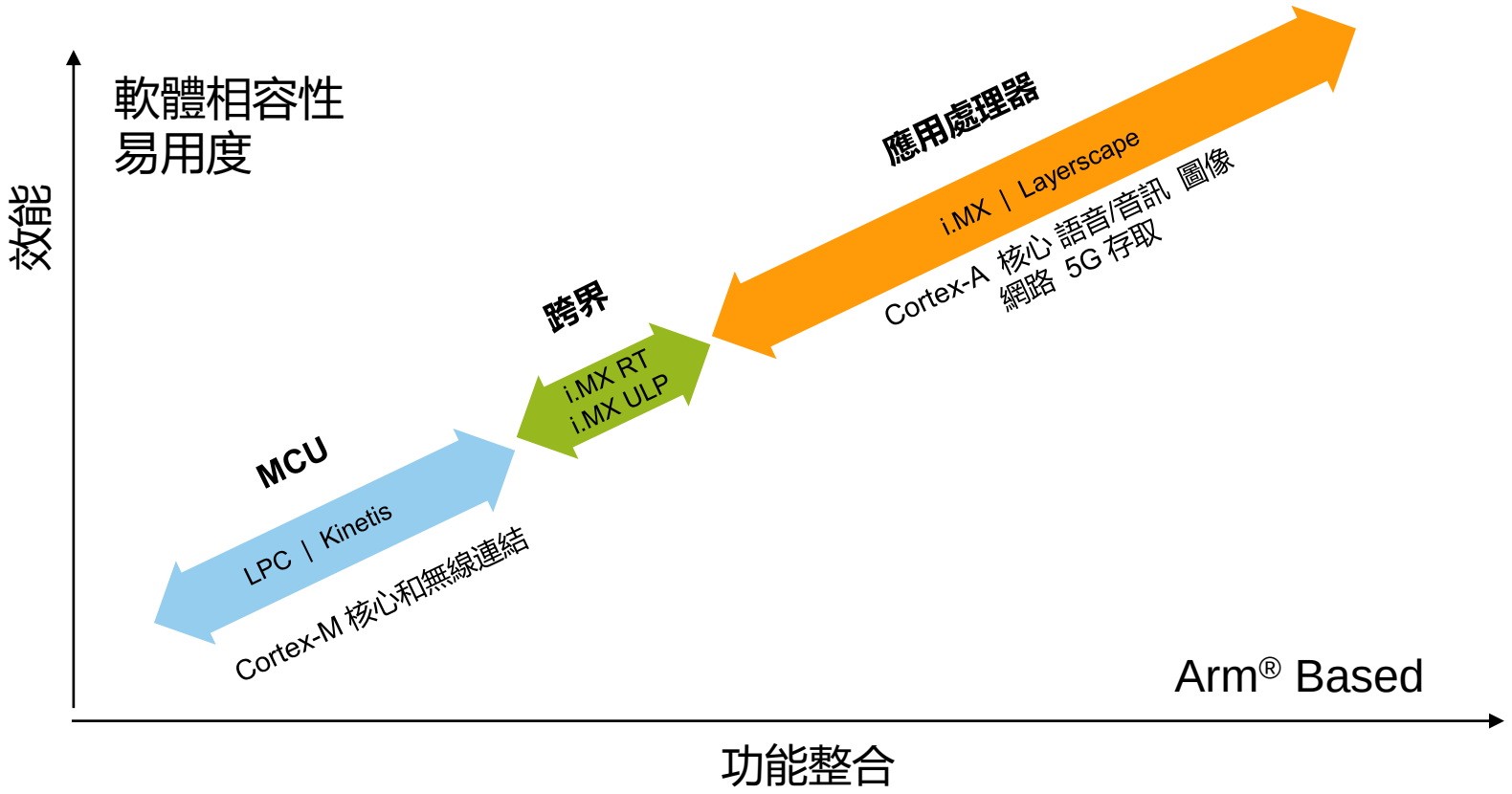


nxp.com/SecureEnclave

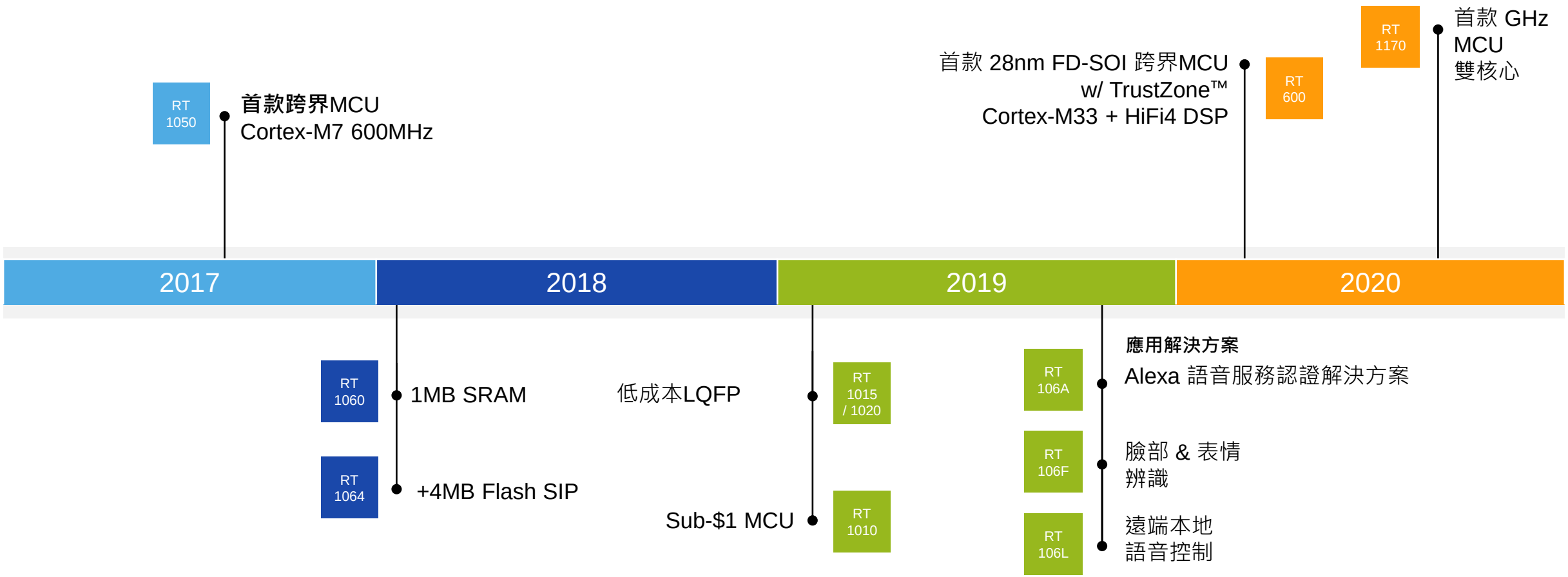


EDGEVerse

可擴展的邊緣處理平台

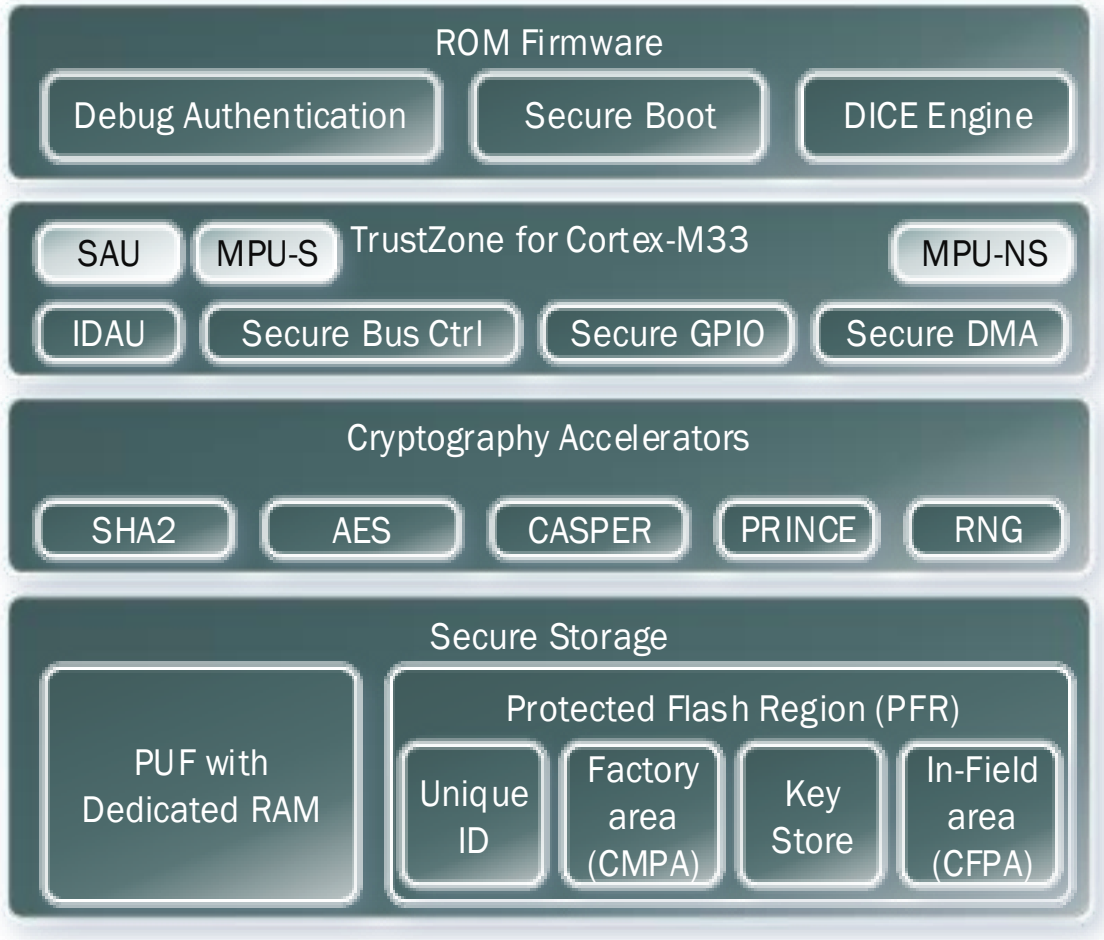


I.MX RT 跨界處理器持續創造新高度



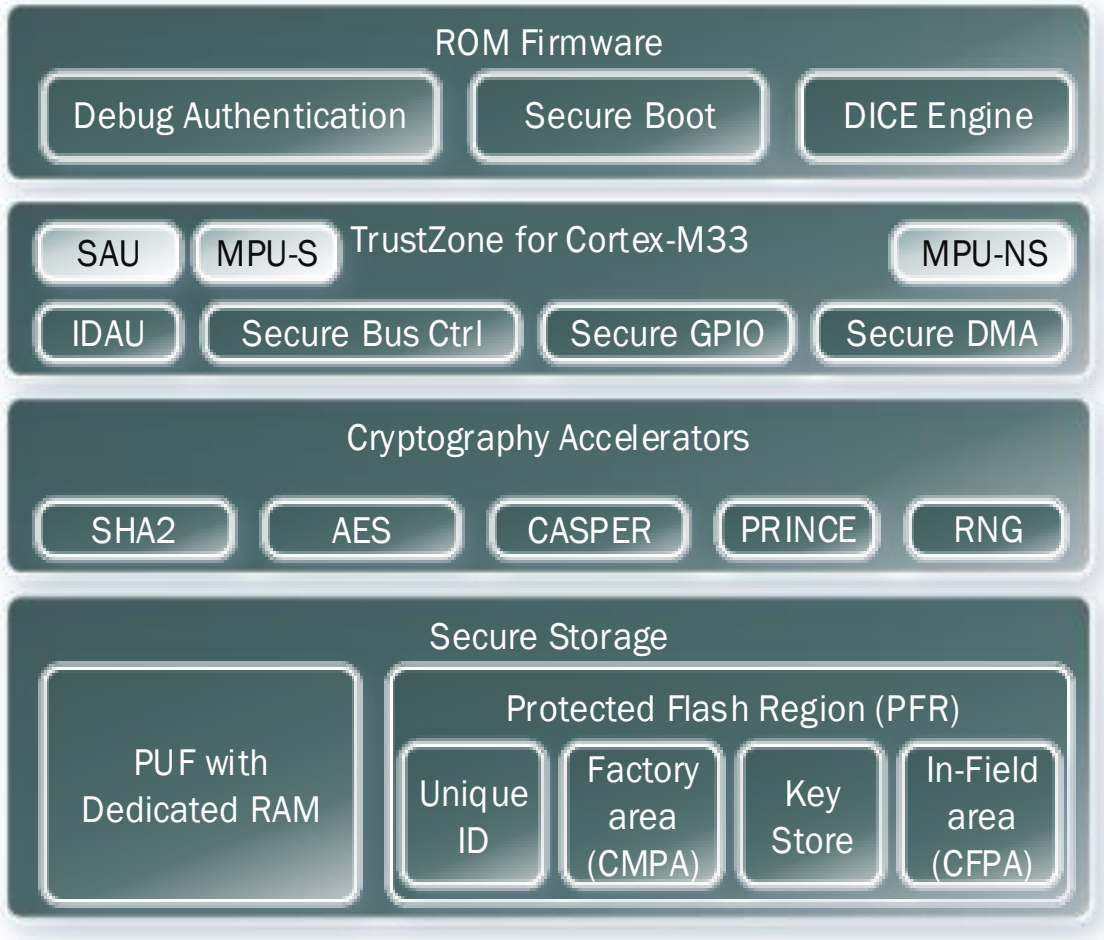
LPC55SXX SECURITY SUB-SYSTEM

- ROM supporting
  - Secure Boot
  - Debug Authentication
  - DICE Engine
- TrustZone for Cortex-M33
  - Security Attribution Unit (SAU)
  - Memory Protection Unit (MPU): Secure & Non-Secure
  - NXP IP
    - Defined Attribution Unit (using IDAU interface)
    - Secure Bus Control
    - Secure GPIO Controller
    - Secure DMA Controller
- Cryptography Accelerators
  - HashCrypt engine: AES and SHA
  - PRINCE on-the-fly flash encryption/decryption engine
  - CASPER: Asymmetric cryptography accelerator
  - Random Number Generator (RNG)



LPC55SXX SECURITY SUB-SYSTEM (CONTD…)

- Secure Storage
  - Physically Unclonable Function (PUF)
    - Device unique root key (256 bit strength)
    - Can store key sizes 64 bit to 4096 bit
  - Protected Flash Region
    - RFC4122 compliant 128-bit UUID per device
    - PUF Key Store
      - Activation code, Prince region key codes, FW update key encryption key, Unique Device Secret
    - Customer Factory Programable Area
      - Boot Configuration, RoT key table hash, Debug configuration, Prince configuration
    - Customer In-Field Programable Area
      - Monotonic counter, Prince IV codes



SECURE CONNECTIONS
FOR A SMARTER WORLD