Trusted Platforms for Cyber Physical Systems

Ravi Malhotra

Strategic Marketing Manager

September 2019 | Session #AMF-SOL-T3813

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

Agenda

- What are Cyber Physical Systems?
- Securing the Complete Lifecycle
- NXP Embedded Security Technology
- Key HW Roots of Trust Explained
- Leveraging NXP HW Root of Trust
- EdgeScale – Simplify Life-cycle Mgmt

1990s – 2016: An Era of Security/Trust Breaches

As computer systems have grown more capable, complex...so have the **attacks**!

9 CERTIFICATES

Stolen across 7 different domains

COMODO Certification Authority Hack

COMODO SSL CERTIFICATE

Google YAHOO! skype Microsoft

4 MILLION

Employee federal records hacked

Department of Defense Hack

77 MILLION

Compromised accounts

Playstation Network Outage

PLAYSTATION® Network

45.7 MILLION

Credit cards stolen

TJX Hack – Albert Gonzalez

TJX THE TJX COMPANIES, INC.

900,000

Deutsche Telekom customers affected in Germany

2,400

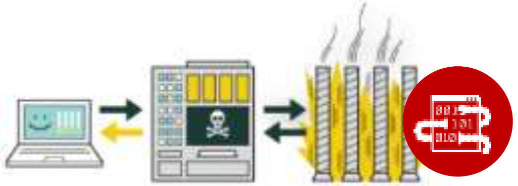
TalkTalk routers affected in the UK

Operation Shady Rat

85%

Share of infected computers – Iran, Indonesia, India

Stuxnet Worm (Targeting Industrial Systems)



71+ ORGANIZATIONS HIT

Defense contractors, United Nations, The Olympic Committee

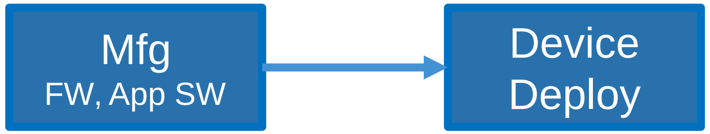
Mirai Botnet Malware

IoT Introduces Cyber Physical Systems

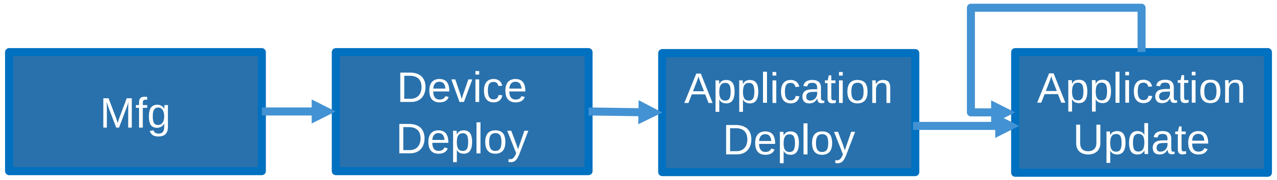
IoT manufacturers focused on **FUNCTIONALITY, EASE-OF-USE OVER SECURITY**

Device Lifecycle Management

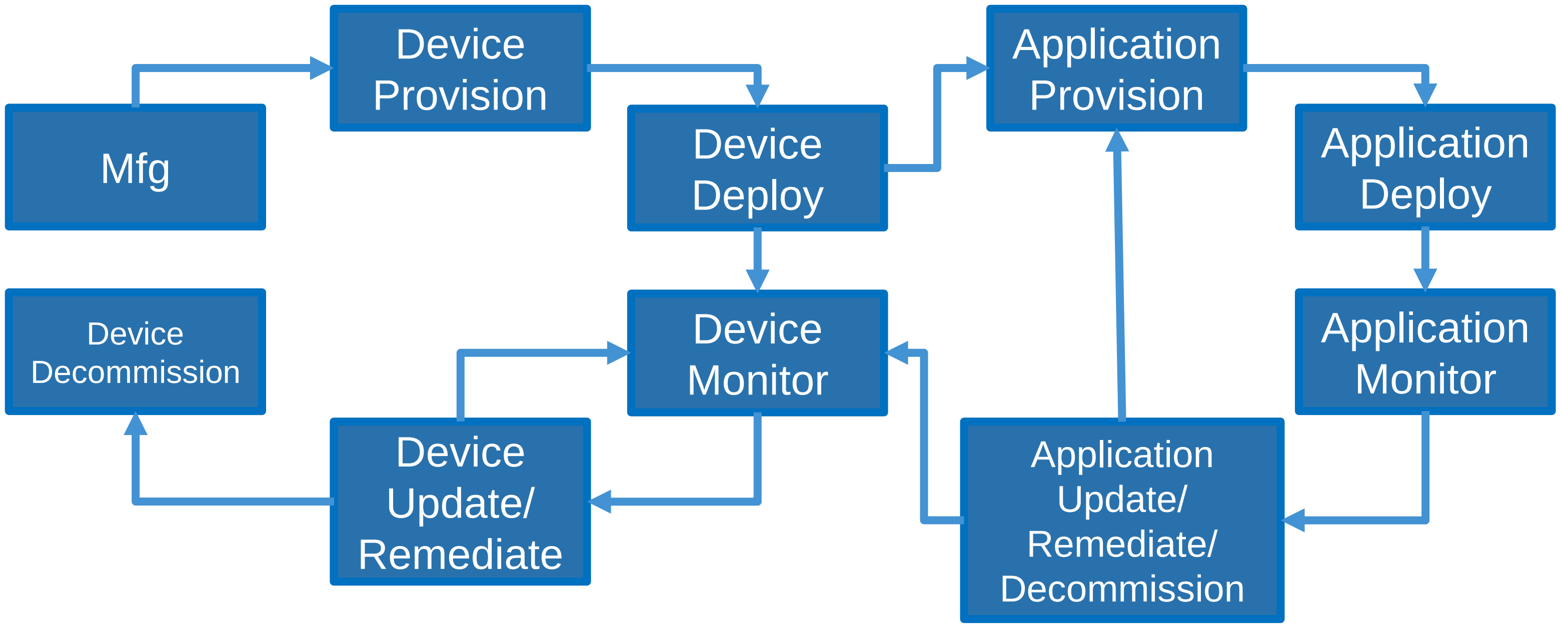
Effectively unmanaged



Minimally managed



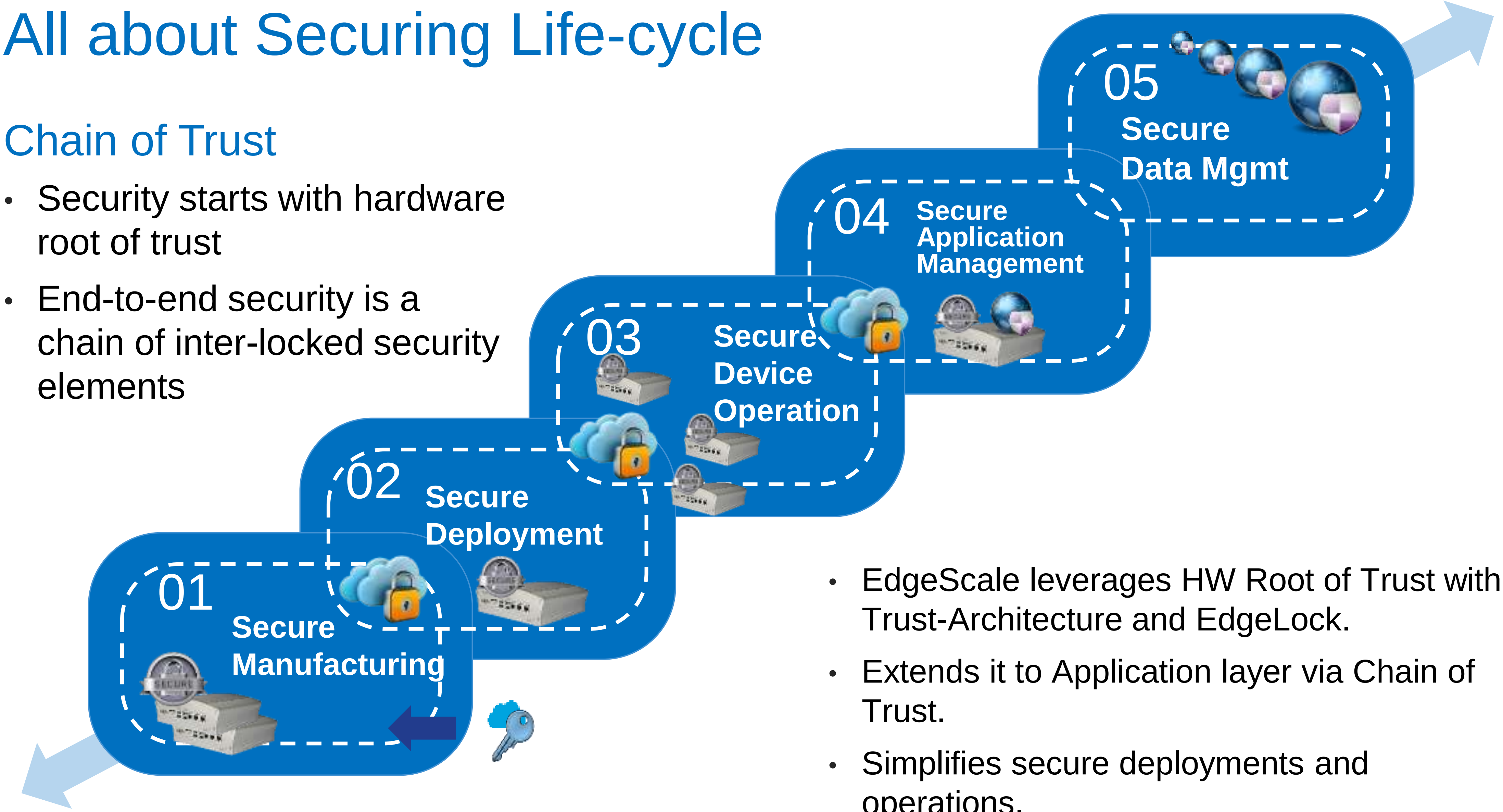
Properly managed



All about Securing Life-cycle

Chain of Trust

- Security starts with hardware root of trust
- End-to-end security is a chain of inter-locked security elements



- EdgeScale leverages HW Root of Trust with Trust-Architecture and EdgeLock.
- Extends it to Application layer via Chain of Trust.
- Simplifies secure deployments and operations.

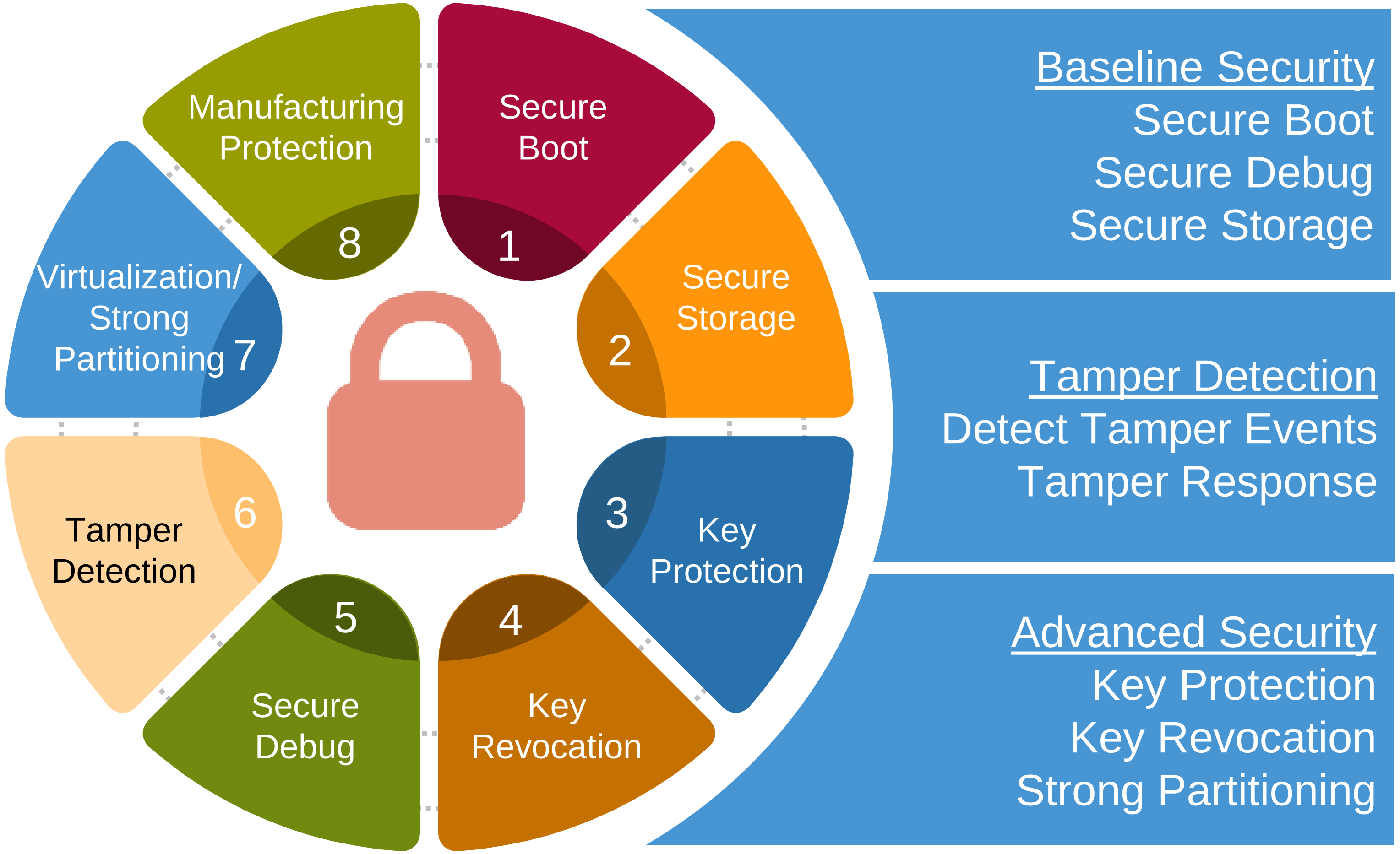
NXP Has a Core Competence in End-to-End System Security

Mobile and stationary machines want full access to cloud-based knowledge

This requires faster, more reliable and secure connectivity

NXP is at the forefront of secure communications and tamper resistance

Leadership experience in security markets: over 10 Billion smart cards sold



Baseline Security
Secure Boot
Secure Debug
Secure Storage

Tamper Detection
Detect Tamper Events
Tamper Response

Advanced Security
Key Protection
Key Revocation
Strong Partitioning

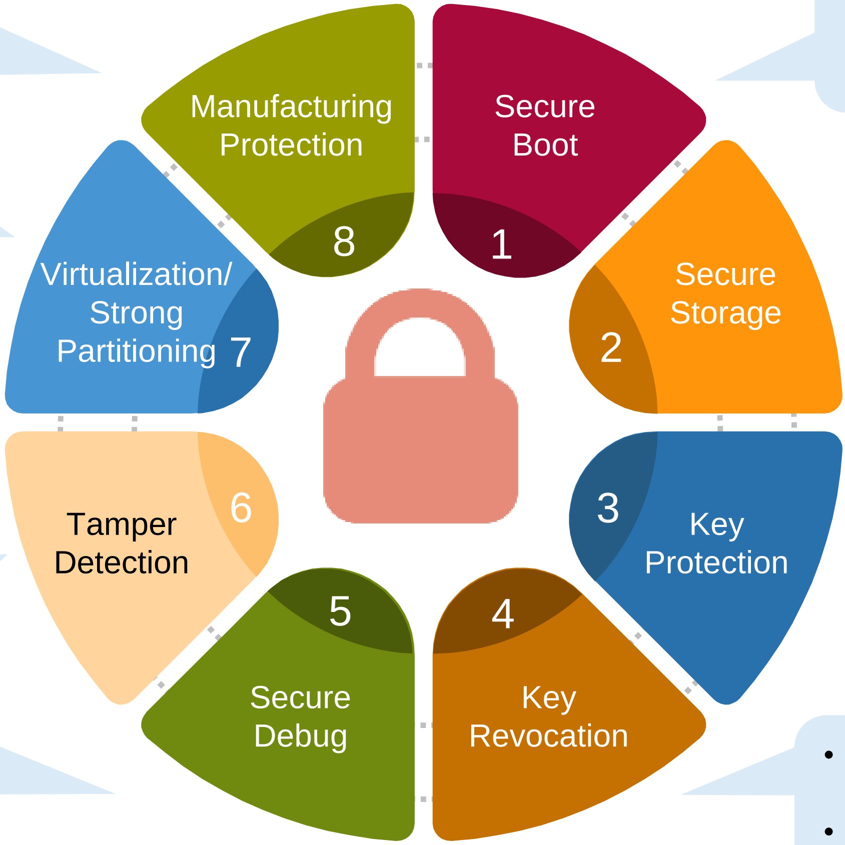
Rich Set of Platform Trust Capabilities

- Generate device/ OEM-specific public/private key-pair
- Use to sign, validate record of fuse configuration and establish identity

- Isolate and assign memory and IO blocks to different applications/VMs
- Prevent tampering of system by malicious applications

- Detect Physical tampering of the device or memory contents
- Lock-down system or zero-ize secrets

- Allow debug-ports to be locked down in field
- Secure access to debug via challenge/response



- Internal BootROM + Fuses validate Trusted Firmware
- Build Chain of Trust from TF-A to OS to Applications

- Internally generate device-specific AES keys
- Use SEC engine to encrypt/decrypt sensitive data, keys, certificates

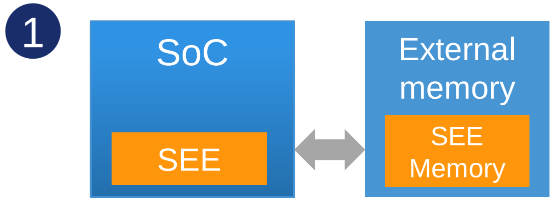
- Internally generate, encrypt and use keys within SEC engine
- Prevent memory-based attacks from stealing TLS/IPsec keys

- Lock-out up to 7 keys used to validate Trusted Firmware and OS.
- Prevent older, vulnerable versions of firmware from running.

Trusted Platform Architectures

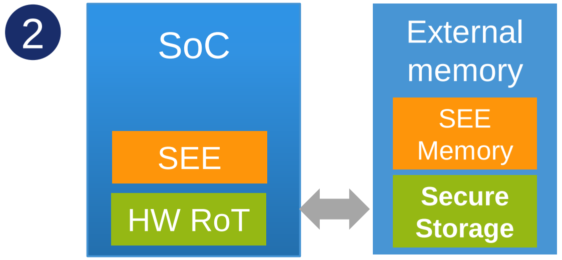
More Hardened

SoC with TrustZone but no HWRoT:
i.e. Raspberry Pi



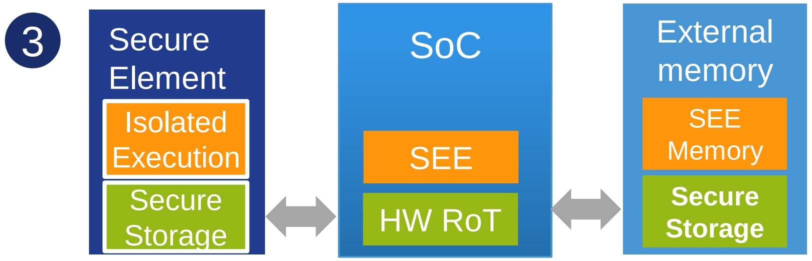
SoC with Separated Execution Environment (SEE)

SoC with TrustZone + Trust-Arch:
i.e. Layerscape, i.MX



SoC with SEE, HW Root of Trust (RoT), HW Root Keys

SoC with TrustZone + Trust-Arch + Secure Element:
i.e. Layerscape, i.MX + Secure Element

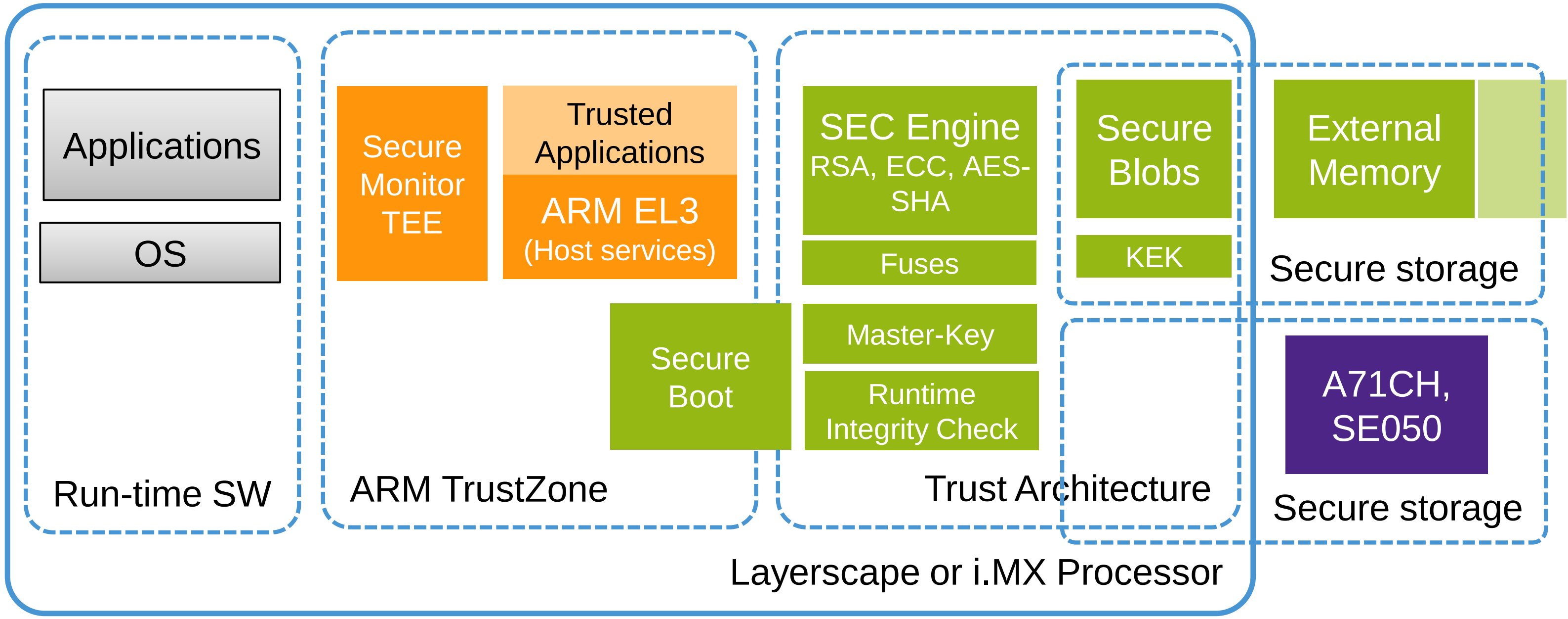


SoC with SEE, HW RoT, HW Root Keys, and Physically Isolated Execution Environment, Storage

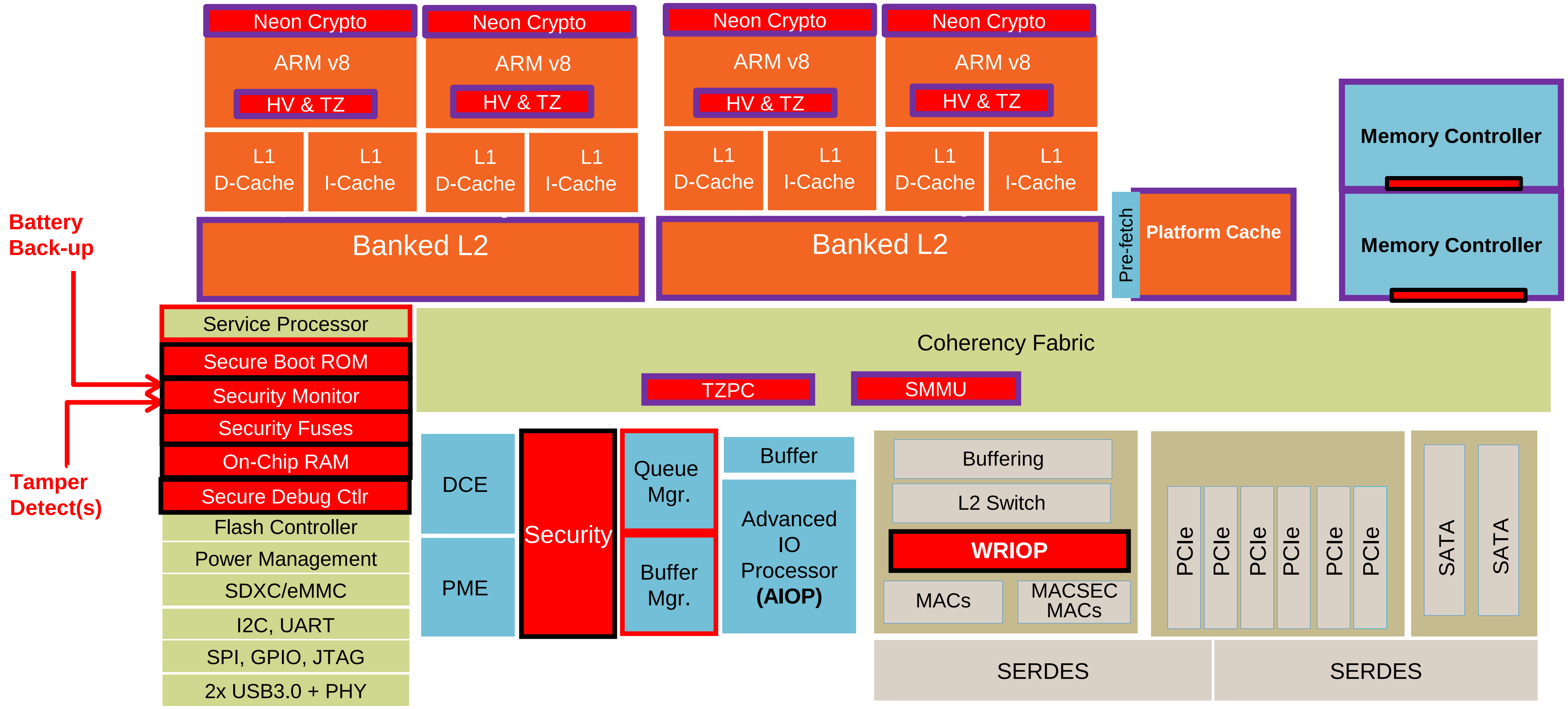
Layerscape, i.MX + SE = Level 3 Hardening

- Layerscape, i.MX have Trust Architecture
  - HW Crypto engine
  - HW encryption of off-chip storage
  - HW Key generation, master-key
  - HW Tamper detection
  - ARM TrustZone for secure host services
  - **Secure boot cannot bypass Trust Arch.**
- Combination of
  - Trust-Architecture (HW RoT)
  - Trust-Zone (SEE→ TEE)
  - Secure Element (Secure storage)

  = Level 3 hardened system



Layerscape Trust Architecture 3.0



🟥 Layerscape Trust Arch Dedicated IP

□ Layerscape Datapath IP with Trust Arch extensions

🟥 TrustZone IP

QorIQ Trust Arch (Trust 3.0): Persistent Storage Security Fuse Processor & Battery Backed Storage

Secret – not readable once written

NXP Section

1b - Factory Section Write Protect
1b - Clear_SFF (disable Scan)
1b - Deploy
1b - Retest
64b - Factory Unique ID
96b - Factory Scratchpad
256b – Factory Secure Mfg Key Split

Battery Backed SecMon Registers

256b – Zeroizable Master Key
128b - Scratchpad 0-3 (configurably zeroized)
48b – Monotonic Counter

OEM Section

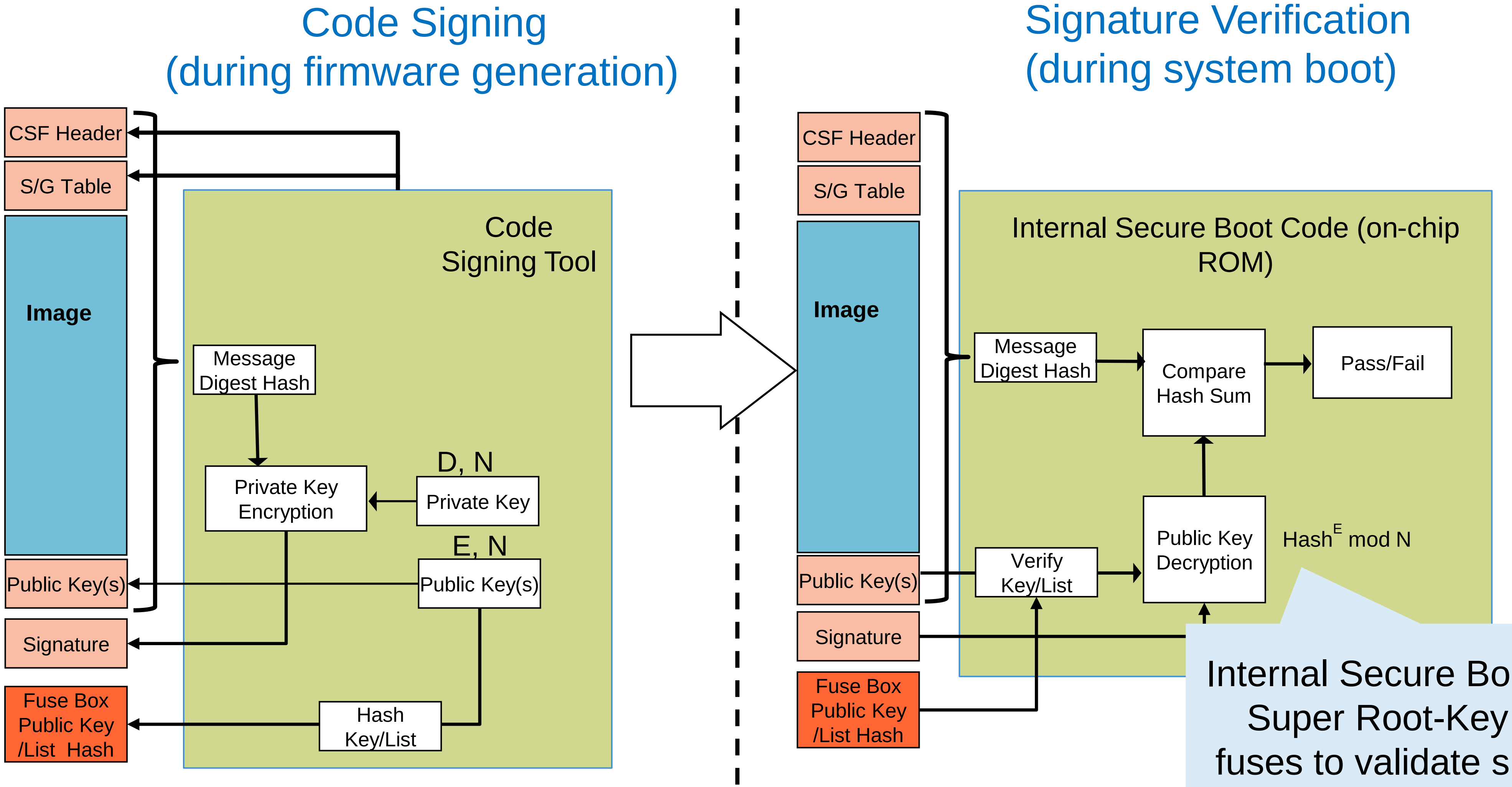
1b - OEM Section Write Protect
1b - Intent to Secure
1b - SEC disable
7b - Key Revocation
16b - 16 ‘era’ bits for BB monotonic counter
2b - Field Return
3b - Debug mode
256b – Super Root Key (List) Hash
64b - Debug Challenge Value
64b - Debug Response Value
256b - One Time Programmable Master Key
32b - OEM Unique ID
128b - OEM Scratchpad

Fuses hold configuration that

- Establish device identity
- Provide credentials for secure operations like secure-boot, storage etc.
- Determine system security state and policy

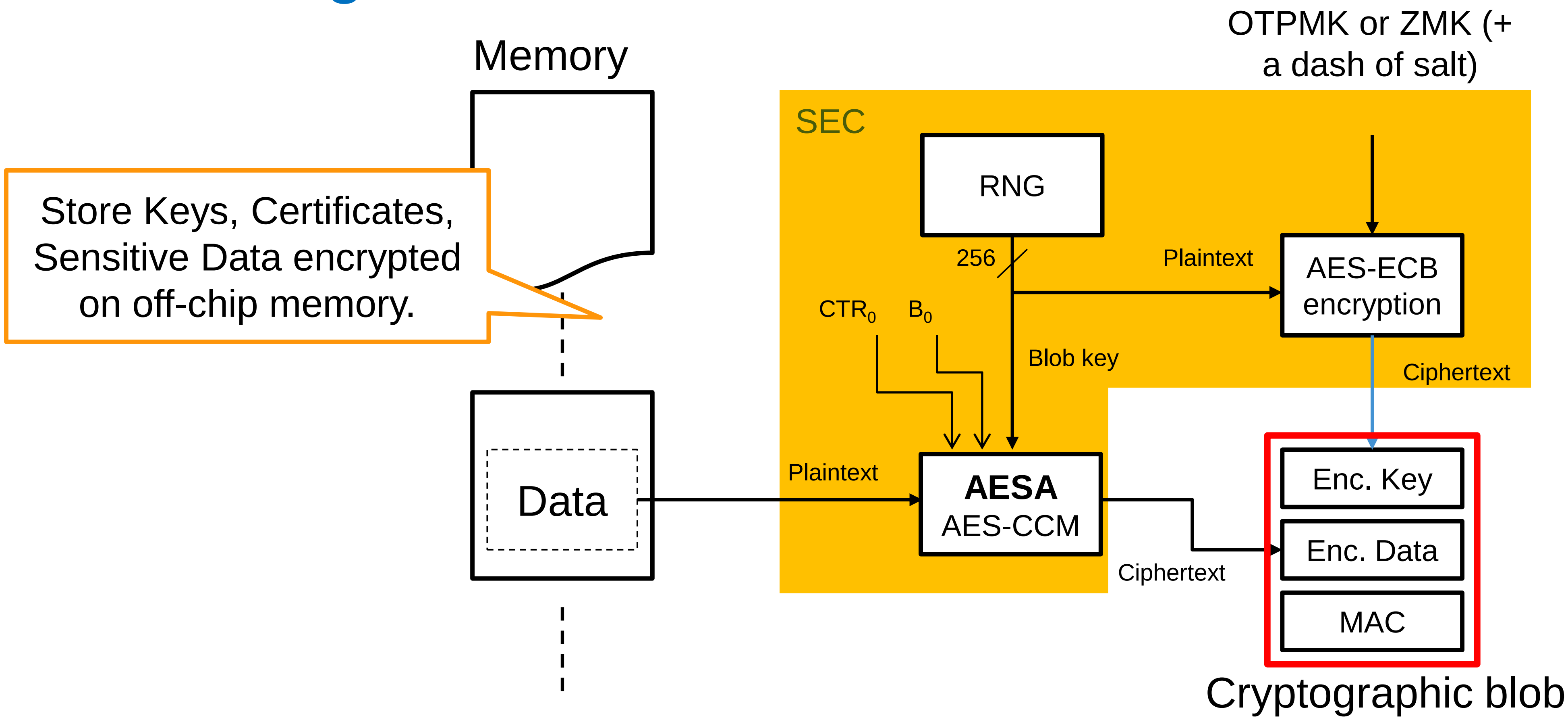
Fuses can be programmed during device/system manufacturing stage.

Secure Boot: Verifying Code Before Execution



Internal Secure BootROM reads Super Root-Key Hash from fuses to validate signed image.

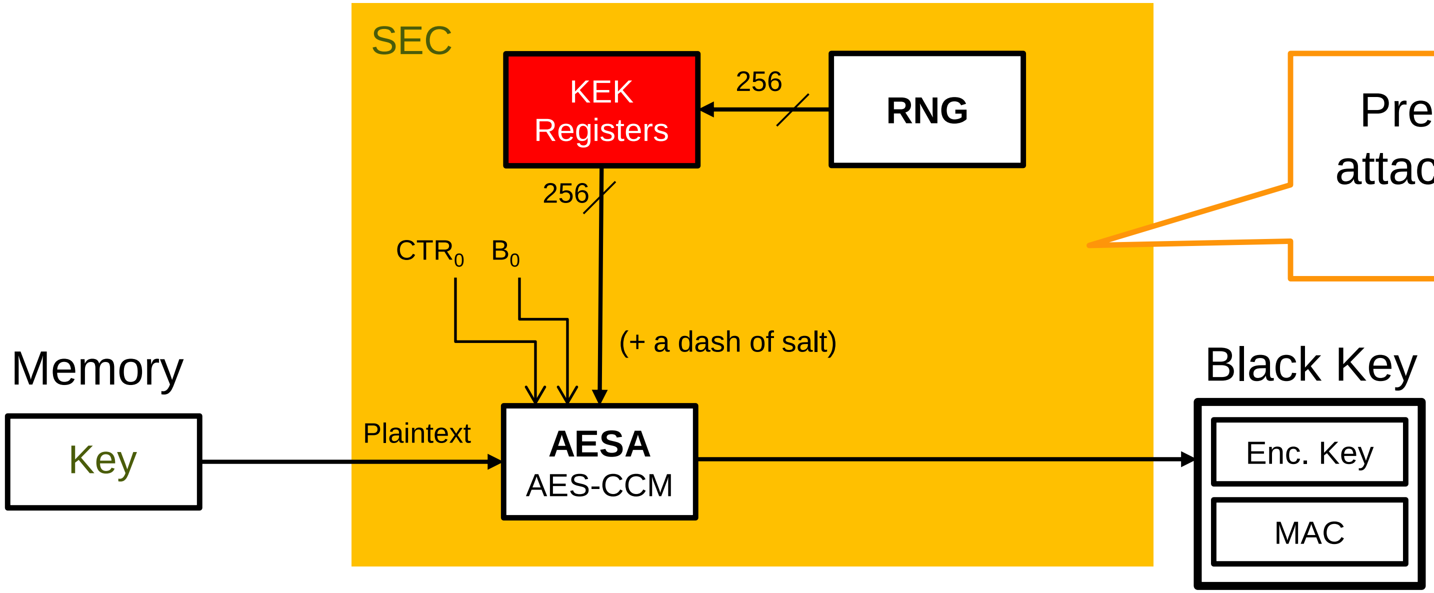
Secure Storage with Blobs



Store Keys, Certificates, Sensitive Data encrypted on off-chip memory.

- Following successful secure boot, the SEC can be commanded to create blobs or decrypt them.
- There are data blobs (user specified input/output pointers) and key blobs.
- Key blobs encrypt the contents of a key register or decrypt the blob into a key register.

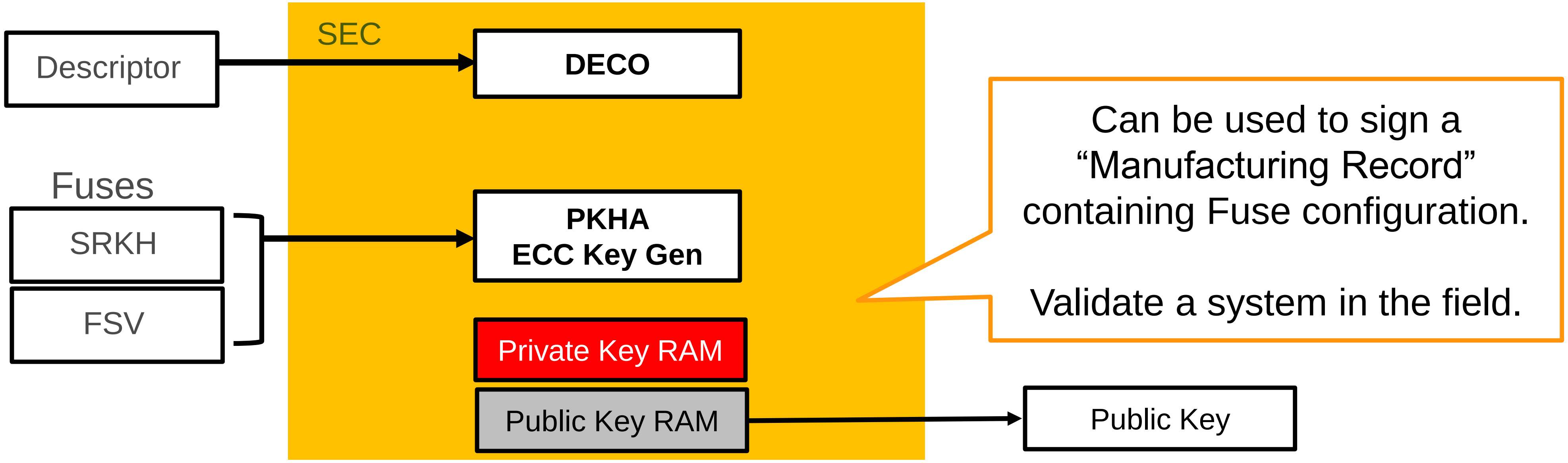
Key Protection



Prevent memory-based attacks from stealing your SSL/TLS keys

- Following successful secure boot, the SEC can be commanded to provision a Key Encryption Key (KEK).
- The KEK registers are loaded from the RNG.
- Once a KEK is provisioned, SEC descriptors can load a plaintext key and store an encrypted black key. Descriptors can also decrypt a key blob and re-encrypt as a black key. This allows provisioned keys to be moved from NVRAM to DDR.
- Black keys can be used by descriptors for normal operations, like Ipsec,. Black keys are always decrypted into SEC key registers, within a minimal performance impact.

Manufacturing Protection



Can be used to sign a "Manufacturing Record" containing Fuse configuration.

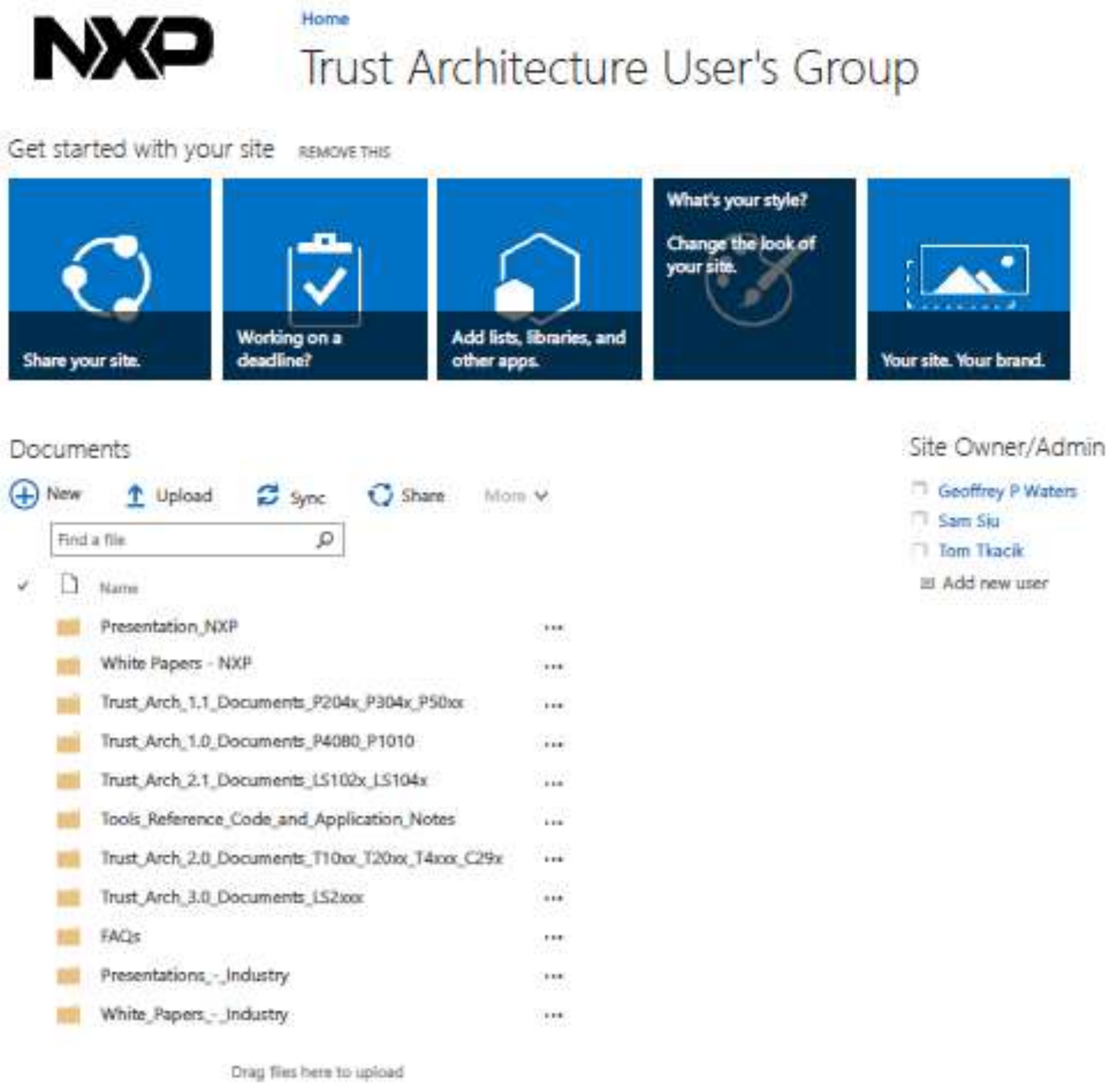
Validate a system in the field.

- Following successful secure boot, the SEC can be commanded to generate an ECC public/private key pair.
- The OEM programmed Super Root Key Hash and a NXP Secret Value are the inputs to the Key Gen process.
- Once the Hardware Key Pair is generated, the Public Key is optionally output. The Private Key isn't readable by software, and cannot be output. It can only be used by the SEC.
- The same Hardware Key Pair is generated each time the Hardware Key Pair Generation is executed. The Keys are locked out & cleared in response to a security violation.

Layerscape Security Life Cycle Stages – Enforced in HW

Stage	Product State	Assets	Operational Restrictions
Virgin	Wafer, die, or pre-test chip	None	None
Deploy Up to 5x	Finished Goods; saleable product	NXP Factory Secret Value	• NXP fuses write protected against updates • Scan disabled • External debug of TZ Secure World disabled
Retest	Pre-test (retest) chip	NXP Factory Secret Value	• NXP fuses write protected against updates • Scan disabled • External debug of TZ Secure World enabled
OEM	Finished good on OEM board	• NXP Factory Secret Value • OEM SRKH, Master Key • Trusted Mfg Key Pair • Key Revocation, Anti-Rollback controls • Additional credentials (protected by Master Key)	• NXP fuses write protected against updates • Scan disabled • External debug of TZ Secure World disabled • Secure Boot Only (ITS) • External Debug access restricted (Debug Permissions) • OEM fuses write protected against updates
OEM Update	Finished good on OEM board	• Same as OEM	• Same as OEM, however one or more keys from SRKH list is revoked, no longer usable to validate image, or monotonic counter/era feature update prevents anti-rollback
Field Return Up to 2x	Finished good removed from OEM board, returned to NXP for CQI	• Same as OEM	• Scan still disabled • External debug of TZ Secure World re-enabled • Secure Boot bypassed • External Debug access controls bypassed (excepted 'Locked')
Re-Deploy	Finished good returned to OEM, remounted onto OEM board	• Same as OEM	• Same as OEM

Trust Architecture User’s Group



Trust Architecture User's Group

Documents

- Presentation_NXP
- White Papers - NXP
- Trust_Arch_1.1_Documents_P204x_P304x_P50xx
- Trust_Arch_1.0_Documents_P4080_P1010
- Trust_Arch_2.1_Documents_LS102x_LS104x
- Tools_Reference_Code_and_Application_Notes
- Trust_Arch_2.0_Documents_T10xx_T20xx_T4xxx_C29x
- Trust_Arch_3.0_Documents_LS2xxx
- FAQs
- Presentations_-_Industry
- White_Papers_-_Industry

Site Owner/Admin

- Geoffrey P Waters
- Sam Siu
- Tom Tkacik

Trust Architecture User’s Group is a NXP hosted community

Uses extranet site to share NDA information with customers & eco-system partners

Trust Tools & Secure Boot

Secure chain of trust

- Internal Secure Boot
- External Secure Boot – Uboot, UEFI
- Partitioning of run-time environment

Rich set of configuration tools

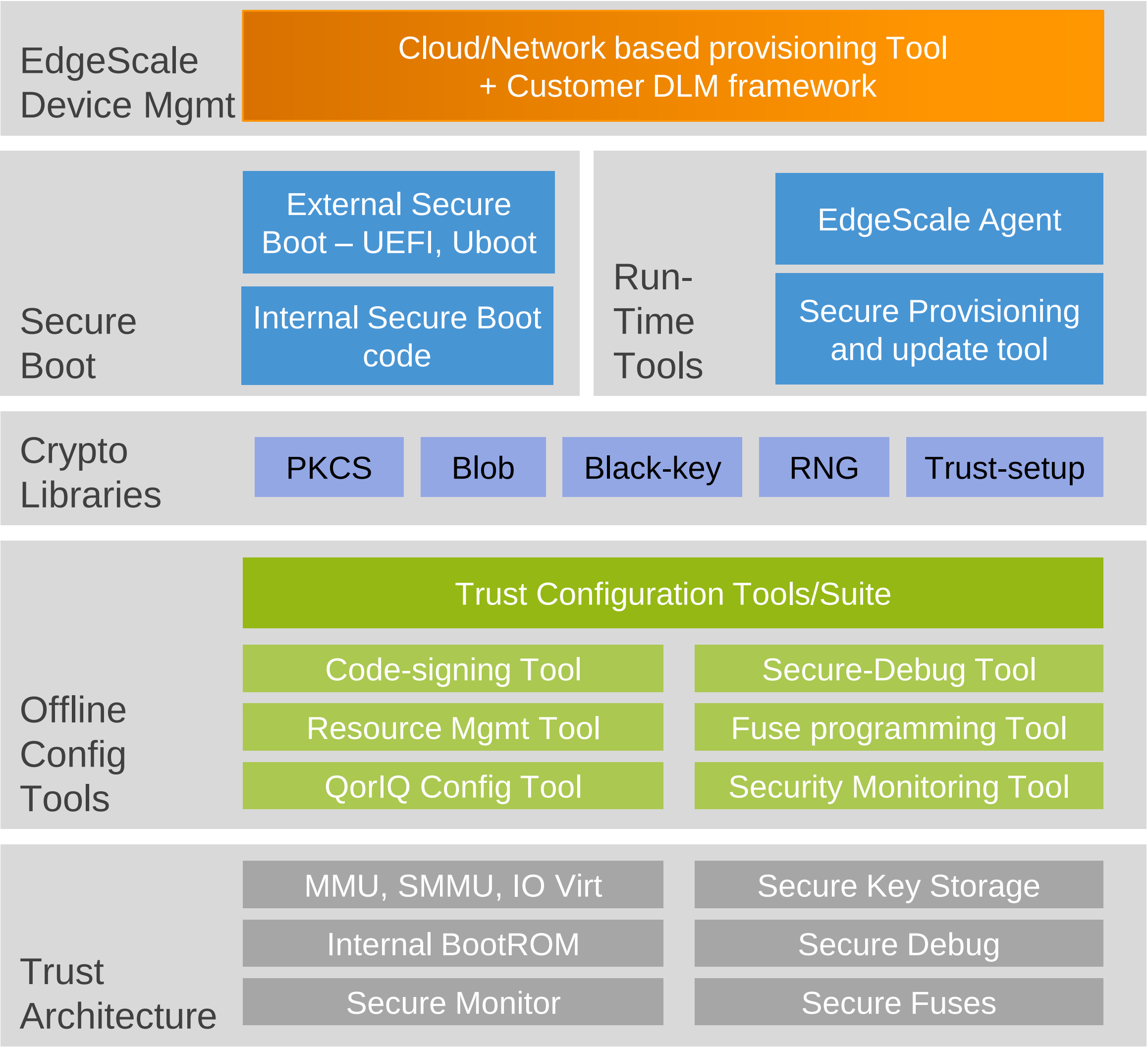
- Programming keys, policies
- Code-signing
- Low-level programmability with ease of use

DLM Middleware

- Hooks up with Cloud provisioning agents
- Flexible API to hook into customer DLM

Leverage Trust Architecture

- HW Root of trust
- Secure provisioning and monitoring



EdgeScale Device Mgmt

Cloud/Network based provisioning Tool + Customer DLM framework

Secure Boot

External Secure Boot – UEFI, Uboot

Internal Secure Boot code

Run-Time Tools

EdgeScale Agent

Secure Provisioning and update tool

Crypto Libraries

PKCS

Blob

Black-key

RNG

Trust-setup

Offline Config Tools

Trust Configuration Tools/Suite

Code-signing Tool

Secure-Debug Tool

Resource Mgmt Tool

Fuse programming Tool

QorIQ Config Tool

Security Monitoring Tool

Trust Architecture

MMU, SMMU, IO Virt

Secure Key Storage

Internal BootROM

Secure Debug

Secure Monitor

Secure Fuses

Trusted Linux

Enhances standard off-the-shelf Linux

Ensures Trusted Applications

- Isolation of resources
- Verified installation
- Controlled launch

Ensures Trusted Data

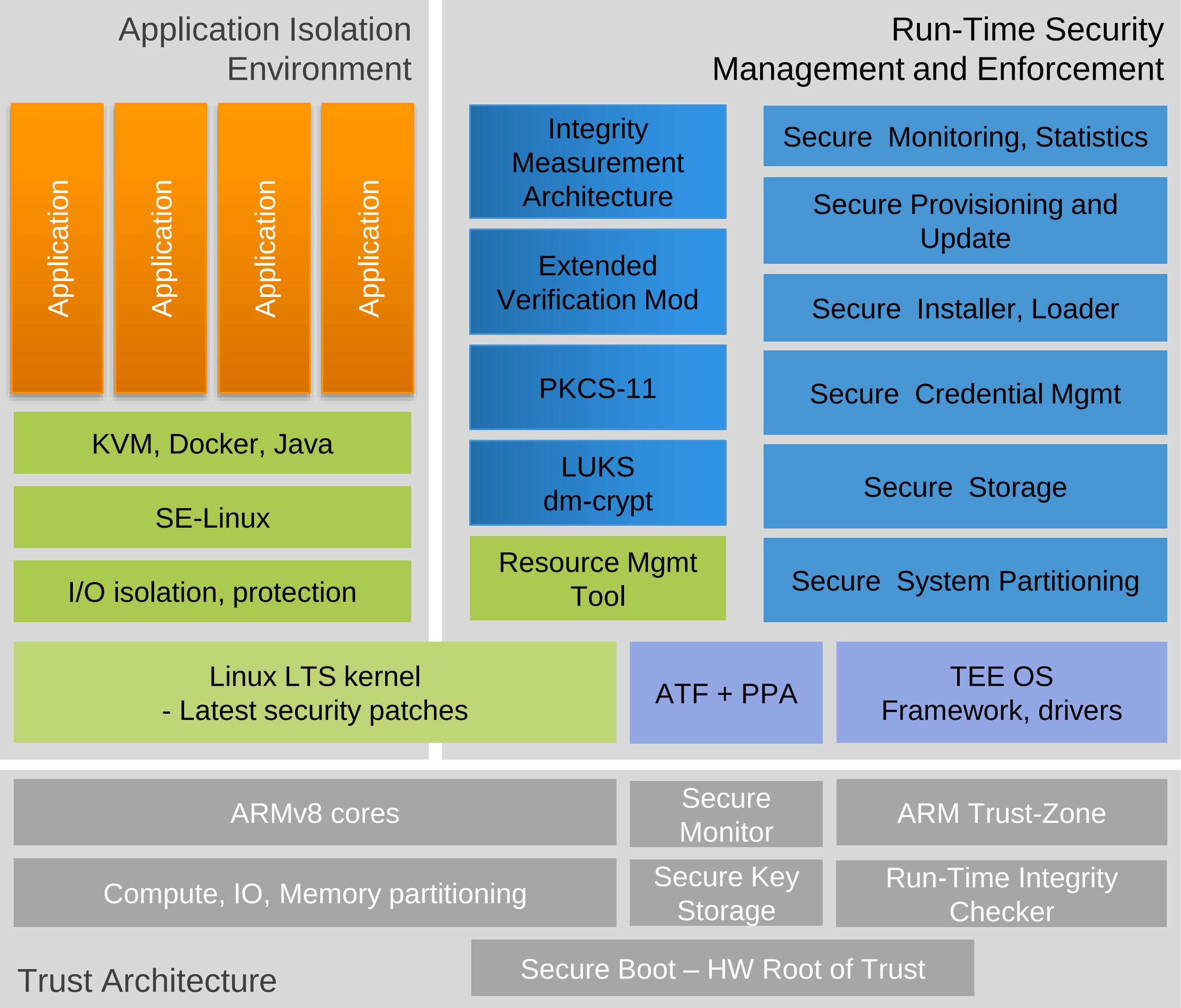
- Isolated, encrypted user data.
- Isolated, secure credentials
- Controlled access

Ensures Trusted System

- Run-time monitoring and statistics
- Firmware update, commissioning

HW Assist by Trust Arch

- HW root of trust during boot process
- Run-time integrity check for kernel, TEE
- Secure monitor, tamper detect



Application Isolation Environment

Application

Application

Application

Application

KVM, Docker, Java

SE-Linux

I/O isolation, protection

Run-Time Security Management and Enforcement

Integrity Measurement Architecture

Extended Verification Mod

PKCS-11

LUKS dm-crypt

Resource Mgmt Tool

Secure Monitoring, Statistics

Secure Provisioning and Update

Secure Installer, Loader

Secure Credential Mgmt

Secure Storage

Secure System Partitioning

Linux LTS kernel
- Latest security patches

ATF + PPA

TEE OS Framework, drivers

ARMv8 cores

Secure Monitor

ARM Trust-Zone

Compute, IO, Memory partitioning

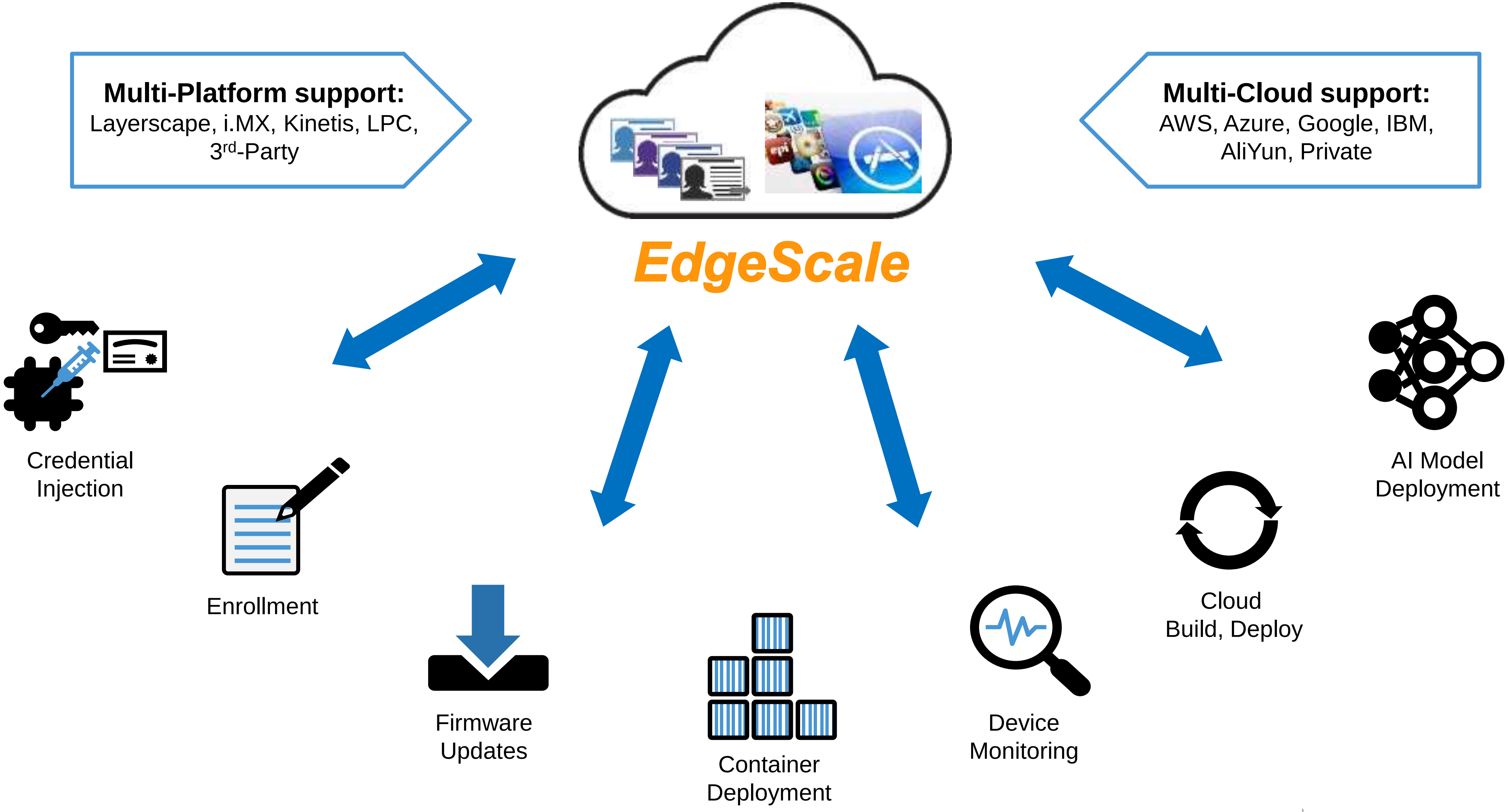
Secure Key Storage

Run-Time Integrity Checker

Trust Architecture

Secure Boot – HW Root of Trust

EdgeScale for Secure Management



Multi-Platform support:
Layerscape, i.MX, Kinetis, LPC,
3rd-Party

Multi-Cloud support:
AWS, Azure, Google, IBM,
AliYun, Private

EdgeScale

Credential
Injection

Enrollment

Firmware
Updates

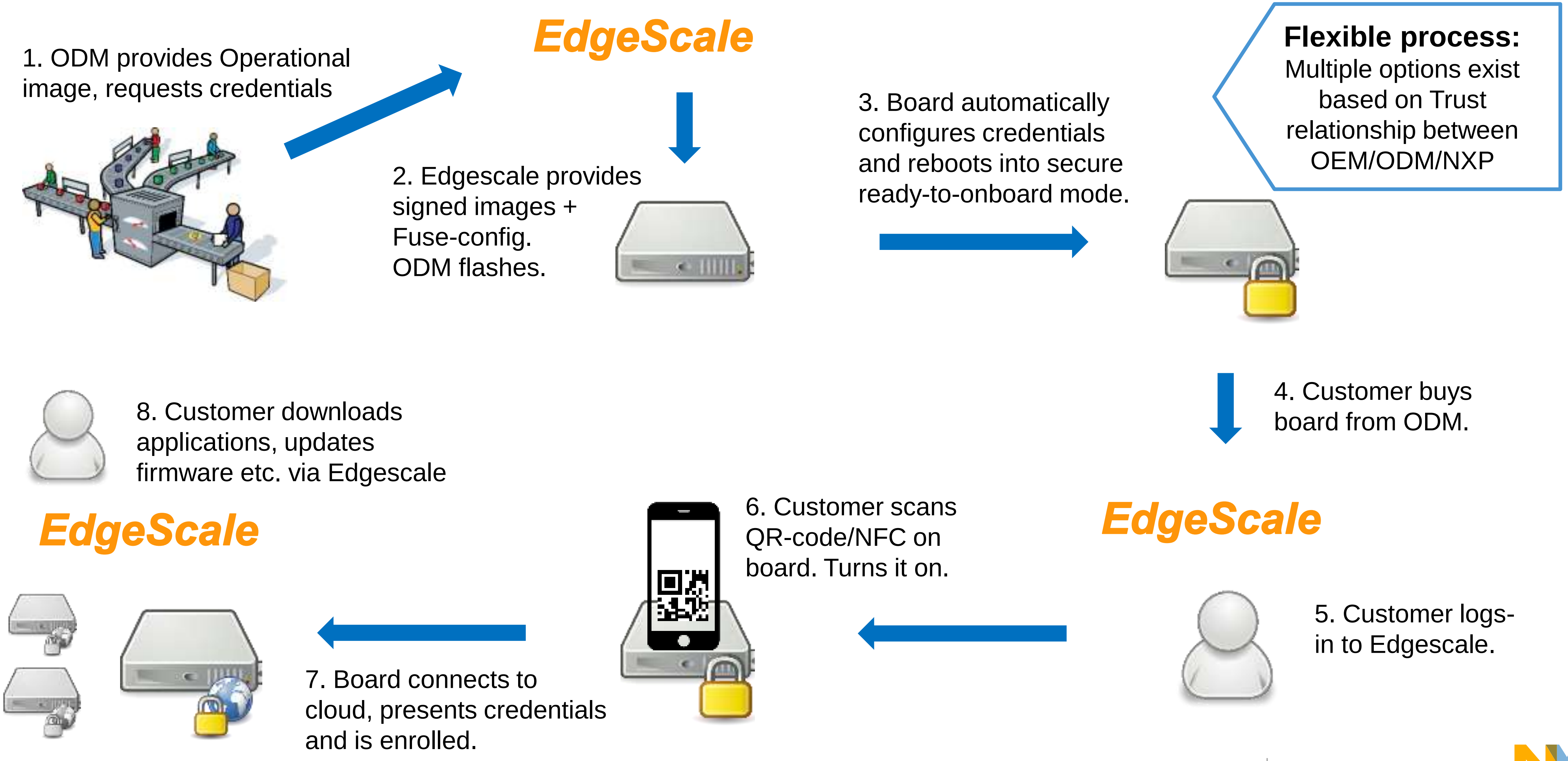
Container
Deployment

Device
Monitoring

Cloud
Build, Deploy

AI Model
Deployment

Simplifying Credential Provisioning with EdgeScale



1. ODM provides Operational image, requests credentials

EdgeScale

2. Edgescale provides signed images + Fuse-config. ODM flashes.

3. Board automatically configures credentials and reboots into secure ready-to-onboard mode.

Flexible process:
Multiple options exist based on Trust relationship between OEM/ODM/NXP

4. Customer buys board from ODM.

EdgeScale

5. Customer logs-in to Edgescale.

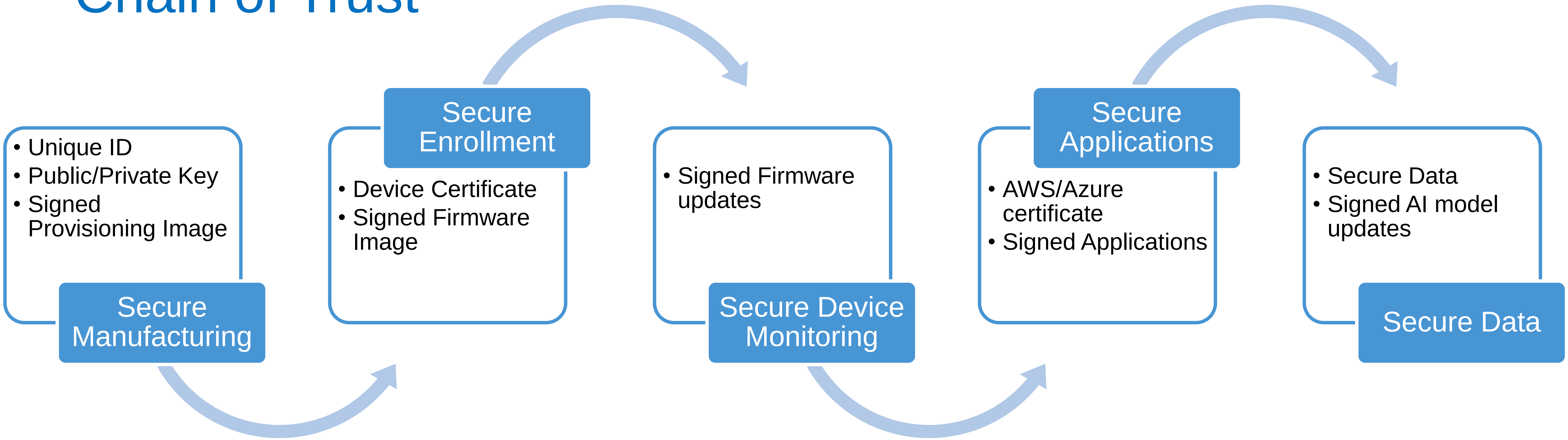
6. Customer scans QR-code/NFC on board. Turns it on.

7. Board connects to cloud, presents credentials and is enrolled.

EdgeScale

8. Customer downloads applications, updates firmware etc. via Edgescale

Chain of Trust



Secure Manufacturing
- Unique ID
- Public/Private Key
- Signed Provisioning Image

Secure Enrollment
- Device Certificate
- Signed Firmware Image

Secure Device Monitoring
- Signed Firmware updates

Secure Applications
- AWS/Azure certificate
- Signed Applications

Secure Data
- Secure Data
- Signed AI model updates

- Hardware forms the Root of trust
- Multiple layers of tamper-detection - each level validates the next
- Multiple levels of secrets – can revoke at any layer
- Mutual authentication between device and cloud using Asymmetric cryptography

Security Consulting and Services

Our Security Technology

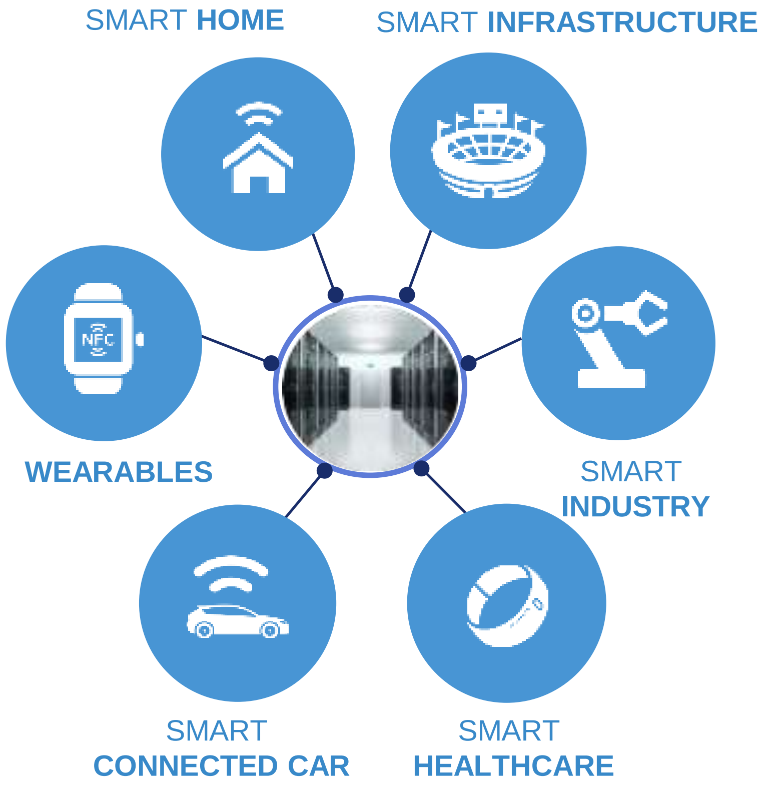
- Application Identification
- Device Identification
- Certification
- Compliance
- Cryptography Acceleration
- Network Security
- NFC
- RFID
- Secure Boot
- Secure Keys
- Secure Memory
- Secure Update
- Trusted Execution
- Unique Chip Identity

Our Security Expertise

E-Passport Mobile Transactions Banking

Security Consulting and Services can **get you to revenue faster**

Your Smart Connected Product



SMART **HOME**

SMART **INFRASTRUCTURE**

WEARABLES

SMART **INDUSTRY**

SMART **CONNECTED CAR**

SMART **HEALTHCARE**

Summary

✓ Security/Trust for Cyber Physical Systems

More important in today’s world than ever before

An integral part of product development and deployment lifecycle

Must be easy to use

✓ Layerscape Security Technology

A suite of Hardware and Software capabilities

Covers every aspect of product lifecycle

Embedded into every Layerscape system solution

EdgeScale simplifies deployment and management of secure devices

SECURE CONNECTIONS
FOR A SMARTER WORLD