i.MX 8 Security Overview

John Cotner

Security Architect - Automotive

October 2018 | AMF-AUT-T3363

SECURE CONNECTIONS
FOR A SMARTER WORLD

"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: Those that have been hacked and will be again."

- Robert Mueller, sixth director of the FBI

“A system is *good* if it does what it’s supposed to do and *secure* if it doesn’t do anything else.”

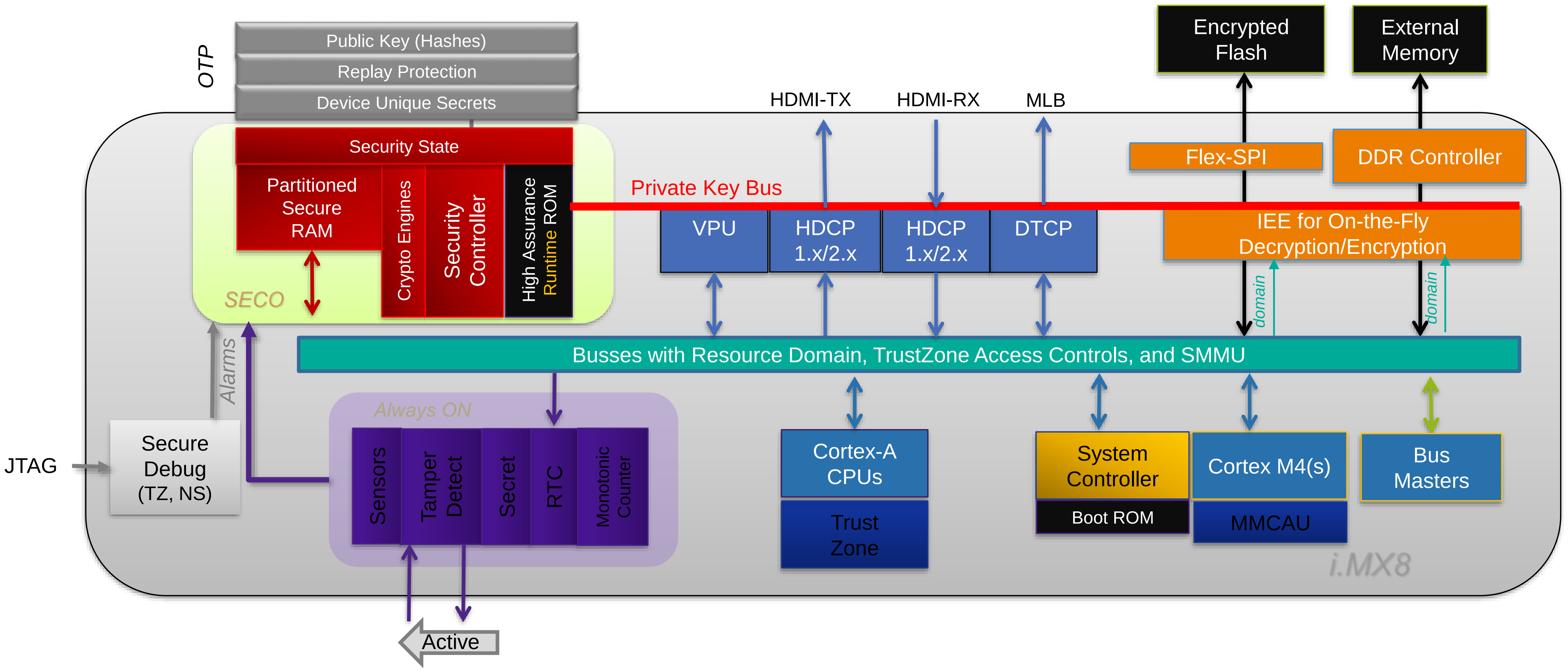
- Dr. Eugene “Spaf” Spafford, Purdue

Core Security Principles in Automotive Systems

	Prevent access	**Detect** attacks	**Reduce** impact	**Fix** vulnerabilities
Secure Interfaces	M2M Authentication & Firewalling	Intrusion Detection Systems (IDS)		Secure OTA Updates
Secure Gateway	Firewalling (context-aware message filtering)		Separated Functional Domains	
Secure Networks	Secure Messaging		Message Filtering & Rate Limitation	
Secure Processing	Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	

i.MX 8 Security

i.MX 8 Series Security Architecture Overview



Security Features

- SECO Security Microcontroller (Cortex-M0+,133Mhz)
  - Isolated security domain
  - Higher protection for root secrets and key management functions
- DTCP (Digital Transport Content Protection) – Authentication engine with secure interface for key loading
- IEE (Inline Encryption Engine) – Cryptographic protection of data in external memory
- ADM (Authenticated Debug Module) – Secure debug, Lifecycle handling, Access and Violation control
- Enhanced CAAM
  - 64KB Secure RAM
  - Cryptographic acceleration on cryptography Algorithms
  - RTIC (Runtime Integrity Checker) : Ensures integrity of the memory contents

Security Features (2 of 2)

- SNVS (Secure Non-Volatile Storage)
  - Secure State Machine
  - 10 external tamper pins that can be configured to support 5 active meshes or 10 passive meshes
  - Analog sensors for temperature, voltage, frequency tamper detection
- Encrypted “execute in place” (XIP) capability from QSPI
- xRDC – HW isolation at chip level (Resource Domains)
- Cryptographic binding of resource domain identity for secure storage
  - Key storage in external flash
- Fast secure boot
  - ECDSA up to 1024 module with SHA-512
- Fast signature verifications using P-256 Elliptic Curve for V2X

i.MX Product Security Features Overview

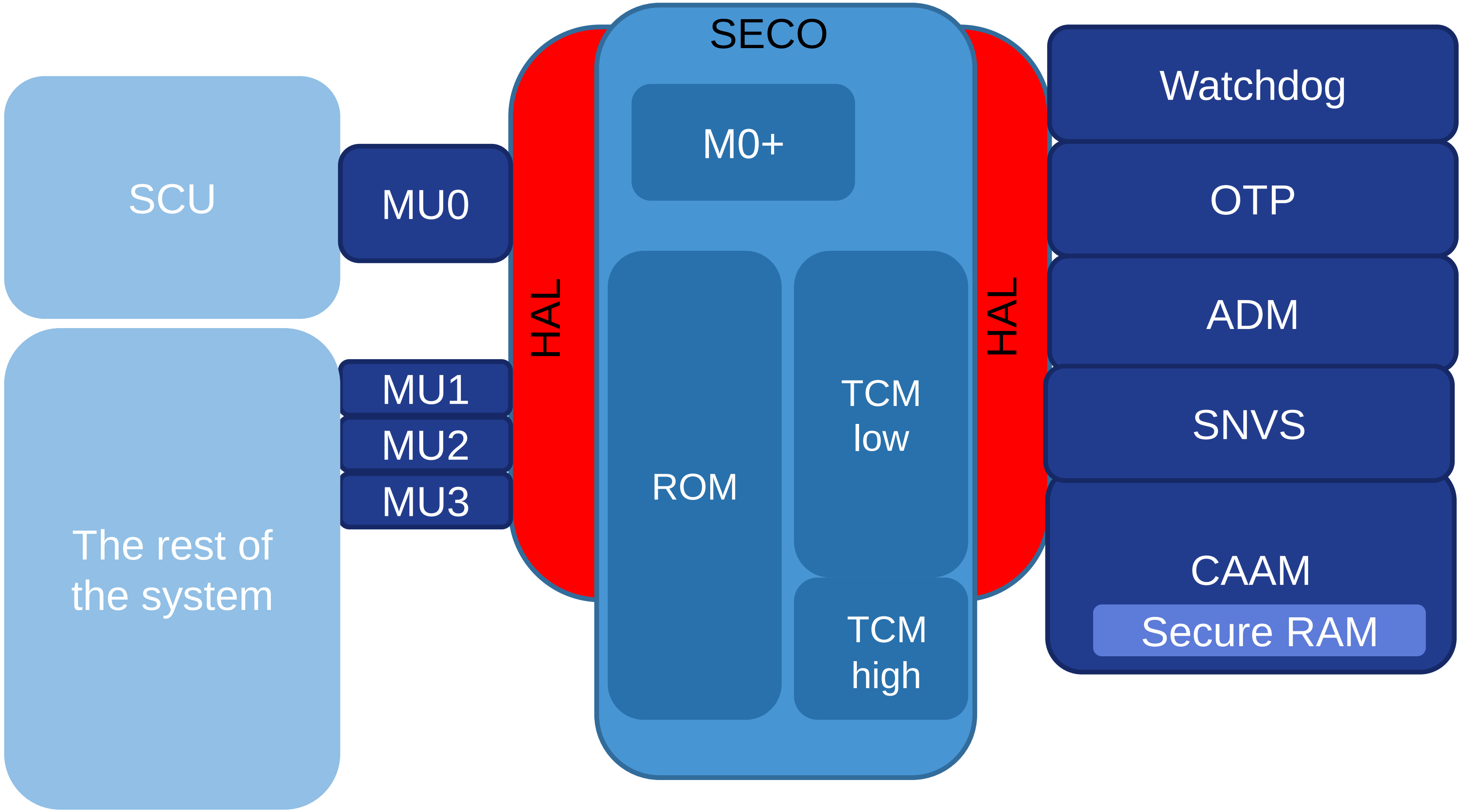
Feature	i.MX6Q/D/S	i.MX6SX	i.MX6UL	i.MX7S/D	i.MX8QM	i.MX8QXP
Security Controller (SECO)	x	x	x	x	✓	✓
AES128/192/256, SHA1/256, DES/3DES	✓	✓	✓	✓	✓ + SHA 384/512	✓ + SHA 384/512
Elliptic Curve DSA (up to P521/B571) RSA (up to 4096)	x	x	✓	✓	✓ High performance	✓ High performance
Crypto Accelerator Unit (CAU) (DES, AES co-processor instruction)	x	x	x	x	✓	✓
Certifiable RNG	✓	✓	✓	✓	✓	✓
Run Time Integrity Protection	x	x	✓	✓	✓	✓
Isolated security applications (e.g. SHE)	x	x	x	x	✓	✓
High Assurance Boot (RSA, ECDSA)	✓RSA	✓RSA	✓RSA	✓RSA	✓	✓
Encrypted Boot	✓	✓	✓	✓	✓	✓
Secure Debug	✓	✓	✓	✓	✓ Domains	✓ Domains
Always ON domain	✓	✓	✓	✓	✓	✓
Secure Storage (non-volatile)	✓	✓	✓	✓	✓	✓
Tamper Detection Signal	✓	✓	✓ Active	✓ Active	✓ Active	✓ Active
Volt/Temp/Freq Detect	x	x	✓	✓	✓	✓
Inline Encryption	x	x	✓ **BEE**	x	✓ **IEE**	✓ **IEE**
Manufacturing Protection	x	x	x	✓	✓	✓
Resource Domain Isolation	x	✓	x	✓	✓	✓
Content Protection	✓ **6Q 1.x only**	x	x	x	✓ **HDCP 1.x/2.x, DTCP**	✓ **DTCP**

SECO

SECO Overview

Manager of the CAAM and other NXP Security-Reliant Subsystems

- Energy efficient M0+ core supporting 133MHz
- Interrupt Controller with up to 32 IRQs
- Security controls through Authenticated Debug Module (ADM)
- Dedicated 80KB ROM, 80KB RAM with Error Correct Code (ECC)
- Dedicated One-Time Programmable (OTP) keys
- Fabric switch to Shared Peripherals, Local Peripherals, and Private Crypto Key Bus



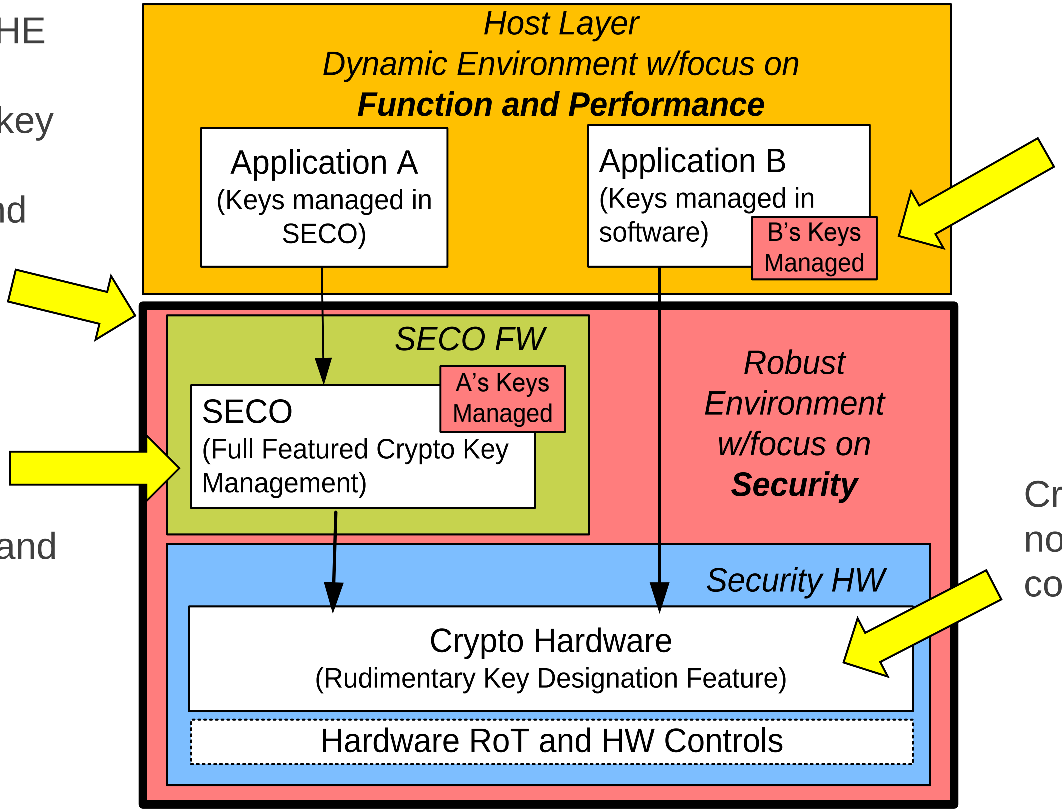
SECO Features

- Secure boot (container/image authentication)
- Services provided to AP/SCU cores via Message Unit interface
- Lifecycle configuration
- Fuse programming
- Debug enablement
- IP secret installation (DTCP keys, HDCP keys, …)
- CAAM management
  - Job Ring assignment
  - Secure Memory
- SNVS management
  - HW security state machine management
- ADM management (locks, timers, LC, ...)
- Power management
- Attestation of SECO FW

SECO enables proper Crypto Key Management

Automotive Security Specs require isolated HSM/SHE modules for full featured crypto key life cycle management and specific usage

SECO + Crypto Hardware offers comprehensive and secure key management



Host Layer
Dynamic Environment w/focus on
Function and Performance
Application A
(Keys managed in SECO)
Application B
(Keys managed in software)
B's Keys Managed
SECO FW
A's Keys Managed
SECO
(Full Featured Crypto Key Management)
Robust Environment w/focus on ***Security***
Security HW
Crypto Hardware
(Rudimentary Key Designation Feature)
Hardware RoT and HW Controls

Key Management in non-secure environment increases chance of exposure

Crypto hardware only not capable of fully controlling key usage

SHE

SHE SECO firmware

- Authenticated as part of the SoC boot process, NXP signed
- Support for all required SHE functionality
- SHE (GPL free) driver provided, ensuring accessibility from any targeted OS/SoC domain
- Off-chip non volatile storage support:
  - eMMC w/RPMB partition can be used for implementing SHE Non-Volatile storage
  - RPMB (Replay Protected Memory Block) uses Authentication mechanism (HMAC) to protect against:
    - Anti-roll back attacks
    - Read/write/erase from CPU applications (or offline attack)
  - Data are stored encrypted on the RPMB partition
    - Key used for the encryption is
      - Unique per chip (derived from the i.MX OTPMK, or ZMK)
      - Not known outside SECO

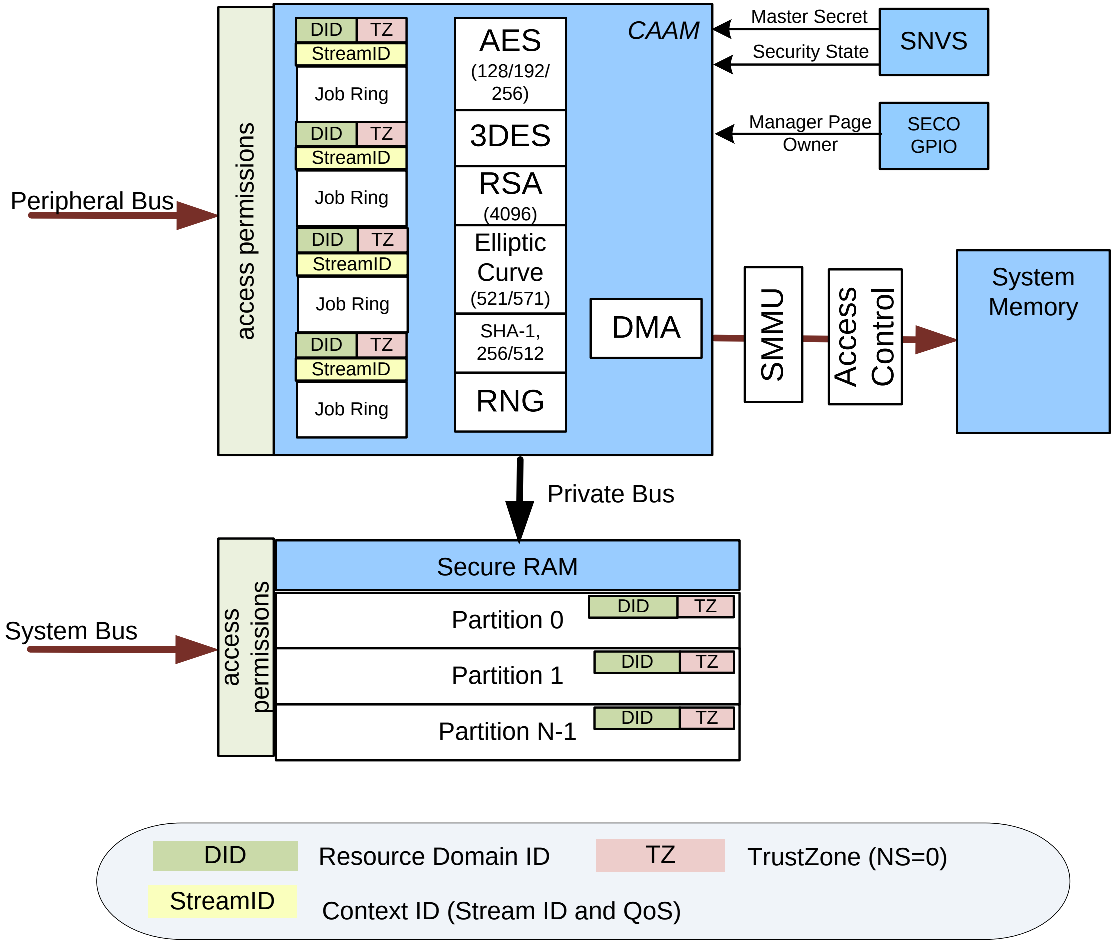
SHE driver – OS independent, non-GPL driver

- SHE services generic driver for the i.MX8 chip families
- Easily portable to different OS or Bare metal implementation
- Development details:
  - c99 standard, standard Makefile
  - Currently supports GCC compiler
  - OS depended functions are implemented in a dedicated folder
- Quality:
  - Complete test coverage provided with the library
  - Driver designed to meet spice level 2 requirements
  - CERT and MISRA coding rules enforced
  - Coverity used for static code analysis
- SHE Library Integration Document will be made available to ease porting

CAAM

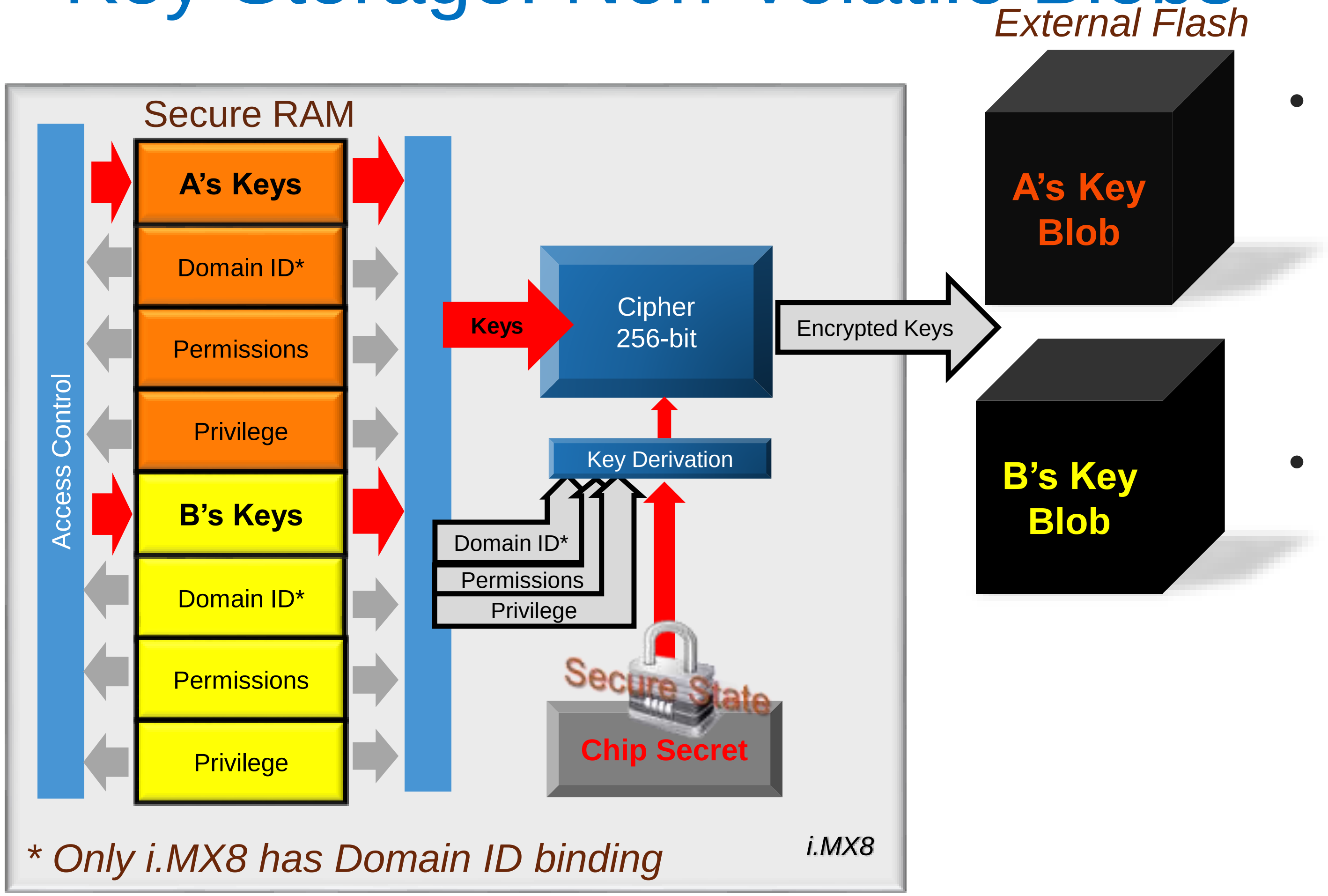
Security: Cryptographic Acceleration and Assurance Module

- **Cryptographic Acceleration**
  - Public Key Hardware Accelerator: **ECDSA, RSA**
  - Encryption Algorithms: **AES, DES/3DES**
  - Hashing Algorithms: **MD5, SHA256/384/512, …**
  - Message Authentication Codes: **HMAC, AES-CMAC, AES-XCBC-MAC**
  - Authenticated Encryption Algorithms: **AES-CCM, AES-GCM**
- **RNG**
- **Export and Import of cryptographic Blobs**
- **Secure Memory Controller and Interface**
  - 64KB with 16 partitions at 4KB page size
  - Automatic Zeroization on SNVS Violation Event
- **Job Rings**
  - descriptor based command interface
  - Assigned to apps cores via SCU API
- **IP Slave Interface**
- **Support the system virtualization by Domain ID (DID) per job ring**
- **DMA**



Secure Storage

Key Storage: Non-Volatile Blobs



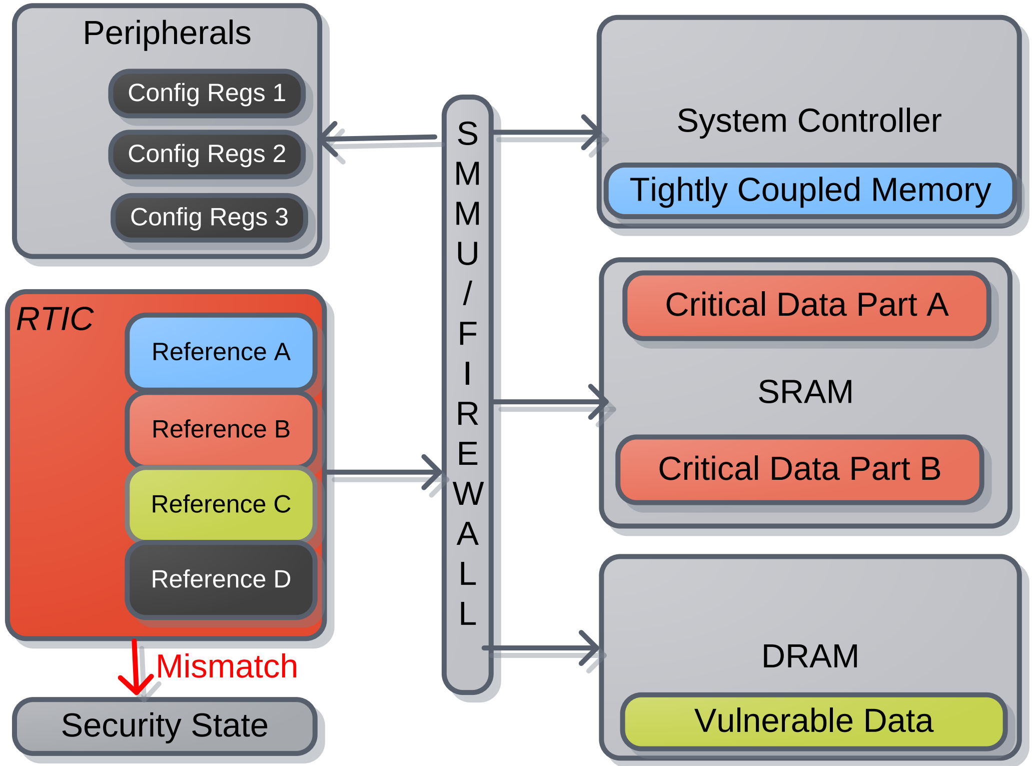
** Only i.MX8 has Domain ID binding*

- **Key Blobs**
  - Protects keys between power cycles
  - Keys are encrypted with key derived from a device unique secret
- **Cryptographic Bindings Include**
  - Security State (Trusted, Secure, Other)
  - Access Permissions
  - Privilege (TZ or NS)
  - Resource Domain (i.MX8)
  - Key Modifier

RTIC

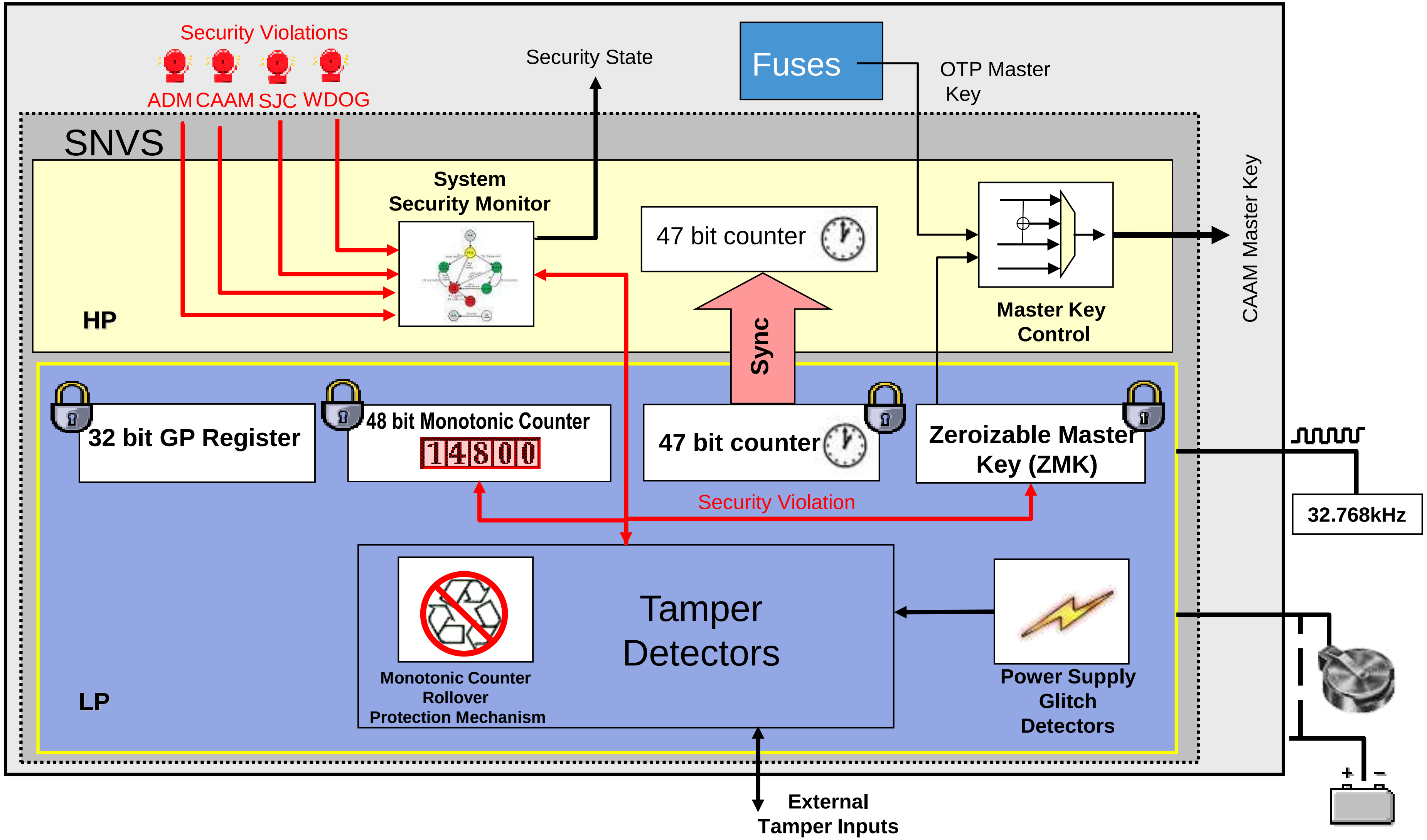
Runtime Integrity Checker (RTIC)

- Ensures integrity of the memory contents
- Verifies memory contents during run-time execution
- If memory contents fail to match then a security violation is asserted
- A security violation changes the security state of the SoC
- Virtualized Addresses, TZ and different Resource Domains supported



SNVS

Security State and SNVS HP and LP



SNVS Features

- Security state machine that transitions to fail state upon security violations and gates access to internal SoC secrets (OTPMK/ZMK).
- 10 external tamper pins that up to 5 active tampers (5 inputs and 5 outputs) or 10 passive tampers (inputs only)
- Security sensor detection of physical attacks using temperature, voltage, frequency detection
- Monotonic Counter
- General purpose registers
- Zeroizable master key (ZMK)
- Real time counter
- High Performance and Low power domain

* SNVS features are enabled via SECO/SCU API

ADM

Authenticated Debug Module/Secure Debug

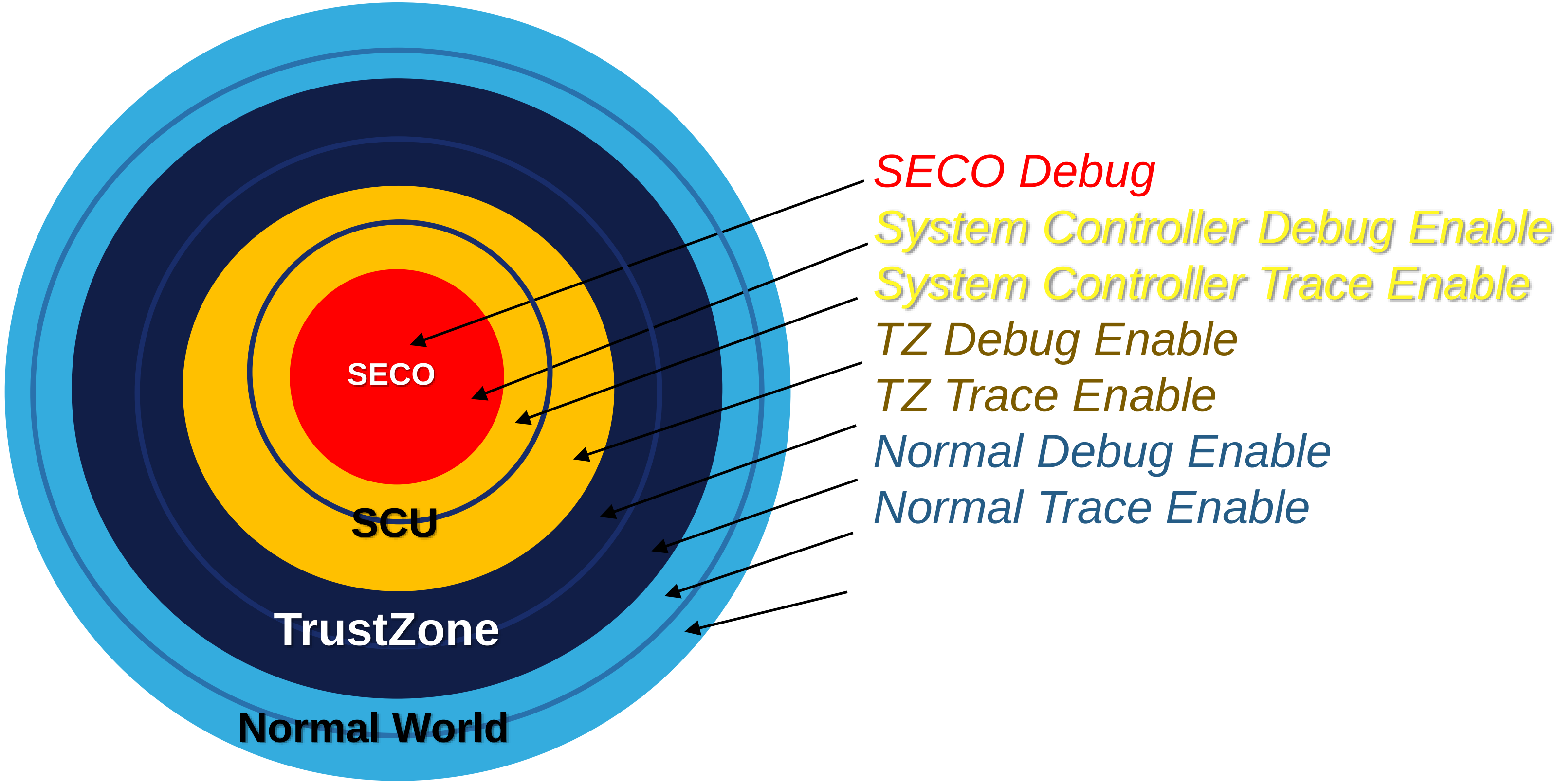
Coresight Authentication Supported with Debug Domains

- For i.MX8, Multiple Debug Domains exist –

- Supports the Coresight Authentication Hierarchy

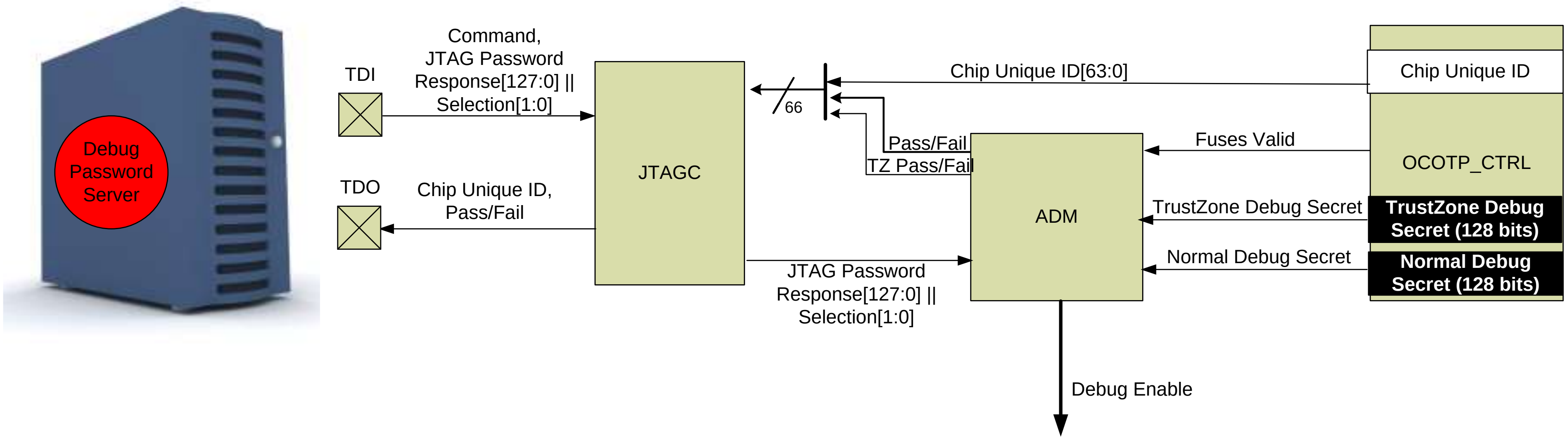
- Debug Apps Core with SECO locked down, for example

- M4’s can be disabled too



Secure Debug - JTAG Challenge/Response

App Cores Trustzone and Normal World Debugging



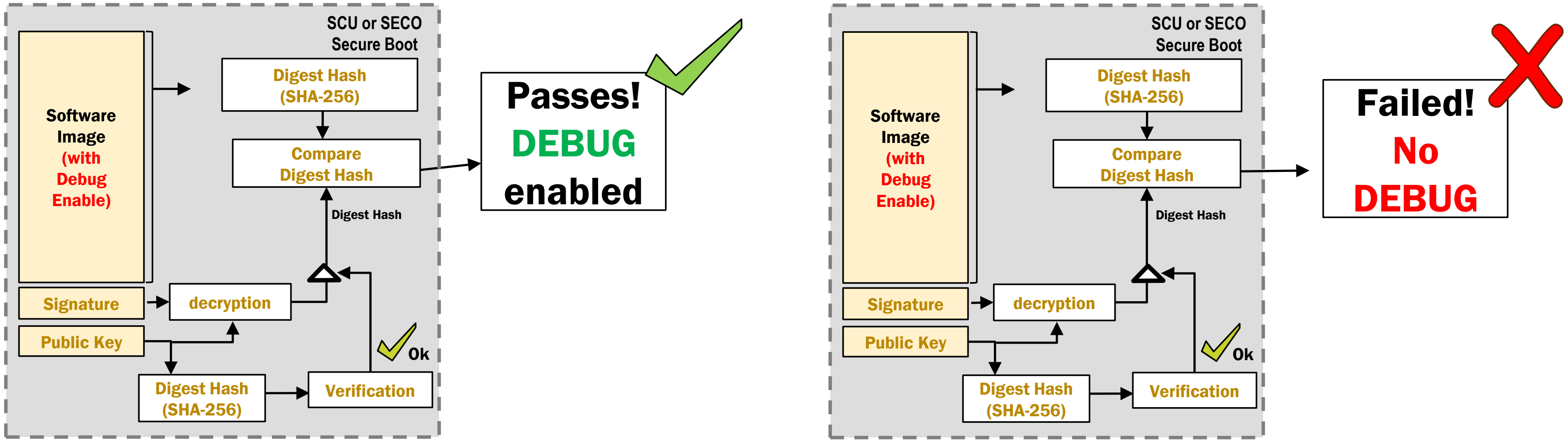
Debug Password Server
TDI
Command, JTAG Password Response[127:0] || Selection[1:0]
TDO
Chip Unique ID, Pass/Fail
JTAGC
66
Chip Unique ID[63:0]
Pass/Fail
TZ Pass/Fail
ADM
JTAG Password Response[127:0] || Selection[1:0]
Fuses Valid
TrustZone Debug Secret
Normal Debug Secret
Chip Unique ID
OCOTP_CTRL
TrustZone Debug Secret (128 bits)
Normal Debug Secret (128 bits)
Debug Enable

1. User requests debug through JTAG interface
2. SOC responds with chip unique ID
3. Server finds corresponding secret (TZ or normal world)
4. User submits secret through JTAG interface
5. Secure JTAG module compares secret to pre-configured secret
6. If a match, debug is enabled (for TZ or normal world)

Enabling Debug on SCU and SECO

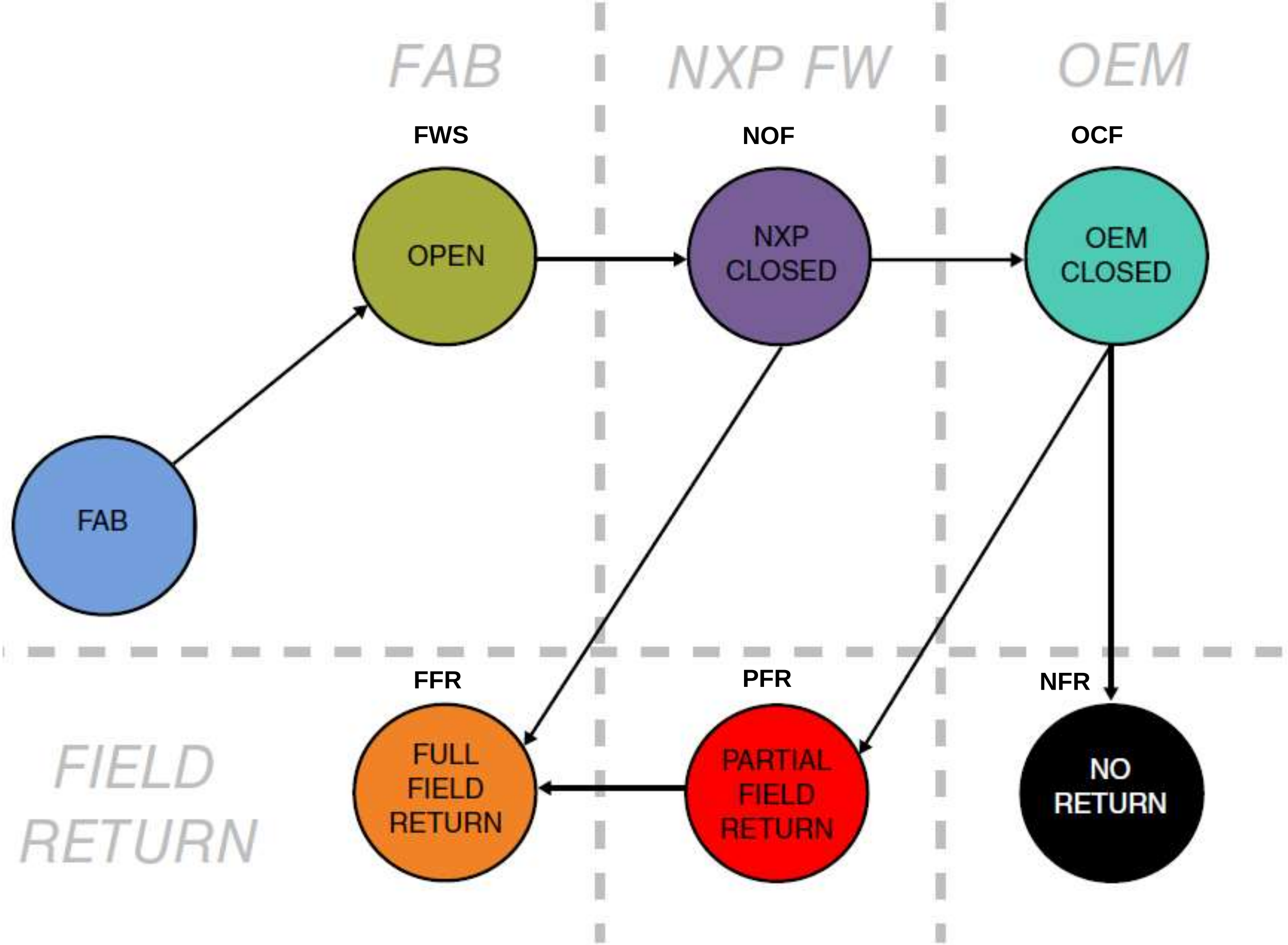
- System Controller Debug or SECO Debug require Signed Commands to open debug on Closed parts (with no fuse DEBUG disablement)
- SECO receives a signed message through MUs.
- Message payload specifies the target subsystem and permission (DBGEN, NIDEN…)
- Once signature is validated, SECO enables the debug to the desired sub system with the requested permissions.

SCU, SECO Secure Boot Authentication



Life cycle update

- The life cycle update procedure involves ADM and SECO.
- ADM implement a fuse programming mask to allow transition to certain life cycle only (as indicated in the figure). Only certain fuses can be blown based on the current life cycle.
- Attempt to update life cycle without involve ADM will result in a life cycle mismatch.
- SECO provide two separate API (MU messages):
  - Update life cycle
  - Return life cycle (signed message)



IEE

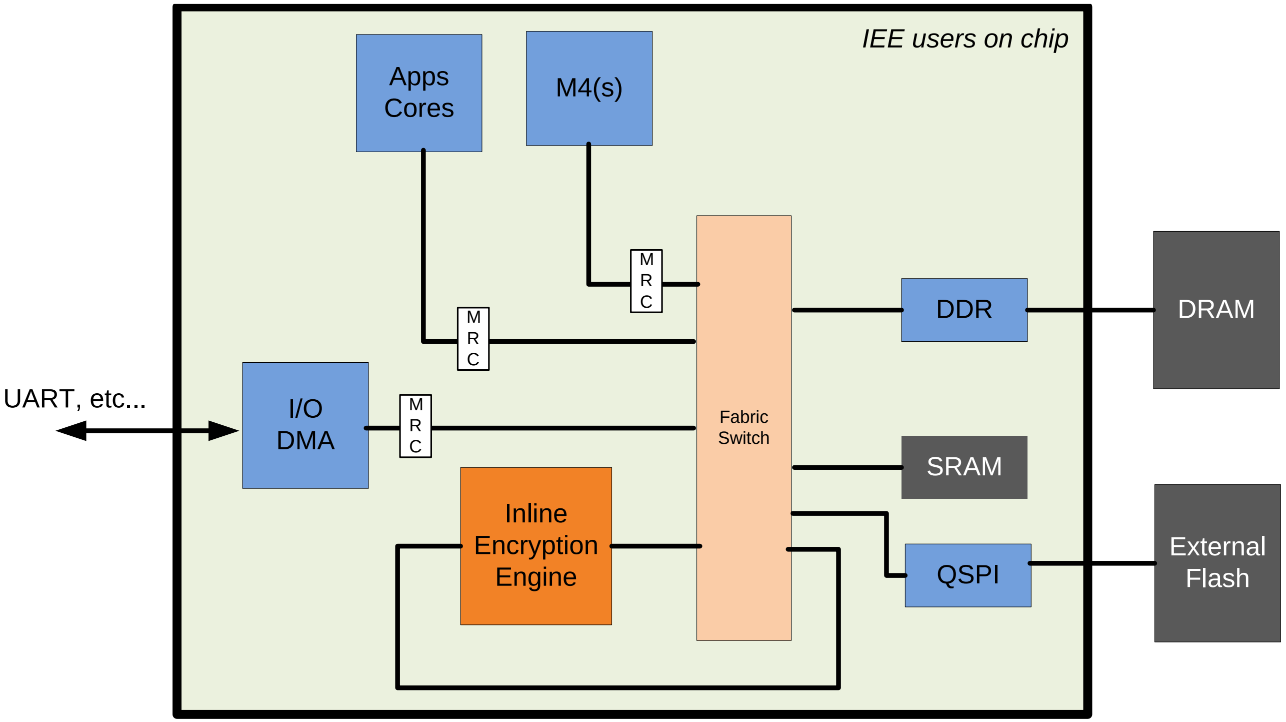
Inline Encryption Engine

IEE

- DDR encryption and decryption in AES-XTS mode
- QSPI flash decryption (also execute-in-place (XIP)) in AES-CTR mode
- I/O DMA direct encrypted storage and retrieval (AES-CTR 128)
- Multi-core resource domain separation
- Transparency to software during encrypted access (i.e. no configuration, control, or interrupts)
- Secure on-chip key loading using private bus between CAAM and IEE
- Differential power analysis (DPA) resistance
- Tamper detection response which key is erased and access to IEE is blocked

Use cases include:

- Execute-in-place code decryption from QSPI primarily
- Encryption of sensitive data at rest
- Ciphering of I/O serial data
- CAAM still used for higher importance data



XRDC

Resource Partitioning on i.MX 8

What is a Partition:

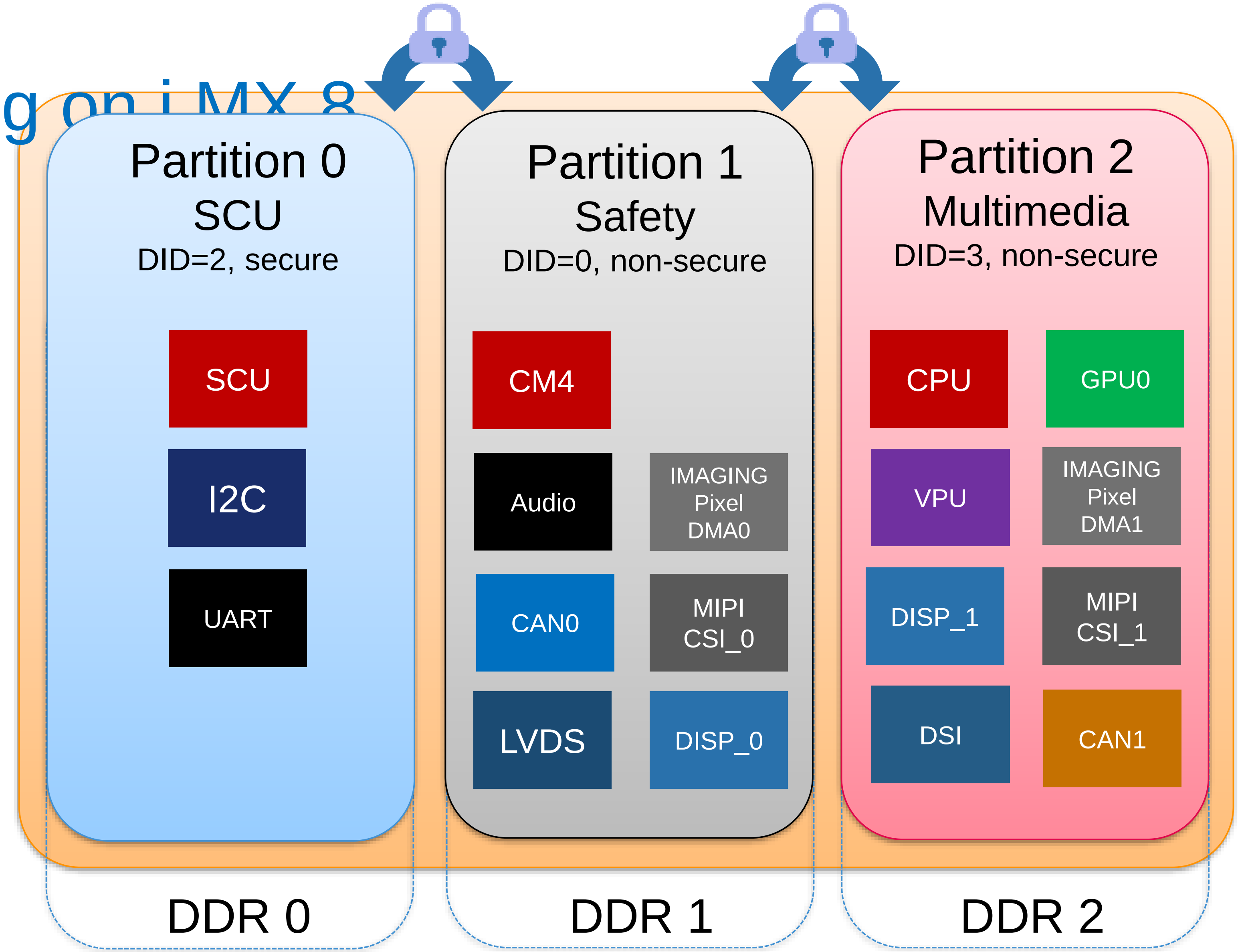
- A collection of resources (master / slave peripherals, memory regions)
- Has a domain ID and a security attribute
- Cores, peripherals and memory can belong to more than one partition

How Partitioning Works:

- The system controller commits peripherals and memory regions into a specific domains. (This is customer defined)
- Any communication between domains are forced to use messaging protocols
- If a domain peripheral tries to access other domains illegally, a bus error will occur.

Benefits of Partitioning:

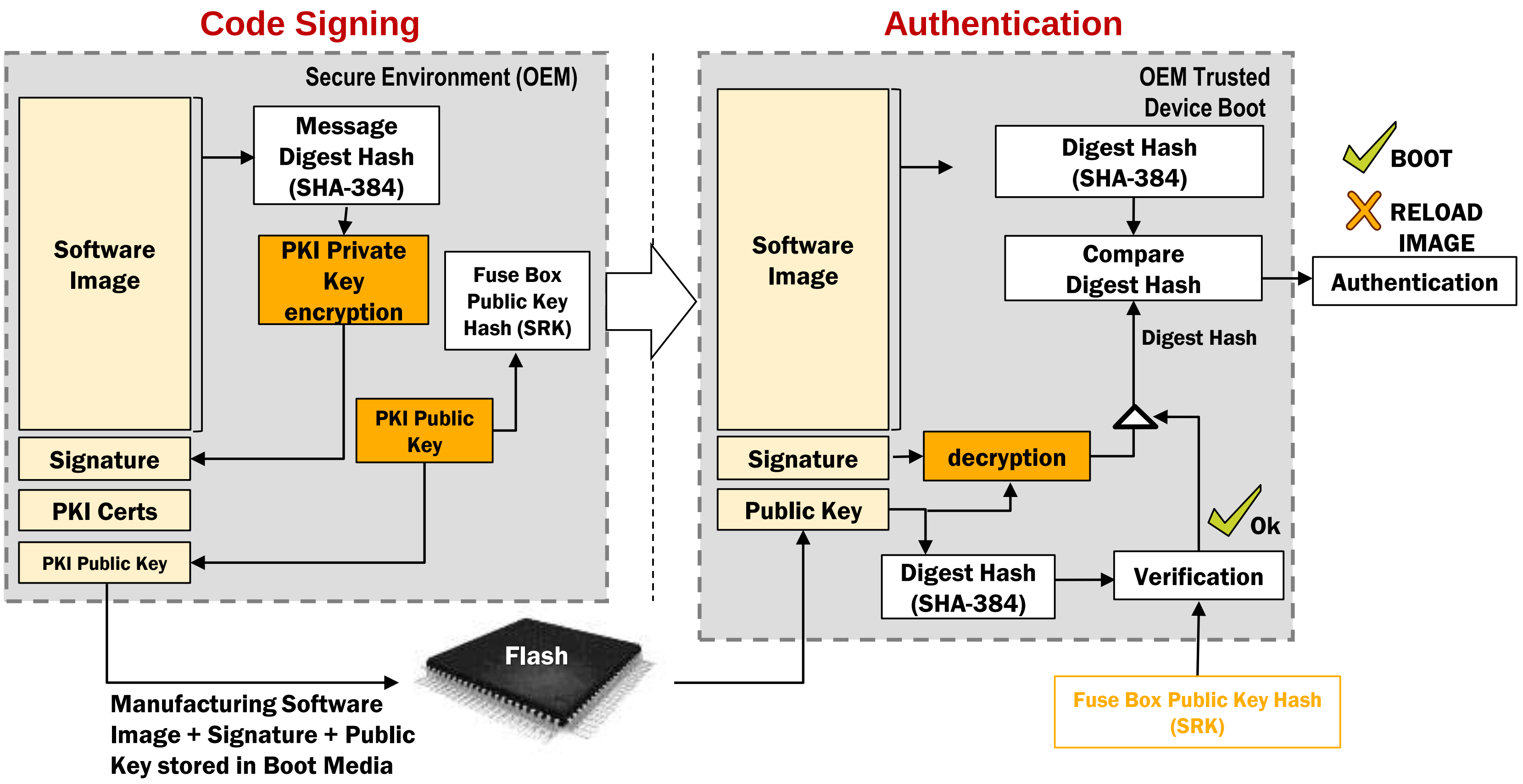
- Reporting of immediate illegal accesses helps track down hard to find race conditions before they go to production. (AKA Sandbox Methods)
- Provides security on a finished product: protects system critical SoC peripherals from less trusted apps



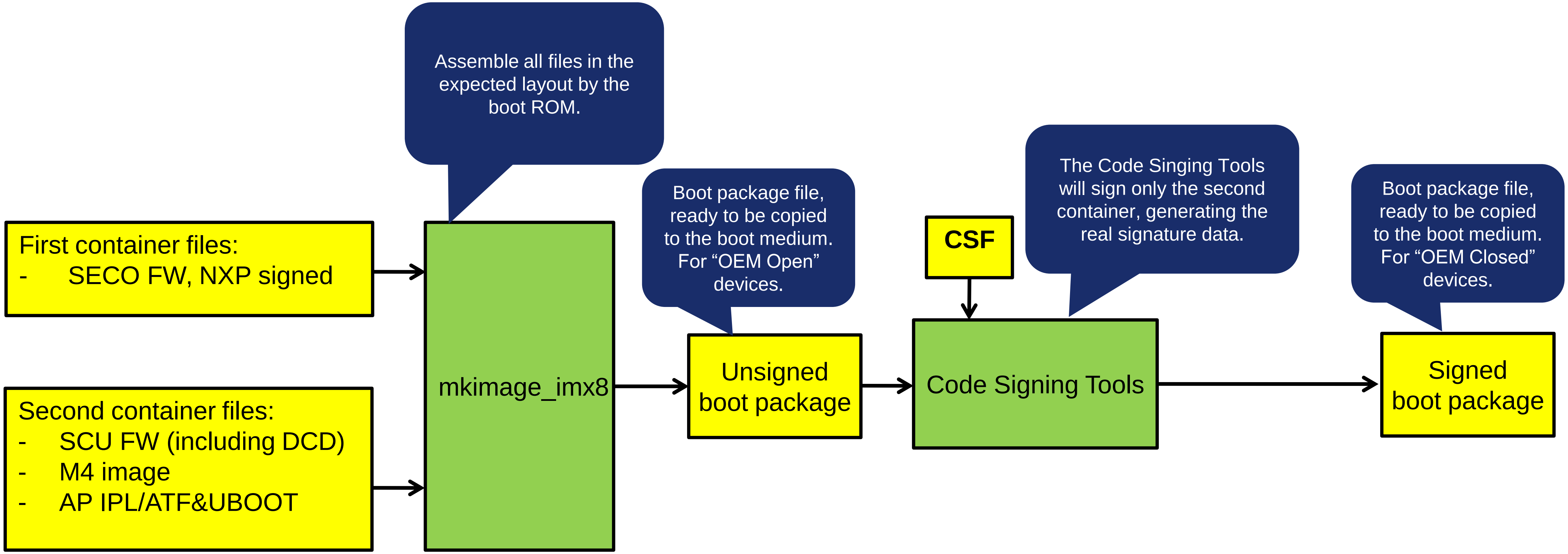
Secure boot & code signing

SoC Code Signing and Secure Boot

- The application core and system controller boot can be signed with separate super root keys
- Security Controller boot authenticates its firmware using its own super root key
- M4 firmware can be included in the Security Controller signature



i.MX 8 Signed Boot Flow – user actions



First container files:
- SECO FW, NXP signed

Second container files:
- SCU FW (including DCD)
- M4 image
- AP IPL/ATF&UBOOT

Assemble all files in the expected layout by the boot ROM.

mkimage_imx8

Boot package file, ready to be copied to the boot medium. For “OEM Open” devices.

Unsigned boot package

CSF

The Code Singing Tools will sign only the second container, generating the real signature data.

Code Signing Tools

Boot package file, ready to be copied to the boot medium. For “OEM Closed” devices.

Signed boot package

Notes:

- The first container is provided by NXP already signed. NXP keys are provisioned in the SoC.
- The DCD functionality is built into the SCU FW, we no longer have a separate file.
- The signing keys for the second container are customer specific.
- The CSF file will use a similar, but updated syntax as on past i.MX solutions.
- The customer SRKs will need to be programmed in the i.MX 8 fuses.

i.MX 8QX/QM – Algorithms and keys

Algorithms

- RSA – 1024, 2048, 3072, 4096 bit keys
- ECDSA - p256, p384, p521
- SHA-256, 384, 512 bit*
- AES-CCM – 128, 192, 256 bit keys**

* Currently supported: ECDSA-P384 / SHA384 – sole allowed configuration for primary container

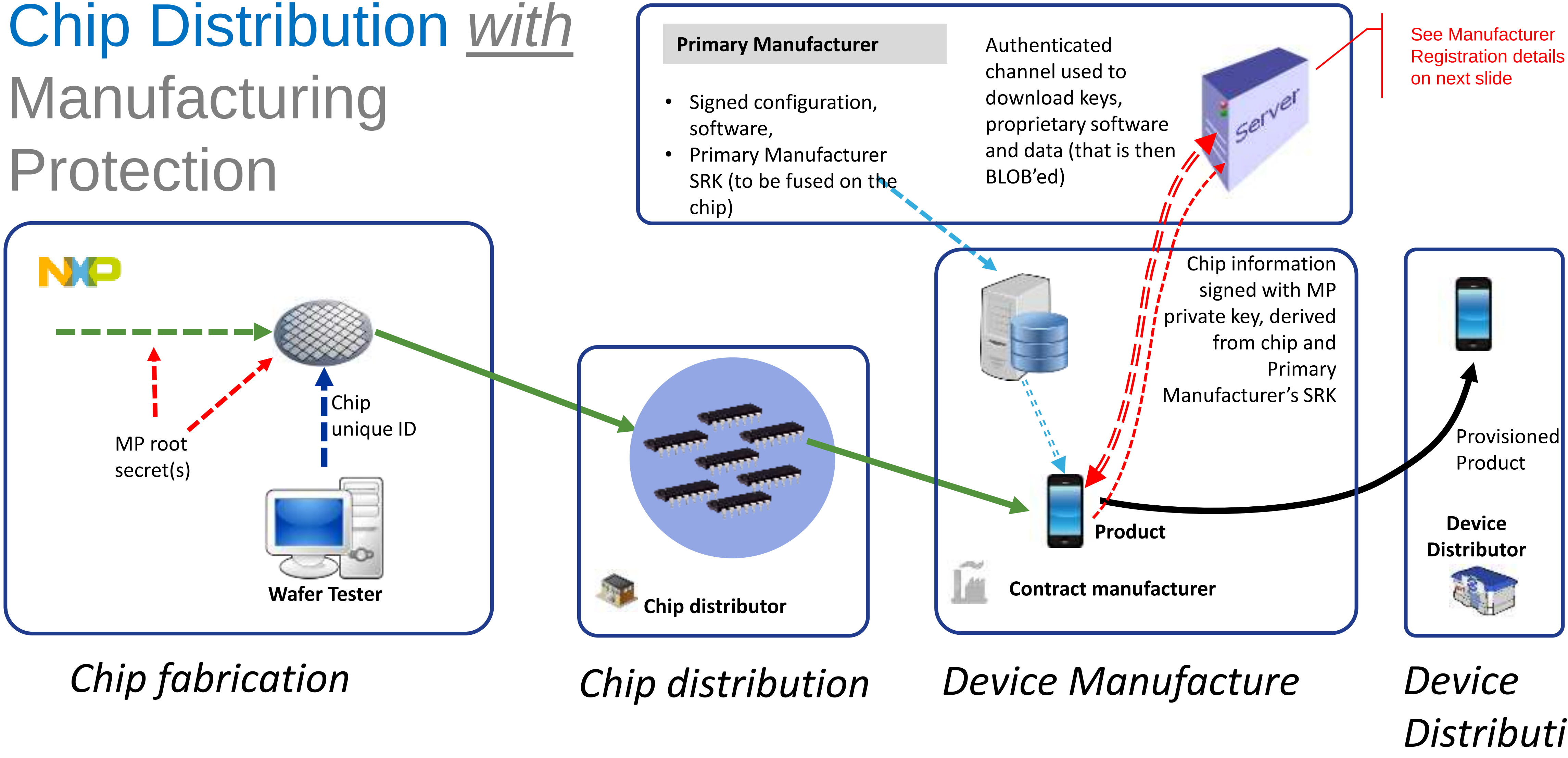
** Not supported for the primary container. Encryption not available in the current versions of the SECO FW.

Keys

- Support up to 4 Super Root Keys (SRKs)
- Any SRK may be revoked
- Hash of SRKs stored in fuses
- The public keys are included in the container
- 2 Root of Trust (NXP and OEM)

Manufacturing protection

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

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

Chip fabrication

Chip distribution

Device Manufacture

Device Distribution

Enablement

Enablement

- BSP
  - Linux and drivers
  - SECO Firmware (NXP signed)
  - SCU Firmware and porting kit
  - ARM Trusted Firmware (ATF)
  - Open Trusted Execution Environment (OP-TEE)

- Tools
  - Image creation tool
  - Code signing tool
  - Manufacturing tool
  - JTAG debug scripts (Lauterbach, ARM DS-5)

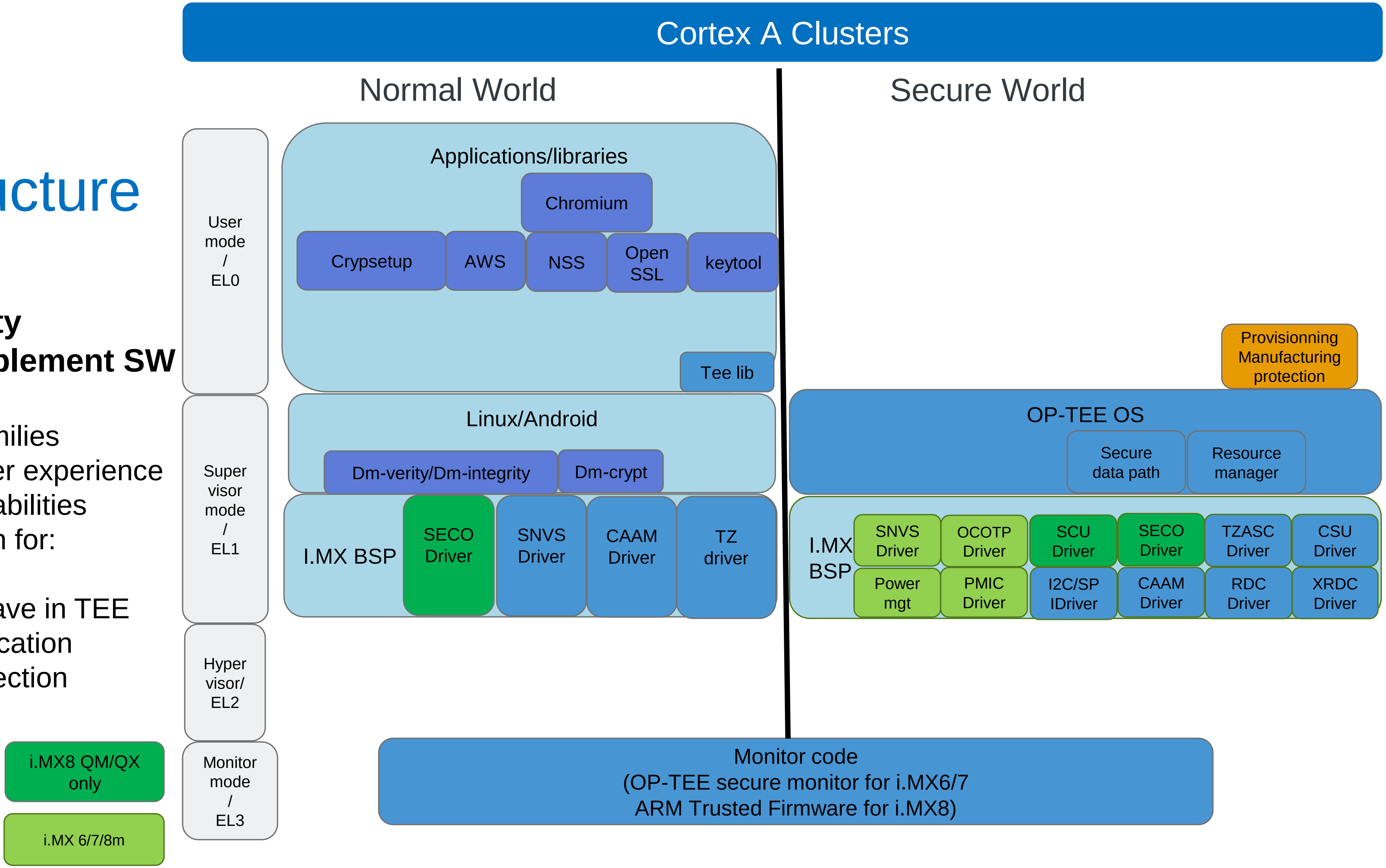
- Documents
  - Security Reference Manual (>1000 pages)
  - SECO FW API (30 pages)
  - SCU FW API (100 pages)

Security Infrastructure

Target:
A solid i.MX security foundation for enablement SW

Unified across i.MX families
Consistent API and user experience
Enables most HW capabilities
Solid secure foundation for:

- Key storage
- Certificate/key enclave in TEE
- IOT device authentication
- Device identity protection
- IP protection



Security MW

Target:

Comprehensive i.MX security architecture

Higher level, industry standard security API provided (PKCS11)

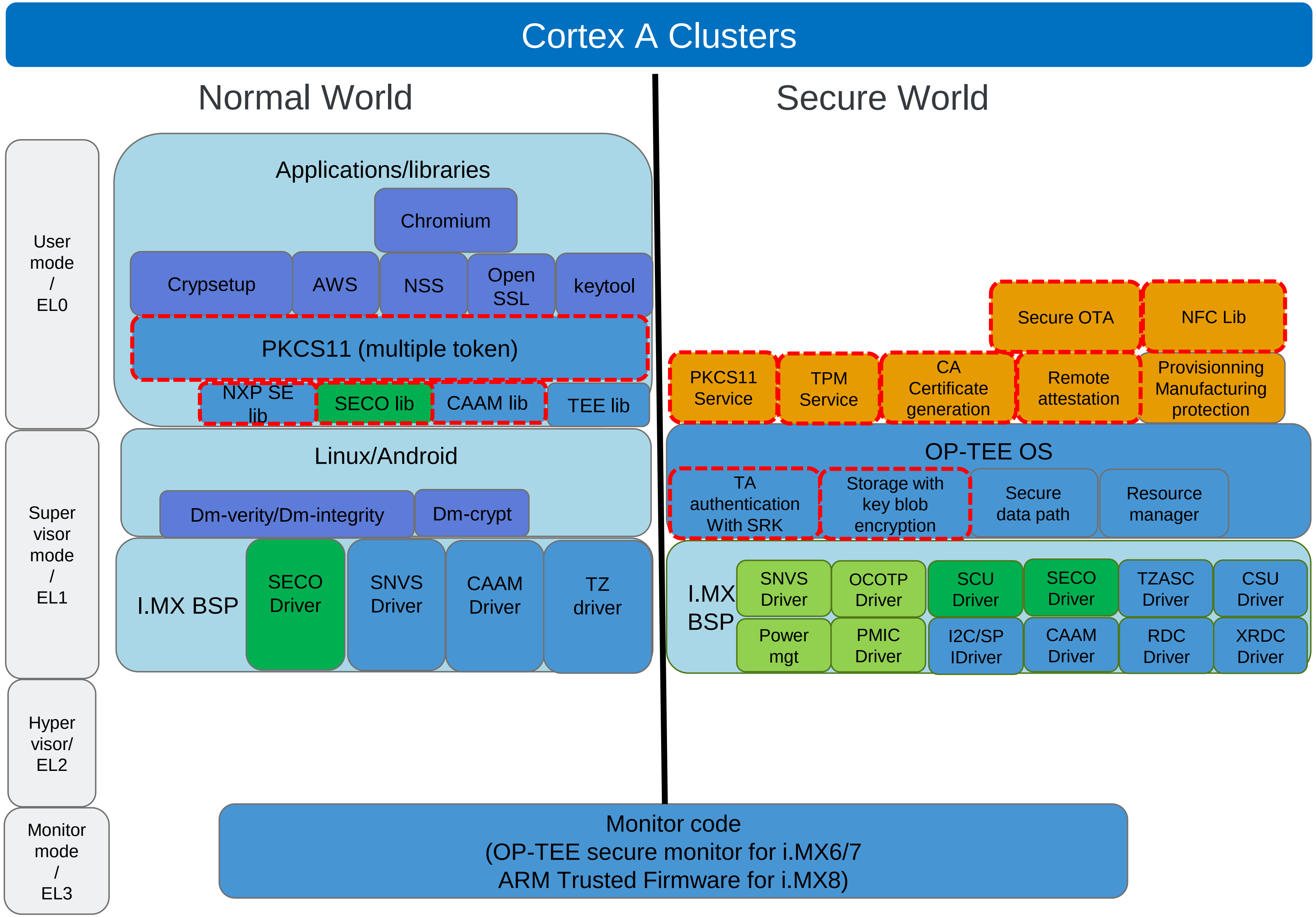
Seamless integration with existing Linux applications
Encrypted storage
Secure Keystore
HSM fully leveraging HW platform
- With CAAM
- With SECO

Extended set of Trusted Apps:
- TPM
- OTA
- Attestation

i.MX8 QM/QX only

Security MW

i.MX 6/7/8m



SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com