AN OVERVIEW OF TRUST FEATURES FOR SECURING EMBEDDED SYSTEMS

ERIC BOST - FAE

22.03.2016

SECURE CONNECTIONS FOR A SMARTER WORLD

Forewords

- Security is key .. isn't it ?
- For reliability, privacy, safety, economics, Intellectual Property ..
- In this session we will speak of **System Security** (not network security) .. how to make a system (more) ''secure''
- When QorIQ processors moved to multicore, NXP identified the need to enrich the SoC with a Security Infrastructure .. what we call **''Trust Architecture''**
- New QorIQ families based on Layerscape architecture (LS1, LS2) combine the NXP-originated Trust Architecture that was already in the P- & T-series with the ARM®-centric TrustZone architecture

AGENDA

- Intro / Background
- QorIQ processors major security components across families
- Trust Architecture (TA) and TrustZone (TZ) in Layerscape architecture.
- Detail of Trust Architecture key components
- Advanced features

System Security – Use Cases

- Handheld / user appliance
  - It is key to isolate a very secure minimal set of functionnalities besides the rich set of illimited applications managed by a full-featured OS (those functions related to user/owner ID, IMEI/SimLock, user interface, sensitive data and actions, DRM ..)

- Networking / infrastructure
  - Network security as key requirement (tunnels, protocols ..)
  - Unlike network security, system security not widely considered a ''must''
  - More and more concerns arising for IP protect, cloning, authentication

- Industrial & critical embedded (transport, avionics, defense)
  - Overall goal is to ensure and monitor deterministic behaviour (for safety & reliabilty)
  - The most sensitive functions incl. those for monitoring must be guaranteed
  - When multiple partitions act on the same system, some form of robust partitioning must be implemented
  - System security required in some cases for IP protect, authentication, tamper protect

Trust Architecture in QorIQ Processors

- Trusted system
  - A system which does what its stakeholders expect it to do, resisting attackers with both remote and physical access, else it fails safe
- NXP Trust Architecture (TA)
  - A set of OEM-controlled HW features + some protocols & SW built on top which simplify the development of trustworthy systems
  - Included for long time and enriched thru several generations of i.MX and QorIQ processors
- ARM® TrustZone (TZ)
  - Both an architecture specification and feature of ARM CPUs processors and IPs
- NXP TA and ARM TZ merged in ARM-based QorIQ LS-series resulting in TA 2.1 and above

QorIQ Processors Trust Architecture in Effect

- While some developers consider security policy enforcement to be a critical feature of the device, other developers may not. Consequently the Trust Architecture is disabled by default. Developers not implementing trust features can ignore their existence.
- Developers who choose to leverage the Trust Architecture are not dependent on NXP to provision devices or sign code. NXP is not part of the system development or manufacturing chain of trust. Developer provisioning of devices is designed to be simple, with minimal impacts on manufacturing cycle times.

On Terminology

- Trust Architecture [TA]
- Trust Zone [TZ]
- Trusted vs secure ?
- Trusted / chain of trust
- Secure world vs non-secure world (& state) [in TZ]
- Trusted Execution Environment - TEE / TrustLet [in TZ]
- Isolation/separation/segregation/partitioning (strong-, robust-)
- Hypervisor – HV
- Secure Monitor [in TA] <> Secure Monitor [in TZ]

QorIQ Processors Trust Architecture in Effect

- **Trusted system**
  - A system which does what its stakeholders expect it to do, resisting attackers with both remote and physical access, else it fails safe

- In the context of the device's implementation of the Trust Architecture, if developers properly leverage the hardware hooks in the device, they can 'trust' that the software they loaded into the system during manufacturing (or during authorized software updates) is the software that executes following system boot.

- Once trusted software is in control, the developer can leverage additional Trust Architecture features to keep the trusted code in control of the system and defend against potential threats.

Question: *Ok, but what is to be considered the "trusted software" in the system? Up to which point?*

QorIQ Processors Trust Architecture in Effect (2)

The security mechanisms within the Trust Architecture allow users to define and enforce security policies. Examples of security policy violations that can be prevented or heavy mitigated by the Trust Architecture are :

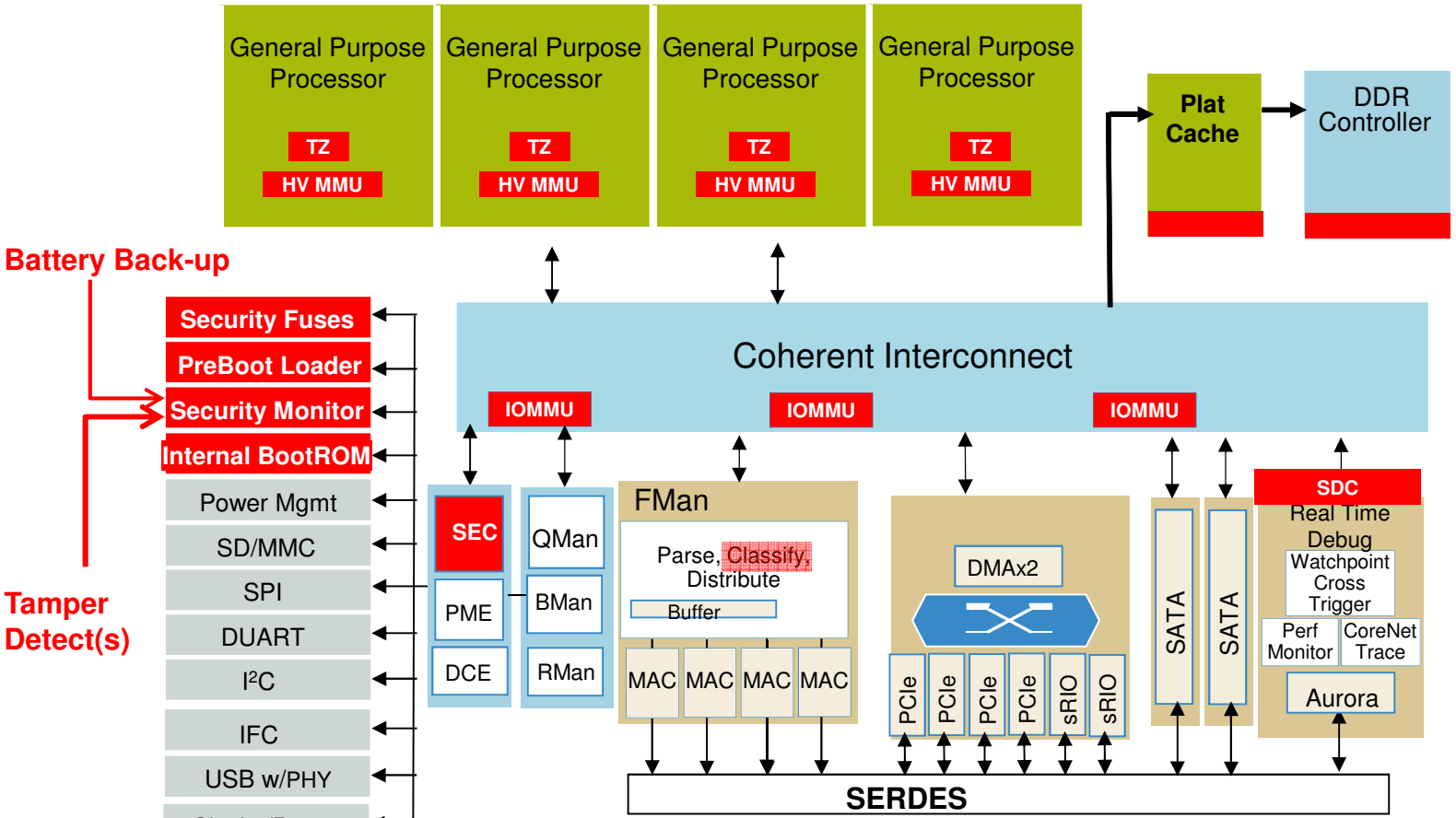
- Unauthorized modifications to developer software and system configuration information (code/data, device trees, certificates). Protection consists of both prevention and after the fact detection mechanisms
- Unauthorized exposure of system persistent secrets. These are secrets that are intended to persist between resets of the system. Trust architecture 2.0 persistent secrets include the chip's One Time Programmable Master Key (OTPMK) and any code, factory installed private asymmetric, and pre-shared symmetric keys encrypted by the OTPMK and stored to non-volatile memory
- Unauthorized exposure of system ephemeral secrets. These are secrets that are intended to be cleared by the system's next reset (or sooner). Trust architecture ephemeral secrets include the chip's Job Descriptor Key Encryption Keys (JDKEKs) and session keys negotiated during normal operation that are encrypted with a JDKEK (also known as, "Black Keys").
- Unauthorized physical external access to the system eg. through debug interface or any tamper
- Accidental or deliberate use of the private resources of one software partition by any other software partition

Note: *on this aspect, some QorIQ processors multicore key architecture features including robust partitioning through MMU + IO-MMU + Hypervisor model are considered a component of the overall Trust Architecture in NXP literature.*

AGENDA

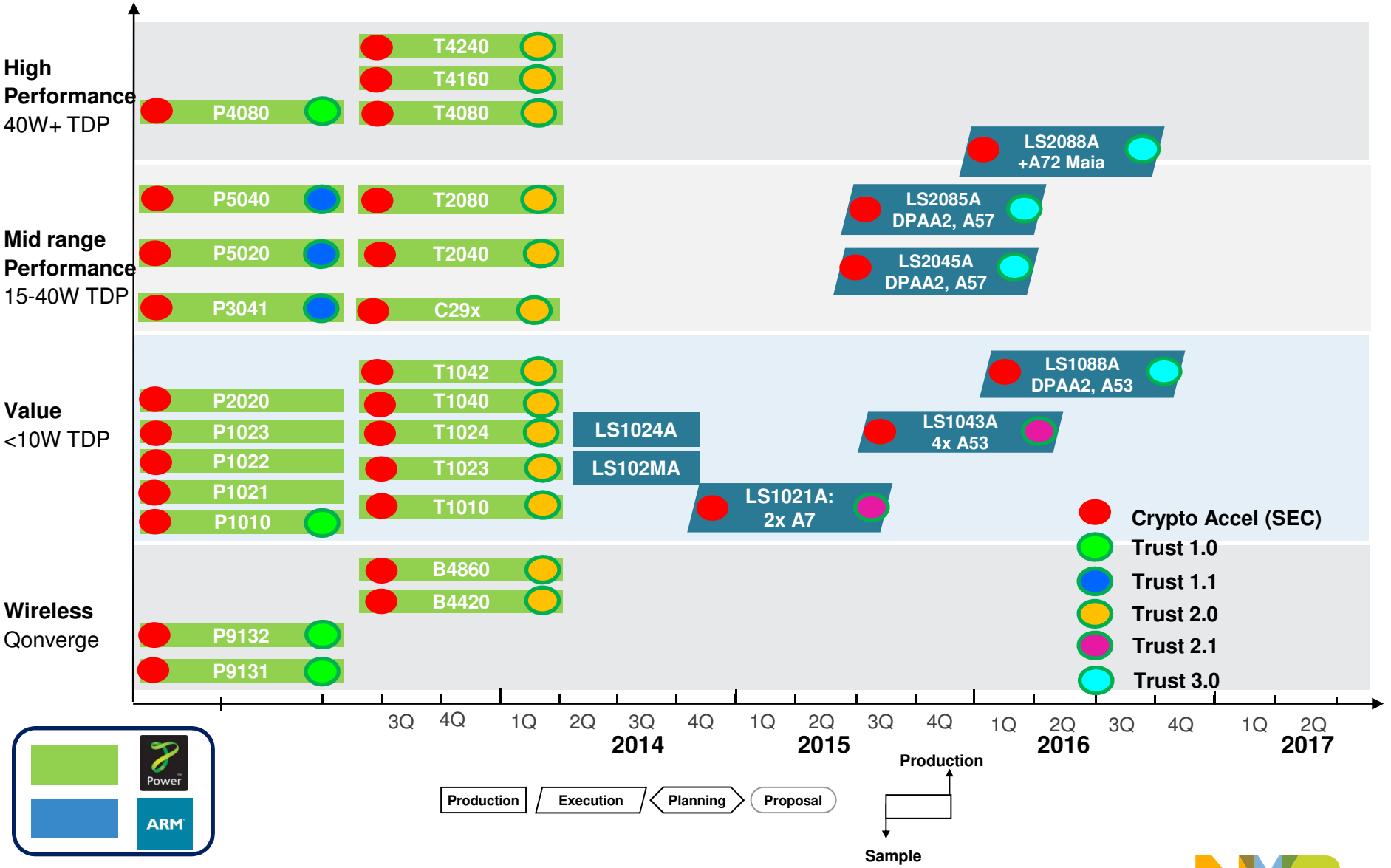
- Intro / background
- QorIQ processors major security components across families
- Trust Architecture (TA) and TrustZone (TZ) in Layerscape architecture
- Detail of Trust Architecture key components
- Advanced features

Where Does Trust Architecture Reside in the SoC ?

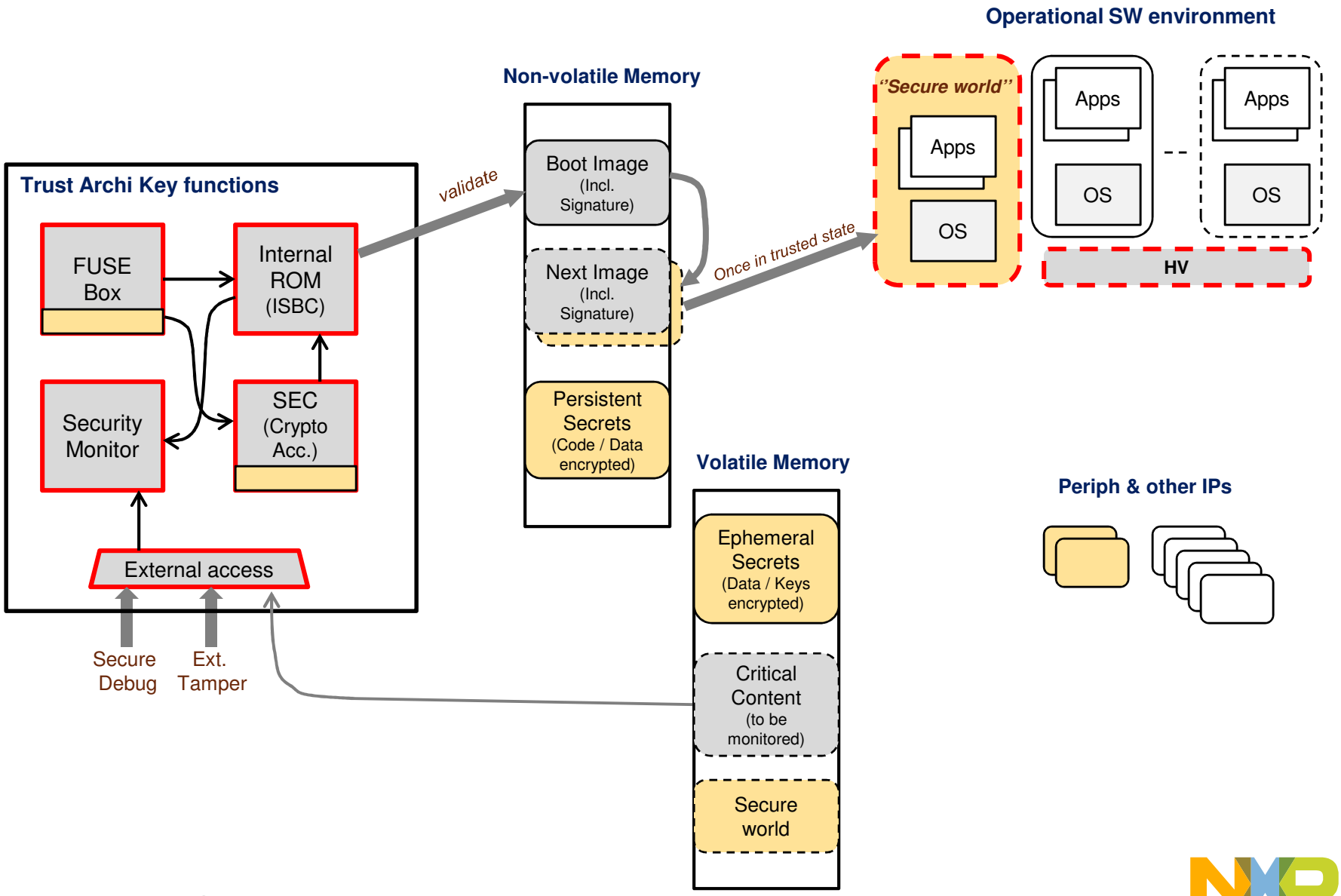


Like for Debug, Trust Architecture is an underlying infrastructure of multiple features spread in the HW

QorIQ Processors Security Features



QorIQ Processors Trusted Platform – Main Components



Trust Architecture – Features Summary

TRUST Version	Trust 1.0	Trust 1.1	Trust 2.0	Trust 2.1	Trust 3.0
Related devices ('E' devices)	**P4080, P1010**	**P2040, P3041, P5020**	**T1040, T2080, T4240, B4860, C290**	**LS1020, LS1043**	**LS2080, LS1088**
Base Features					
Secure Boot	Y				
Secure Boot -offloaded thru SEC (HW accel.)	N		Y		
Secure Debug Controller	Y			Y + TrustZone "Secure World" add'l protections	
Security Fuse Processor (SFP)	Y				
Security Monitor	Y				
Security Monitor Dual-power sections (incl. Key zeroization & ext. Tamper)	N	Y	Y (not in T1 & B4)	Y	
External Tamper Detection	Y				
Real-Time Integrity Checker (RTIC)	Y				
SEC-supported Blobs based on Master Key	Y				
SEC-supported Ephemeral Key Encryption Keys	Y				
CPU Memory Access Control	Power ISA MMU w/HV			ARM ISA MMU w/HV and TrustZone	
I/O Memory Access Control	Platform MMU (PAMU)			Platform MMU (SMMU)	
ARM TrustZone	N			Y	
Advanced Features					
Secure Boot - Alternate (secondary) signed Image	N		Y		
Secure Boot - Key list and Key revocation	N		Y (List of 4 keys)	Y (List of 8 keys)	
Monotonic Counters	N		1 (not in T1 & B4)	1	
HW Key Pair (aka Trusted Manufacturing)	N			Y	

Reference Literature / Spec

- QorIQ processors reference manuals:
  - Chapter *"Secure Boot and Trust Architecture"*
  - Chapter *"Security Engine (SECx.y)"*
- White papers including *QORIQTAWP*: *"An introduction to the QorIQ platform Trust Architecture" and QORIQSECBOOTWP* : *"Secure Boot for QorIQ Communications Processors"*
- *"Manufacturing guide for Trust Architecture" and Code Signing Tool (CST) –* ***under NDA***
- QorIQ processors reference manuals
  (for PAMU, SoC-level partitioning)
- Core (e500mc, e5500, e6500) reference manuals
  (for Hypervisor model, MMU, Core-level partitioning …)
- ARM® Datacenter (for ARM related incl. Trust Zone)
- NIST crypto algorithm validation program certificates for Digital Networking products
- Export control summary sheets (ECCN, CCATS, algorithms, key lengths)

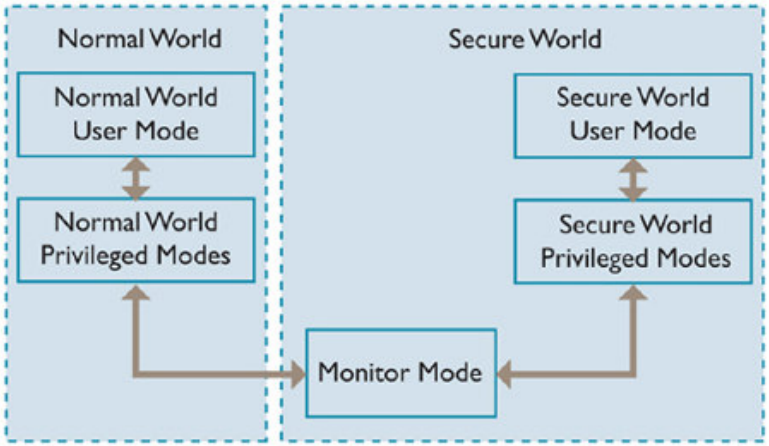
AGENDA

- Intro / background
- QorIQ processors major security components across families
- Trust Architecture (TA) and Trust Zone (TZ) in Layerscape architecture
- Detail of Trust Architecture key components
- Advanced features

Trust Zone Concept/Foundation

- Developed 10 years ago as a versatile & flexible trust platform module vs previous more specific TPM solutions
- Initially targeted to ARM® Cortex® -A main market eg. mobile devices
- Trust Zone uses a hardware-enforced security domain in order to systemize the implementation of secure systems.
- Typically, a device will run its rich conventional OS, like Linux or Android, in the **normal world**, while running a small vendor specific secure OS and its applications in the **secure world**
- Typical secure applications:
  - Secure PIN entry
  - SIMLock security
  - Terminal identity
  - Over-the-air reprogramming
  - Managing content
  - Virtual Private Networks
  - Digital Rights Management (DRM)

Trust Zone – Principles



- The ARM® GPP execution modes are divided into two “worlds”, secure and non-secure.
- The secure world is enforced by HW at core, interconnect and SoC IPs such that resources allocated to secure world are unvisible from non-secure world, whatever the execution level
- Monitor Mode is an intermediate mode executing code switching between worlds
- SW running in secure world can range from very simple services to more complex dedicated secure world OS + apps
- Switching between modes can be initiated by instruction or interrupt
- Secure world allows strict containment of system secrets and system security related services, providing services to non-secure world via a well-controlled single point of entry.

***Questions**: How is secure world software secure? Can normal world be secure?*

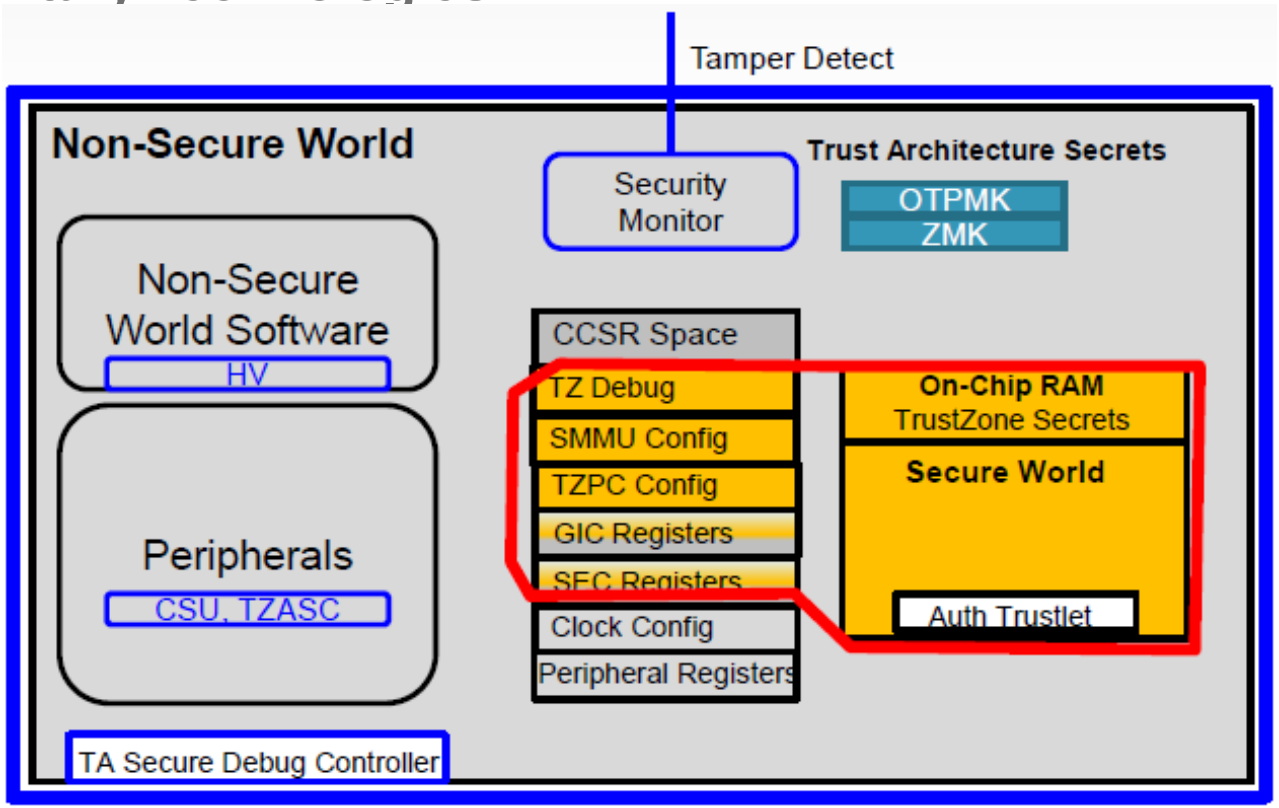
Trust Zone Hardware - Principles

At HW level, Trust Zone is enforced at several physical blocks/IPs

- At ARM® core: execution context, registers banking and a few extra instructions for switching between secure/non secure (S/NS) world
- The AXI bus adds an extra ‘’address’’ signal (NS) to differentiate between trusted and non-trusted requests. Every SoC I/O block connected to the AXI has to respect this signaling
- At SoC level some access control mechanisms for setting security access permission, acting as firewalls for the various SoC ressources.
  eg. TrustZone Address Space Controller (TZASC), Trust Zone Protection Controller (TZPC), Central Security Unit (CSU in LS102x)

Trust Architecture + ARM® Trust Zone

Complementary Technologies

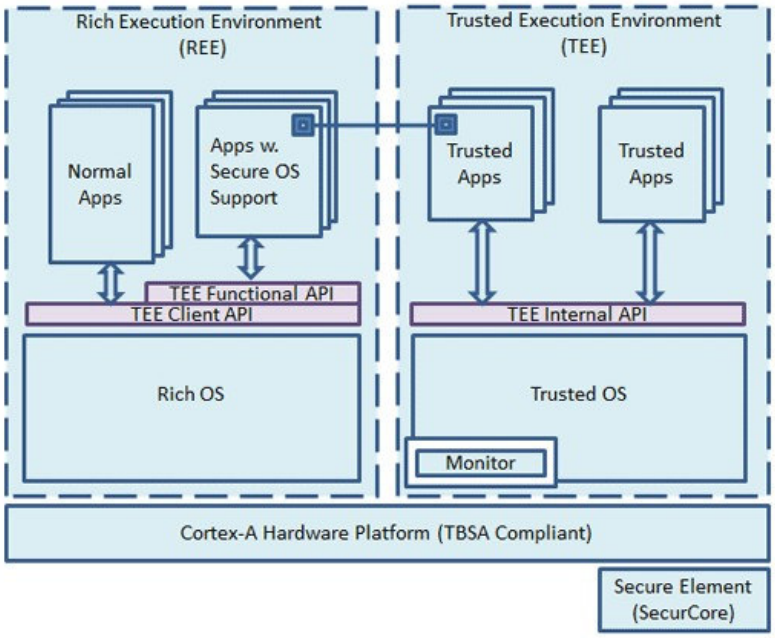


• **Trust Zone** provides an inner keep for especially trusted software, it doesn't protect the whole SoC, it defends the secure world /TEE

• **Trust Arch** provides a secure perimeter for trusted software across the whole SoC

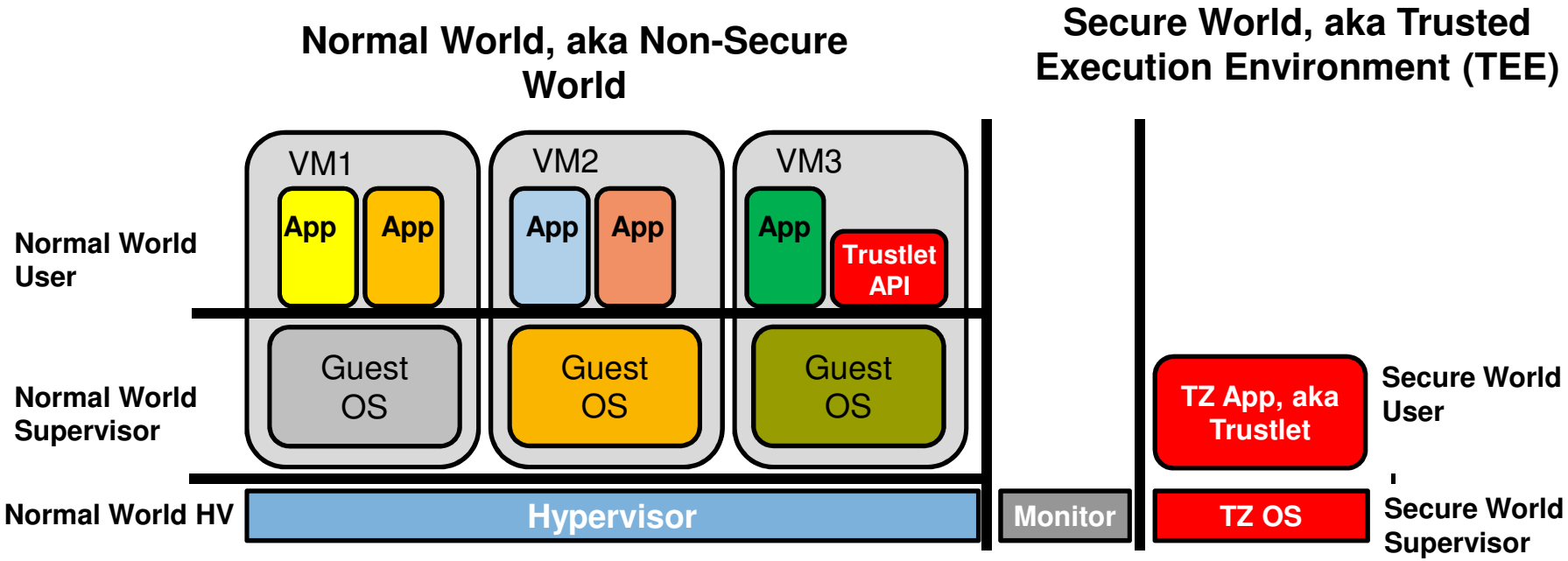
TrustZone - TEE Model

Showing a single core / single REE platform



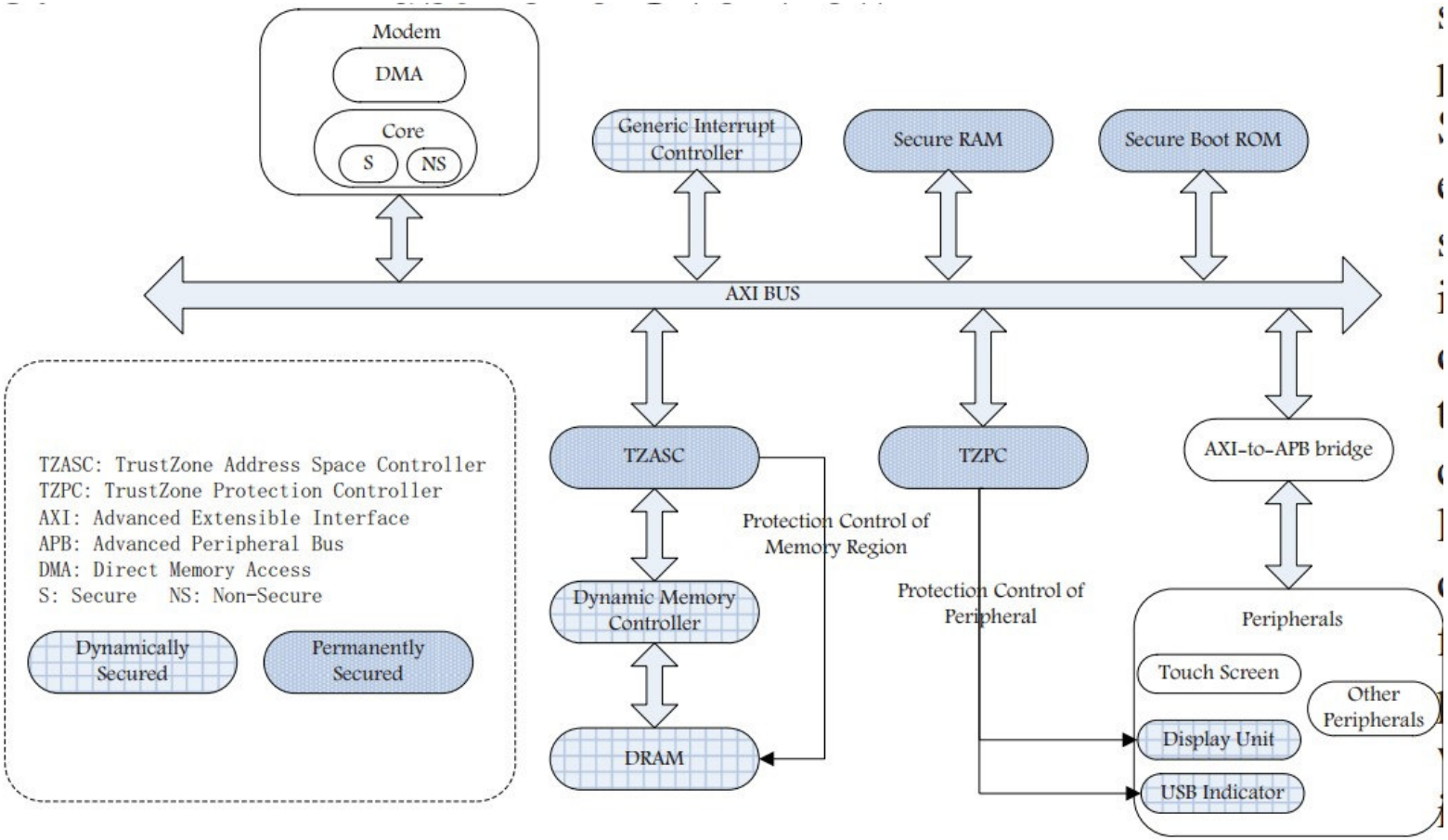
- Some standardized and generic software API (eg. ARM® TZAPI) has been developed to define interfaces between client applications in the NS-world and services from the TEE.
- Among API features:
  - Applications authentication
  - Query of available secure services
  - Secure data exchange and sharing

TA+TZ in Multicore / Multi-Partition Context



Hypervisor not required, non-secure world can be single OS.

Trust Zone Hardware



Considerations on TA,TZ, HV in Multicore SoC (1)

- Use Trust Architecture Secure Boot to secure/authenticate those SW entities that need to be trusted. If TZ is implemented for secure/non-secure world, this should include the TZ secure world SW.

- TZ architecture has been designed for and supports a one-level of asymetric partitioning with one very trusted partition and .. the rest.

- Depending on the type of SoC (single/multicore) and use case, the rest can range from very simple to more sophisticated models with their own security concerns

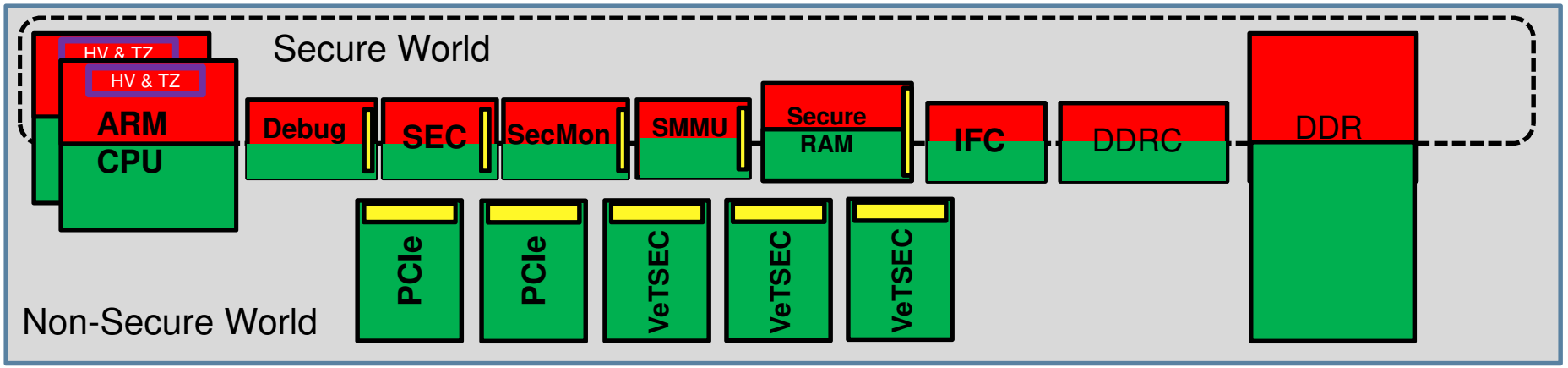
Considerations on TA,TZ, HV in Multicore SoC (2)

- Multi-partition implementation with rich-set partitions allowed by multicore SoCs is better supported through HV architecture and related built-in protections and virtualization means (eg: 3-level hierarchy, MMU + IOMMU)

- Use Trust Architecture toolbox and/or leverage some Trust Zone TEE functions to ensure the whole system keeps trusted during operation … no magic here, two different & complementary approaches

- Secure debug restriction can be implemented through TA and/or TZ

Trust Architecture with Trust Zone



ARM® Terminology

Secure, secure world – A parallel execution environment, isolated from normal, non-secure world software. ARM CPUs come out of reset running in secure world.

Non-secure, Non-secure world – SW running in any mode other than TZ (HV, Guest, User)

Trusted Execution Environment – (TEE), the Trust Zone RTOS & Monitor. The TEE + trustlets make up secure world.

Trustlet –
An application running in the TEE. Trustlets have access to the crown jewels, and have been developed for digital wallet, DRM, and device authentication.

Trust Architecture Terminology

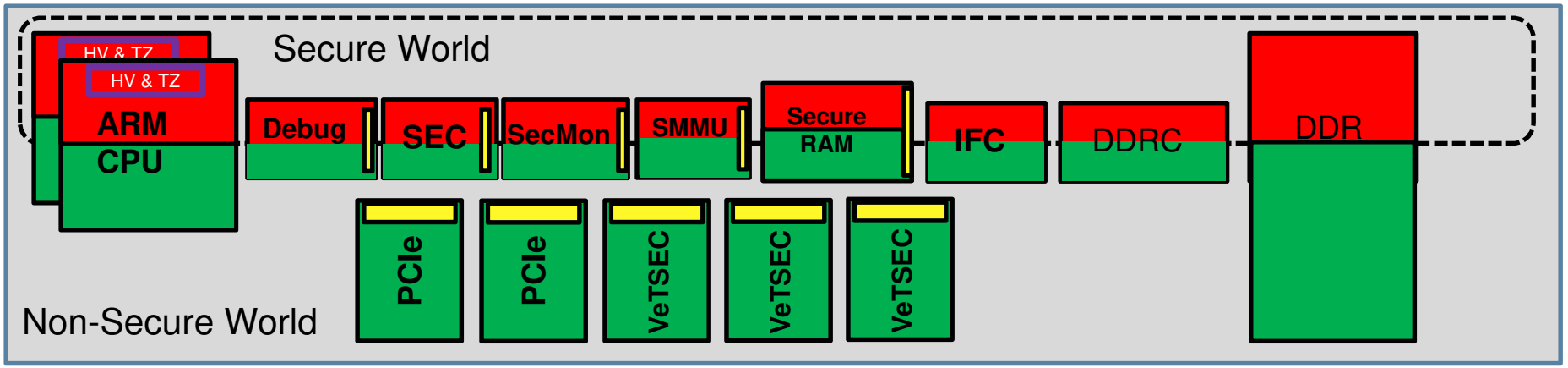
Secure – State of the HW SecMon in which trusted software can tell the SEC to use the crown jewels.

Non-secure – State of the HW SecMon in which software can't tell the SEC to use the crown jewels (SW is untrusted).

Trusted – SW which has passed secure boot validation is trusted to tell the SEC open the treasure chest.

Trusted/Privileged – SW which, in addition to being trusted to do its normal applications, is allowed to access Trust Arch HW registers.

Who Trusts Who?



Can ARM® Non-Secure World be Trusted?

• QorIQ processors secure boot validates the ARM TEE (Red), plus Hypervisor & Guest Oses (Green) which run in non-secure world. From the QorIQ processors HW Security Monitor's perspective, the validated SW running in non-secure world is as trusted as the ARM TEE to command the SEC to use the secret key. But Trust Zone access protections will stop green from accessing red resources, despite green being trusted.

Can ARM Secure World be untrusted?

• ARM CPUs come out of reset in Secure World. The SW running on secure world doesn't have to be validated, and consequently, the QorIQ processors HW Security Monitor doesn't trust it. Even if the secure world software is successfully validated, if a hardware security violation is detected, the whole SoC and all software is considered untrusted (Fail state).

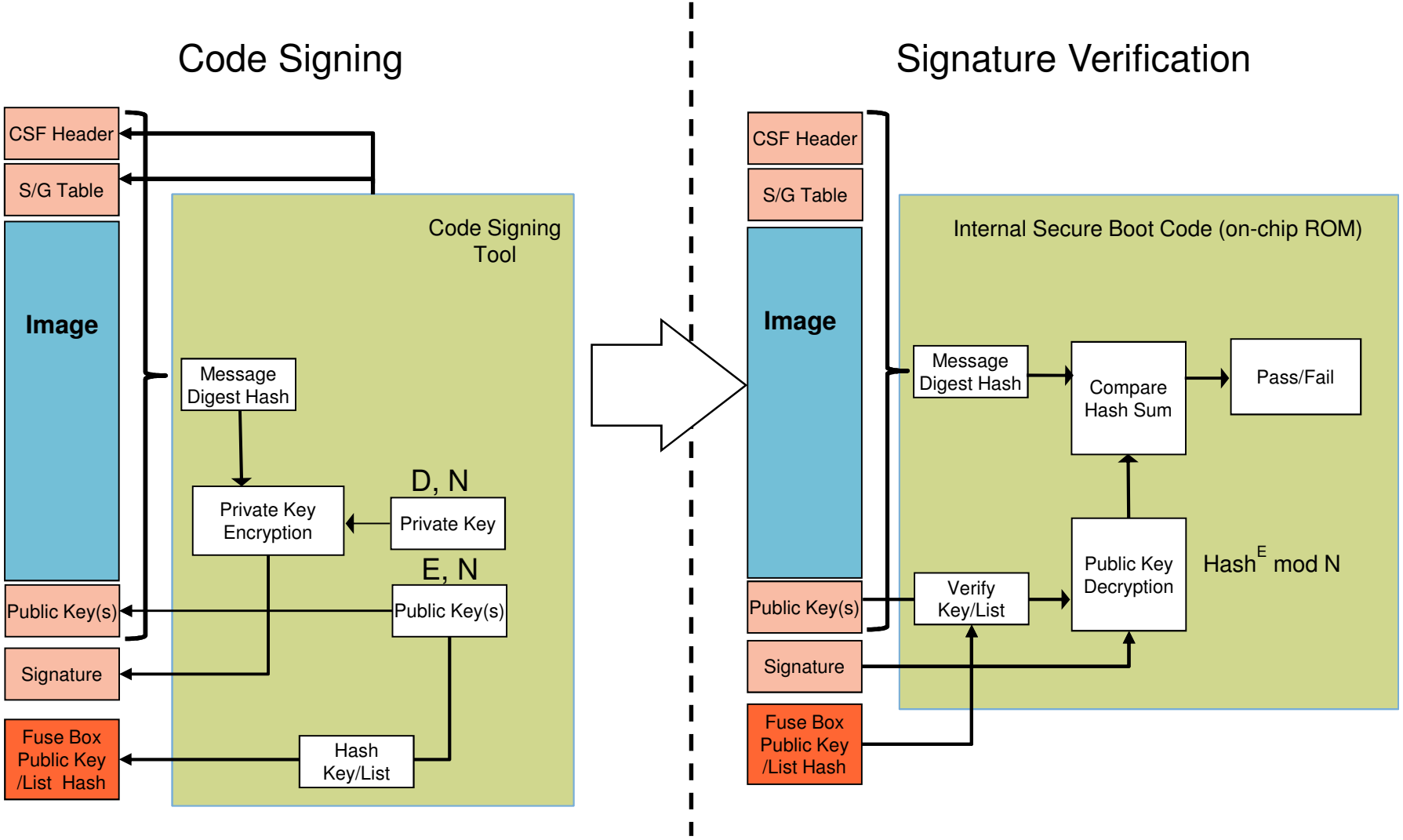
AGENDA

- Intro / background
- QorIQ processors major security components across families
- Trust Architecture (TA) and Trust Zone (TZ) in Layerscape architecture
- Detail of Trust Architecture key components
- Advanced features

Secure Boot – in Principle

- Optional Secure Boot implemented by OEM (enabled thru ITS or SB-EN)
- Boot validation performed by running Internal Secure Boot Code (ISBC) provided by NXP in internal ROM.
- Principle:
  - At **manufacturing**, External boot code is signed by OEM : Hash value calculated thru SHA-256 on boot image, secured (encrypted) with RSA Private Key and appended to boot in external non-volatile memory.
  - In **operation**, at boot time, ISBC (in internal ROM) validates the boot image by decrypting signature with public key, recalculating hash value on boot image and compare to hash value from signature.
  - Public key itself is kept in internal fuses (in fact just a hash of it)
  - Any mismatch fails booting in secure mode

Secure Boot – in Action



Question:

- *Any risk if OEM is not manufacturer?*

Secure Boot – a Few More Things and Q&As

- Using secure boot requires some pre-boot Initialization (PBL) at least for loading an ESBC pointer to the SCRATCHRW1 before ISBC starts executing from core0.
- If ISBC 1st stage secure boot succeeds, what happens?
  - If no further boot and validation required, then enters ‘’Trusted’’ state and the SEC is allowed to use the provisioned keys OTPMK, ZMK, and secret KEKs.
  - If next is ESBC with trusted bootscript and bootloader, then next stage image is validated as in previous stage
- If ISBC 1st stage secure boot fails, what’s next?
  - Can optionally validate an alternate boot image
  - Transition Secure Monitor to either soft or hard failed state leading to either reduced security usage mode or leading to hard reset
- On QorIQ ARM® -based LS-series, the ISBC and ESBC run in Trust Zone secure world

Questions:

- *Until which point do we need to secure?*
- *Can other TA features (eg. secure debug, RTIC, Blobs) be implemented without implementing secure boot? In that case, what happens if there is a HW security violation?*

Chain of Trust

Secure boot can validate several non-contigous memory ranges and can chain several validation sequences

ESBC U-Boot can be written to use the SEC to decrypt some or all of the client. Portions of the client could be decrypted back into main memory, while particularly sensitive code or data could be decrypted into internal SRAM.

Security Fuses

(Showing QorIQ T1040 case)

In RED not readable

FSL Section fuses

- 1b - FSL section write protect
- 32b - FSL unique ID
- 64b - FSL scratchpad
- 32b - FSL CRC

OEM Section fuses

- 1b - OEM section write protect
- **1b - Intent to secure**
- 1b - Clear_SFF
- 1b - **SEC disable**
- 4b - Key0-2 revocation
- 3b - Debug permissions
  - Open
  - Conditionally closed w/o notification
  - Conditionally closed w notification
  - Closed

(for secure boot)

- **256b - Super Root Key Hash (hash of Public key)**

(for secure debug)

- **64b - Debug challenge value**
- **64b - Debug response value**

(for long-term keys & data protection)

- **256b - One time programmable master key (OTPMK)**
- 32b - OEM unique ID
- 64b - OEM scratchpad
- 32b - OEM CRC

Generated by SEC at each boot, not in fuses

(for short-term session keys protection)

- **256b - Key Encryption Key (KEK)**

Internal Fuses

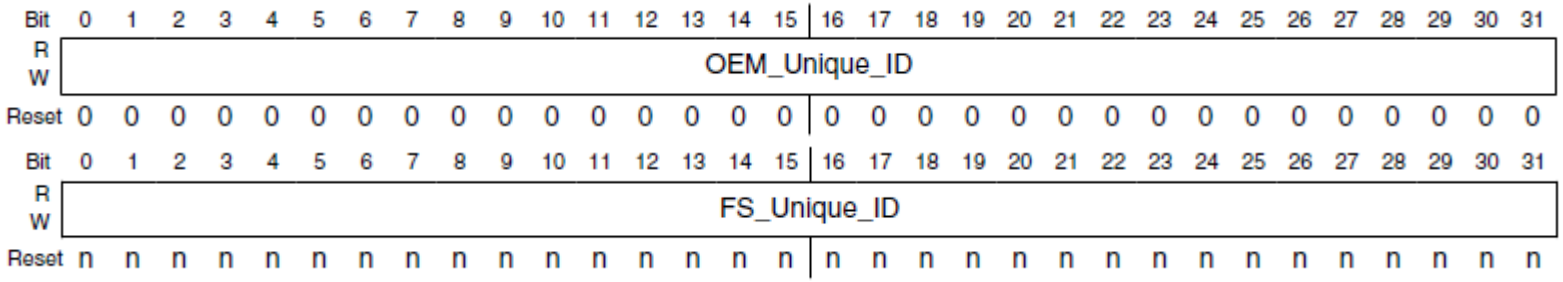
- Includes NXP and OEM sections. Sensitive content cannot be read, modified or scanned-out

- OEM section burned during device provisionning through SW + external pin powering or through debug control interface

- Holds secret values used for secure boot and further ‘’chain of trust’’, including:
  - **ITS** (Intent to Secure) bit which enforces secure boot through internal ROM code (ISBC)
  - **OTPMK** (One Time Programmable Master Key): a 256bit key to be used by the SEC as an AES key. Primary purpose being encryption/decryption of additionnal session keys further used by the SEC to protect data.
  - **SRK (**Super Root Key): a 256bit SHA-256 hash of the RSA public key that is used by the ISBC (Internal Secure Boot Code) to validate the ESBC (External Secure Boot code). The full SRK is included in the ESBC; ISBC first hash and validates it with regard to the fused SRK-Hash.

- Holds other key fixed values:
  - Debug access permission & challenge/response values, OEM unique ID, fuse values checksums, scratchpad values, NXP unique ID, SEC disabling

On NXP and OEM Unique ID Fuses



Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
R W	OEM_Unique_ID																															
Reset	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
R W	FS_Unique_ID																															
Reset	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n

• The **OUIDR** is set by OEMs to configure an unalterable 32-bit software readable value which can be (optionally) included as part of the ESBC for the purposes of digital signature validation. It is up to the OEM to determine whether each device is provisioned with a truly unique ID.
• The **FUIDR** is set (and write protected) by NXP prior to device shipment to provision a pseudo-random software readable value.
• Note that to bind an image to a specific device, the FUIDR must also be included in the ESBC for digital signature validation. Otherwise it would be possible for an attacker with access to a new chip to program the OUIDR to match the value found in a fielded chip.

Security Fuse Processor & Battery Backed Storage

(Showing LS1020 case)

In RED not readable

NXP Section
1b - NXP Section Write Protect
1b - Clear_SFF (disable Scan)
64b - NXP Unique ID
32b - NXP Scratchpad 0
32b - NXP Scratchpad 1
32b - NXP Scratchpad 2
256b - NXP Secure Mfg Key Split

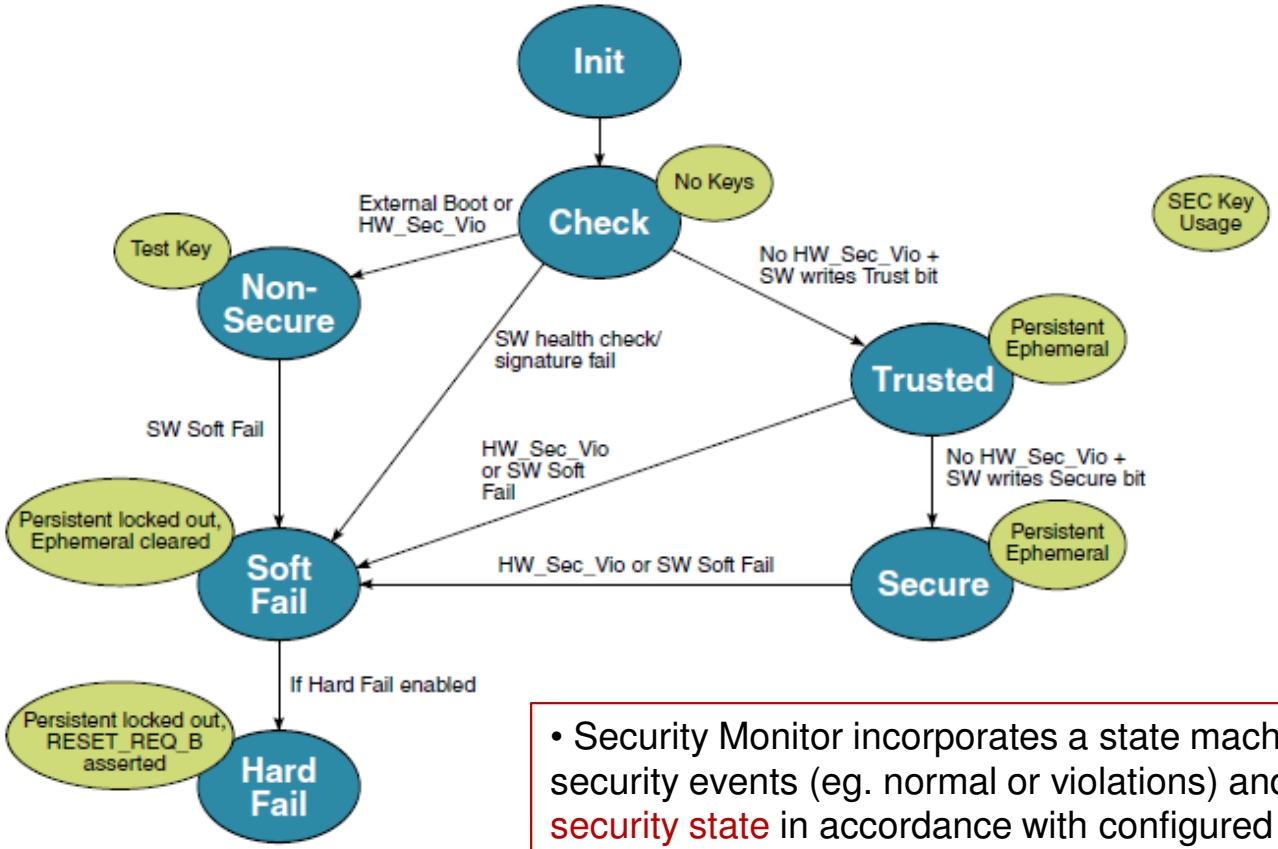
Battery Backed Section (OEM)
256b – Zeroizable Master Key
128b - Scratchpad 0-3 (configurably zeroized)
48b – Monotonic Counter

OEM Section
1b - OEM Section Write Protect
1b - Intent to Secure
1b - SEC disable
6b - Key Revocation
16b - 16 'era' bits for BB monotonic counter

2b - Debug mode
Open
Conditionally closed w/o notification
Conditionally closed w/ notification
Locked

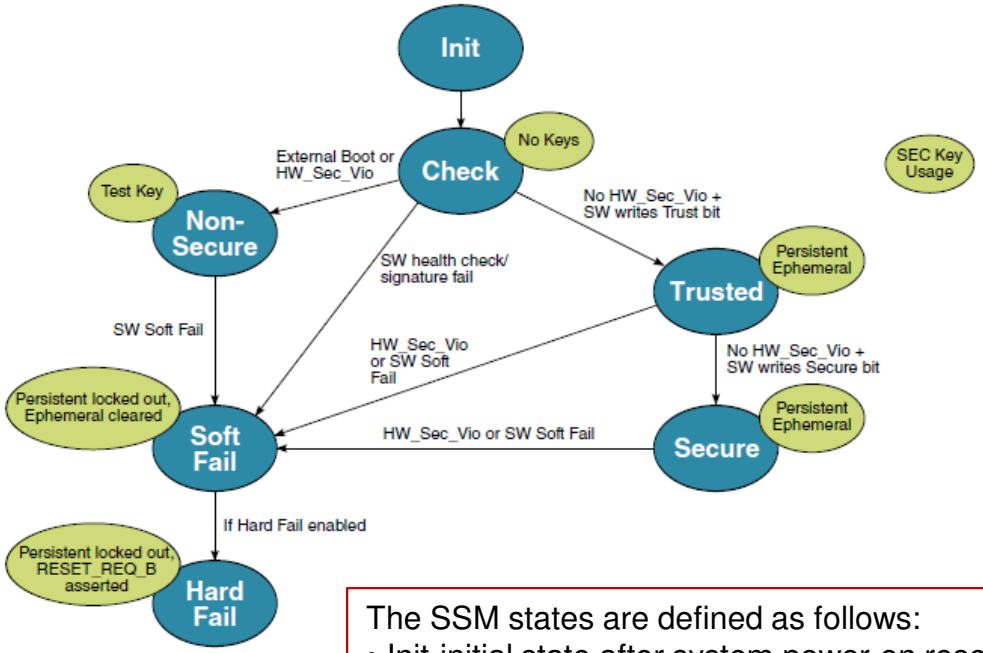
256b – Super Root Key (List) Hash
64b - Debug Challenge Value
64b - Debug Response Value
256b - One Time Programmable Master Key
32b - OEM Unique ID
32b - OEM Scratchpad 0
32b - OEM Scratchpad 1
32b - OEM Scratchpad 2
32b - OEM Scratchpad 3

Security Monitor



- Security Monitor incorporates a state machine (SSM) that detects security events (eg. normal or violations) and manages the system security state in accordance with configured security policy.
- On some QorIQ processors (all except P4, T1, B4), a portion of the Security Monitor can operate on battery power while the rest of the SoC is powered off.
- Once in the trusted/secure state, the SecMon provides ongoing monitoring of the QorIQ processor's security, with security violations causing configurable actions ranging from master key lock-out or zeroization to full SoC reset.

Security Monitor



The SSM states are defined as follows:
- Init-initial state after system power-on reset
- Check-system performs security checks
- Non-secure (functional)-system operates in non-secure state
- Trusted (functional)-system operates in trusted state
- Secure (functional)-system operates in secure state
- Soft fail-security violation/tamper was detected. The system state may be unpredictable. Access to persistent and ephemeral secrets locked out, zeroization of secrets within the SEC.
- Hard fail-system hard reset is requested. All behaviors of Soft fail, plus zeroization of some SoC caches and main memory, SoC reset initiated.

trusted, **secure**, and **non-secure**, are considered functional states.

Security Monitor - Security Violation Sources

- Hardware:
  - External Tamper Detection via TMP_DETECTs
  - Secure Debug Controller (if set to Conditionally Closed with Notification)
  - Run Time Integrity Checker
  - Security Fuse Processor
    - On fuse array read fails, including hamming code check
  - Security Monitor (OTPMK hamming code check)
  - All sensitive flops upon detection of scan entry (expert mode debug)
  - Monotonic Counter Rollover
- Software:
  - Internal Secure Boot Code
  - Trusted U-Boot
  - Any SW with write access to the Security Monitor can declare a security violation.

Security Violation Response

The response is configurable.

- Soft Fail
  - Persistent device secrets are locked out
  - Ephemeral device secrets (if in use) are cleared
  - All SEC registers containing sensitive data are cleared
  - Sec_Mon generates IRQ.
- Hard Fail
  - Fatal security violations start a High Assurance Counter, when counter reaches zero, the device initiates soft fail consequences plus:
    - Battery backed device secret and non-secret values are cleared
    - Active zeroization of the device platform caches and system main memory, while concurrently triggering the RESET_REQ signal.
    - System designer must ensure that the RESET_REQ output signal triggers a device reset (HRESET or PORESET).

External Tamper Detection

QorIQ processors Trust Architecture enables an OEM to add **external tamper detection circuitry** to the system, such as:

- Access-panel-open switch
- Light sensor inside the electronics chassis
- Voltage out of range

… and route an event signal from this external circuitry into the Sec_Mon by means of a dedicated signal **TMP_DETECT**.

If this input signal is interrupted, the Sec_Mon **transitions to a non-secure or soft fail state** preventing the system from decrypting secrets that were previously protected by the OTPMK or KEK while in the secure or trusted states.

Secure Debug Controller

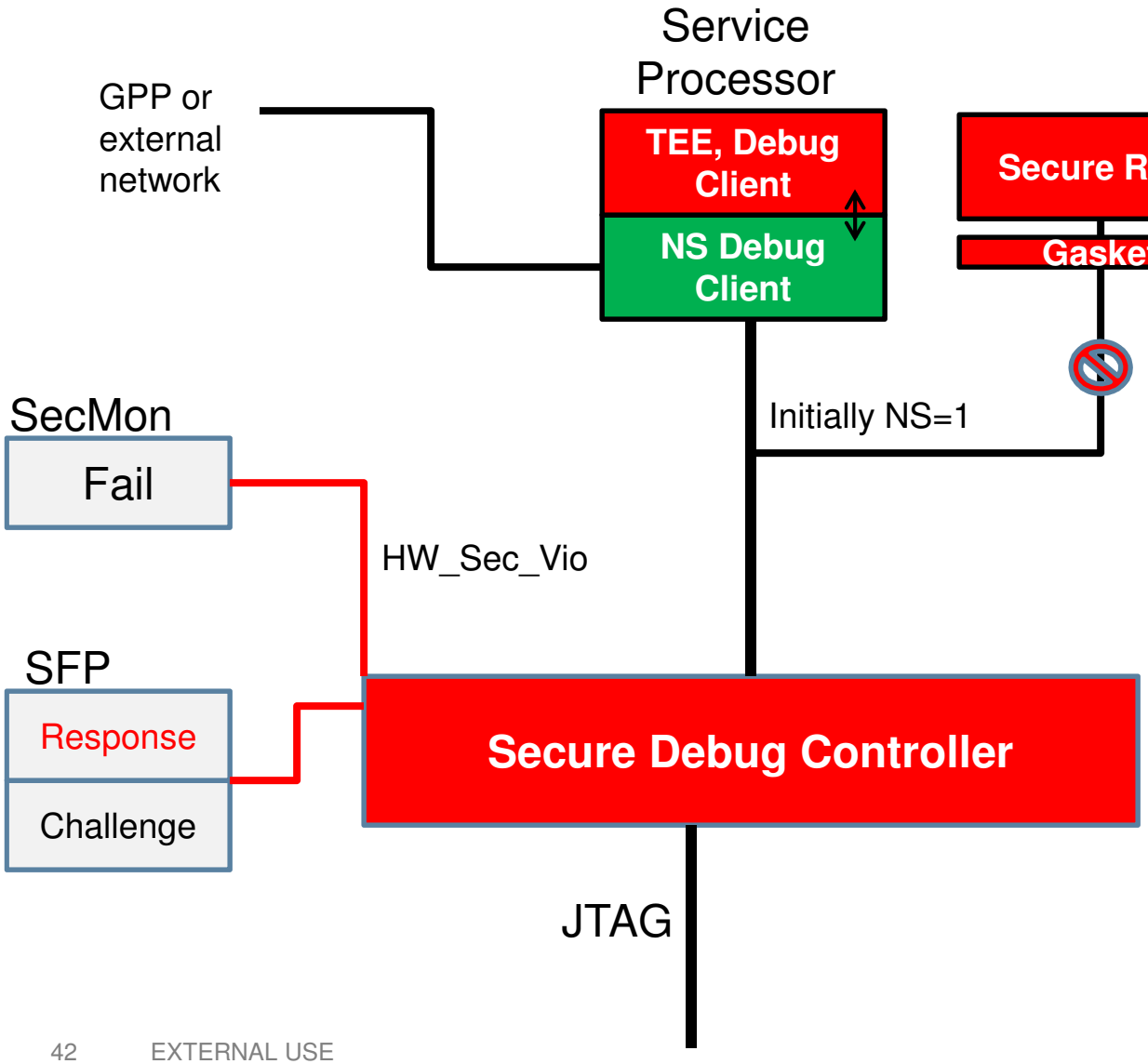
OEMs can control the level of debug access available to external debuggers. The Secure Debug Controller supports 4 levels of access.

- **Open:** external debug agents connected to the Aurora or SAP/JTAG interfaces have full access to P4080 memory space. Activation of debug is not considered a security violation, and if the Sec_Mon is in Trusted/Secure state, it will remain there. This setting is appropriate to secure system in a lab environment or for non-secure system.

- **Conditionally Closed:** (with or without Notification): External debug agents are blocked until successful challenge/response sequence. 64b response value compared to secret value in the security fuse processor.
  With/without notification refers to how the system continues or not to operate if challenge/response fails, with OTMK and KEK usage enabled or disabled.

- **Closed:** attempts by external debug agents to access P4080 memory space are always blocked, and are not reported as security violations. The JTAG interface can still be used for boundary scan physical interconnect testing.

Secure Debug
(case of LS devices with TA+TrustZone)



Once beyond HW secure debug (and depending on configuration), external debugger can perform Trust Zone signature based authentication to TEE/Secure World Debug Client, which can give SDC secure world access, or access secure world registers itself.

.

Hardware challenge/response and violation control methods for HW debug interfaces.

Low Power Domain

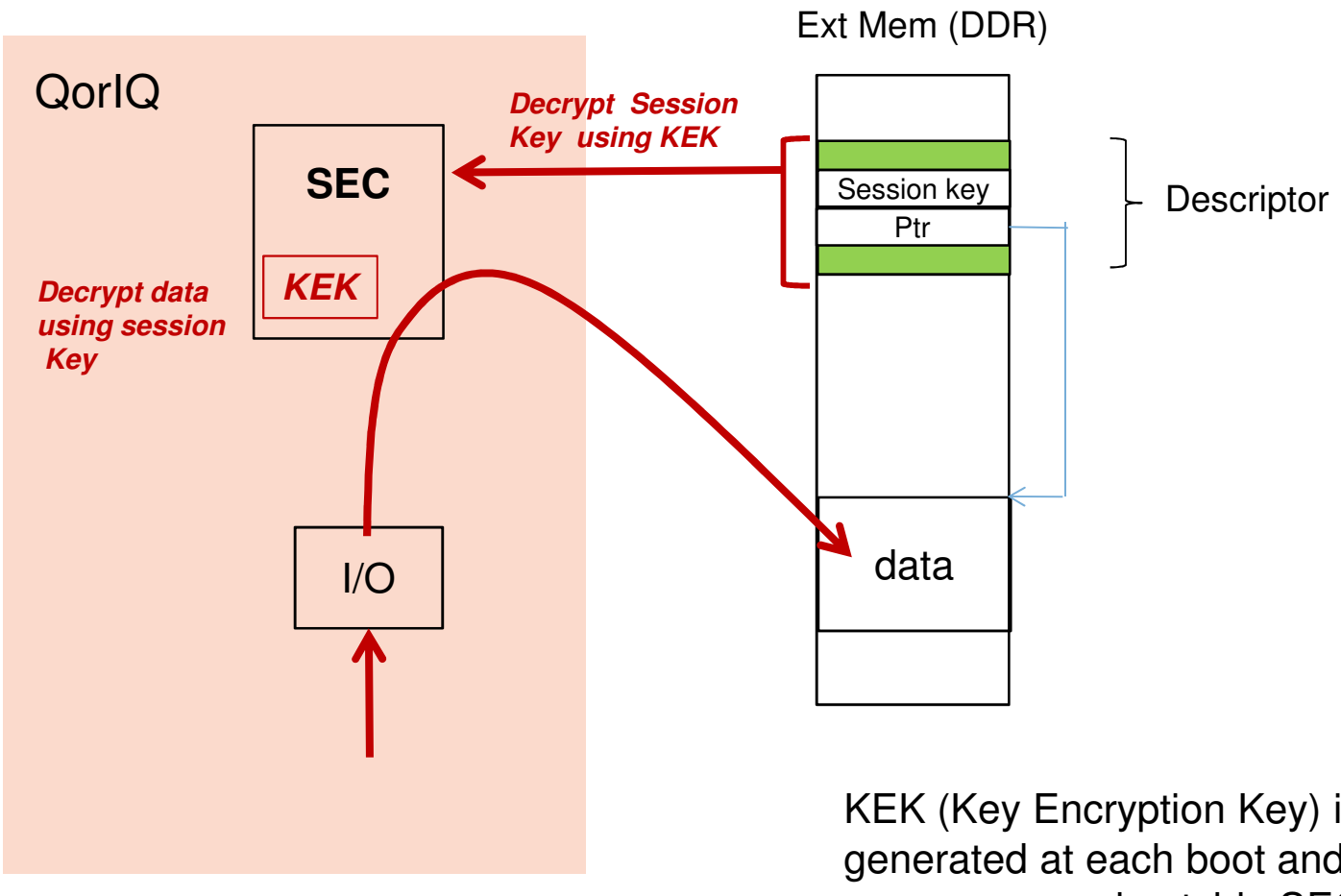
Available in all QorIQ processors from P3/P5 except T1 & B4

- Implemented through **two separate voltage domains** (SM_LP and SM_HP)
- SM_LP is typically supplied thru battery, this is a separate always-powered-up domain with its own power supply. Its purpose is to store and protect system data and enforce security regardless of the main system power state .
- There is an option for a battery backed Zeroizable Secret Key (ZSK) which can be used instead of the OTPMK in the security fuses. On a security violation, rather than being locked out until the next successful secure boot cycle , the ZSK is zeroized. Anything encrypted with the ZSK is unrecoverable, potentially including encrypted part of system software This significantly raises the consequence of a security violation.
- A secondary external tamper detection input is featured for when the QorIQ processors device's main power is off.
- On QorIQ LS, low power domain adds more advanced features (eg. monotonic counter)

Sensitive Data Protection

- Trust Architecture provides support for protection of internal and external storage of developer-provisioned sensitive instructions and data. Implemented through SEC assistance + some externally protected key
- **Long-term secrets** = code/data/key in non-volatile memory, decrypted for use in on-chip memory, do not change accross boot
  - Ex: system private keys, pre-shared session keys, certificates , sensitive data …
  - Principle: data + assoc. key stored externally (notion of **Cryptographic Blob**) , key itself is encrypted with a AES key derived from either OTPMK or ZMK, decrypted directly in the SEC without being ever exposed unencrypted externally.
- **Short-term secrets** = code/data/key in external volatile memory, change accross boot
  - Ex: volatile session keys, data/packets flowing through the system
  - Implemented through SEC and a randomly initialized key **KEK** (Key Encryption Key)
  - Principle: KEK is initialized to a cryptographically secure random value after each boot cycle and is never exposed outside the SEC
  - Session keys like those temporarily negotiated and referenced millions of time per life of IPSec tunnels can be transparently encrypted & decrypted by the SEC using the KEK (“Black Keys”)

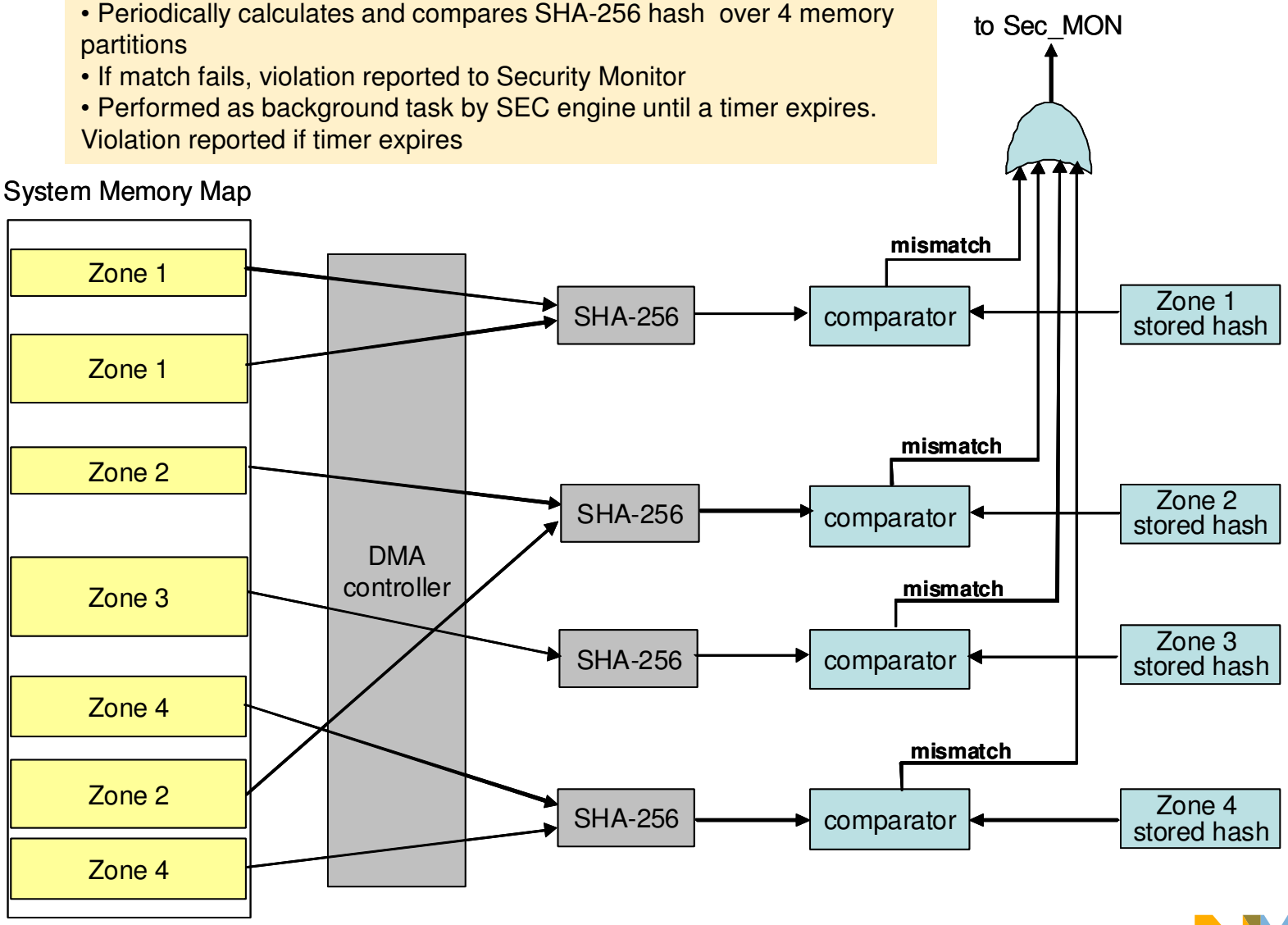
Protecting Short Term Secrets with the SEC



KEK (Key Encryption Key) is generated at each boot and never exposed outside SEC

Run Time Integrity Checker

- Periodically calculates and compares SHA-256 hash over 4 memory partitions
- If match fails, violation reported to Security Monitor
- Performed as background task by SEC engine until a timer expires. Violation reported if timer expires



AGENDA

- Intro / background
- QorIQ processors major security components across families
- Trust Architecture (TA) and TrustZone (TZ) in Layerscape architecture
- Detail of Trust Architecture key components
- Advanced features

Trust Architecture – Features summary

TRUST Version	Trust 1.0	Trust 1.1	Trust 2.0	Trust 2.1	Trust 3.0
Related devices ('E' devices)	**P4080, P1010**	**P2040, P3041, P5020**	**T1040, T2080, T4240, B4860, C290**	**LS1020, LS1043**	**LS2080, LS1088**
Base Features					
Secure Boot	Y				
Secure Boot -offloaded thru SEC (HW accel.)	N		Y		
Secure Debug Controller	Y			Y + TrustZone "Secure World" add'l protections	
Security Fuse Processor (SFP)	Y				
Security Monitor	Y				
Security Monitor Dual-power sections (incl. Key zeroization & ext. Tamper)	N	Y	Y (not in T1 & B4)	Y	
External Tamper Detection	Y				
Real-Time Integrity Checker (RTIC)	Y				
SEC-supported Blobs based on Master Key	Y				
SEC-supported Ephemeral Key Encryption Keys	Y				
CPU Memory Access Control	Power ISA MMU w/HV			ARM ISA MMU w/HV and TrustZone	
I/O Memory Access Control	Platform MMU (PAMU)			Platform MMU (SMMU)	
ARM TrustZone	N			Y	
Advanced Features					
Secure Boot - Alternate (secondary) signed Image	N		Y		
Secure Boot - Key list and Key revocation	N		Y (List of 4 keys)	Y (List of 8 keys)	
Monotonic Counters	N		1 (not in T1 & B4)	1	
HW Key Pair (aka Trusted Manufacturing)	N			Y	

Trust Architecture Enhanced Features

Differences between Trust 1.x and 2.0 (T-series):

- Reduced secure boot time by offloading cryptography to the SEC
  → full ISBC SW implementation with Trust 1.0
- Support for a primary and alternate (secondary) signed image
  → ISBC attempts to validate a secondary image if the primary fails
- Support for revocation of super root keys
- Monotonic counter
  → battery-backed zeroisable persistent secret value
- Battery-backed, general purpose storage registers

Added in Trust 2.1 & 3.0 (LS-series) :

- Trusted Manufacturing

Trust Architecture Rev2.1/3.0 (LS-Series)

Manufacturing Protection

The Trust Architecture 3.0 supports a manufacturing protection feature OEMs may use to gain the following assurances:

- The OEM is building systems using legitimate NXP chips of the correct type.
- The contract manufacturer is burning the chip's fuses correctly (especially the SRKH – public key for secure boot)
- The system has booted securely and authorized OEM software is running on the chip prior to provisioning of credentials
- OEM additional secrets can safely be downloaded to the chip
- The manufacturing protection process includes steps taken at the OEM once per production lot and steps taken at the contract manufacturer (or upon field installation).

SECURE CONNECTIONS
FOR A SMARTER WORLD