FTF FREESCALE TECHNOLOGY FORUM 2015

Overview of Secure Embedded Processing in QorIQ Platforms

FTF-SNT-F1234

AUG.2015

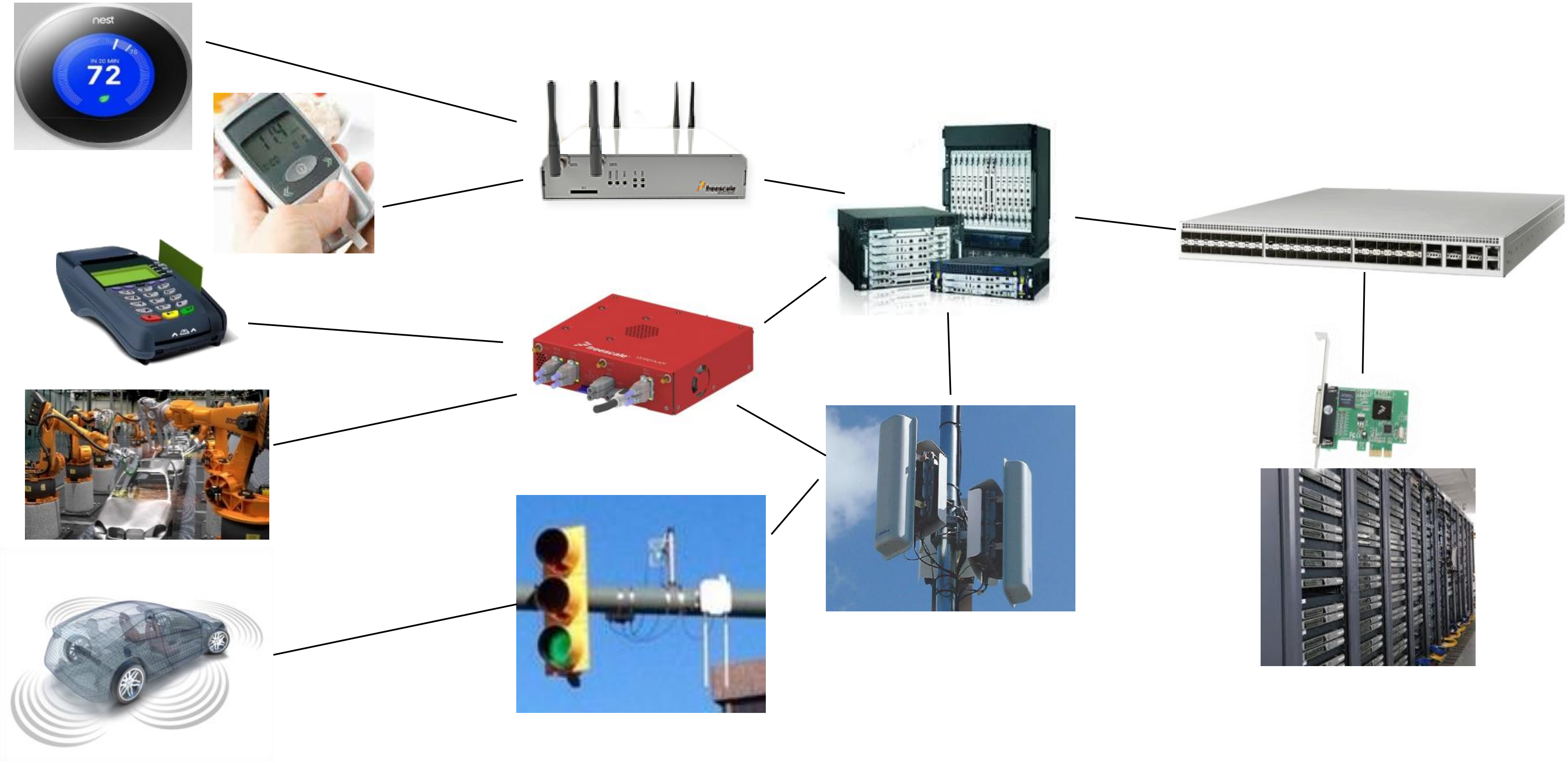
freescale™

External Use

Agenda

- What is Secure Embedded Processing?
- Trusted Platforms
  - QorIQ Trust Architecture
  - ARM® TrustZone®
- Secure Data Transport
  - Security Protocols
  - Security Acceleration
  - Drivers, APIs, and Stacks

Embedded Processing in the Internet of Tomorrow



Internet of Things End Points

Software Defined Network Infrastructure

Cloud Data Centers

Secure Embedded Processing in the Internet of Tomorrow

- Trusted Platform for consumer privacy

- Trusted Platform for PCI & HIPAA compliance

- Trusted Platform + Strong Functional Safety
- Low (& Determininstic) Latency Secure Message Exchange

- Software Defined Multi-Protocol Security
- High Performance Secure Data Transport
- Trusted Platform
- Virtualization and acceleration ease of use

- Data at rest protection
- High Secure Connection Rates

Internet of Things End Points → **Software Defined Network Infrastructure** → **Cloud Data Centers**

Trusted Platform and Secure Data Transport

Trusted Platform

- Secure Boot
- Secure Debug
- Secure Storage
- Tamper Detection
- Virtualization/Containerization

Protects against:

- Theft of user & 3rd party data
- Theft of functionality
- Theft of uniqueness (cloning)

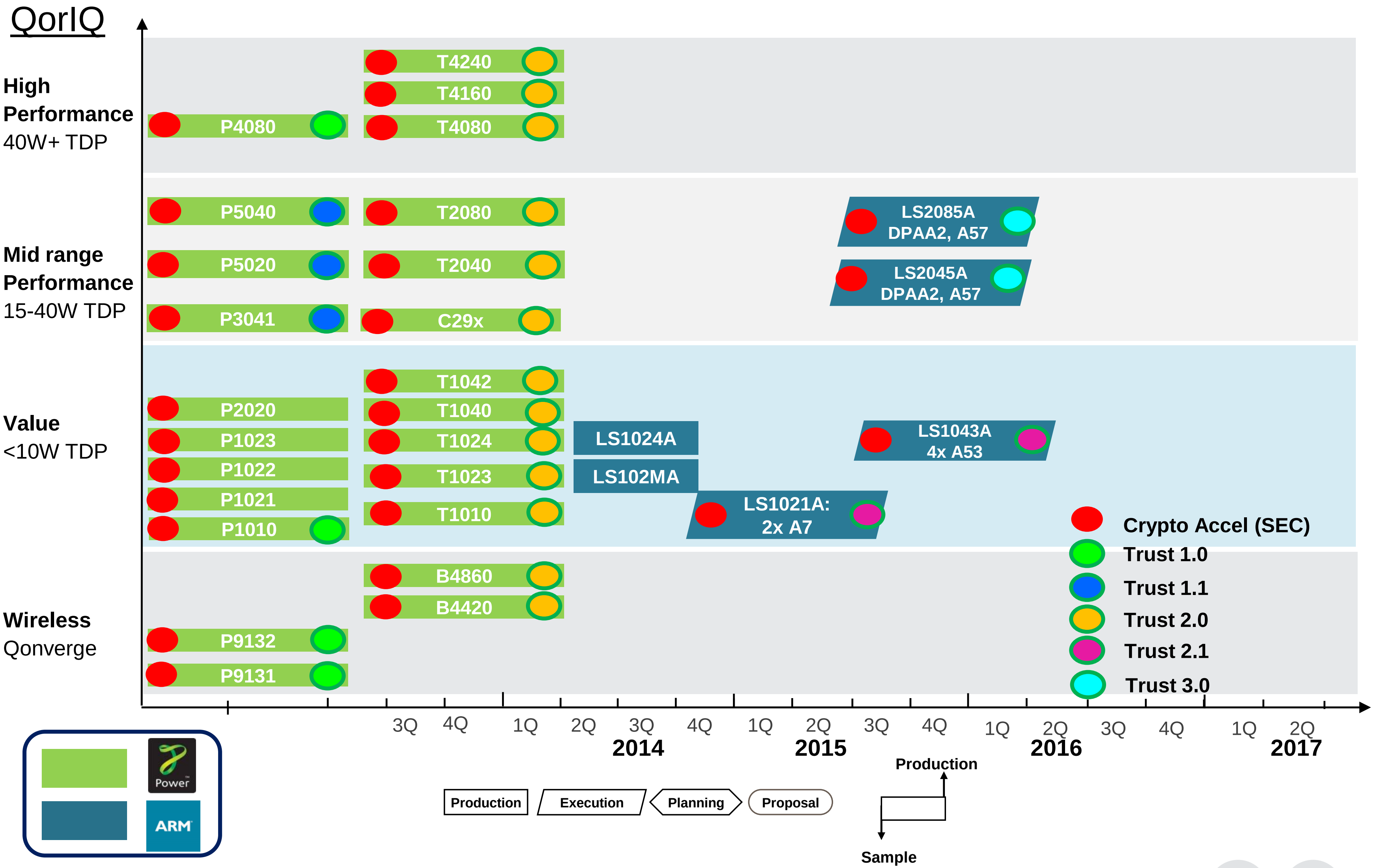
Secure Data Transport

- MACSEC
- PDCP
- IPsec
- SSL/TLS
- SRTP

Protects against:

- Masquerading
- Eavesdropping
- Data Manipulation
- Replay

QorIQ Security Features



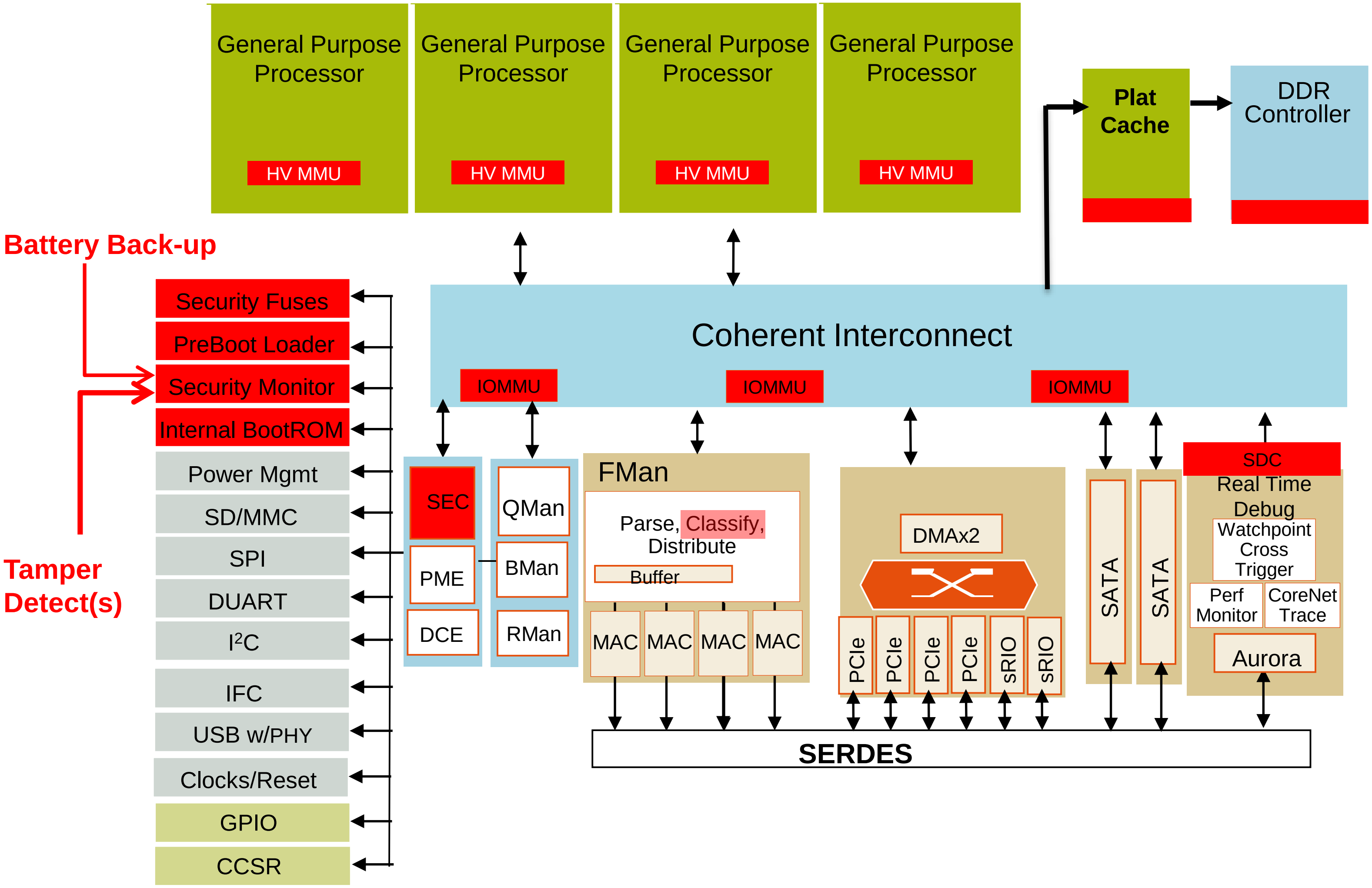
Freescale investing in both Power and ARM portfolio

Trusted Platform

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

- Freescale Trust Architecture
  - SoCs provide OEM-controlled silicon features which simplify the development of trustworthy systems
  - The Trust Architecture is an opt in scheme, with OEM controlled trade-offs in cryptographic strength, debug visibility, sensitivity of tamper detection, and anti-cloning mitigation

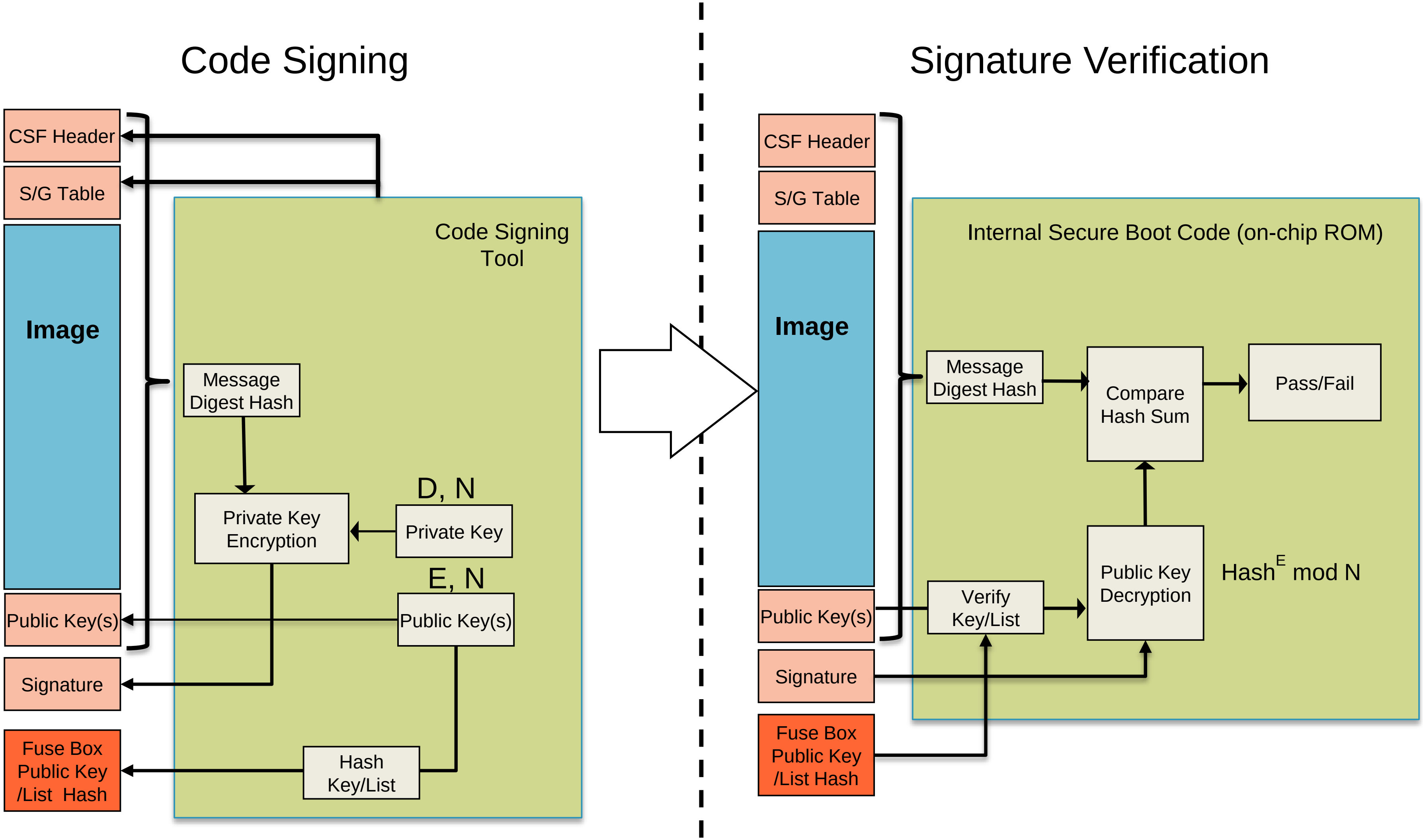
Generic Trust Architecture SoC



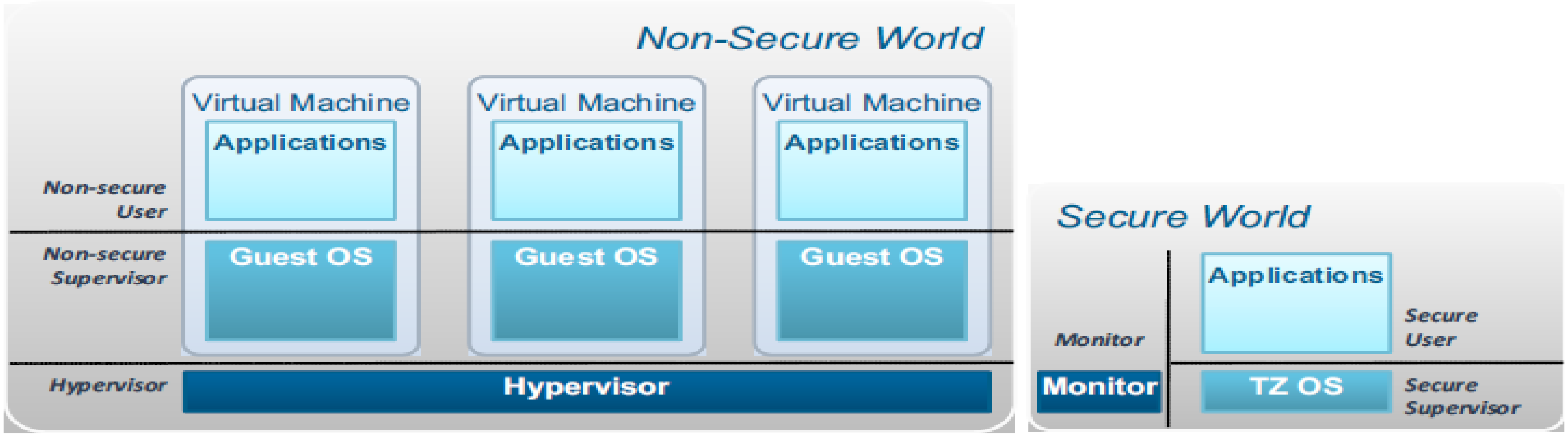
Trust Architecture Key Components

- Secure Boot
  - A staged secure boot and chain of trust of authenticated software
- Security Fuse Processor (SFP)
  - Use the values burned into the fuses to enforce security policy in pre-boot phase, and to securely pass provisioned persistent secrets to other hardware blocks when the system is in a trusted/secure state
- Chain of Trust
  - Boot script contains information about the next level of images, e.g. Linux, dtb, etc.
- RTIC
  - Maintenance of the trusted environment during runtime
- Tamper Detection
  - Ability to define system-level, physical security policies and report violations to the security monitor
- SECMON
  - SOC's central reporting point for security-relevant events such as the success or failure of boot software validation and the detection of potential security compromises
- BLOB
  - A cryptographic data structure which provides both confidentiality and integrity protection
- Secure debug controller
  - Debug Port Challenge and Response setting (DCV and DRV)

Secure Boot: Verifying Code Before Execution

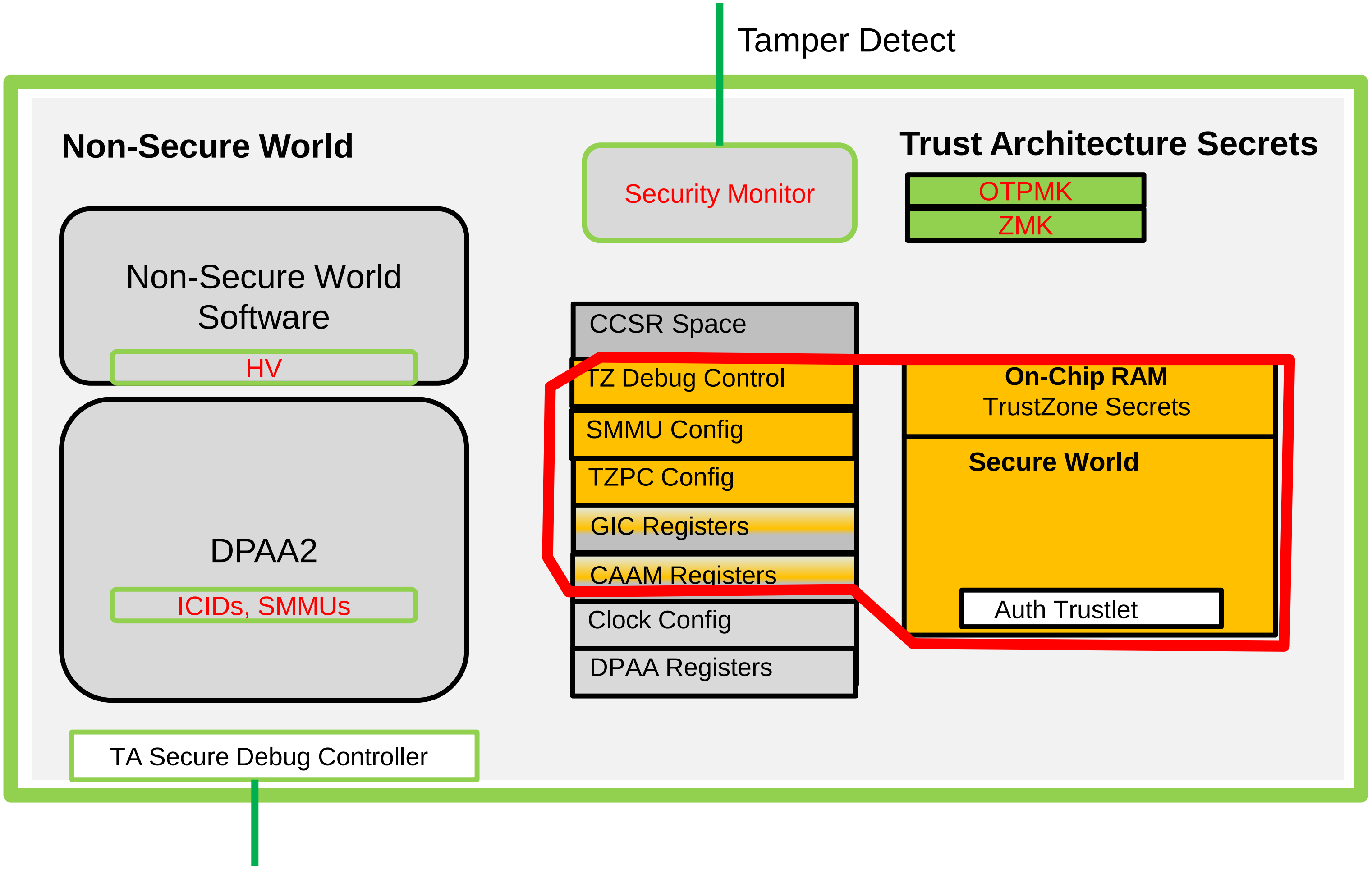


ARM Operational Modes



Trust Architecture + ARM TrustZone

Trust Arch provides a secure perimeter for trusted software



TrustZone provides an inner keep for especially trusted software

Trust Architecture Generations & Features

Feature	Trust 1.0	Trust 1.1	Trust 2.0
Devices	P4080, P1010, BSC913x	P204x, P3041, P50xx	C29x, T4240, T2080, T1040, B4
Secure Boot	Yes	Yes	Yes
HW Acceleration of Secure Boot	No	No	Yes. Only ‘E’ devices support secure boot
Alternate Image	No	No	Yes, failure of primary image leads to validation attempt for alternate image
Key List & Key Revocation	No	No	Yes, SRKH is hash of a list of up to 4 public keys; up to 3 can be revoked with fuses
Blobs based on Master Key	Yes, only Master Key option is OTPMK.	Yes, Master Key can be either OTPMK or ZMK. ZMK not available in BSC913x.	Yes, Master Key can be either OTPMK or ZMK. ZMK not available in B4
Ephemeral Key Encryption Keys	Yes	Yes	Yes
Secure Debug Controller	Yes	Yes	Yes
Security Monitor High Power Section	Yes, including security state tracking and HW_Sec_Vio inputs from RTIC, SDC, SFP, & TMP_DETECT_B	Yes, including security state tracking and HW_Sec_Vio inputs from RTIC, SDC, SFP, TMP_DETECT_B , and SecMon LP section	Yes, including security state tracking and HW_Sec_Vio inputs from RTIC, SDC, SFP, TMP_DETECT_B , and SecMon LP section

Trust Architecture Generations & Features Continued

Feature	Trust 1.0	Trust 1.1	Trust 2.0
Security Monitor Low Power Section	No	Yes, including ZMK, and HW_Sec_Vio detection from Power Glitch, LP_TMP_DETECT_B. Not present in BSC913x.	Yes, including ZMK, 4 GPRs, and HW_Sec_Vio detection from Power Glitch, LP_TMP_DETECT_B , and Monotonic Counter Roll-Over. Not present in T1040 or B4.
Monotonic Counters	No	No	1 (Not present in T1040 or B4)
CPU Memory Access Control	Power ISA MMU w/HV (HV level not available in P1010)	Power ISA MMU w/HV (HV level not available in BSC913x)	Power ISA MMU w/HV (HV level not available in C29x)
IO Memory Access Control	Platform MMU (PAMU) in P4080. CCSR Access Control and PCIe ATMU in P1010	Platform MMU (PAMU) in QorIQ. CCSR Access Control and PCIe ATMU in BSC913x.	Platform MMU (PAMU) in QorIQ. CCSR Access Control and PCIe ATMU in C29x.

Trust Architecture Generations & Features Continued

Feature	Trust 2.0	Trust 2.1	Trust 3.0
Devices	C29x, T4240, T2080, T1040, B4	LS102xA, LS1043A	LS208xA, LS1088A,
Secure Boot	Yes	Yes	Yes
HW Acceleration of Secure Boot	Yes. Only 'E' devices support secure boot.	Yes. Only 'E' devices support secure boot.	Yes. Only 'E' devices support secure boot.
Alternate Image	Yes, failure of primary image leads to validation attempt for alternate image.	Yes, failure of primary image leads to validation attempt for alternate image.	Yes, failure of primary image leads to validation attempt for alternate image.
Key List & Key Revocation	Yes, SRKH is hash of a list of up to 4 public keys, where up to 3 can be revoked with fuses.	Yes, SRKH is hash of a list of up to 8 public keys, where up to 7 can be revoked with fuses.	Yes, SRKH is hash of a list of up to 8 public keys, where up to 7 can be revoked with fuses.
Blobs based on Master Key	Yes, Master Key can be either OTPMK or ZMK. ZMK not available in B4.	Yes, Master Key can be either OTPMK or ZMK.	Yes, Master Key can be either OTPMK or ZMK.
Ephemeral Key Encryption Keys	Yes	Yes	Yes
Secure Debug Controller	Yes	Yes, plus TrustZone 'Secure World' additional protections	Yes, plus TrustZone 'Secure World' additional protections
Security Monitor High Power Section	Yes, including security state tracking and HW_Sec_Vio inputs from RTIC, SDC, SFP, TMP_DETECT_B , and SecMon LP section.	Yes, including security state tracking and HW_Sec_Vio inputs from RTIC, SDC, SFP, TMP_DETECT_B , and SecMon LP section.	Yes, including security state tracking and HW_Sec_Vio inputs from RTIC, SDC, SFP, TMP_DETECT_B , and SecMon LP section.
Security Monitor Low Power Section	Yes, including ZMK, 4 GPRs, and HW_Sec_Vio detection from Power Glitch, LP_TMP_DETECT_B , and Monotonic Counter Roll-Over. Not present in T1040 or B4.	Yes, including ZMK, 4 GPRs, and HW_Sec_Vio detection from Power Glitch, LP_TMP_DETECT_B , and Monotonic Counter Roll-Over.	Yes, including ZMK, 4 GPRs, and HW_Sec_Vio detection from Power Glitch, LP_TMP_DETECT_B , and Monotonic Counter Roll-Over.

Trust Architecture Generations & Features Continued

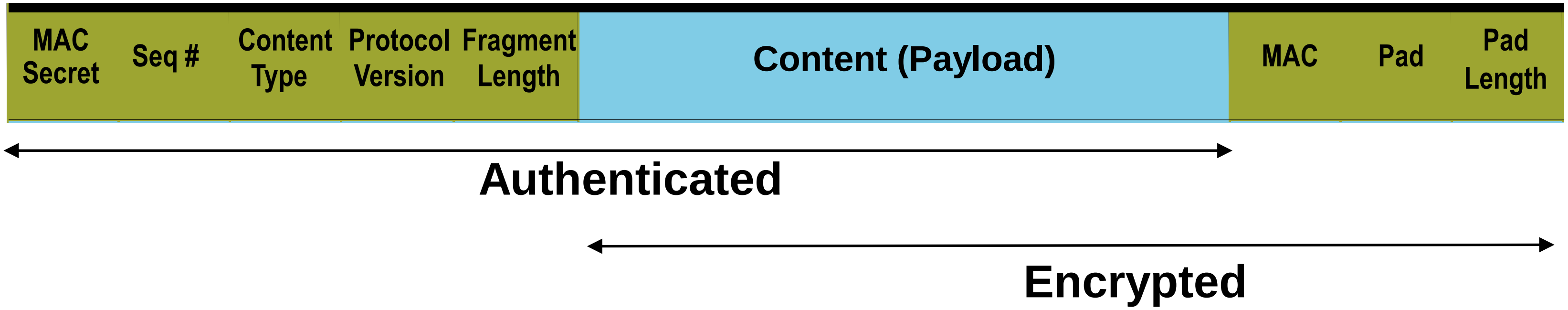
Feature	Trust 2.0	Trust 2.1	Trust 3.0
Monotonic Counters	1 (Not present in T1040 or B4)	1	1
CPU Memory Access Control	Power ISA MMU w/HV (HV level not available in C29x)	ARM ISA MMU w/HV and TrustZone	ARM ISA MMU w/HV and TrustZone
IO Memory Access Control	Platform MMU (PAMU) in QorIQ. CCSR Access Control and PCIe ATMU in C29x.	Platform MMU (SMMU) in QorIQ Layerscape.	Platform MMU (SMMU) in QorIQ Layerscape, improved ICID scheme in DPAA2
Hardware Key Pair (aka Trusted Mfg)	No	Yes	Yes

Major Enhancements and Their Use

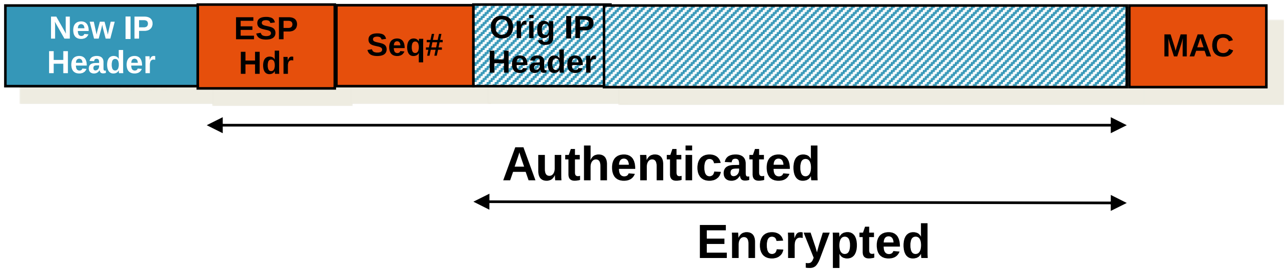
Enhancement	First Appears	Benefit	Impact when used
Zeroizable Master Key	Trust 1.1	OEM can elevate the consequences of a security violation.	Requires battery back-up of portion of SoC (SecMon LP section), additional configuration registers and LP_TMP_DETECT
HW Acceleration of Secure Boot	Trust 2.0	Makes secure boot time closer to non-secure boot time	Trust only available in ‘E’ devices
Alternate Image	Trust 2.0	Adds resiliency to the secure boot process	Requires signing of 2 images, additional PBI commands
Key Revocation	Trust 2.0	Permanently revoke flawed images which were signed with a super root key.	Need to manage more pub/pri keys Need to develop key revocation images
Monotonic Counter	Trust 2.0	Prevent ‘roll back’ to a flawed image without revoking a super root key	Requires battery back-up of portion of SoC (SecMon LP section), need to include anti-rollback check in chain of trust
Hardware Key Pair (aka Trusted Mfg)	Trust 2.1	More intrinsic method of provisioning a device public/private key	Requires additional steps to generate key pair, export pub key. Requires database of IDs + public keys.
ARM TrustZone	Trust 2.1	Creates secure container (Secure World) where trusted applications can perform tasks on behalf of Non-Secure World applications. 3rd party software offerings.	Must still use Trust Arch to validate TrustZone software. Additional images to sign.

User Datagram Protection 101

SSL/TLS



IPsec ESP TUNNEL MODE



SEC 5.0 – As Featured in QorIQ T4240 Processor

(1) Public Key Hardware Accelerator (PKHA)
- RSA and Diffie-Hellman (to 4096b)
- Elliptic curve cryptography (1024b)
- Supports Run Time Equalization

(1) Random Number Generators (RNG4)
- NIST Certified

(4) Snow 3G Hardware Accelerators (STHA) (~12Gbps)
- Implements Snow 3.0 Keystream Generator
- f8 encryption per ETSI/SAGE 128-UEA2 (and 128-EEA1)
- f9 authentication per ETSI/SAGE 128-UIA2 (and 128-EIA1)

(4) ZUC Hardware Accelerators (ZHA) (~10Gbps)
- Implements ZUC Keystream Generator (per spec v1.5)
- Authentication per ETSI/SAGE 128-EIA3 (spec v 1.5)
- Encryption per ETSI/SAGE 128-EEA3 (spec v 1.5)

(2) ARC Four Hardware Accelerators (AFHA)
- Compatible with RC4 algorithm (~7.5Gbps)

(8) Kasumi F8/F9 Hardware Accelerators (KFHA)
- F8 , F9 as required for 3GPP (~20Gbps)
- A5/3 for GSM and EDGE, GEA-3 for GPRS

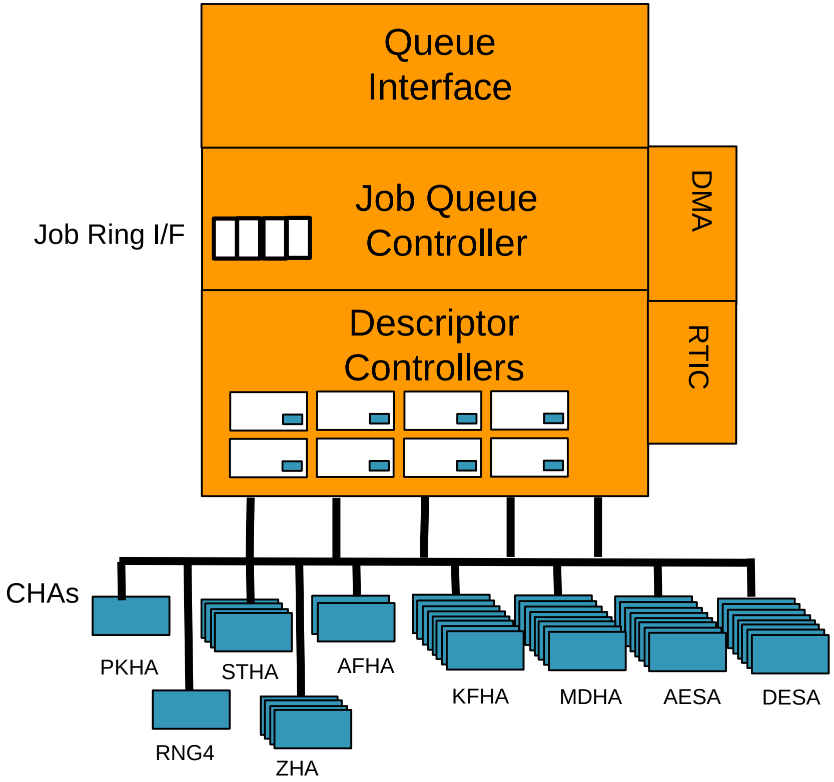
(8) Message Digest Hardware Accelerators (MDHA)
- SHA-1, SHA-2 256,384,512-bit digests (~40Gbps)
- MD5 128-bit digest
- HMAC with all algorithms

(8) Advanced Encryption Standard Accelerators (AESA)
- Key lengths of 128-, 192-, and 256-bit (~40Gbps)
- ECB, CBC, CTR, CCM, GCM, CMAC, XCBC, OFB, CFB, and XTS
- Supports LTE 128-EEA2 / 128-EIA2

(8) Data Encryption Standard Accelerators (DESA)
- DES (~40Gbps), 3DES (2K, 3K) ~20Gbps
- ECB, CBC, OFB modes

(8) CRC Unit
- CRC32, CRC32C, 802.16e OFDMA CRC (~48Gbps)

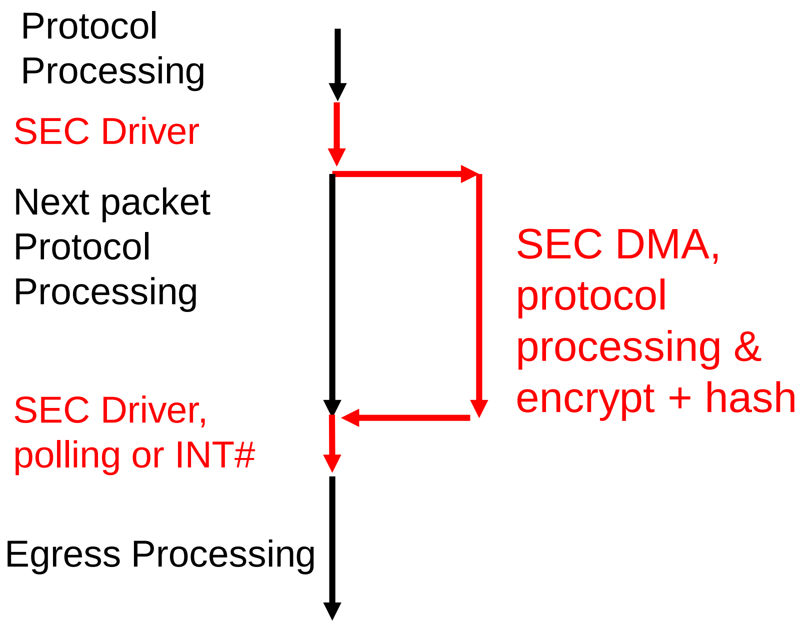
Header & Trailer off-load for the following Security Protocols:
- IPSec, SSL/TLS, 3G RLC, PDCP, SRTP, 802.11i, 802.16e, 802.1ae



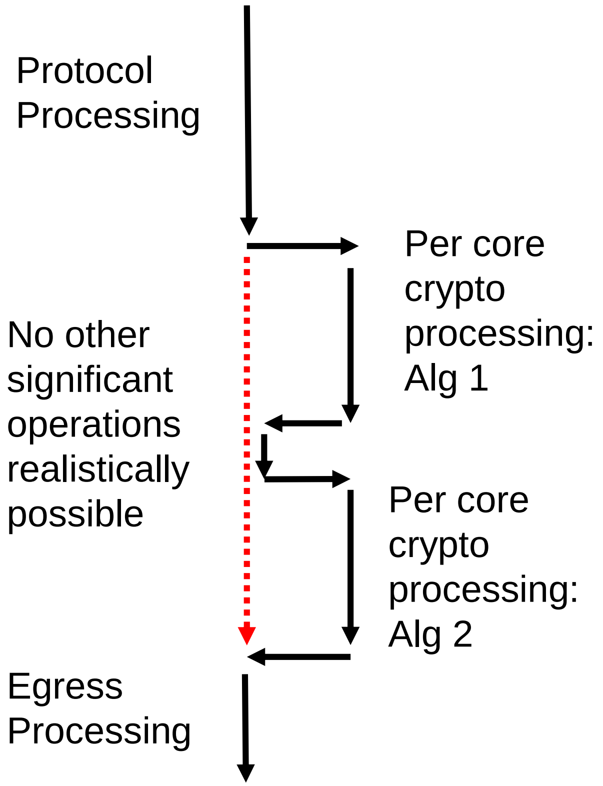
Benefits of SEC Architecture

Centralized engine (SEC) with protocol offload, single pass encryption and authentication (ie, AES-HMAC-SHA-2).

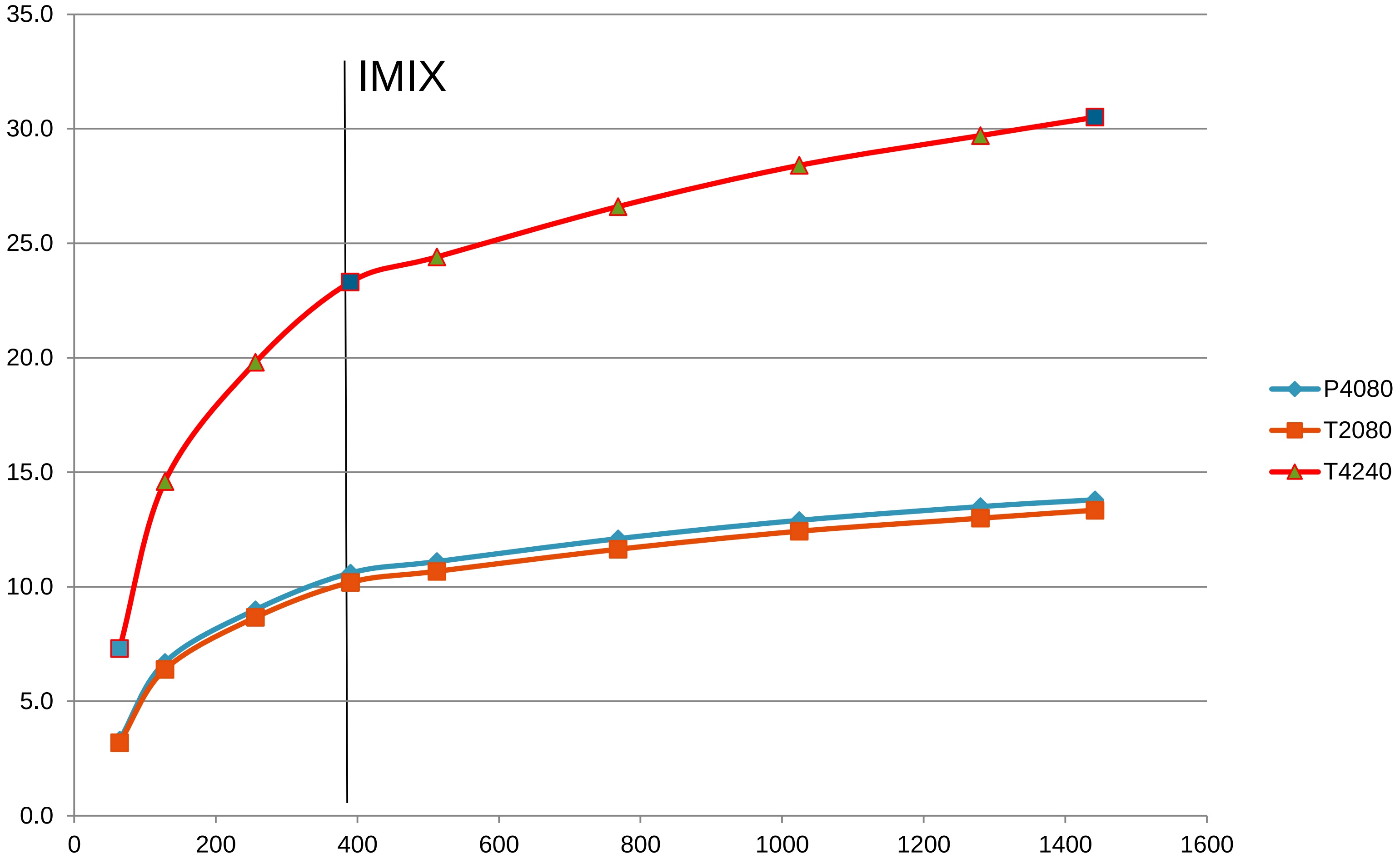
CPUs can perform other tasks while SEC processes packets. Many packets can be processed with CPU periodically gathering results.


Protocol Processing
SEC Driver
Next packet Protocol Processing
SEC DMA, protocol processing & encrypt + hash
SEC Driver, polling or INT#
Egress Processing

Per CPU low level accelerators/special instructions. No protocol acceleration, non-crypto operations blocked during 2-pass processing.

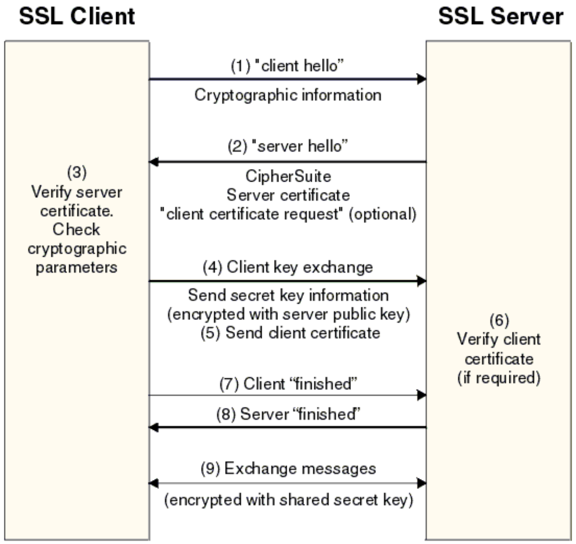

Protocol Processing
Per core crypto processing: Alg 1
No other significant operations realistically possible
Per core crypto processing: Alg 2
Egress Processing

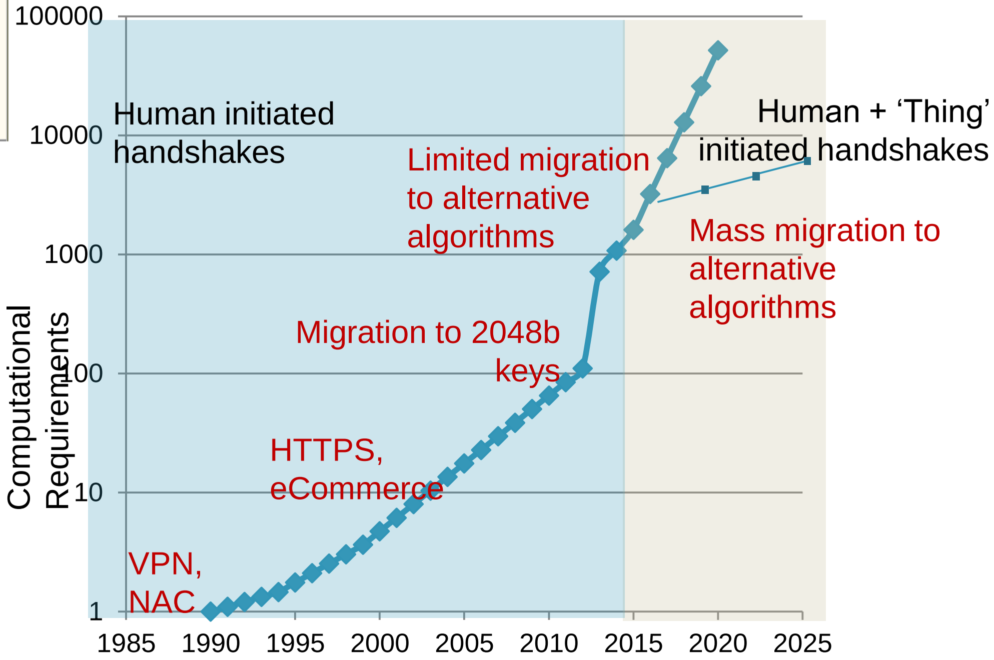
P4080, T2080, & T4240 IPsec



P4080 data is measured, T4240 64, 390, & 1442B points measured. Other data points extrapolated.

Secure Handshaking


SSL Client
SSL Server
(1) "client hello"
Cryptographic information
(2) "server hello"
CipherSuite
Server certificate
"client certificate request" (optional)
(3)
Verify server certificate.
Check cryptographic parameters
(4) Client key exchange
Send secret key information
(encrypted with server public key)
(5) Send client certificate
(6)
Verify client certificate
(if required)
(7) Client "finished"
(8) Server "finished"
(9) Exchange messages
(encrypted with shared secret key)

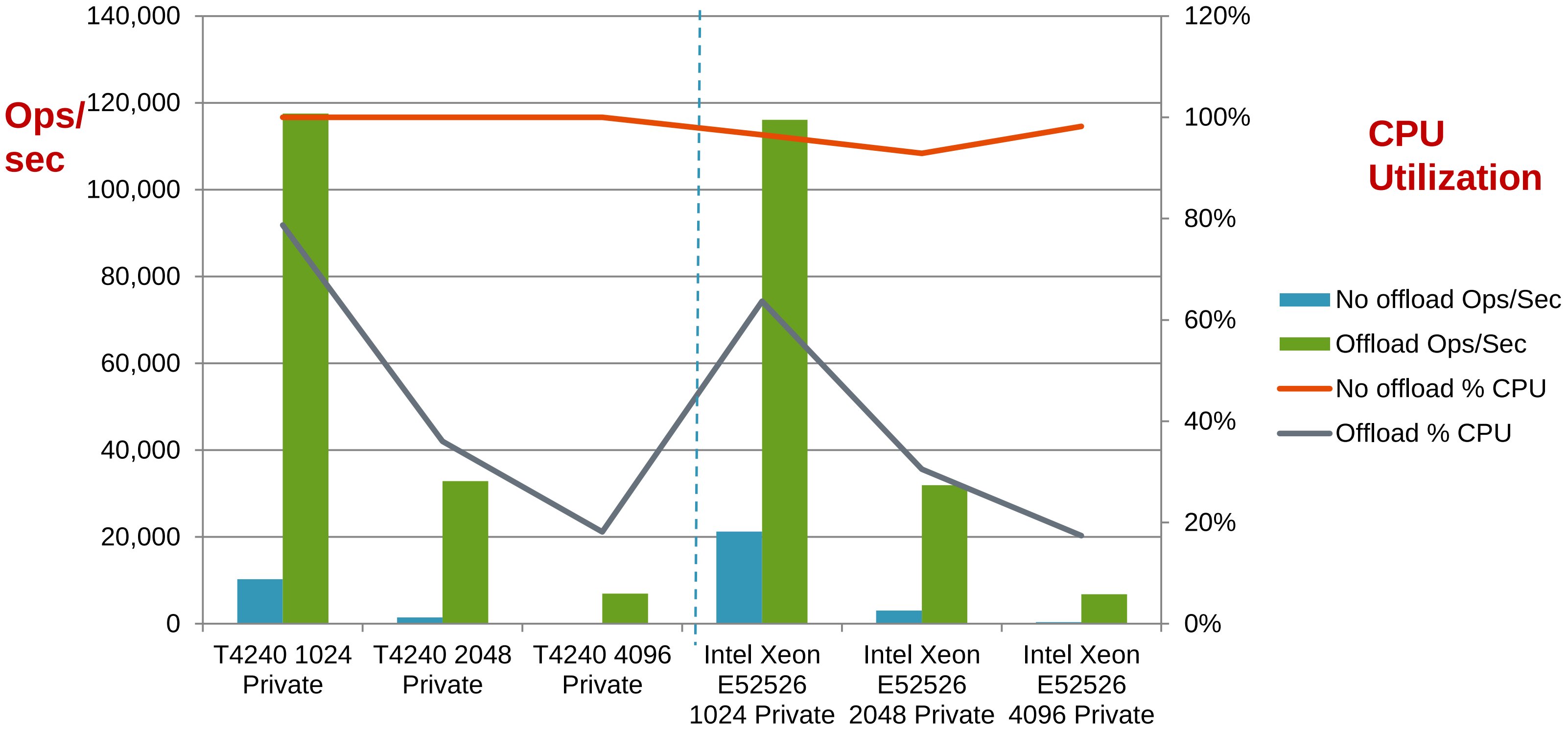


Shaking Hands with a Cloud

- Can a cloud of commodity hardware systems service all these handshakes?
  - Yes, at ~10 handshakes/sec/watt (2048b)
  - Yes, at high risk of keys being exposed
    - Criminal organizations are selling SSL keys as low as $1,000

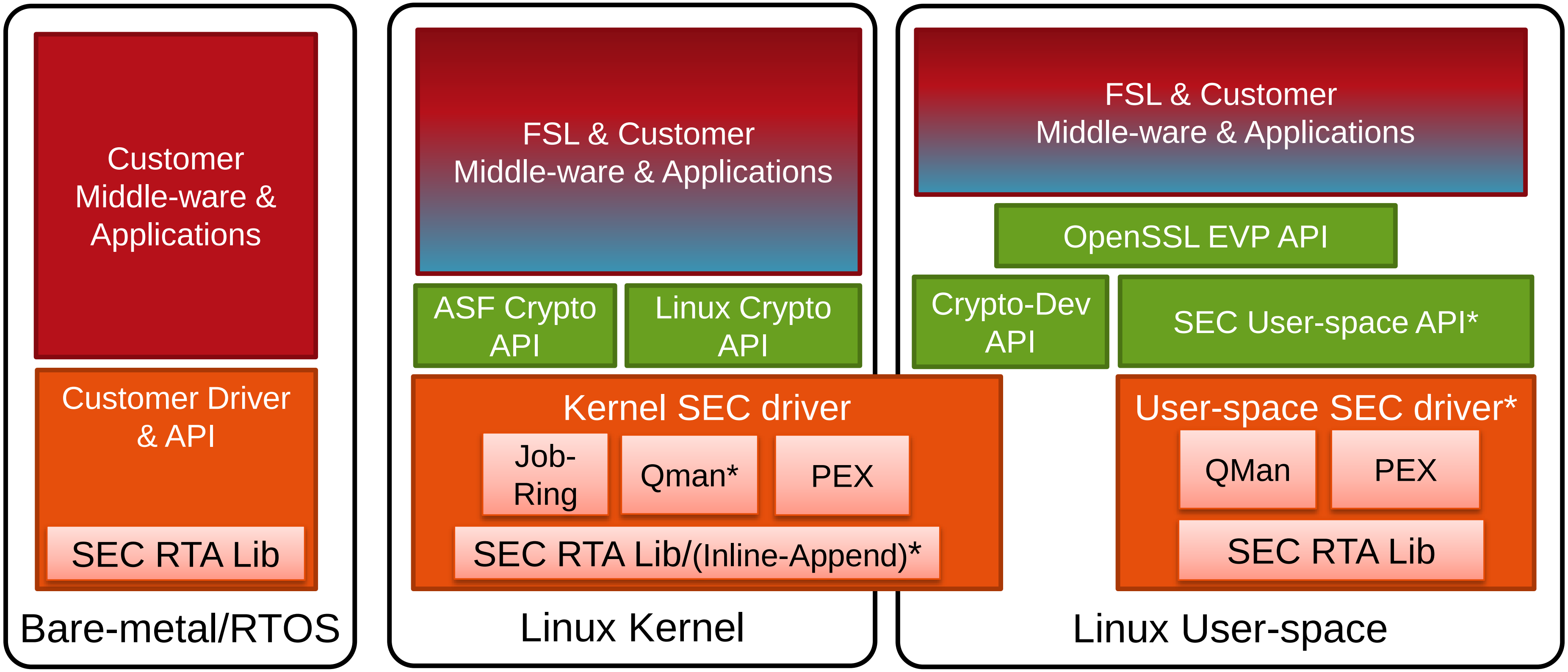
- Hardware Security Modules (HSMs) can address these deficiencies
  - Provide accelerated cryptographic services within a hardened boundary
    - >200 handshakes/sec/watt (2048b)
  - Protect and manage provisioned keys; keys cleared if HSM tampered

C293 Crypto Coprocessor Performance Benefits



```
# openssl speed rsa – engine cryptodev – elapsed – multi 200
```

SEC RTA, Kernel and User-space Drivers



- Freescale provides drivers for both Linux® kernel and user-space
  - Use various means like Job-ring, QMan and PEX to access the SEC engine
- Freescale provides a SEC RTA library for bare-metal or RTOS environments
  - SEC RTA library re-used across environments

Freescale Has World Class Support….and MORE

Global Technical Information Center
Design & Support Resource

Networking Applications Team
Depth of Expertise & Knowledge

Design With Freescale, Freescale Technology Forum
Training

Networking Software and Services Group

- Commercial Solutions
- Engineering Services
- Guaranteed Performance
- Service Level Agreement Support…and MORE

- Visit Pedestal 415 in the Technology Lab freescale™

www.Freescale.com