# Security from Freescale Processors

*Secure Embedded Processing Solutions for the IoT*

Tilo Weissenbach

Q 3 . 2 0 1 5

External Use

Freescale, the Freescale logo, AltiVec, C-5, CodeTEST, CodeWarrior, ColdFire, ColdFire+, C-Ware, the Energy Efficient Solutions logo, Kinetis, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, Qorivva, SafeAssure, the SafeAssure logo, StarCore, Symphony and VortiQa are trademarks of Freescale Semiconductor, Inc., Reg. U.S. Pat. & Tm. Off. Airfast, BeeKit, BeeStack, CoreNet, Flexis, Layerscape, MagniV, MXC, Platform in a Package, QorIQ Qonverge, QUICC Engine, Ready Play, SMARTMOS, Tower, TurboLink, UMEMS, Vybrid and Xtrinsic are trademarks of Freescale Semiconductor, Inc. All other product or service names are the property of their respective owners. © 2014 Freescale Semiconductor, Inc.

# Still ***Internet of Things*** nodes are insecure

24. November 2014, 16:54 Uhr

**Sicherheit von "Smart Home" offen wie ein Scheunentor**

Source: http://www.sueddeutsche.de/digital/sicherheit-von-smart-home-offen-wie-ein-scheunentor-1.2227389

# Still ***Internet of Things*** nodes are insecure

02.03.2015 09:59

## CNN: Flugzeuge können gehackt werden!

„Nach einem aktuellen Bericht des Government Accountability Office könnten hunderte heutiger kommerzieller Flugzeuge eine Sicherheitslücke haben und ihre an Bord befindlichen Computer könnten gehackt und von jemandem übernommen werden, der das für die Passagiere zur Verfügung gestellte Wi-Fi-Netzwerk benutzt, oder gar durch jemandem am Boden.

Einer der Autoren des Berichts, Gerald Dillingham, sagte gegenüber CNN, dies beinhalte Flugzeuge wie den Boeing 878 Dreamliner, die Airbus-Flugzeuge A350 und A380 und alle, die moderne Cockpits haben, die mit dem selben Wi-Fi-System verbunden sind, welches auch von den Passagieren genutzt wird.

Connection of Sub-Networks via Router
[Don’t rely on Router for IoT Security]

# 7 New Security Challenges

The embedded community has a social responsibility to secure the smart and connected world…

- New challenges for the smart, secure, connected world include:
  - Connected accessibility: Connectivity opens new doors for attacks
  - Physical accessibility: Unlimited attacks of remote nodes
  - Data dependence: Harmful repercussions for missing data
  - Number: Network overload threats
  - Data miss-use: Data used beyond intended methods
  - Mitigation of weaknesses as they arise: Need for secure firmware updates.
  - Social responsibility: The public is no longer forgiving of security breaches

# Categories of Attack in Embedded Systems

- **Classification**
  - Per investment (equipment),
  - Time
  - Expertise needed

- **Classification per type**
  - Invasive or semi-invasive
  - Non invasive i.e. side channel attack
  - Software

- **Electrical**
  - Over/Under voltage
  - Power analysis
  - Frequency analysis
  - Electrostatic discharge
  - Circuit probing
  - Electro Magnetic Analysis
- **Software**
  - Spy software insertion
  - Flow analysis
  - Trojan horse
  - Virus
- **Physical**
  - Temperature variation (to extremes)
  - Temperature analysis
  - De-processing
  - System theft
  - Partial destruction
  - Hardware addition/substitution

# How Much Security?

**When protecting a system you must consider:**

- What are you trying to protect? What is the value?
- What types of attack do you need to protect against?
- What are the likely attack points and methods?
- How much security do you require?
- How much are you willing to pay?
- How will security impact the underlying system?
- How will you upgrade/maintain the system and security over time?

- **Analogy: How much do you protect your home?**

# What can an Embedded Devices Designer do?

# Security: what we want to achieve

## Authentication

I can prove to another party that I am User 12345 and only User 12345, or I can verify firmware authenticity.

- Certificates, Keys, User Passwords
- Authentifizierung, Echtheitsprüfung, Legitimierung

## Non-repudiation

I can send a message, but cannot later claim that I did not send it.

- Integrity and Origin of Data
- Data Hash (SHA2, Certificates, Digital Signatures
- Nichtabstreitbarkeit, Nachweisbarkeit

## Data Validation

I can send a message & guarantee it was not altered in transmission

I can run firmware and guarantee that it has not been altered

- Encryption, Plausibility Checks, Secure Boot
- Sicherheitsprüfung

## Secrecy

I can send a message and know that, even if it is intercepted, it cannot be read

- Encryption
- Geheimhaltung

## Protection

**My equipment must:**
- Prevent compromises in security,
- Detect if system is tampered with,
- Store secret keys

- Sensing of system voltages and currents
- Sensing of physical quantities (acceleration, electromagnetic fields, etc.
- Geräteschutz

# Freescale hardware assisted security

# Benefits of Hardware Assisted Security

- Hardware security is an essential part of meeting the demands of today's embedded designs
  - Reduce development time
    - Software complexity is reduced as hardware accelerators replace lines of software algorithms
    - Hardware protection reduces the need for external tamper protection schemes and the need for a companion security IC
  - Meet power and performance targets
    - With HW acceleration of cryptographic algorithms
  - Lower system cost
    - Less external tamper hardware needed
    - Long term protection against security attacks, protecting the unique identity of your device
    - Reduced BOM cost and PCB complexity for creating secure designs

# Freescale Hardware for Authentication [1]

**Authentication**

I can prove to another party that I am User 12345 and only User 12345, or I can verify firmware authenticity.

**Non-repudiation**

I can send a message, but cannot later claim that I did not send it.

**Validation**

I can send a message & guarantee it was not altered in transmission

I can run firmware and guarantee that it has not been altered

**Secrecy**

I can send a message and know that, even if it is intercepted, it cannot be read

**Protection**

**My equipment must:**
- Prevent compromises in security,
- Detect if system is tampered with,
- Store secret keys

**Asymmetric Ciphers 'Public Key'**

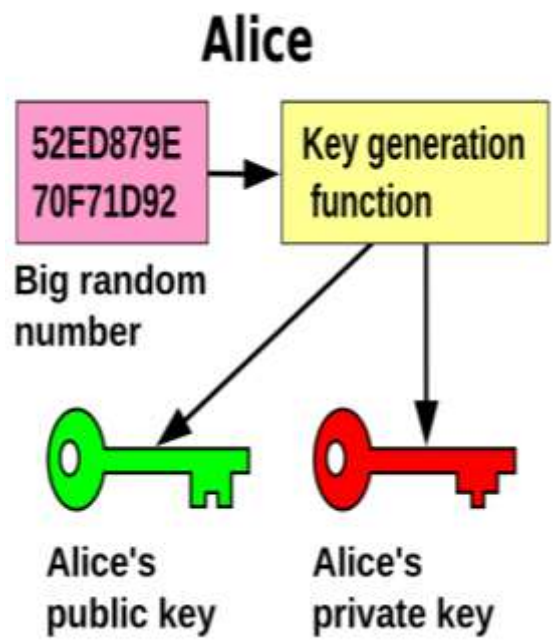
# Still ***Internet of Things*** nodes are insecure

The traffic sign should only accept an incoming connection from an ***authenticated*** server.

Only if the identity of the server can be confirmed should the sign accept text (and it should restrict the text to numeric data or ‘Closed’, nothing else).

Authentication uses Public Key cryptography and is widely available in SSL, TLS libraries.

# Asymmetric Ciphers: Random Number Gen.




- Create a pair of keys (public and secret key) using a random number

Random Number Generator

- Deterministic
  - →Weak seed states
  - →Lack of uniformity of distribution
  - →Correlation of successive values
  - →No random distances in distribution
  - →Poor dimensional distribution, periodic
- Non-Deterministic, True
  - →Software algorithm uses a physical process
  - →Aperiodic

Source: http://de.wikipedia.org/wiki/Public-Key-Verschlüsselungsverfahren/

# Freescale Hardware for Validation [2]

**Authentication**

I can prove to another party that I am User 12345 and only User 12345, or I can verify firmware authenticity.

**Non-repudiation**

I can send a message, but cannot later claim that I did not send it.

**Validation**

I can send a message & guarantee it was not altered in transmission

I can run firmware and guarantee that it has not been altered

**Hashes, secure boot, runtime checks**

**Secrecy**

I can send a message and know that, even if it is intercepted, it cannot be read

**Protection**

**My equipment must**:
- Prevent compromises in security,
- Detect if system is tampered with,
- Store secret keys

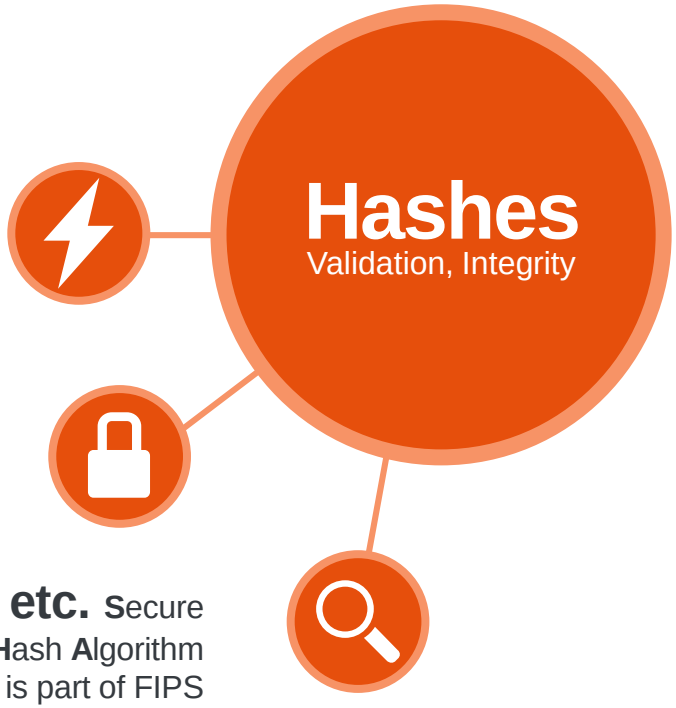
# Using Hash Functions for Validation

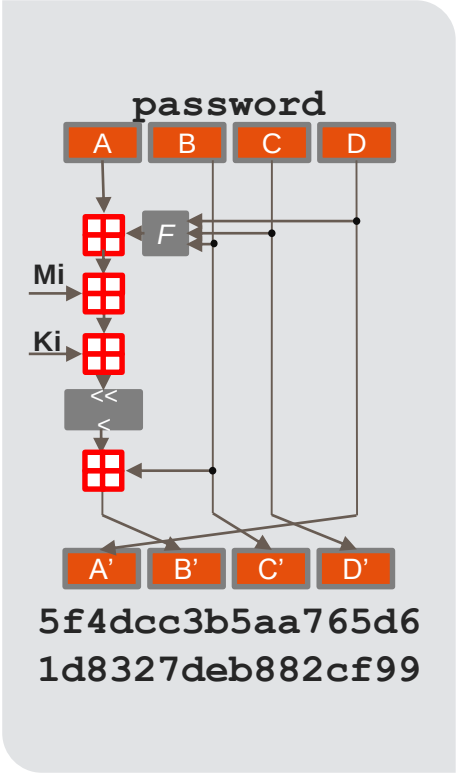
## Create a Unique Signature of some data

'Fingerprint' of Pre-Image
"Digital DNA"
One-way function or 'non-invertible'
Commonly used to 'fingerprint' code image

**MD5** Message Digest 5
Creates 128-bit hash, fastest
Commonly used to protect passwords

**SHA1, SHA256 (SHA-2) etc.** **S**ecure **H**ash **A**lgorithm
Promoted by NIST, is part of FIPS
Produces 160-bit hash
"No known cryptographic attacks against SHA2"



# Security: Techniques [3]

**Authentication**

I can prove to another party that I am User 12345 and only User 12345, or I can verify firmware authenticity.

**Non-repudiation**

I can send a message, but cannot later claim that I did not send it.

**Validation**

I can send a message & guarantee it was not altered in transmission

I can run firmware and guarantee that it has not been altered

**Secrecy**

I can send a message and know that, even if it is intercepted, it cannot be read

**Symmetric Ciphers**
**Asymmetric Ciphers 'Public Key'**

**Protection**

**My equipment must:**
- Prevent compromises in security,
- Detect if system is tampered with,
- Store secret keys

# Security: Secrecy or Privacy

**Simple substitution ciphers**
A->B, B->C etc.
Frequency analysis
***Obsolete***

**AES** Advanced Encryption Standard
Based on Rijndael, NIST (2001)
128/192/256-bit keys & 128 bit blocks
***Preferred symmetric cipher***.

**~~DES~~, 3DES** Data Encyption Standard
Promoted by NSA, limited to 56-bit key (1976) → 168 key bits
Public algorithm, secret keys
Symmetric data block size: 64-bits in, 64-bits out
Same algorithm + keys to encrypt and decrypt

**Symmetric Ciphers**
Secrecy & privacy
Encryption & decryption

Secret Key

**Key Distribution Problem**

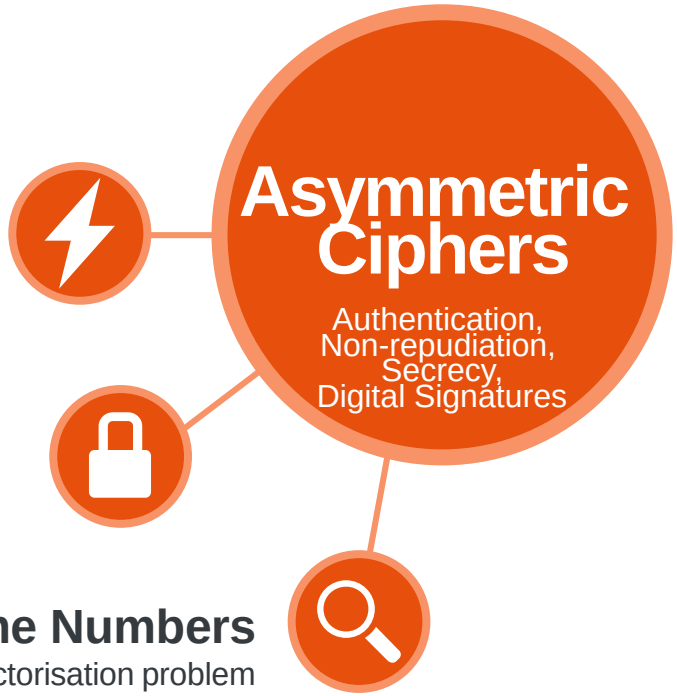
# Security: Public Key Cryptography

## Two-Factor Security

**Public** / **Private** Key Cryptography
One-way functions
Security, Authentication

## RSA Algorithm

Created '77: **R**ivest, **S**hamir, **A**dleman
Invented '73 in GCHQ, UK by Cocks
(Another common technique is Elliptic Curve cryptography, ECDSA algorithm)




## Uses Very Large Prime Numbers

Modular arithmetic and the factorisation problem
Also, see **Diffie-Hellman** key exchange
Very slow, Less secure 168-bit 3DES = 2048 RSA
Mostly used for key exchange, then use AES to exchange secure data.

# Security: Techniques [4]

**Authentication**

I can prove to another party that I am User 12345 and only User 12345, or I can verify firmware authenticity.

**Non-repudiation**

I can send a message, but cannot later claim that I did not send it.

**Validation**

I can send a message & guarantee it was not altered in transmission

I can run firmware and guarantee that it has not been altered

**Secrecy**

I can send a message and know that, even if it is intercepted, it cannot be read

**Protection**

**My equipment must:**
- Prevent compromises in security,
- Detect if system is tampered with,
- Store secret keys

**Hardware**

# Many other features are required to protect system

## A) Secure Key Storage

Cryptographic keys must be stored securely
Private keys 'the Crown Jewels'
Adversaries may try to compromise Public Keys

## B) Tamper Detection

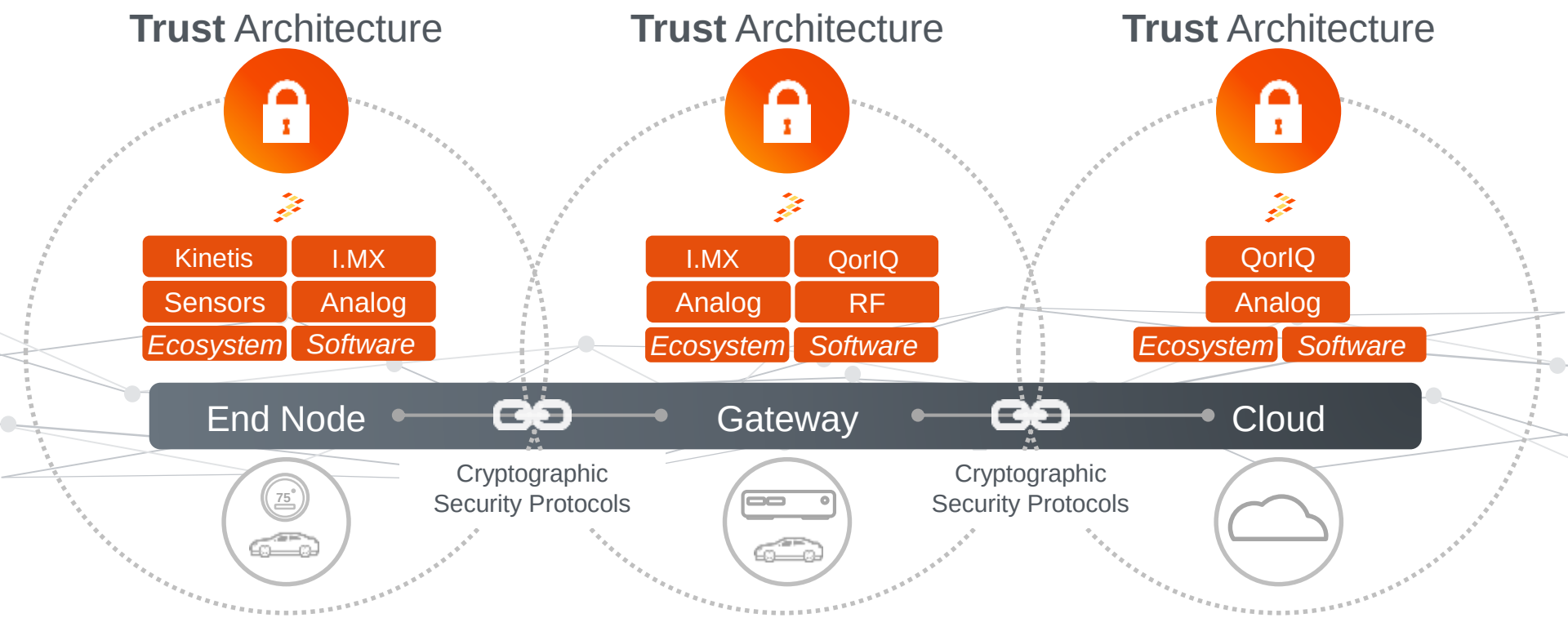
Physical attack
Over/Under voltage, temperture attacks
Differential power analysis

## C) Random Number Generation

Used to generate seeds for session and transaction keys

**Note:**
Security implementation must be a complete, unified system, not discrete elements

# Freescale IoT Security Solutions



# Kinetis Micrcontrollers & how they rise to meet the challenge

# Kinetis MCUs
# Scale – from 8KB Flash to Infinity

**Kinetis K Series**

- Scalable performance and optimized integration
- ARM Cortex-M4 core running 50–180 MHz | 32 KB–2 MB Flash | Up to 256 KB SRAM

**Kinetis L Series**

- World's most energy-efficient ARM®-based MCUs
- ARM Cortex-M0+ running up to 48 MHz | 8 KB–512 KB Flash | Up to 32 KB SRAM

**Kinetis E Series**

- Robust and 5V with enhanced ESD/EMC performance
- ARM Cortex-M0+ running up to 48 MHz | 8 KB–128 KB Flash | Up to 16 KB SRAM

**Kinetis V Series**

- Designed for motor control and digital power conversion applications
- ARM Cortex-M0+, Cortex-M4, and Cortex-M7 cores running 75–240 MHz |16 KB–1 MB Flash | Up to 256 KB SRAM

**Kinetis M Series**

- Designed for metering and measurement applications
- ARM Cortex-M0+ core running at 50 MHz | 64 KB–128 KB Flash | Up to 16 KB SRAM

**Kinetis W Series**

- Designed for wireless connectivity, integrated with sub-1 GHz and 2.4 GHz RF transceivers
- ARM Cortex-M0+ and Cortex-M4 cores running at 48-50 MHz | 128 KB–512 KB Flash | Up to 64 KB SRAM

# K63F / K64F Block Diagram

**Core/System**
- Cortex-M4 up to 120MHz with FPU

**Memory**
- up to 1MB Flash,
- **up to 256KB SRAM**
- up to 4KB EEPROM (FlexMemory)

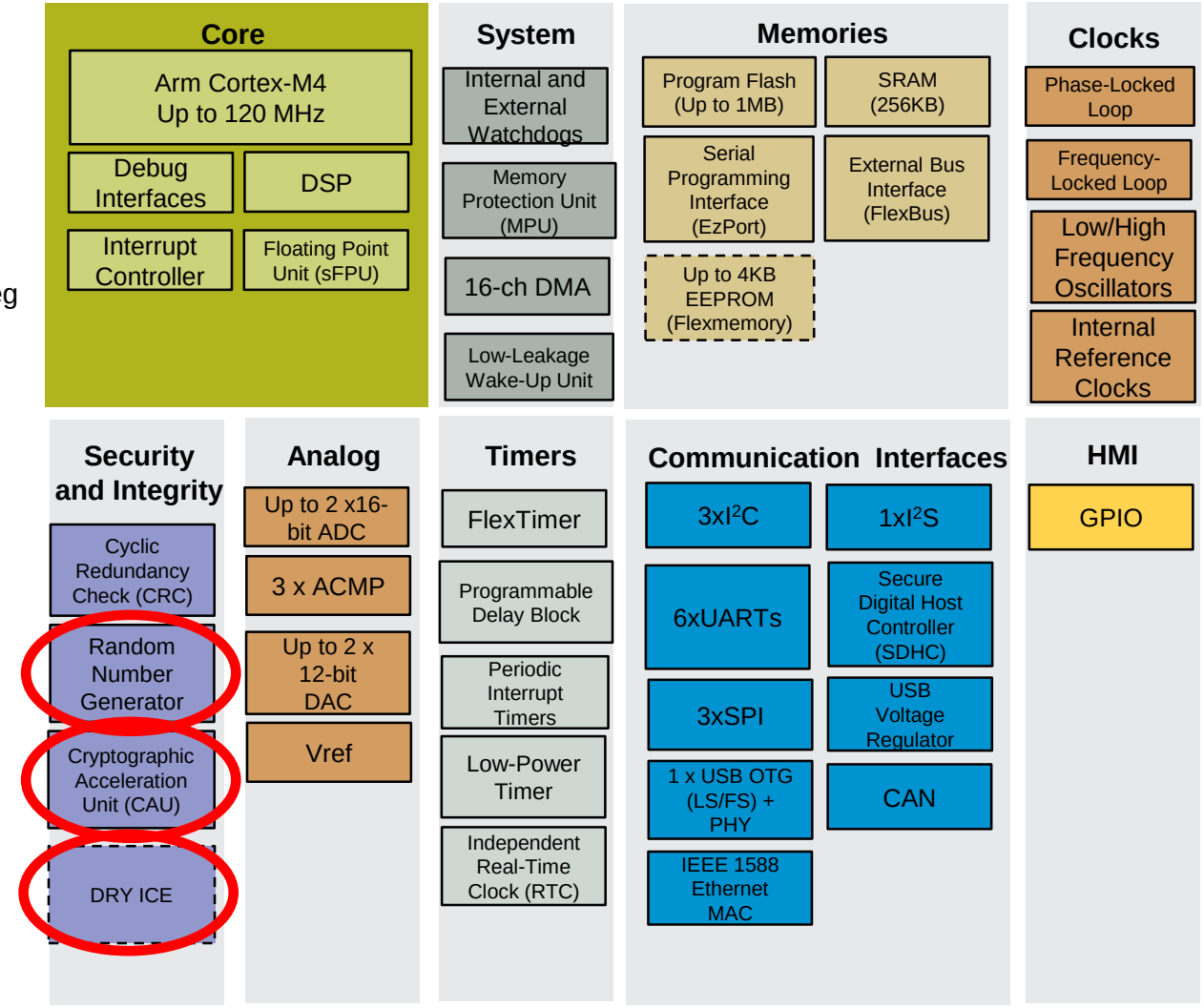
**Communications**
- USB OTG FS/LS w/ PHY and USB Vreg
- Ethernet w/ IEEE1588
- CAN
- Multiple serial ports

**Analog**
- 2x 16-bit ADC
- 2 x 12-bit DAC;  3 x ACMP

**Timers**
- 2x8ch FTM (PWM)
- 2x2ch FTM (PWM/Quad Dec.)
- Low Power Timer
- RTC with independent Vbat supply

**Others**
- 1.71V-3.6V; -40 to 105ºC
- Up TBD to x I/Os (5V tolerant)
- Tamper and Crypto acceleration

**Packages:**100 LQFP, 121 MAPBGA, 144LQFP, 144BGA



# Kinetis : DryIce Tamper Detection Module

**DryIce**

K11, K21, K61, K63, K65, K70, KW2x

## 256-bit Secure Key Register

Erased on tamper
RAM – powered from VBAT
DRY_SKR[0:7]

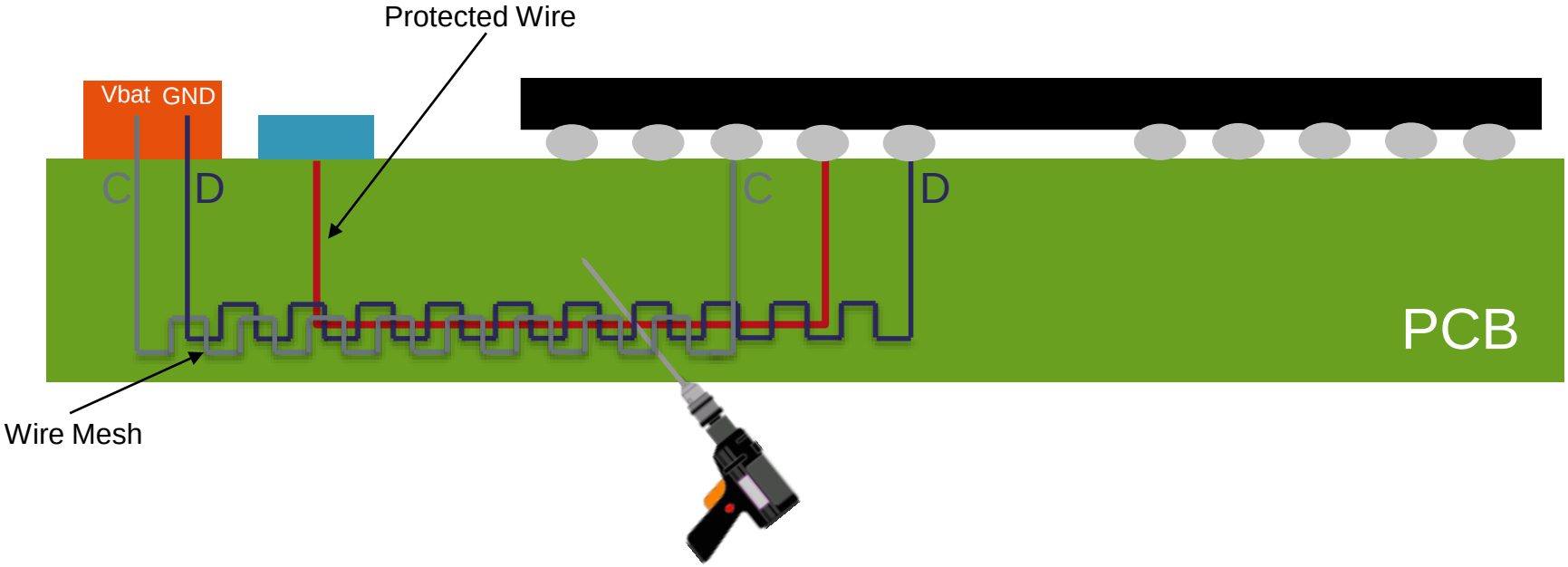
## Tamper Detection

Hardware GPIO
Voltage & temperature
Clock frequency

## Secure Real-time Clock

Timestamps tamper events
Independant VBAT, power-on reset and 32kHz osc

# Differential PCB Tamper Detection (Wire Mesh)




DryIce can output up to two unique active tamper output signals. Each of the active tamper output pins outputs a random value that can change every second (1 Hz).

- **Module will detect Tamper and initiate key erasure when:**
  - C is disconnected (floating)
  - D is disconnected (floating)
  - C and D are short-circuited

# Hash Acceleration in Kinetis microcontrollers

## mmCAU

K11, K21, K24, K26,
K52, K53,
K6x, K70,
KM34, KW2x

***memory mapped Crypto Acceleration Unit***

### Cryptographic Co-processor

Dedicated hardware
Designed to accelerate
cryptographic algorithms

### Supported Algorithms

***Hashing: MD5, SHA-1, SHA256***
Symmetric Ciphers
DES, 3DES
AES

### Software

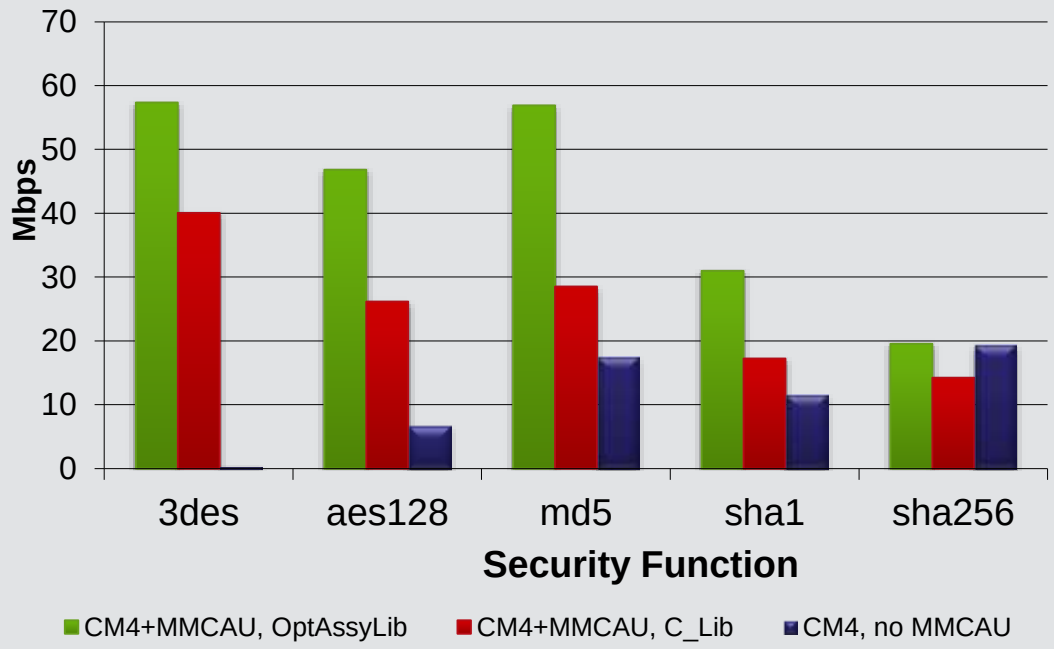
Freescale's MMCAU_SW_LIB
API User guide: CAUAPIUG.pdf
**AN4307**: Using the mmCAU in Kinetis

# Benchmark: Kinetis CAU - Mbps Performance

**Performance: mmCAU_SW_Lib**

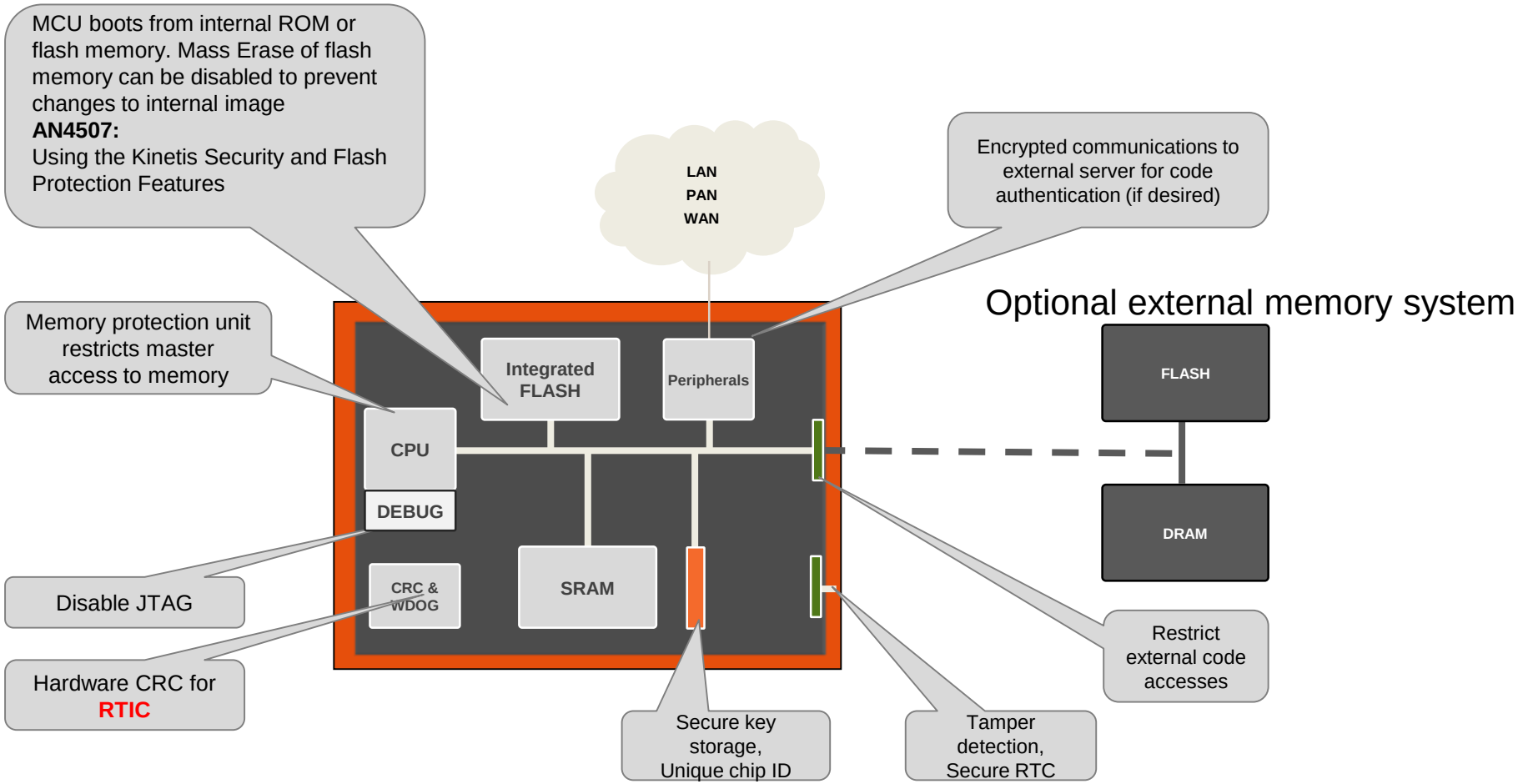
Taller is better

mmCAU accelerates all supported algorithms, but makes only a modest improvement on SHA256




**CAU + core @ 100MHz**

# Secure Code Execution: Kinetis MCU



# i.MX Secure processors & how they rise to meet these challenges

Red indicates change from column to the left

# i.MX6 Supreme Scalable & Flexible Family

## Leverage One Design Into Diverse Product Portfolio

### i.MX 6UltraLite

- ARM® Cortex™-A7 at 528MHz
- 128 KB L2 cache
- 16-bit DDR3/LV and LPDDR2 at 400MHz
- eMMC 5.0/ SD 3.0
- Display: RGB
- Camera: RGB
- 10/100 Ethernet IEEE1588 (x2)*
- USB (x2)*

### i.MX 6SoloLite

- **ARM® Cortex™-A9 at 1GHz**
- **256KB L2 cache**
- 32-bit DDR3/LV and LPDDR2 at 400MHz
- eMMC
- 2D graphics
- Display: RGB, E-Ink
- Camera: RGB
- 10/100 Ethernet

### HMP i.MX 6SoloX

- ARM Cortex-A9 up to 1GHz
- **ARM Cortex-M4 at 200MHz**
- 256KB L2 cache
- 32-bit DDR3/LV and LPDDR2 at 400MHz
- eMMC, **QSPI, NOR, NAND**
- 2D and **3D** graphics
- Display: RGB, **LVDS**
- Camera: RGB, **Analog**
- **Dual Gigabit Ethernet**
- **PCIe (x1 lane)**

### i.MX 6Solo

- ARM Cortex-A9 up to 1GHz
- **512KB** L2 cache
- 32-bit DDR3 and LPDDR2 at 400MHz
- eMMC, NOR, NAND
- 2D graphics
- **3D graphics with 1 shader**
- Display: RGB, LVDS, **E-Ink, MIPI, HDMI**
- **1080p30 video**
- Camera: Parallel, **MIPI**
- Gigabit Ethernet
- PCIe (x1 lane)

### i.MX 6DualLite

- **Dual** ARM Cortex-A9 up to 1GHz
- 512KB L2 cache
- **64-bit** DDR3 and dual-channel 32-bit LPDDR2 at 400MHz
- eMMC, NOR, NAND
- 2D graphics
- 3D graphics with 1 shader
- 1080p30 video
- Display: RGB, LVDS, E-Ink, MIPI, HDMI
- Camera: Parallel, MIPI
- Gigabit Ethernet
- PCIe (x1 lane)

### i.MX 6Dual / i.MX 6DualPlus

- Dual ARM Cortex-A9 up to **1.2GHz**
- **1 MB** L2 cache
- 64-bit DDR3 and 2-channel 32-bit LPDDR2 at **533MHz**
- eMMC, NOR, NAND
- 3D graphics with **4 shaders**
- **Two** 2D GFX engines
- **Up to 1080p60 video**
- Display: RGB, LVDS, MIPI, HDMI
- Camera: Parallel, MIPI
- PCIe (x1 lane)
- Gigabit Ethernet
- **SATA-II**

### i.MX 6Quad / i.MX 6QuadPlus

- **Quad** ARM Cortex-A9 up to 1.2GHz
- 1 MB L2 cache
- 64-bit DDR3 and 2-channel 32-bit LPDDR2 @ 533MHz
- eMMC, NOR, NAND
- 3D graphics with 4 shaders
- Two 2D GFX engines
- Up to 1080p60 video
- Display: RGB, LVDS, MIPI, HDMI
- Camera: Parallel, MIPI
- PCIe (x1 lane)
- Gigabit Ethernet
- SATA-II

Pin-to-pin and Power Compatible (*except PoP)

Software Compatible

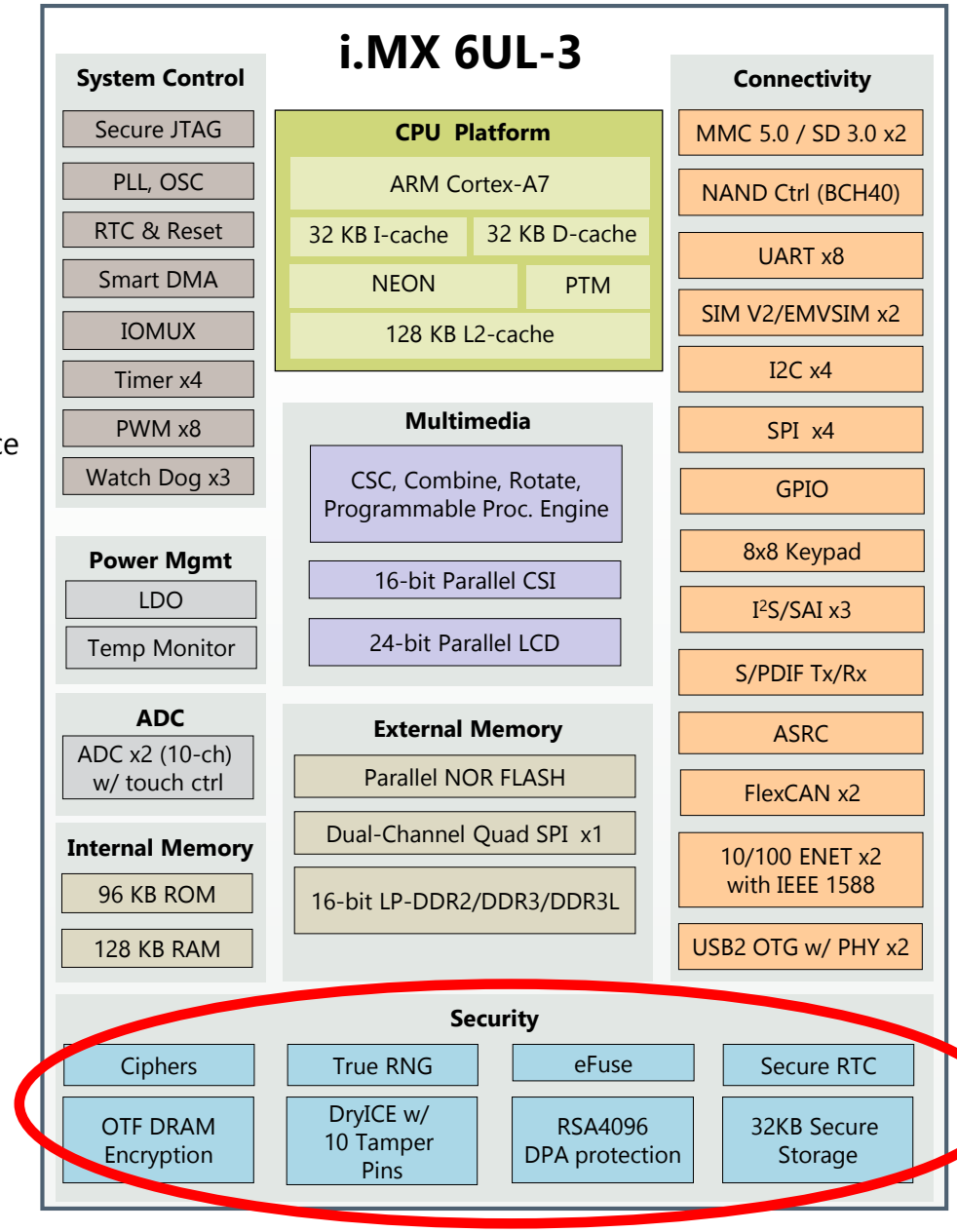
- **ARM Cortex-A9 based solutions ranging up to 1.2GHz**
- **HD 1080p encode and decode (except 6SoloLite/6SoloX), 3D video playback in high definition (except 6SoloLite/6SoloX)**
- **Integrated IO's may include HDMI v1.4, MIPI and LVDS, display ports, MIPI camera, Gigabit Ethernet, multiple USB 2.0, SATA and PCI-Express**
- **SW support: Google Android™, Linux®, QNX (3rd party), Windows® Embedded CE (3rd party)**



* Depending the part number

# i.MX 6UL-3 High Security Processor

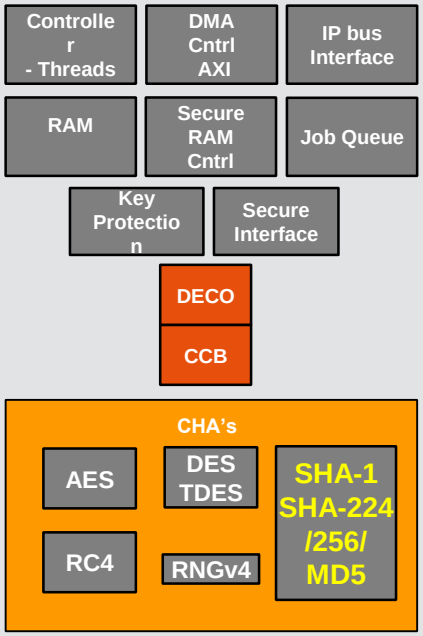
- **Specifications**
  - **Process:** TSMC 40LP
  - **Core Voltage:** 1.1V
  - **Package:**
    - 289 MAPBGA (14x14, 0.8 mm pitch)
    - 289 MAPBGA (9x9, 0.5mm pitch)
  - **Temperature:** -40C to 105C (Tj.)
- **Key Features and Advantages**
  - ARM Cortex-A7 @ 528 MHz, 128 KB L2 cache
  - LCD Display up to WXGA (1366x768)
  - 8-bit/10-bit/16-bit Parallel Camera Sensor Interface
  - 16-bit LP-DDR2, DDR3/LV-DDR3
  - 16-bit Parallel NOR FLASH / PSRAM
  - Dual-channel QuadSPI NOR FLASH
  - 8-bit Raw NAND FLASH with 40-bit ECC
  - 2x MMC 5.0/SD 3.0/SDIO Port
  - 2x USB 2.0 OTG, HS/FS, Device or Host with PHY
  - Audio Interfaces include I2S/SSI, S/PDIF Tx/Rx
  - 10/100 Ethernet with IEEE 1588 x 2
  - **Security Block**: TRNG, Crypto Engine (AES/TDES/SHA/RSA with DPA), Tamper Monitor, Secure Boot, SIMV2/EVMSIM X 2, OTF DRAM Encryption, PCI4.0 pre-certification
  - Partial PMU Integration
- **Enablement**
  - Linux BSP from Freescale
  - Brillo *(Under Investigation)*



# Hash Acceleration in i.MX

## Hashing Algorithms

- SHA-1,224/256-bit digests
- MD5 128-bit digest
- HMAC




**CAAM**

*Crypto Acceleration & Assurance Module*

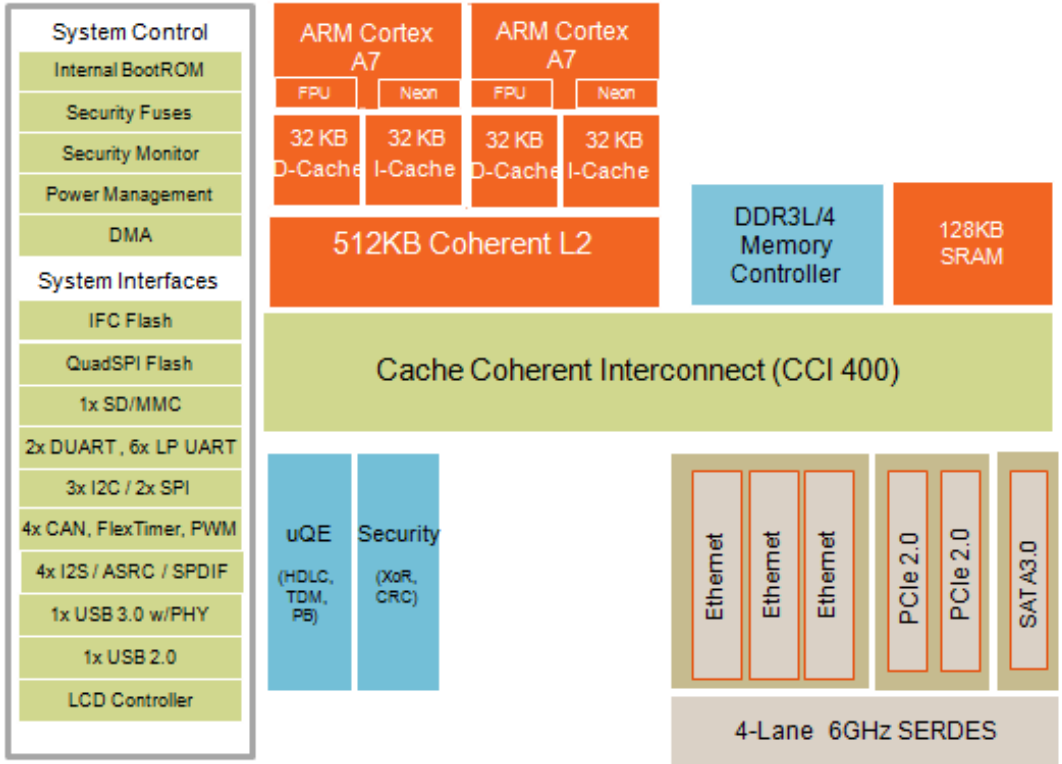
# i.MX 6UL-3 – Key Security Features

| Security Features | Freescale Comments |
|---|---|
| **Hardware Cryptographic Accelerators (CAAM)** | Symmetric key authentication:<br>– AES-128/256, with DPA protection<br>– DES, 3DES, with DPA protection<br>– ARC4<br>Asymmetric Authentication (public key)<br>– RSA (up to 4096)<br>– Elliptic curve "ECDSA" (up to P-521). |
| **Cryptographic hash function** | SHA-1, SHA-224, SHA-256 |
| **Tamper detection & Protection** | – DryICE (On-Chip Voltage, Temp, Freq Monitoring)<br>– Dedicated tamper pins, 10 pins total (Can be configured to be 10 passive or up to 5 active pairs - up to 20uA with 10 Tamper active)<br>– Tamper Logging |
| **Hardened readback disable** | Yes, lock bit can disable the access of the key |
| **DPA resistant** | DPA Protection for DES/3DES and AES |
| **Obfuscated key Storage protection** | On-chip zeroizable 8x4kB Secure RAM |
| | Off-chip key/data blobs AES-256 master key (CAAM/SNVS) |
| **Permanent JTAG disable** | Yes - Secure JTAG Controller (with electrical fuses) |
| **Internal key clearance** | On-chip zeroizable 8x4kB Secure RAM (32KB) |
| **Unique ID (Device DNA)** | Yes, as the OTPMK secret, which is unique per part. The OTPMK cannot be directly read but can be used to encrypt a constant to create a unique number, for use as a unique ID. |
| **Unique ID (User eFuse)** | Yes |
| **Secure storage** | – Zero-able master key (256-bit)<br>– General purpose 32-bit register<br>– Secure High Assurance Boot<br>– 2K-bit E-Fuse |
| **Permanent decryptor disable** | Yes (export disable fuse – disable all crypto except hash engine and RNG) |
| **Secure RAM w/ battery backup** | Yes - Secure real-time clock (SNVS) |
| **Additional Security Features** | – Run-time Integrity Checker and Security Controller<br>– Random Number Generator (NIST SP 800-90)<br>– ARM TrustZone<br>– 2x EMV compatible SIM V2 & EMVSIM module |

# Layerscape processors & how they rise to meet these challenges

# Trust Architecture on LS1

# QorIQ LS1021A




- **Dual ARM Cortex-A7 cores up to 1.0 GHz**
  - ECC protected L1/L2 caches
  - DDR3L/4 up to 1.6GHz
- **Over 6,000 Coremark at under 3.7W (TDP power)**
- **Industry best Coremark / mW ratio**
- **Outstanding security and IP forwarding**
- **High integration reduces BOM costs** for targeted applications:
  - Industrial gateways
  - Industrial Automation
  - Printing & Imaging
  - HMI
  - M2M, Smart "X"

**Key Architectural Features:**

- ARM AMBA4 MPCore™ Virtualization
- DDR3L/4 32-bit with ECC support
- 3-port GigE with IEEE 1588
- 2x PCI Express Gen2
- Multi-protocol 4-Lane SerDes
  - PCIe-2, SATA3, SGMII
- QUICC Engine – HDLC/TDM/ProfiBUS
- EnergyStar support with fast wakeup
- 2Gbps IP forwarding

**Key System Integration Features:**

- Low-cost NAND/NOR flash systems
- Low-cost DRAM systems
- USB3 SuperSpeed
- Audio networking and motor control
- QorIQ Trust Architecture and ARM TrustZone support
- Alignment with Kinetis/Vybrid portfolio

## Package & Board:

| | |
|---|---|
| Package: | 525-pin, 19x19mm, 0.8mm ball pitch |
| Power: | ~2.8W @1.0GHz Typical |
| Temp: | -40C (TA) to 105C (Tj) |
| Boards: | Tower low-cost board, IoT Gtwy<br>Freescale Linux BSPs |

# LS1 Security Engine Overview (SEC 5.5)

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

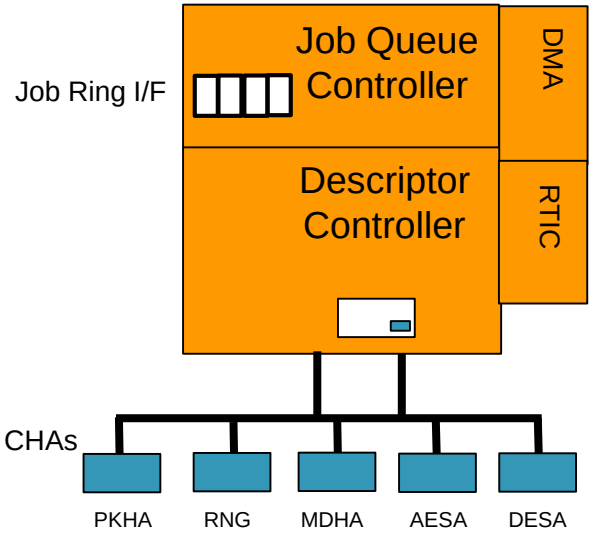
**(1) Random Number Generator (RNG)**
- NIST Certified
- RNG supports key generation algorithm

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

**(1) Advanced Encryption Standard Accelerators (AESA)**
- Key lengths of 128-, 192-, and 256-bit
- ECB, CBC, CTR, CCM, GCM, CMAC, OFB, CFB, and XTS

**(1) Data Encryption Standard Accelerators (DESA)**
- DES, 3DES (2K, 3K)
- ECB, CBC, OFB modes

**(1) CRC Unit**
- CRC32, CRC32C, 802.16e OFDMA CRC

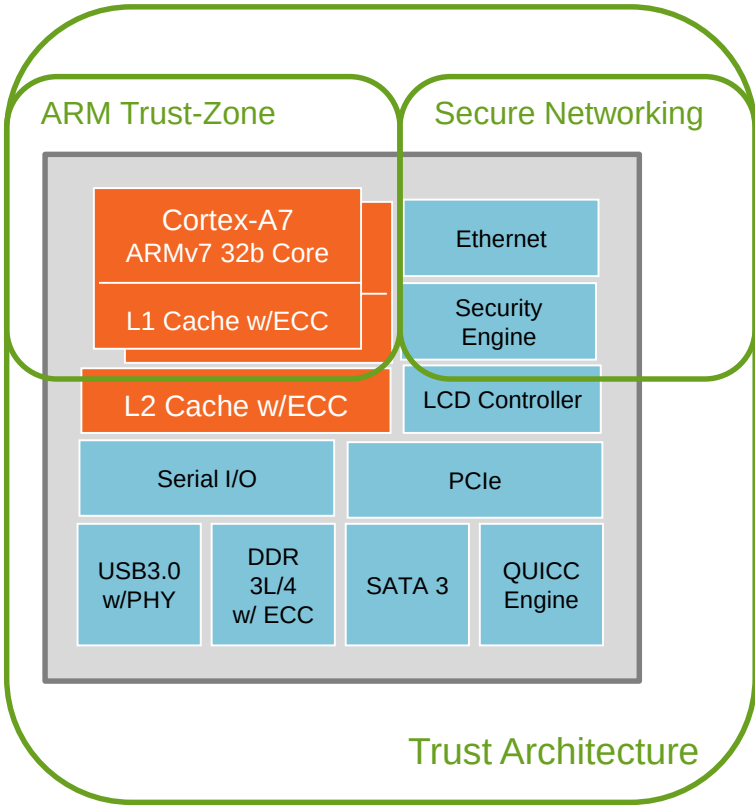



**Header & Trailer off-load for the following Security Protocols:**
- IPSec
- SSL/TLS
- SRTP
- 802.11i
- 802.16e
- 802.1ae

# LS1 Trust Architecture

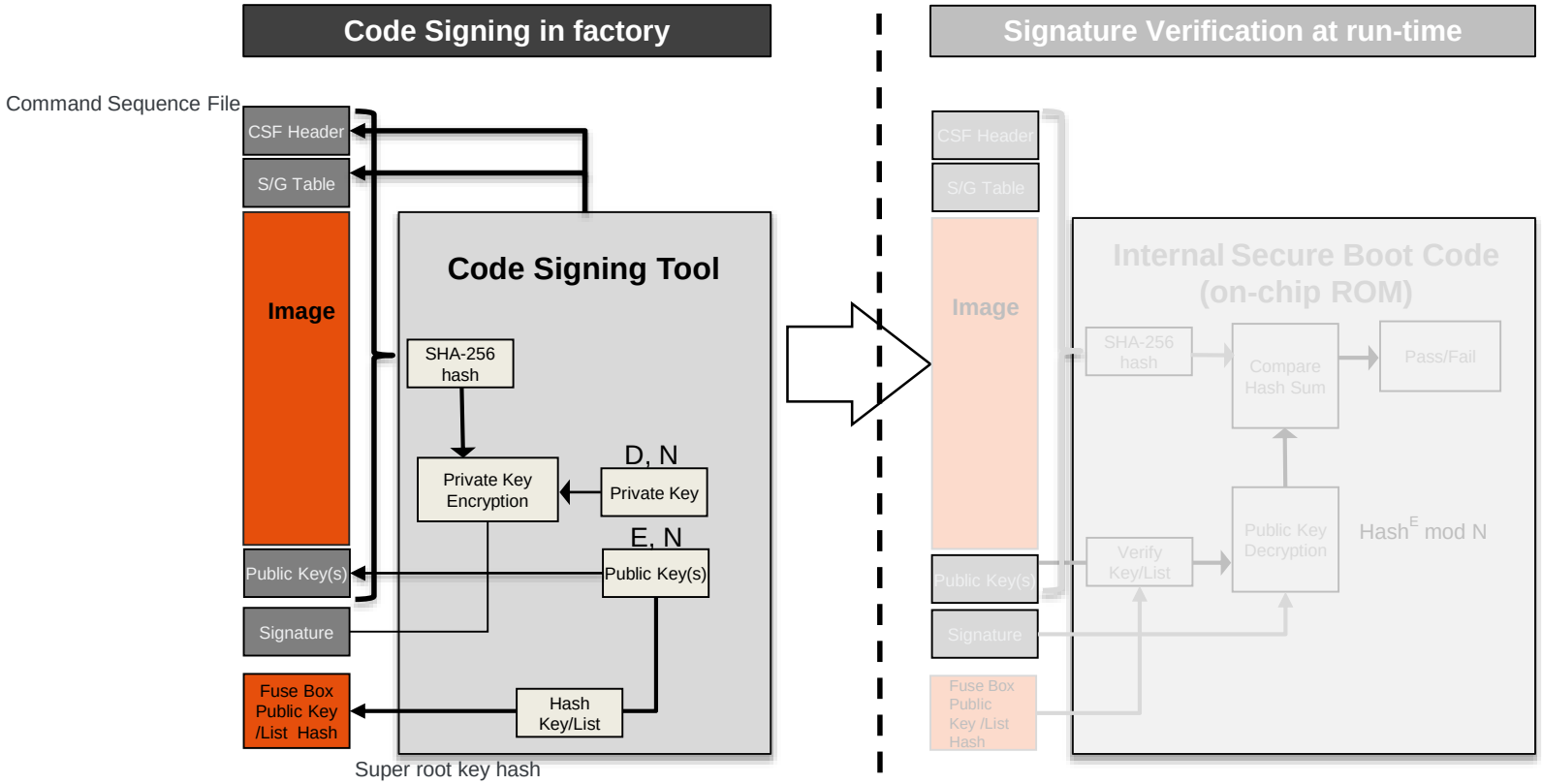
- **ARM Trust-zone** - Trusted execution environment for security-critical SW
- **Secure Boot** – authenticates the software load at boot time
- **Software tamper protection**
  - System-MMUs prevent unauthorised access via I/O Controllers
  - run-time integrity checking can be performed on areas of memory sub-system (for early warning of any unauthorised changes)
  - the debug port can be protected
- **Hardware tamper protection**
  - Can detect and react safely to external physical tamper events
- **Secure Networking**
  - The fully featured LS1 security engine can fully-offload IPsec (authentication, crypto and packet construction)

LS1 Trust Architecture extends the Trusted Zone beyond the CPU/Cache/Memory sub-system to the System level

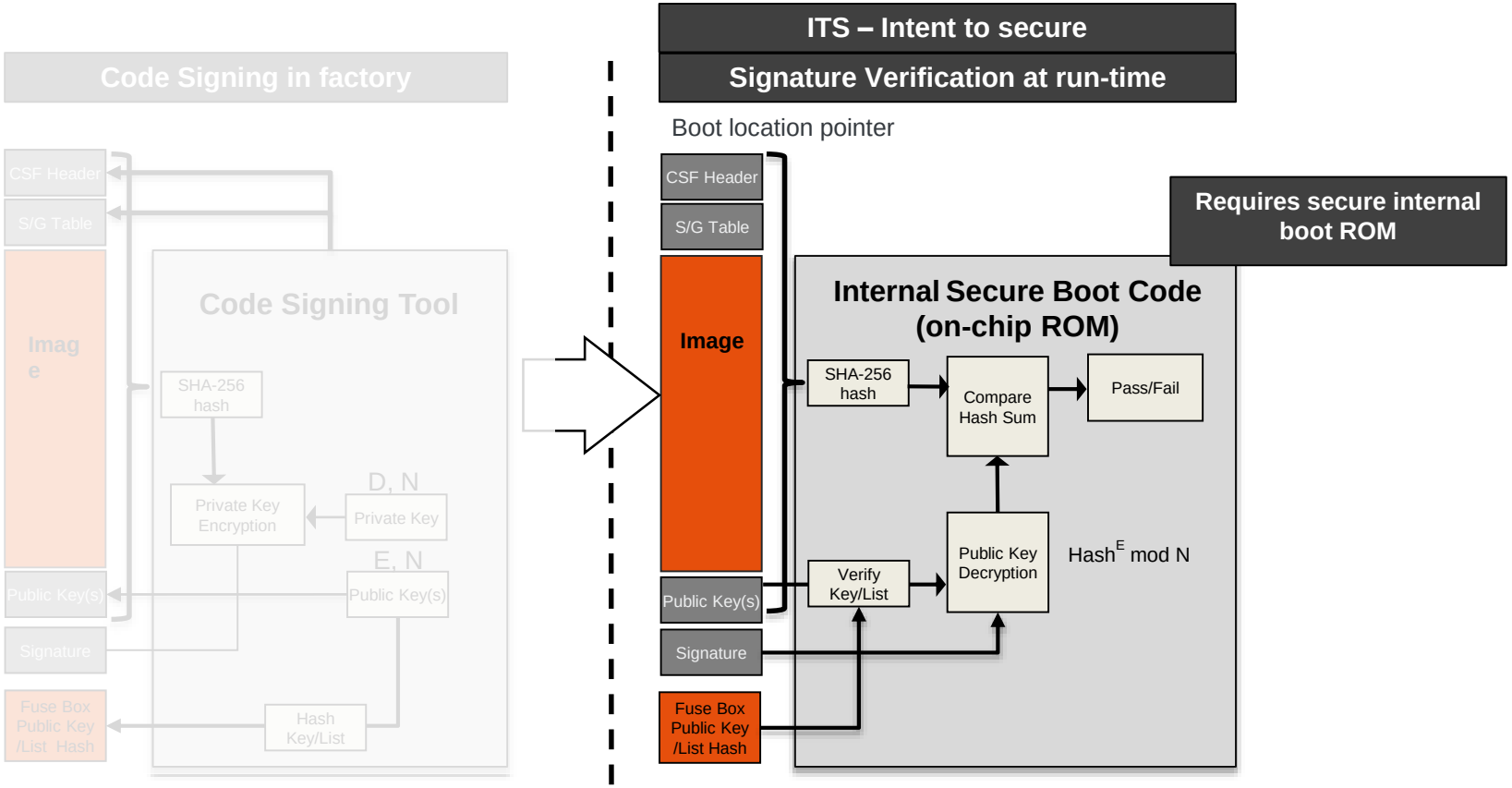



- Trust Architecture ensures that only OEM software can execute
- Trust Architecture protects the OEM software against theft

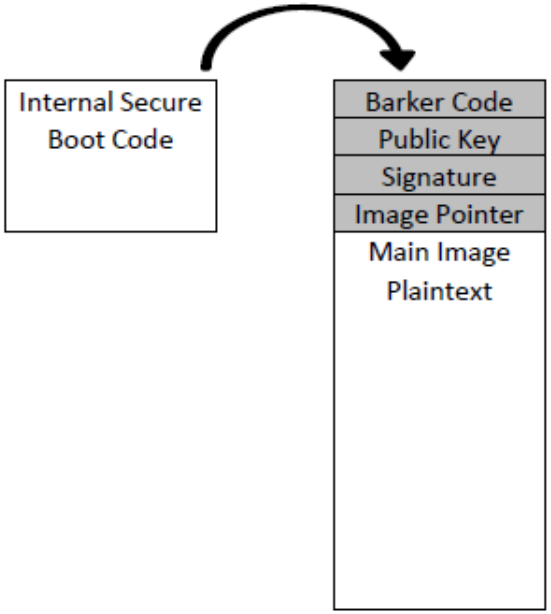
# Secure Boot: Verifying Code *before* Execution



# Secure Boot: Verifying Code *during* Execution

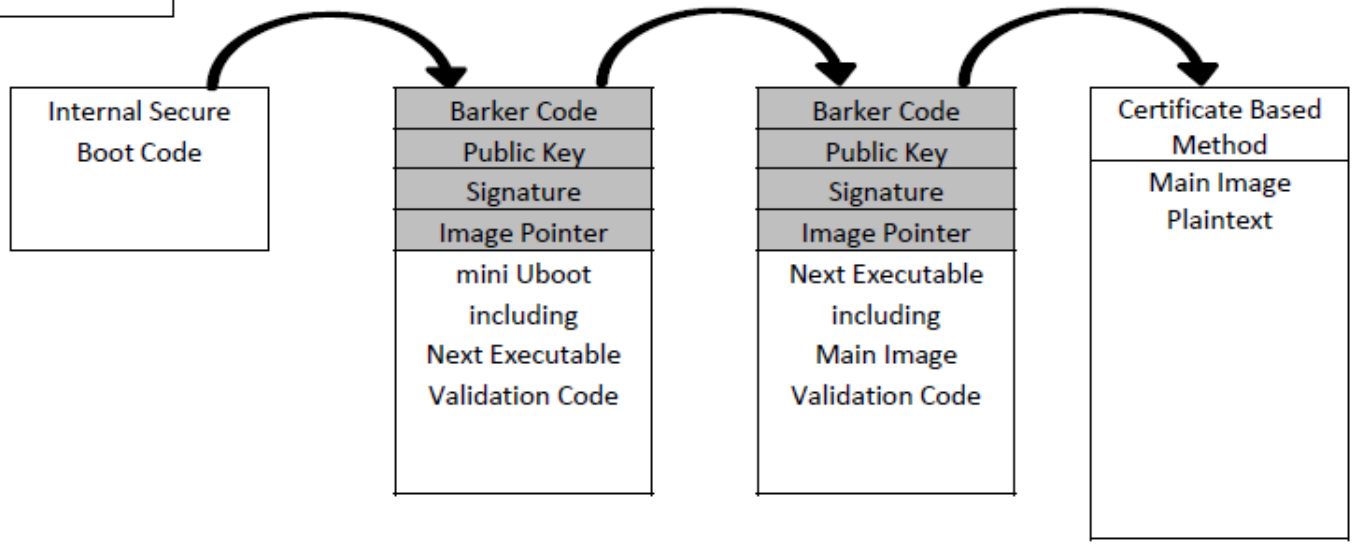


# Chain of Trust



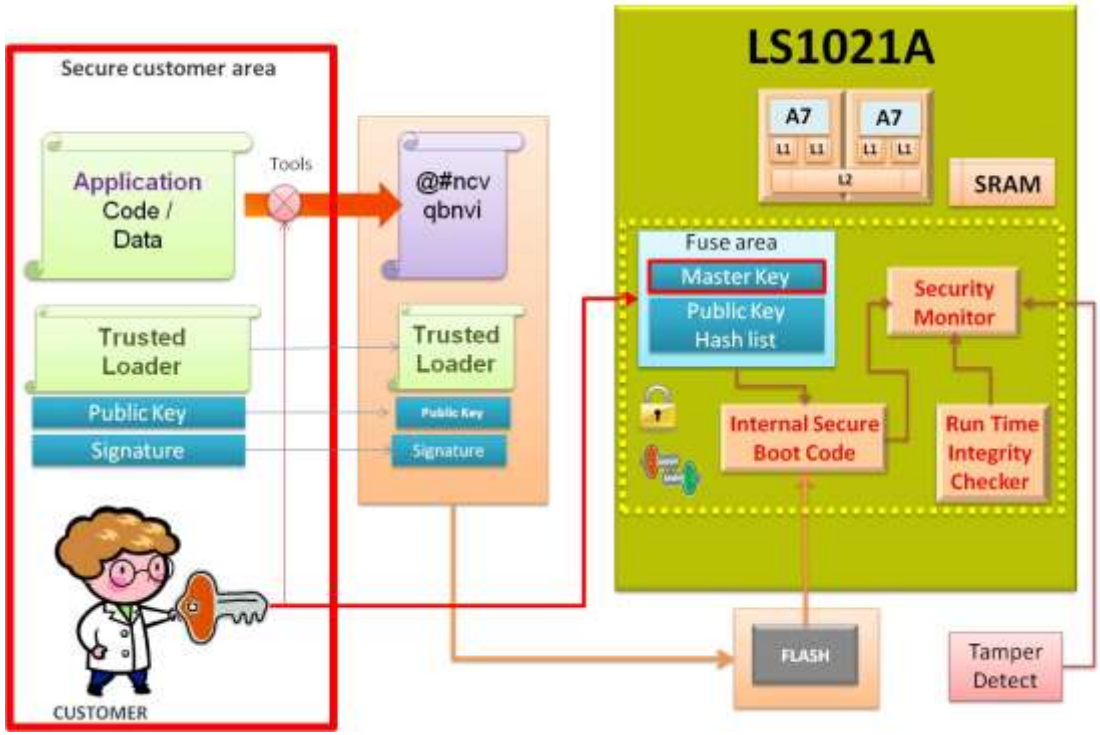

Minimum Implementation:
Single Stage Validation

Layered Implementation:
Multi-Stage Validation Only



# LS1 Secure Boot

1. **Customer** blows keys into device and sets the debug permissions with OTP Debug fuses
2. **Customer** builds **Trusted Loader** with signature using private key and the list Public key(s) is/are embedded
3. **Customer** encrypts the **Application** (code /data) via random number generated key (**Blob key**), which are in turn encrypted using OTP Master Key and embedded in the BLOB
4. **Device** at RESET runs **Internal Secure Boot Code**, which validates and loads the **Trusted Loader**. Now in **TRUSTED** state
5. **Trusted Loader** request security block to validate and decrypt the **Application** (code/data) by decrypting the **Blob key** using the OTP Master Key
6. **Application** can communicate using SSL via a private key included in its data
7. **Security Monitor** can act on S/W violations, external Tamper and code/fixed data changes flagged by Run Time Integrity Checker



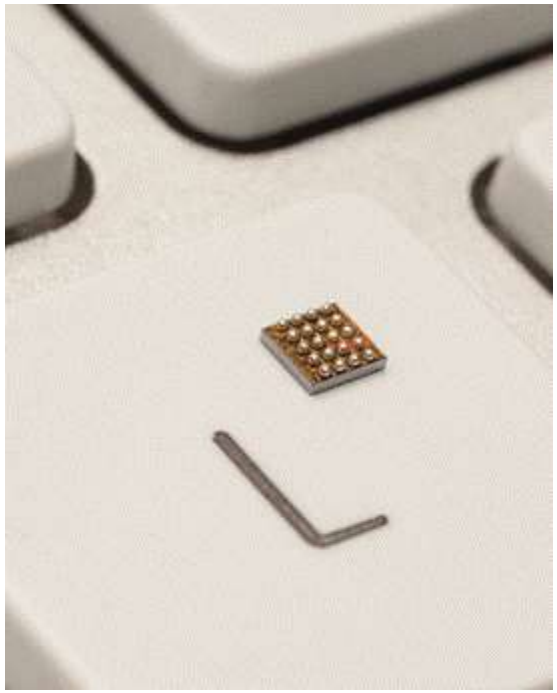

**OTP** – One Time Programmable
**SSL** – Secure Sockets Layer

**De/Encryption**

**Trust Architecture**

**BLOB** Cryptography - securing symmetric key using asymmetric key

# LS1021A Family Customer Enablement Boards



**TWR-LS1021A Evaluation board**

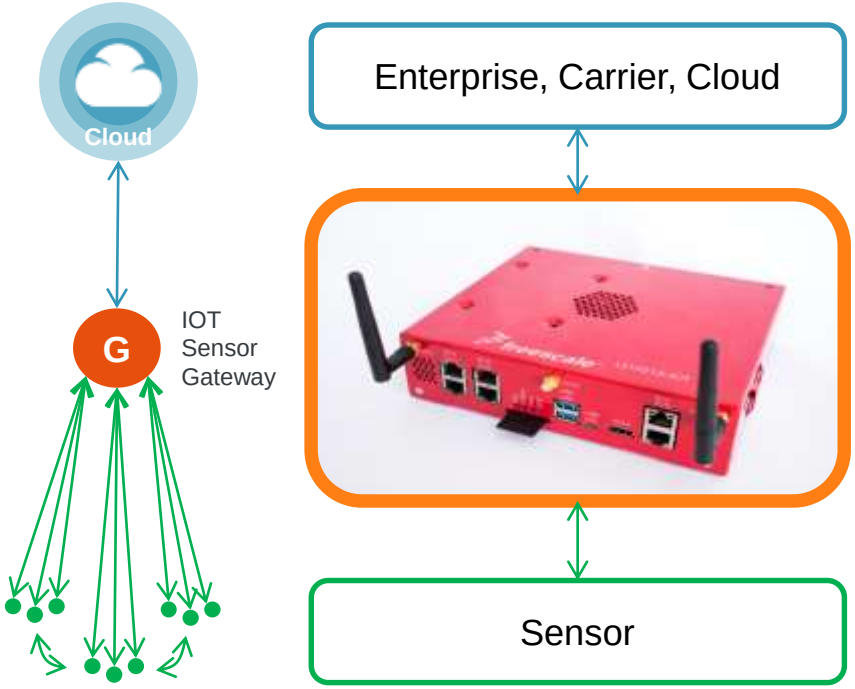
- **Rapid prototyping platform** for Industrial applications
- **Modular design** supports a range of connectivity options
- **Cost-effective**, open source development platform
- Designed to **simplify product evaluation**
- **MSRP $269, available NOW**

**LS1021A-IoT Gateway Reference Design**

- **Multi-protocol support** for IoT devices
- **High speed WAN / LAN** for Cloud connectivity
- **Cost-effective**, open source platform
- Designed to **accelerate time to market**
- **MSRP $429, avail Oct-14**

SECURITY

# LS1021A Solution for IoT Gateway




**Home – Building - Automotive - Factory - Street**

## LS1 IOT Enablement and Key Features

### Trust/Security
- only OEM authenticated SW runs
- anti-tamper : physical and software
- IPsec offload, Elliptic Curve Crypto
- robust partitioning

### Networking
- MQTT, RESTful, JSON, CoAP
- SDN/Openflow
- GigE, Wifi, 3G/4G

### LS1 Compute Efficiency
- 2x ARM CortexA7 – 5000 Coremark
- 512KB L2 Cache
- ECC on L1/L2 & DRAM improves Soft Error Rate
- <3W

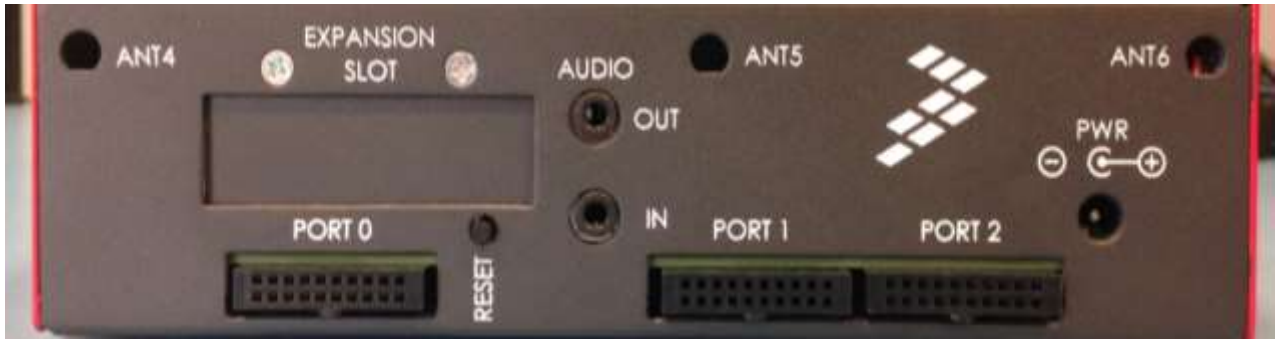
### Ease of Use
- Linux, Java VM, OSGI
- OpenWRT
- Node-RED

### Sensor Networking
- UART, SPI, I2C, Ethernet
- Zigbee, 6lowPAN, BTLE, Thread
- Kinetis-W w/ integrated 802.15.4 radio and software stacks

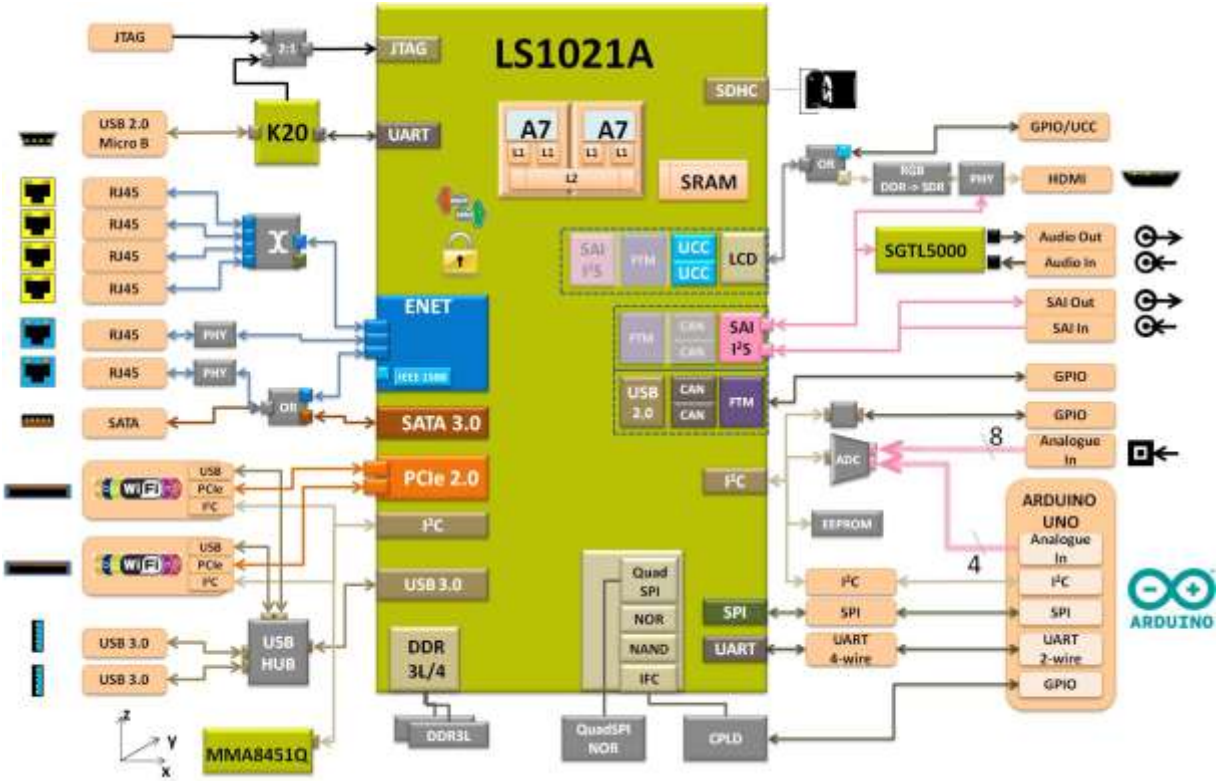
# LS1021A-IOT Gateway Board and Enclosure

- uATX form factor (6.25 x 6.25”)

# LS1021A-IOT Gateway Ports



# LS1021A IoT Base Board




Generic Connectivity Availability

- **Memory**
  - DDR3L 1GB
  - QuadSPI NOR Flash 128MB

  **Connections**
  - Up to 2 x RJ45 GigE direct connect
  - 4 x RJ45 GigE Switch
  - Up to 1 SATA
  - 2 x USB 3.0
  - 2 x mini PCIe (USB, I²C, PCIe)
  - Up to one display (LCD) via HDMI
  - Audio
    - OUT via HDMI or Jack
    - In via Jack
  - Console port/JTAG via USB 2.0
  - GPIO
  - GPIO or FTM
  - LCD or UCCs or GPIO
  - Analogue inputs [8]
  - Arduino connectors
    - Analogue, inputs [4], I2C, SPI, UART (2-wire) and GPIO
- **Accelerometer**
  - MMA851Q

www.Freescale.com

© 2014 Freescale Semiconductor, Inc. | ***External Use***