FTF FREESCALE TECHNOLOGY FORUM 2014

# Emerging Financial Payment Applications Powered by **Freescale Security Solutions**

FTF-CON-F0484

Starle Li | Marketing Manager, AP

M A Y . 2 0 1 4

freescale™

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.

# Agenda

- Explosive Growth of China POS Industry
- Call for Security in Financial Application
- Introduction of Kinetis Security MCU
- Introduction of the i.MX Trust Architecture
- Summary

# China 3rd Party Payment Market is Booming

- According to PBOC's report of 2013:
  - Payment transaction via mobile phone
    - Transaction times: 1.67Billion, **212.86% increase.**
    - Transaction volume: RMB 9.64Trillion, **317.56% increase.**
  - Payment transaction via telephone
    - Transaction times: 0.45Billion, **-6.59% increase.**
    - Transaction volume: RMB 4.74Trillion, **-8.92 % increase.**

# Direct Acquiring vs. 3rd Party Payment

Acquiring Surcharge Share
7:2:1

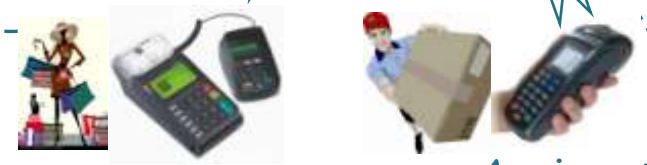
7

Inter-bank Settlement

Inter-bank Settlement

1

Acquiring



Acquirer

Acquirer

2

Paying

# Lakala mobile POS Reshapes Mobile Payment

- Low cost
- Leverage resource of mobile phone
  - BT interface with mobile phone, no 3G/LTE modem is needed.
  - Low power to provide longer battery life.
- Mini form factor for mobile application

# China POS Products Evolution

Payment carriers approved by PBOC will penetrate into acquiring business by selling mPOS to micro merchants.

PBOC approved 250 payment carriers from March 2011 to July 2013, and 47 out of 250 have the license of acquiring.

http://www.hkrt.cn/pc.asp?id=39

CUP and banks began to promote mPOS to expand the online payment business to defeat 3rd party payment carriers.

http://cn.unionpay.com/online_pay/minipay/file_94977279.html

# mPOS vs. Traditional POS

| | Traditional POS | mPOS |
|---|---|---|
| **Target Users** | Medium and big merchants | **Micro and smaller merchant** |
| **Operators** | Banks, CUP | **Banks, 3rd party payment providers** |
| **Business Model** | Surcharge of transaction paid by merchants | Surcharge of transaction paid by merchants, but much lower than traditional POS |
| **Platform Requirement** | High, Application processor with security module | Low, MCU and security module |
| **Interface to mobile devices** | N/A | **USB, Bluetooth** |
| **Cost** | High | **Low** |
| **Safety Level** | High | High |
| **Freescale Product** | i.MX258 | K21D, K21F |

# Security in POS

# How Much Security?

When protecting a system you must consider:

- What are you trying to protect?
- 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?

# Categories of Attack in Embedded Systems

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

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

- **Classification per type**
  - Invasive or semi invasive
  - Non invasive >side channel attack
  - Software

# How are Systems Protected Today?

**Physical security:**

- Secure packaging
- Secure packaging with tamper detect (i.e. micro-switch, pressure monitoring)
- Secure packaging with tamper detect and destruction (i.e. dynamite)
- Obscured part numbers
- Hidden layers
- Protected location

**Electronic Security:**

- **Security bit, to protect on-chip non-volatile memory (e.g. Flash on MCUs)**
  - Prevent external access to on-chip resources:
    - Locks device into Single Chip mode (disables external parallel bus)
    - Disables Background Debug Mode
    - Disables Test Mode
    - Disables JTAG
    - Disables any (serial) “Bootstrap” functions
  - Memory array bulk erase turns security bit off (user selectable option)
- **Secure System (e.g. Trust Zone)**
  - Code signing to prevent software tampering
  - Assurance for stored IP
  - Data stored encrypted in internal or external memory
  - Data decrypted and stored in on-chip private memory at runtime
    - How do you protect software IP in external memory systems?
- **Proprietary (CPU) Design**
- **Silicon Obfuscation (e.g. obscuring metal layer)**
- **On-Chip Encryption Acceleration**
  - How do you protect the keys?

# Example 1 : power analysis : SPA, DPA…

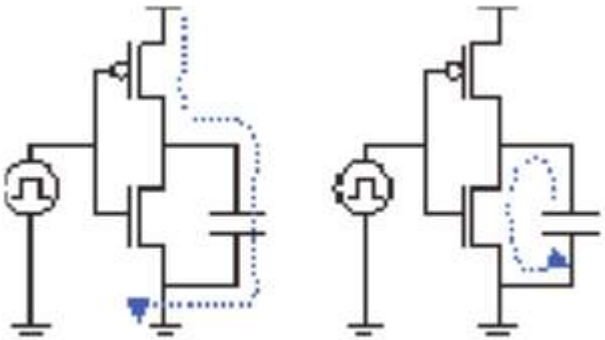
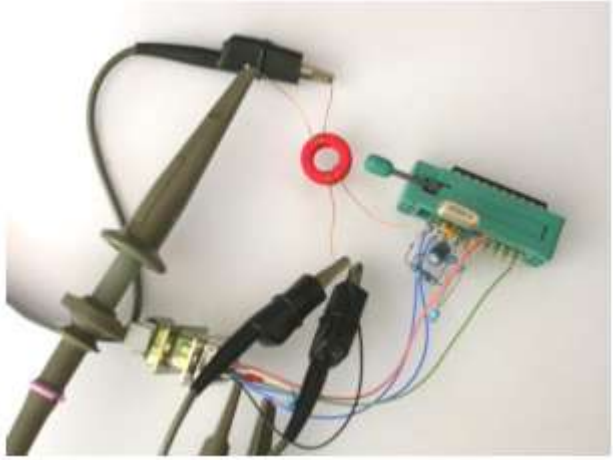


*Figure 2: Current through CMOS inverter (source: Peeters et al., 2006)*



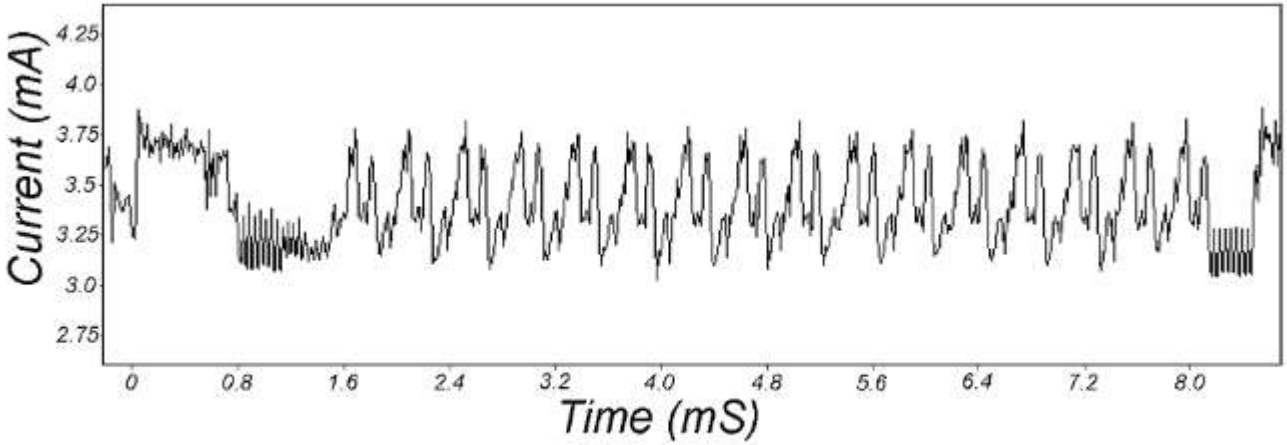
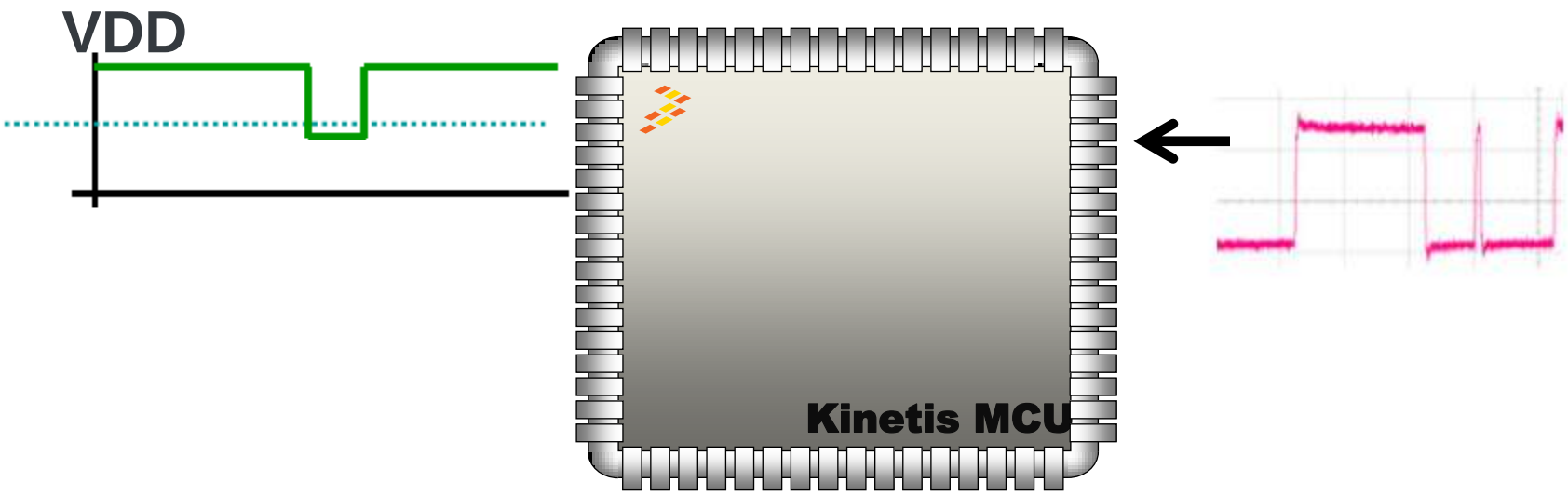


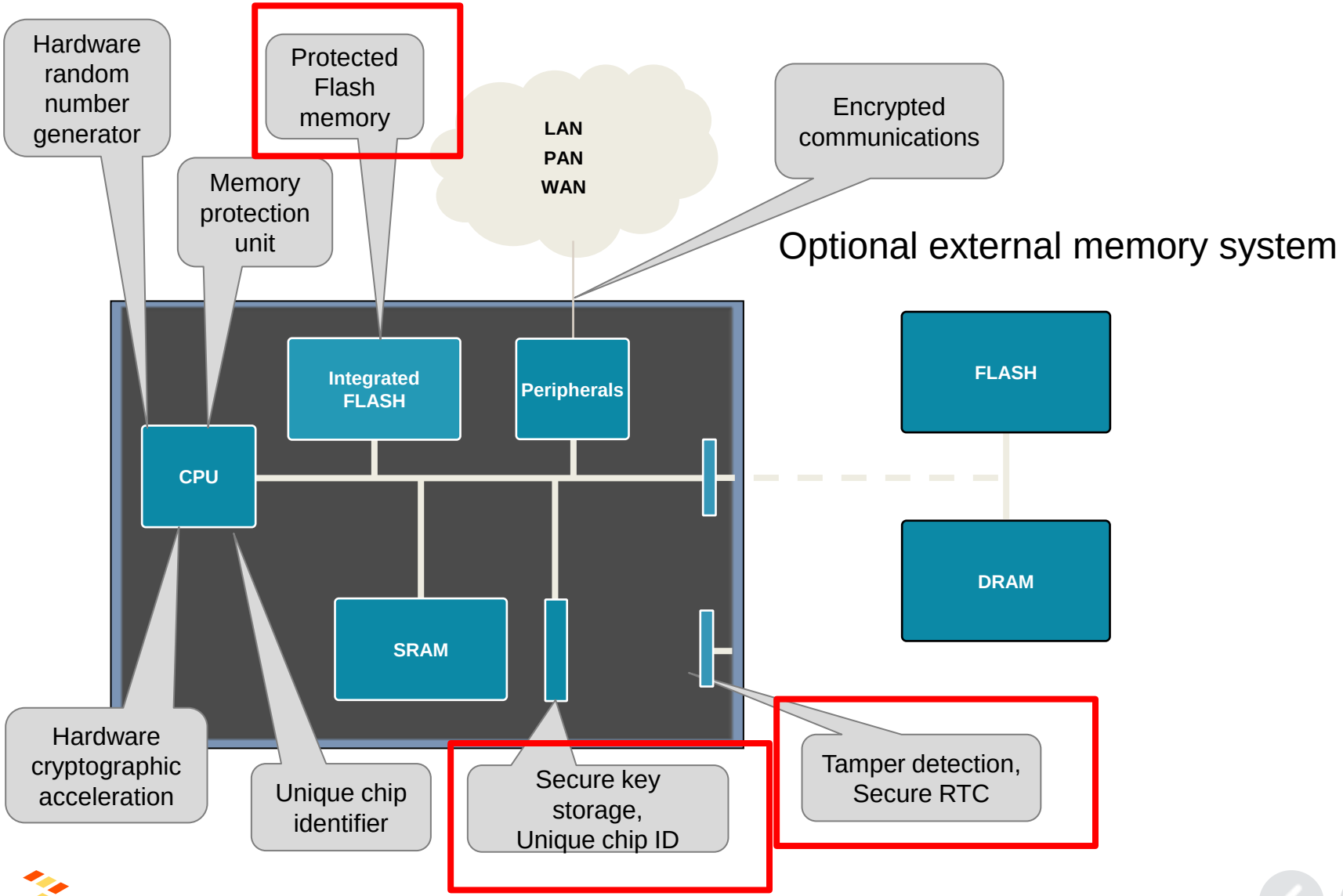

*Figure 3: SPA trace from typical smartcard showing 16 rounds of DES operation (source: Kocher et al, 1999)*

# Example 2 : spike/glitch attack

- Glitch attacks are fast changes in the signals supplied to the device and designed to affect its normal operation. Usually glitches are inserted in power supply and clock signals

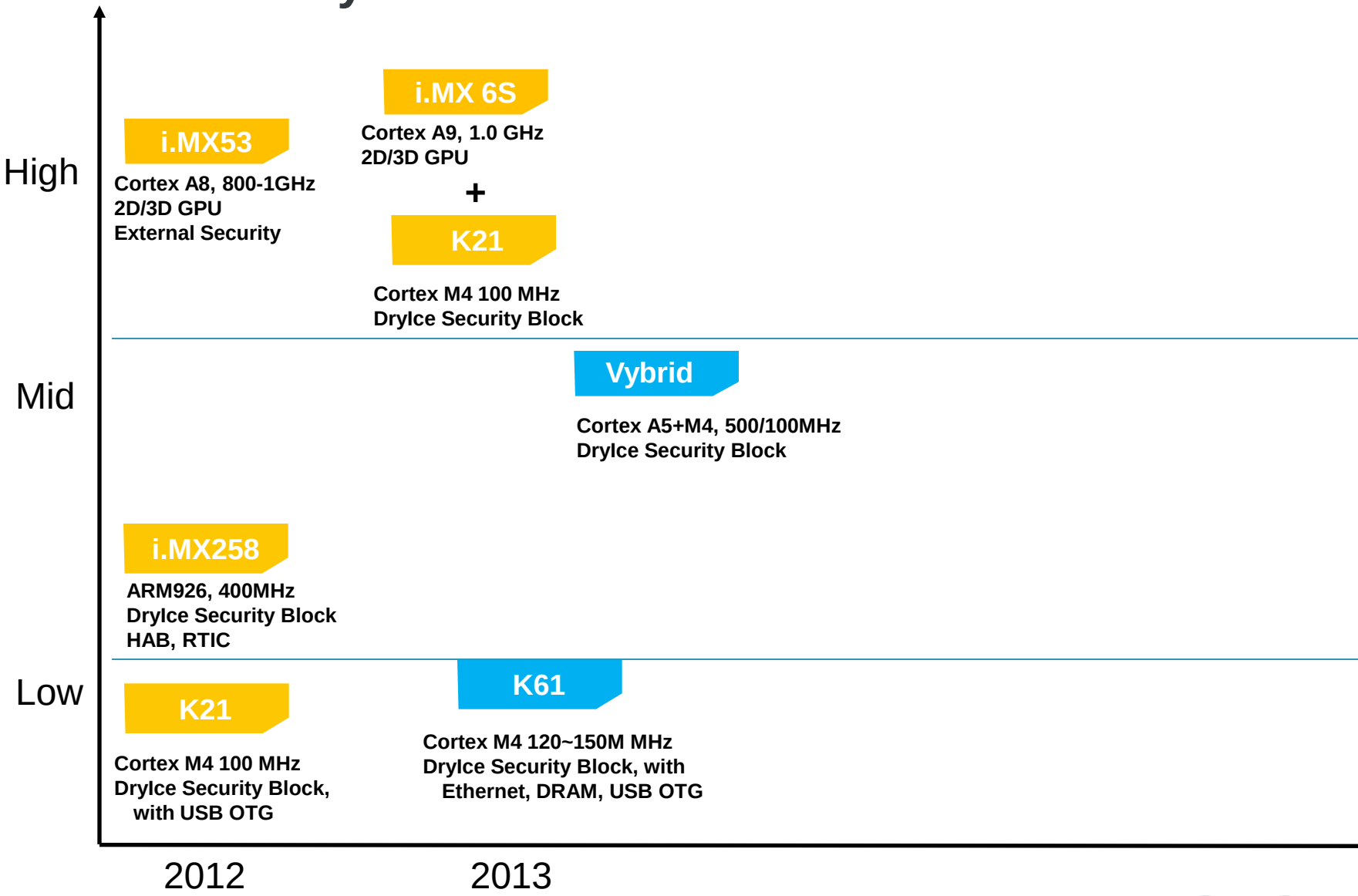


# Microcontroller System Security Requirement



# Freescale Products for Security

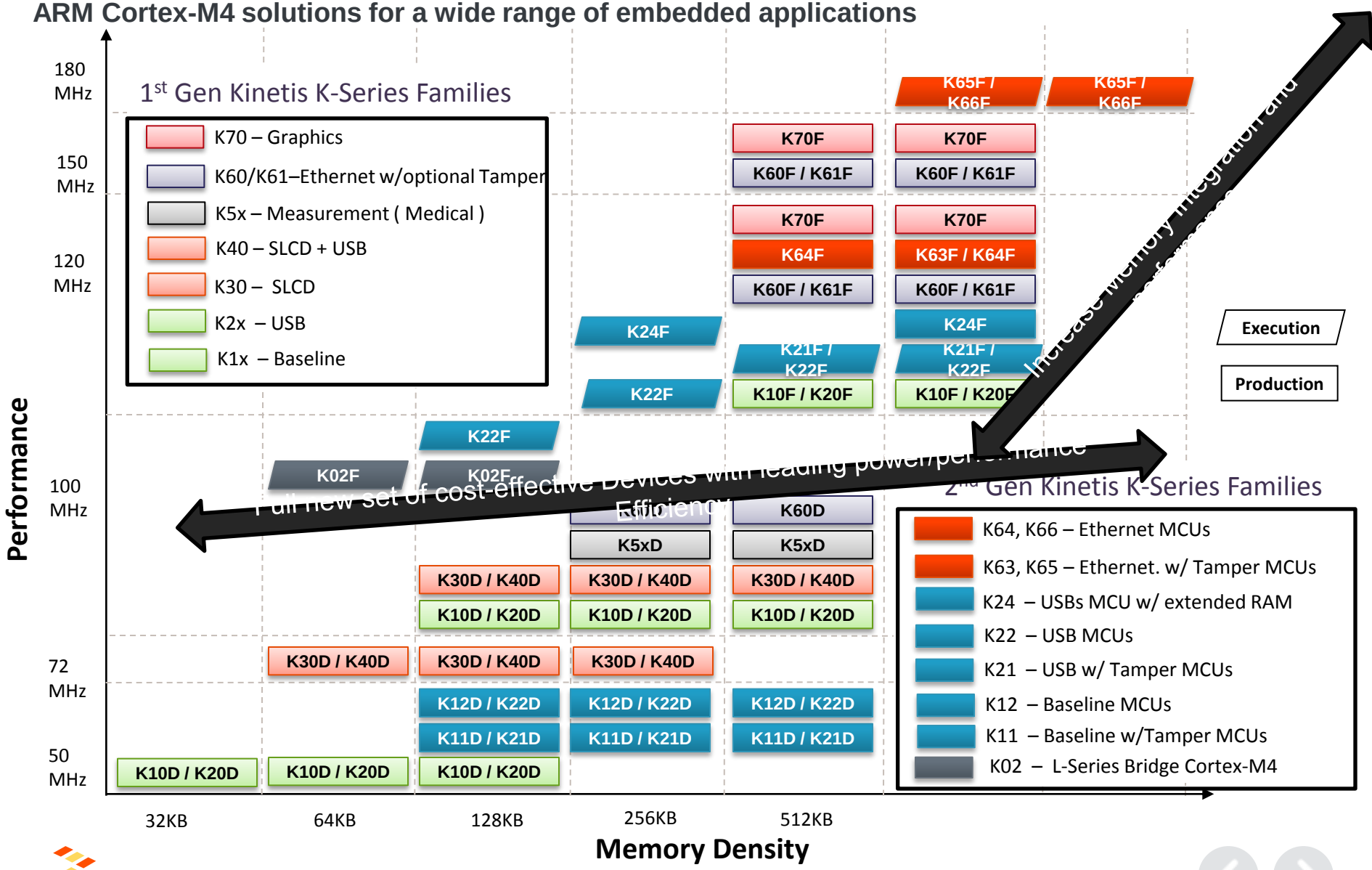
# Freescale Security MPU/MCU Overview



# Kinetis MCU for Security

# Kinetis K-Series Portfolio

## ARM Cortex-M4 solutions for a wide range of embedded applications



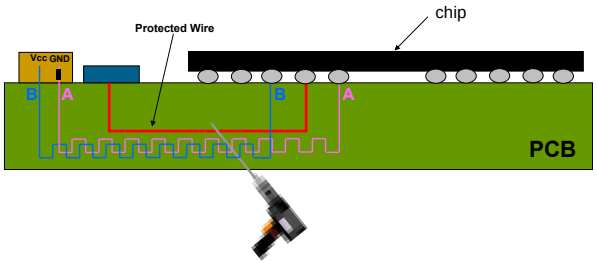
# Kinetis: Security

| | |
|---|---|
| Flash Security<br>*(All Kinetis families)* | 4-level protection limits access to flash resources safeguarding user's IP |
| Memory Protection Unit<br>*(All Kinetis families)* | Data protection and increased software reliability |
| Tamper Detection & battery back-up<br>*(K60, K70 families)* | Voltage, frequency, temperature & external sensing for physical attack detection |
| Cryptographic Acceleration Unit<br>*(K1x, K2x, K50, K60, K70 families)* | •Faster than s/ware implementations with only minimal CPU intervention<br>•Wide variety of algorithms supported |
| H/w Cyclic Redundancy Check<br>*(All Kinetis families)* | Validation of memory contents and communication data for enhanced system integrity |

# Kinetis Security Summary

- The entire (current) Kinetis family includes enhanced Flash security, with user selectable:
  - Security bit, disables external and debug access
  - Backdoor access enable
  - Factory access enable
  - Block erase & re-program disable
  - Hardware protection against "Noise injection" attacks
  - Memory Protection Unit
  - 128-bit unique part identifier

- K60 and K70 120/150 MHz parts in 256 MAPBGA packages, and K11 and K21 50 MHz parts add:
  - Battery backed up Tamper detection, monitoring-
    - Supply voltage
    - Clock frequency
    - Temperature
    - External sensors
    - External physical tampering (e.g. drilling into PCB)
  - 256-bit secure user storage (key), erased on tamper
  - Secure real time clock



# Kinetis: Security

## K10/K20/K30/K40/K50/K60/K70

### Flash Security Options:

- User backdoor access disable
- Factory access disable
- Mass erase disable
- Multiple transfers from Flash to config register

Prevent External accesses for reading or programming

Prevents block and security bit erase, and re-programming. Protects against system impersonation

Protects secure system against electrical noise attacks

### Memory Protection Unit (MPU):

- 16 areas, supervisor/user (config registers are fully accessible)

Allows “sandboxing”, running software with restricted access permissions

### Cryptographic Acceleration Unit (CAU): (K10/20/50/60/70 only)

- Symmetrical crypto
- Hashing functions
- Random Number Generator (RNG)

Reduces CPU loading for cryptographic functions

Facilitates detection of data tampering

Facilitates generation of FIPS140 certifiable random numbers

### Enablement:

- Crypto stacks

Facilitates certificate and authentication to a specific MCU

### Secure storage:

- 128 bit unique chip identifier

### Hardware Cyclic Redundancy Check (CRC)

Accelerates basic data integrity checking

# Kinetis: Security

## K10/K20/K60/K70, 50/120/150MHz

**Flash Security Options:**
- User backdoor access disable
- Factory access disable
- Mass erase disable
- Multiple transfers from Flash to config reg

Protects against a wide range physical attacks on MCU, even during low power modes

**Memory Protection Unit (MPU):**
- 16 areas, supervisor/user (config registers are fully accessible)

**Tamper Detection (with battery backup):**
- Integrated sensors –
  - Frequency
  - Voltage
  - Temperature
- 4x passive external tamper sources (inputs)
- 2x active external tamper sources (2x output and input)

Protects against a wide range physical attacks on hardware system outside the MCU

**Cryptographic Acceleration Unit (CAU):**
- Symmetrical cryp
- Hashing function
- Random Number

Highly secure firmware verification, with secure firmware upgrade capability

**Enablement:**
- High Assurance Boot (HAB) with tools
- Crypto stacks

Protected storage of user key or authentication code, may be used as master key to encrypt additional key depository

**Secure storage:**
- 256 bit user area, erased by tamper
- 128 bit unique chip identifier

**Secure Real Time Clock (RTC):**
- Monotonic
- Overflow and reprogram protection

**Hardware Cyclic Redundancy Check (CRC)**

May be used to prevent firmware downgrading

# Kinetis MCUs with Security and integrity solutions

- http://cache.freescale.com/files/32bit/doc/brochure/BRKINETISSECSOLS.pdf?&Parent_nodeId=&Parent_pageType

# High-end POS Powered by i.MX

# ViewAt Multimedia POS with i.MX6Q+K21D

- Android 4.3 OS
- i.MX6Q
  - 4 ARM Cortex-A9 cores deliver outstanding performance
- K21D
  - Security MCU provides uncompromising protection for financial application

# i.MX258 based PCIPED Certified Product

- **MB400**
  - Product Info

  http://www.miurasystems.com/downloads/MB400-ProductSheet.pdf
  - Certification:

  https://www.pciseccuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php
- **W280**
  - https://www.pciseccuritystandards.org/popups/pts_device.php?appnum=4-40072
- **G810**
  - https://www.pciseccuritystandards.org/popups/pts_device.php?appnum=4-60146

MB400

G810

W280

# i.MX Trust Architecture Features

## Trusted Execution

- Isolates execution of critical SW from possible malware
- TrustZone Secure & Normal Worlds (processor modes)
- Hardware firewalls between CPU & DMA masters and memory & peripherals

## High Assurance Boot

- Authenticated boot: prevents unauthorized SW execution
- Encrypted boot: protects SW confidentiality
- Digital signature checks embedded in on-chip boot ROM
- Run every time processor is reset

## HW Cryptographic Accelerators

- i.MX family dependent
- Symmetric: AES-128, AES-256, 3DES, ARC4
- Message Digest & HMAC: SHA-1, SHA-256, MD-5

# i.MX Trust Architecture Features (continued)

## Secure Storage

- Protects data confidentiality and integrity
- Off-chip: cryptographic protection including device binding
- On-chip: self-clearing Secure RAM
- HW-only keys: no SW access

## HW Random Number Generation

- Ensures strong keys and protects against protocol replay
- On-chip entropy generation
- Cryptographically secure deterministic RNG

## Secure Clock

- Provides reliable time source
- On-chip, separately-powered real-time clock
- Protection from SW tampering

# i.MX Trust Architecture Features (continued)

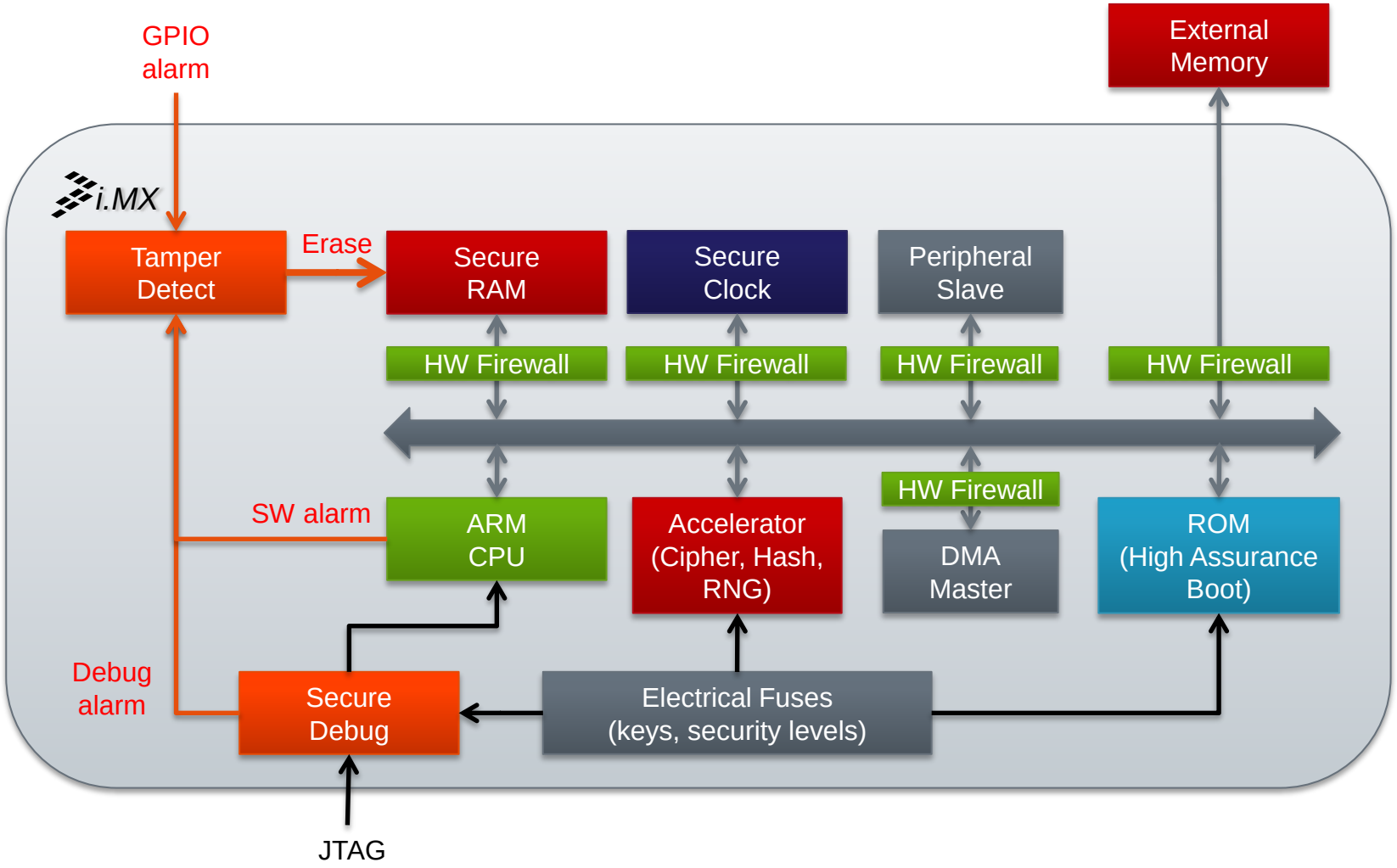
Secure Debug:

- Protects against HW debug (JTAG) exploitation for:
  - Security circumvention
  - Reverse engineering
- Three security levels + complete JTAG disable

Tamper Detection

- Protects against run-time tampering
- Monitoring of various alarm sources
  - Debug activation
  - External alarm (e.g. cover seal)
  - SW integrity checks
  - SW alarm flags
- HW and SW tamper response
- Support varies by i.MX family

# i.MX Trust Architecture – Overview



# i.MX Trust Architecture Deployment

| Feature | i.MX 25 | i.MX 27 | i.MX 28 | i.MX 35 | i.MX 50 | i.MX 51 | i.MX 53 | i.MX 6 |
|---|---|---|---|---|---|---|---|---|
| Trusted Execution | | | | | | ✓ | ✓ | ✓ |
| High Assurance Boot | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Secure Storage | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Hardware RNG | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Secure Clock | ✓ | | | | ✓ | ✓ | ✓ | ✓ |
| Secure Debug | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ |
| Tamper Detection | ✓ | ✓* | | ✓* | | ✓* | ✓* | ✓ |

* External Digital Tamper only monitored when main power is supplied.

# i.MX6 Family Security HW

| Feature | i.MX6 Family |
|---|---|
| Assurance Boot | Authenticated Boot + Encrypted boot (HABv4.1) |
| Secure Storage | On-chip zeroizable 4x4kB Secure RAM<br>Off-chip storage protected using unique HW master key (AES-256)<br>(CAAM/SNVS) |
| Cryptographic Accelerators | Symmetric: AES-128/256, DES, 3DES, ARC4<br>Hash & HMAC: MD5, SHA-1, SHA-224, SHA-256<br>HW Random Number Generator – follows NIST/BSI recommendations > 2015<br>(CAAM) |
| Run-time Monitoring | None |
| Secure Real Time Clock | SNVS |
| Hardware Firewalls | External memory (TZASC)<br>On-chip peripherals (CSU)<br>On-Chip Memory (CAAM, OCRAM) |
| Resource Domain Separation | None |
| Secure JTAG | Full or Controlled Disable (3 modes) |
| Physical Tamper Detection | Tamper Input GPIO<br>Tamper Response (SNVS) |
| Device Configuration | Open, Closed, Field Return |
| TrustZone Support | Peripheral DMA access control (CSU)<br>Memory DMA access control (ARM TZASC)<br>Interrupt separation (ARM GIC)<br>Secure storage separation (CAAM/SNVS)<br>Cryptographic separation (CAAM)<br>OCRAM protected region (OCRAM, CSU) |

# Compliance

# Federal Information Protection Standard - FIPS

- **The US Government publishes a 'Federal Information Protection Standard', known as FIPS, which describes how governmental agencies should protect sensitive data.**
- FIPS 140-2 is the standard pertaining to cryptography modules used by the federal government.
- The FIPS standard is published by the National Institute of Standards and Technology (NIST). www.nist.gov
- Certification of one system using a specific processor provides no pass through benefit to our customers
  - The tests are system level tests, so every new system must go through the process
  - For this reason, there are no plans for Freescale to pursue FIPS testing/certification of Kinetis.

# Payment Card Industry – PCI Compliance

- PTS (PIN transaction security) is the PCI standard governing security for POS and PIN entry devices
- Like FIPS, PCI-PTS is a system level compliance test.
- Freescale has no plans to create a reference system and pass it through PCI-PTS certification; however, we hired an outside company to perform a security review of the Kinetis K70 specification.
- We have a customer version of the report that can be shared as needed.

# Europay, Mastercard, Visa – EMV compliance

- Standard for IC cards or “chip cards” – credit cards with a chip in them for authentication of transactions
- This is a system level compliance test, but in this case there is a defined standard for the interface to the outside world—ISO7816-3.

# EMV Compliance (cont.)

- We support ISO7816-3 using the UART
- There are three classes determined by voltage:
  - Class A (4.5V-5.5V)
  - Class B (2.7V-3.3V)
  - Class C (1.62V-1.98V)
  - Kinetis can only support class B and C without external voltage translation hardware

# Useful References

- The DryIce and RTC chapters of the applicable device's reference manual
- The DryIce and RTC sections of the applicable device's data sheet (under NDA)
- Anxxxx: Using the DryIce Tamper Detection Unit on Kinetis Microcontrollers (under NDA)
- AN3795: Using the CRC Module on the Flexis AC Family
- AN4507: Using the Kinetis Security and Flash Protection Features
- AN4307: Using the CAU and mmCAU in ColdFire, ColdFire+ and Kinetis
- CAU/MMCAU Performance Analysis – Internal Document
- RSA Performance using Kinetis MCU – Internal Document

# Designing with Freescale

## Tailored live, hands-on training in a city near you

**2014 seminar topics include**

- QorIQ product family update
- Kinetis K, L, E, V series MCU product training

freescale.com/DwF

www.Freescale.com

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