Market Drivers and Use Cases for **Automotive Cyber Security**

AMF-ACC-T1660

John Cotner | Field Systems Engineer

SEPT.2015

freescale™

External Use

Agenda

- High-level overview of automotive security definitions and use cases
- History and organization of Freescale's support for security
- Security concept and features for Freescale's current automotive microcontrollers / microprocessors
- Using security features to meet automotive use cases

- Semiconductor industry trends that affect Automotive security
  - embedded flash memory, rising design/tooling cost, etc.
- Security features used in other industries that Freescale could include in automotive MCU/MPU's

CBS NEWS

By MICHAEL CASEY / CBS NEWS / July 24, 2015, 12:41 PM

Fiat Chrysler recalls 1.4M cars after hack revelations

6:00 am ET
Aug 6, 2015

THE WALL STREET JOURNAL.

Hackers Take Control of a Tesla

Car-hacking: A New Fear For Drivers of Tech-Loaded Vehicles

NBC NEWS

by JOSEPH SZCZESNY, THE DETROIT BUREAU

Car hack uses digital-radio broadcasts to seize control

By Chris Vallance
BBC Radio 4

22 July 2015 | Technology

BBC NEWS

abc NEWS

The Scary Things Hackers Can Do to Your Car

CNN

Automakers don't protect you enough from car hackers, senator says

Security: Questions the Auto Industry is Asking?

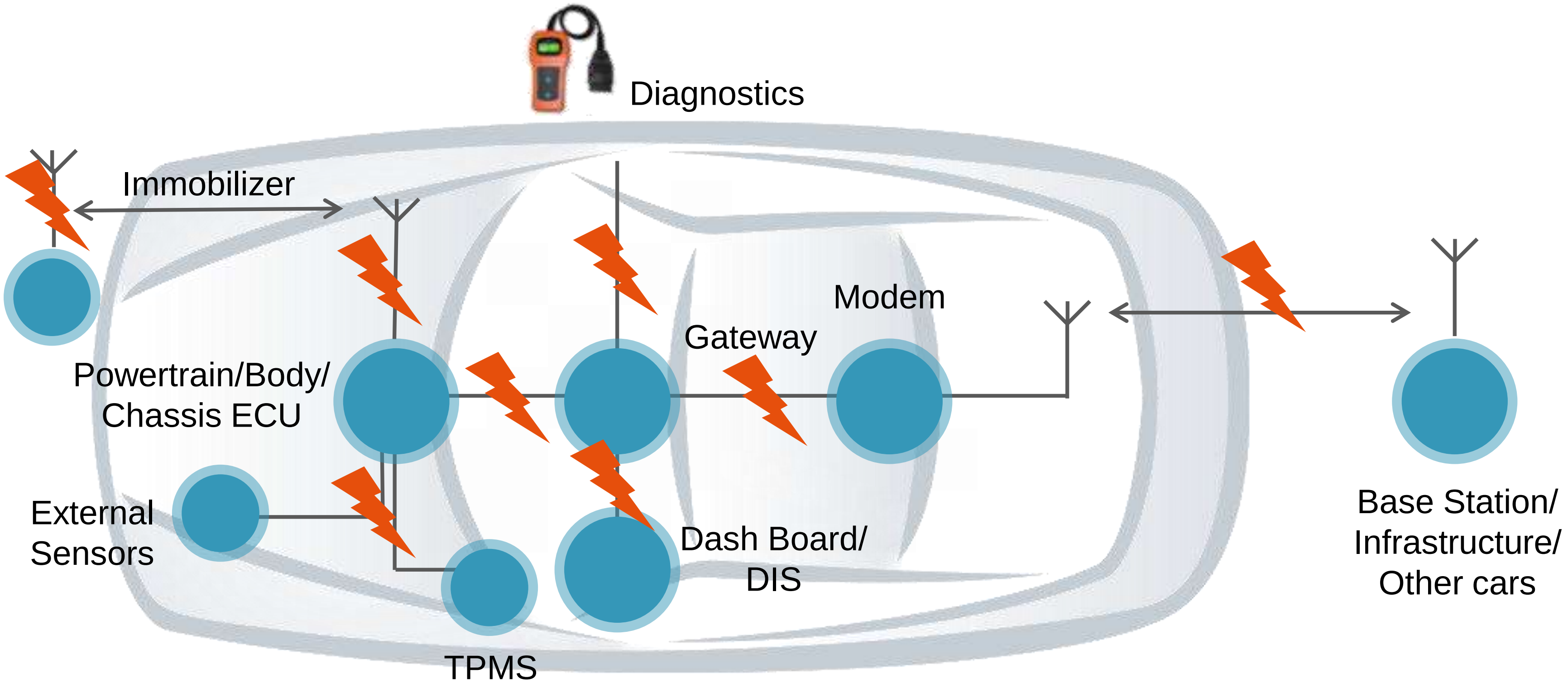
- What needs to be protected?
- What types of attack can be expected?
- What are the attack motivations and methods?

- How much security do we really want?
- How much are we willing to pay for it?

- What is the impact on system complexity?
- How can the security system be maintained and upgraded over time?

- Is it better for the system to be unavailable or to possibly be compromised?

Automotive Security Attack Surface



The Connected Vehicle

Infotainment + Communication + Security

- **Consumer electronics trends** are dictating features in the car
- Always **connected, applications driven, advanced graphics**
- **Infotainment systems** becoming battleground for Auto differentiation
- As more connected systems get introduced into the vehicle, the need for **security is critical**
  - Increasing external communication features (Bluetooth, TPMS, Ethernet, Wi-Fi, etc).
  - Future interface for vehicle-to-vehicle and vehicle-to-infrastructure.

Automotive Security Definitions and Use Cases

Automotive Security Application Level Use Cases

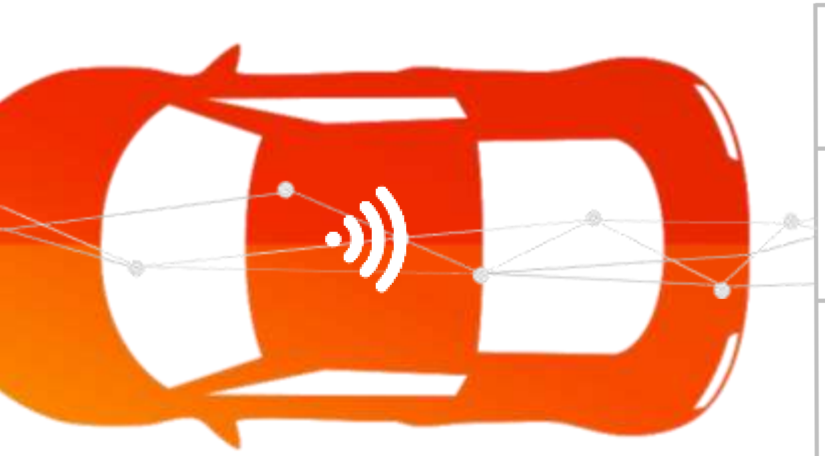
- **In-Vehicle Security**
  - Immobilizer / Component Protection
  - Mileage Protection
  - Secure Boot and Chain of Trust
  - Secure Communication
  - DRM – for batteries

- **Connected Vehicle Security**
  - Android application download
  - DRM for content download/streaming
  - Remote ECU firmware update
  - Black-box for due government or insurance
  - Car-to-Car communication

Automotive Security Functional Use Cases

- **THEFT PROTECTION** of the car and of individual components
- **SECURE BOOT** (HW is running intended code)
- **SECURE SOFTWARE FLASHING** (file signature verification)
- **SECURE STORAGE** of cryptography keys and other secrets
- **SECURE DIAGNOSIS AT THE ECU LEVEL** (securely give convenience)
- **IP PROTECTION** (of reading out firmware to reverse engineering secrets)
- **AUTHENTICATE MESSAGES IN-VEHICLE** (lessen spoofing or its impact)
- **BROADCAST/MULTICAST AUTHENTICATION** (prevent legitimate xmtr from sending false messages)
- **SECURE KEYSTORE** which includes many key handling functions
- **REMOTE ATTESTATION** Desire of a attester (remote) entity to get a trustworthy statement about the current configuration of the Attestee (local)
- **SECURE LOGGING** a sequential storage of records of events
- **SECURE ERASE** the ability to securely erase information (Destructible Storage)
- **PREVENT ACCESS TO PRIVATE DATA** from parties capable of reprogramming the Secure Hardware Environment
- **ANONYMIZATION** of PII (personally identifiable information_

Automobiles as End Node Challenges



⚠ To enable autonomous driving, autos now connecting
to the internet, other autos & infrastructure

⚠ Wireless connectivity being added to ECUs in a car in order to implement V2x

⚠ How to enable robust network security that lasts the lifetime of the car

⚠ New Safety Critical challenges for auto manufacturers
Already shown to be vulnerable to attack (Darpa/ GM)*

⚠ Over the air updates

*Fox News

How is Security different from Safety?

- Security is the prevention of malicious manipulation

- Safety is the protection against technical failures.

System Security: Some definitions & Requirements

- **Confidentiality** – To protect sensitive information; prevents eavesdropping

- **Authentication** – to ensure the information comes from the expected user; prevents impersonation

- **Data Integrity** – to assure the content has not been altered; prevents tampering

- **Non-repudiation** - to ensure the sender cannot deny the information was sent

Encryption vs. Authentication

- Data Content
  - Should the data transmitted be obscured?
- Privacy
  - Is it important to keep the source anonymous?
- Verification of Source
  - Is this message from an authentic source?
- Latency
  - Is the protection of the data delaying its use outside of the requirement?

Types of Attacks

Electrical

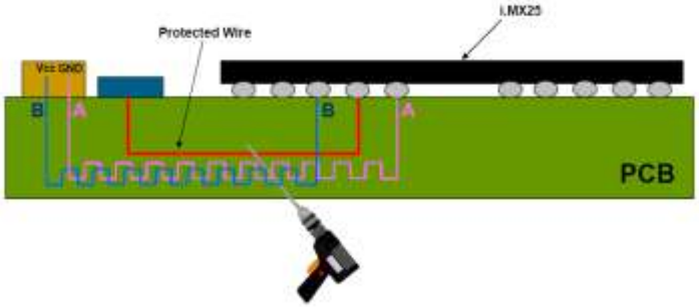
- Over/Under voltage
- Power analysis
- Frequency analysis
- Electrostatic discharge
- Circuit probing

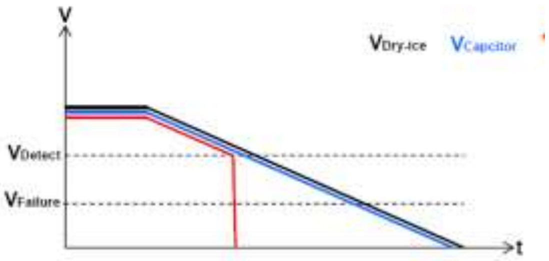
Software

- Spy software insertion
- Flow analysis
- Trojan horse
- Virus

Physical

- Temperature variation (into extremes)
- Temperature analysis
- De-processing
- System theft
- Partial destruction
- Hardware addition/substitution





Slow voltage drop

List is not exhaustive….

Freescale Participation in Standards/Consortium

- HIS – SHE specification
  - SHE module (CSE) implementation in 2011
- EVITA Specification
  - 3 levels of definition: Light, Medium and Full
  - HSM module (Evita medium) implementation ir
- Preserve
  - Project duration 2011-2014
  - V2X Security Subsystem
  - Based on EVITA Full

SAE Vehicle Electrical System Security Committee Committee Activities

- Current Work Items
  - Development of Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (J3061)
  - Development of automotive requirements for hardware security solutions (J3101)
  - Automotive cybersecurity information sharing, investigate/create Automotive ISAC (Information Sharing and Analysis Center)

Regulations & Standards

EMV, PCI and FIPS

$ Banking & Business €

EMV*	Eurocard Mastercard Visa JCB	to ensure **interoperability** between chip cards (i.e. Smart Cards) and terminals on a global basis, regardless of the manufacturer, the financial institution, or where the card is issued. Address the Authentication of the card

PCI-PTS	Visa Mastercard Amex Discover JCB	To **protect** the cardholder's PIN when used in connection with a financial transaction. Address the Security and protection of the data during the whole transaction. Linked to confidentiality, integrityand non-repudation

Government & Enterprise

FIPS	Government Bodies from US, Canada and UK	To specify the security requirements which must be met in order for products to be validated under the Cryptographic Module Validation Program (CMVP). This standard issued by the National Institute of Standardization gives rules for cryptography modules

Freescale’s Support for Security

Freescale MCU Security Overview

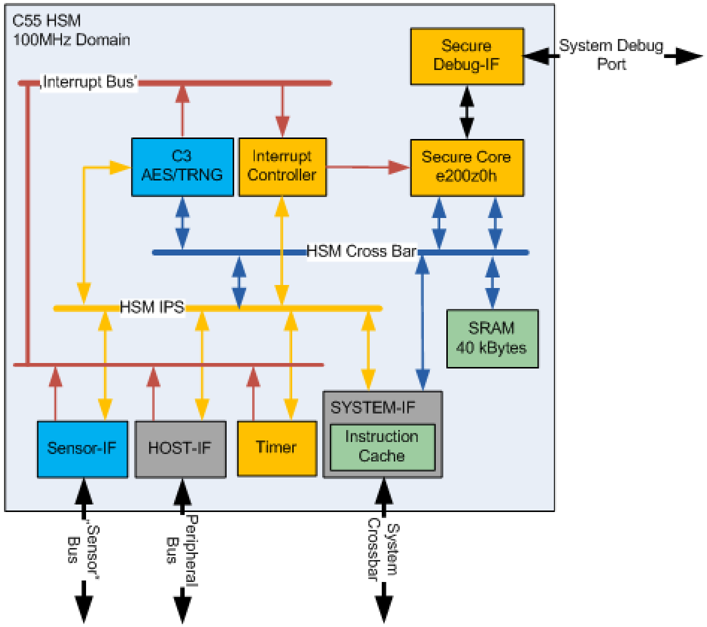
- Freescale History
  - As Motorola, manufactured Smart Cards in the '90s for Gemplus and Schlumberger
- Technology & Expertise
  - Security Technology Center in Arizona
    - Develops hardware accelerators: AES, RSA, SHA, ECC
  - Resilient Microcontroller security architectures across the family
    - Adaptable integrated hardware security modules
      - for future-proof security solutions
    - Non reversible Security Lifecycle
      - protects customer assets
    - Patented Tamper Detection hardware
      - detects unauthorized flash modifications
- Applications
  - Networking, industrial, consumer, automotive.

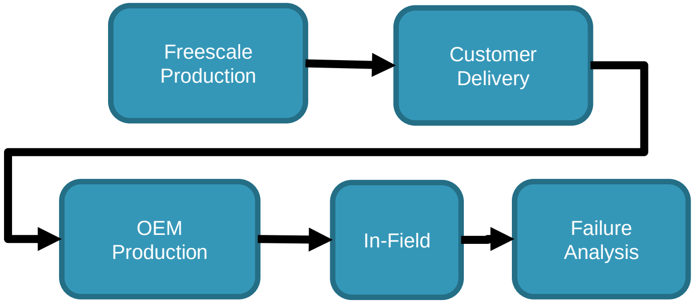
Leverage Leadership
Automotive Connectivity Security

- **Our credentials**
  - Helped drive **HSM** and **SHE automotive security standards** and first to implement into Silicon
  - First to implement **SHE** security on silicon (MPC5646C)
  - First to implement **HSM** security in production (MPC5777M)
  - First to implement SHE on **Flashless** device (S32V234)

- **But, Security is way more than cryptography**
  - Device Life-Cycle scheme
  - Debugger access
  - Flash Protection
  - CSE/HSM crypto system
  - MCU Resource control

- **And needs software to provide the application functionality**
  - HSM SDK (incl crypto, key mgmt, etc)
  - FOTA manager
  - Bootloader
  - External memory manager

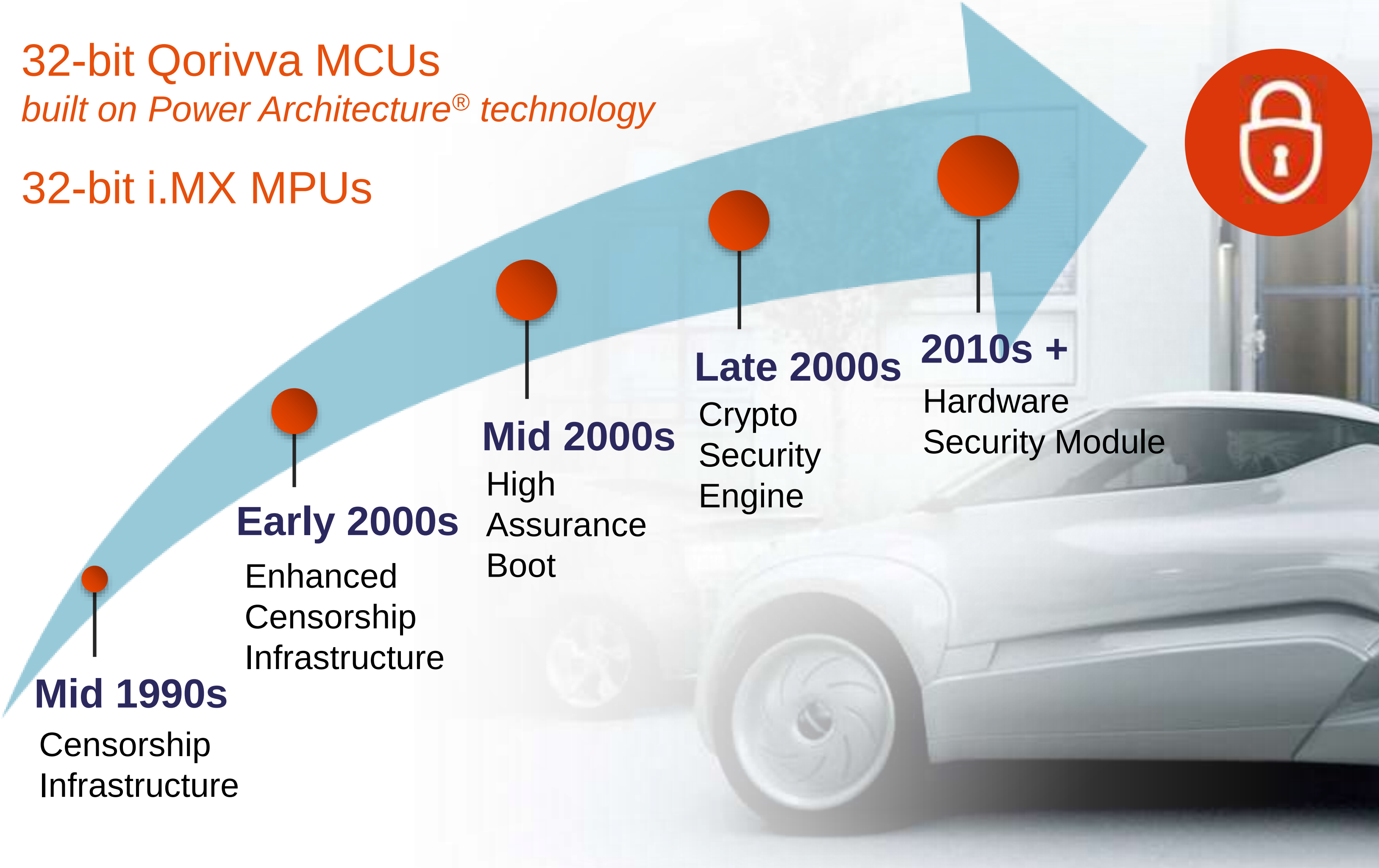




A Proven History in Driving Automotive Security

32-bit Qorivva MCUs
built on Power Architecture® technology

32-bit i.MX MPUs



Mid 1990s
Censorship Infrastructure

Early 2000s
Enhanced Censorship Infrastructure

Mid 2000s
High Assurance Boot

Late 2000s
Crypto Security Engine

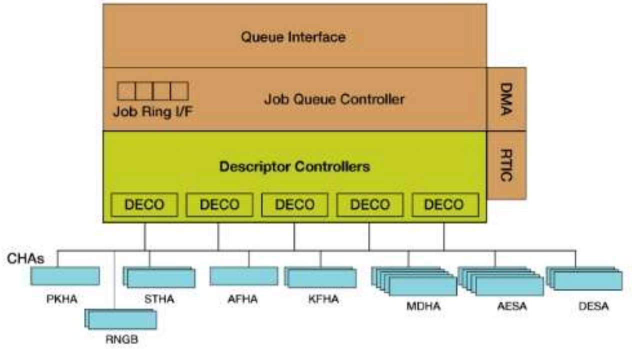
2010s +
Hardware Security Module

The Freescale Solutions

- Creating an attack-proof system is a practical impossibility if you assume the attacker has infinite time and resources. The real objective is to create a system that is sufficiently attack resistant to discourage attackers from even trying to compromise the system, and should they persist, the cost of the attack will outweigh the potential benefits.

- Freescale products with trust architecture provide system developers with the hardware anchor points they need to develop a trusted system.

Cryptographic Technology SEC 4.x Block Diagram



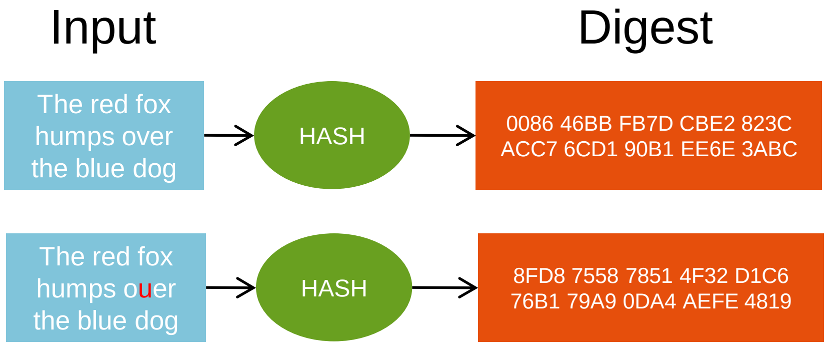
General Issues for Automotive Cybersecurity Implementation

Cipher Summary

	DES	AES	RSA	ECC
Secure for the next few years	☹	☺	☺ Key size > 2048	☺
Type	symmetric	symmetric	asymmetric	asymmetric
Typical key size [bits]	56	128, 192, 256	1024, 2048, 3072	180, 224, 256,320, 512
Execution time	short	short	long	long
Authentication / verification	☹	😐	☺	☺
Implementation	HW – good SW – lot of bit ops	HW / SW - good	Could combine into one module, req. big number math functions (e.g. GMP)	
Key Management	☹		☺	

Secure Hash Algorithms

- A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string.
- Detection of accidental or intentional change.
- **Main or significant properties:**
  - It is easy to compute the hash value for any given message,
  - It is infeasible to generate a message that has a given hash,
  - It is infeasible to modify a message without changing the hash,
  - It is infeasible to find two different messages with the same hash.



Input

Digest

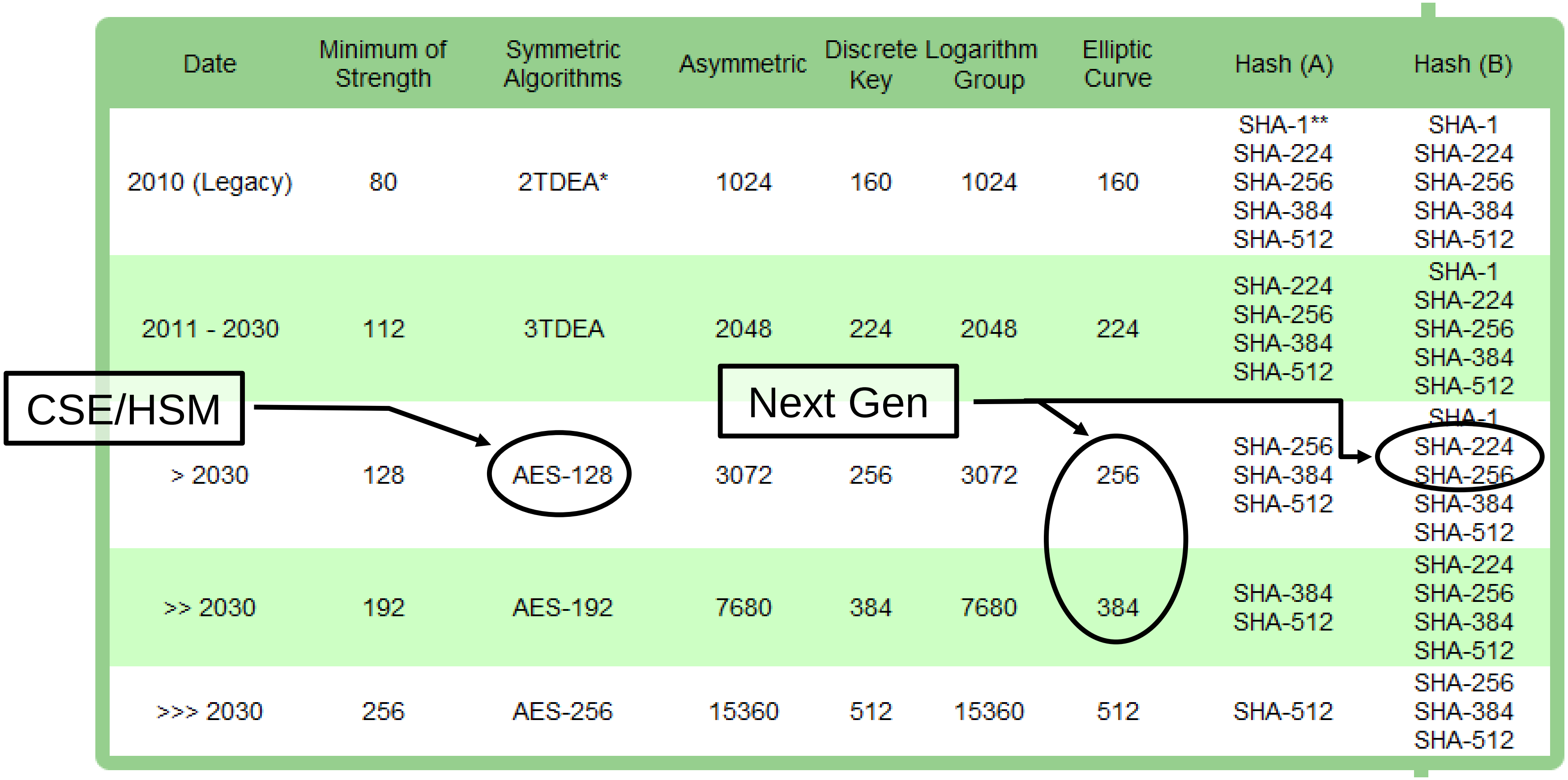
The red fox humps over the blue dog → HASH → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

The red fox humps ouer the blue dog → HASH → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

Algorithm	Output size [bits]	Internal state size [bits]	Block size [bits]	Length size [bits]	Word size [bits]	Collision attacks	Preimage attacks
MD5	128	128	512	64	32	Yes	Yes
SHA-1	160	160	512	64	32	Yes	
SHA-256/224	256/224	256	512	64	32	No	No
SHA-512/384	512/384	512	1024	128	64	No	No
WHIRLPOOL	512	512	512	256	8	No	

Cryptographic Strengths of different Algorithms

- NIST recommendations, 2012
- The Date is a projection of the time frames during which the algorithms could be expected to provide adequate security
- The security Strength is a measure of the difficulty of discovering the key



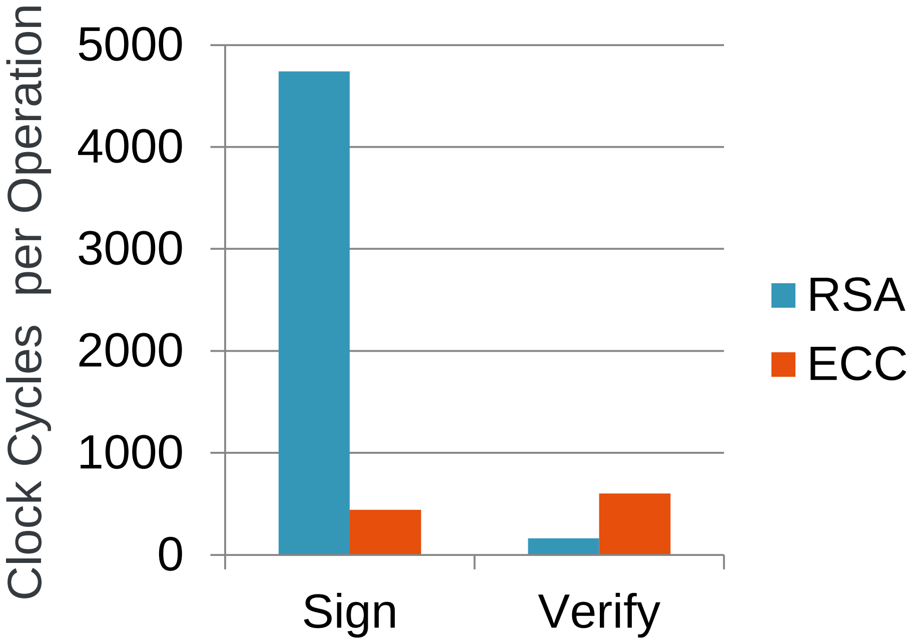
Date	Minimum of Strength	Symmetric Algorithms	Asymmetric	Discrete Logarithm		Elliptic Curve	Hash (A)	Hash (B)
				Key	Group			
2010 (Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
2011 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
>> 2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
>>> 2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 SHA-384 SHA-512

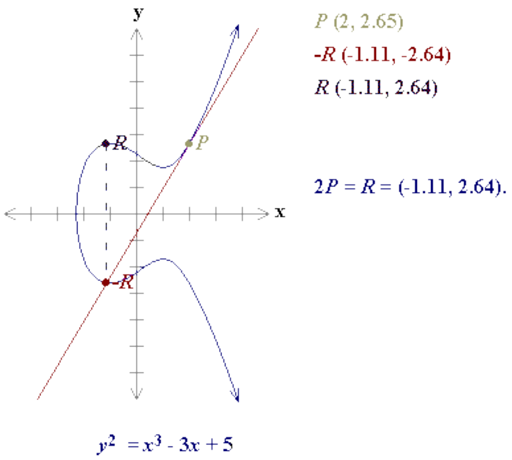
CSE/HSM

Next Gen

Relative Performance of hardware RSA and ECC

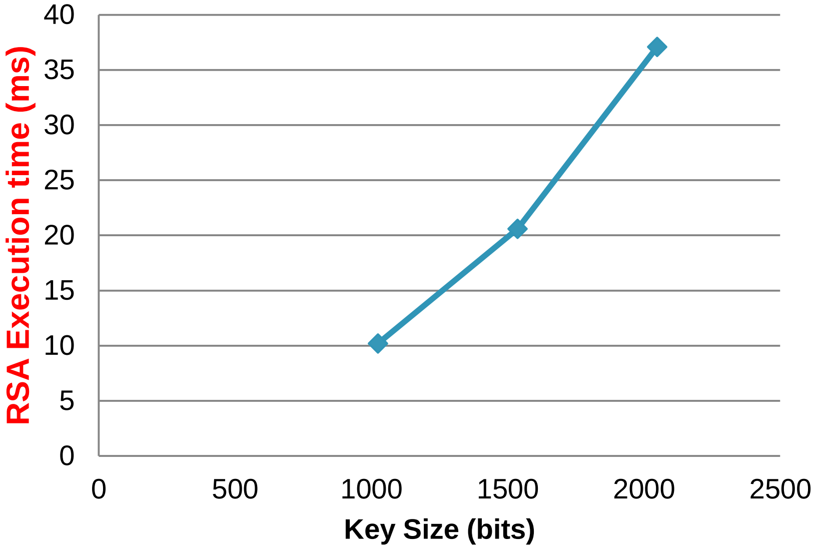
- Compares equivalent security strength algorithms
  - RSA-2048 vs. ECC-224
- Example is for hardware implementations with 32 bit multipliers
  - Larger multipliers give higher performance, but at a cost
- Both performance and implementation size get closer between RSA and ECC as key sizes increase

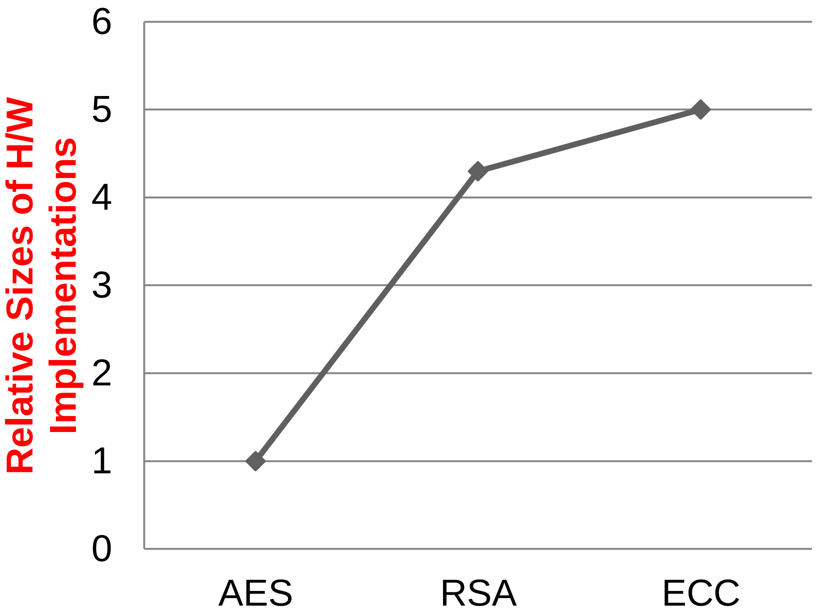




Crypto Algorithm Metrics

- AES-128, RSA2048, ECC224/256, and SHA-256 are commonly used cryptographic algorithms
- Each of these can be accelerated by one to two orders of magnitude (depending on the complexity of the accelerator)
- Cost, performance, and key handling complexity tradeoffs need to be considered





Secure Key Storage

- Required for Passwords, Cryptography Keys
- Key Handling includes: provisioning, management, generation, derivation, usage, and storage, erasure
- On-chip or in-package storage offers significant advantages
  - OTP flash memory is ideal from a security perspective
    - easy to provision
    - difficult to extract values
    - memory bus architecture requires careful design (firewalling)
    - can provide a degree of flexibility (revocation)
  - e-fuses are also used
    - might be more susceptible to attack (i.e. easier to read)
    - limited flexibility – not re-programmable
    - large structures, so limited number can be implemented cost effectively
  - Should not require encryption
- Off-chip storage can be subject to snooping attacks
  - requires keys to be encrypted/decrypted

Power Up Time

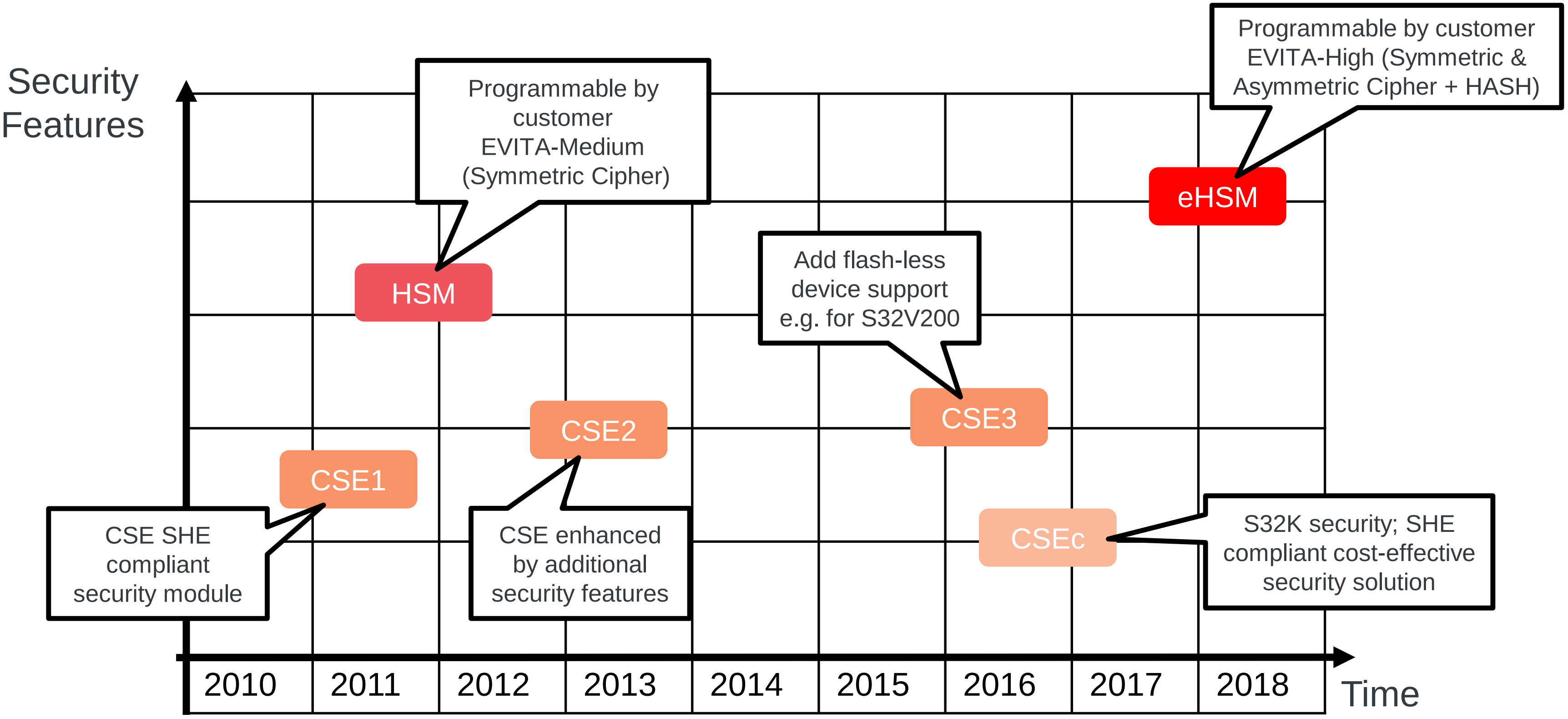
- Power up time is a major concern for automotive applications
  - In the order of a few milliseconds is required
- Other device behaviors affect power up time
  - e.g. Oscillator startup, self-test
- Security operations introduces a potential additional startup delay
  - In the form of secure boot
- Security Delay Time Mitigations
  - Implement a hardware secure boot
  - Incorporate a chain of trust approach
  - Enable a Run Time Integrity checker

Freescale's Current Automotive Security Solutions

Freescale Devices with Hardware Security

Freescale Security Solution for Automotive products				
	Device	Platform	Module	
MCU (internal flash)	MPC564xB / C	Power Architecture e200	CSE	Automotive
	MPC5746M / MPC5777M		HSMv1	
	MPC5748G / MPC5746C		HSMv2	
	MPC5777C		CSE2	
	MAC57D5xx	ARM	CSE2	
MPU (flash-less)	S32V234	ARM Cortex-A53	flashless CSE3	
	VFxxx	ARM Cortex-A5/M4	Trust Zone CAAM	Consumer
	i.MX 2x / 3x / 5x / 6x / 7x	ARM9/11 Cortex-A8/A9		

S32 Freescale Security Modules


Security Features
Programmable by customer EVITA-Medium (Symmetric Cipher)
Programmable by customer EVITA-High (Symmetric & Asymmetric Cipher + HASH)
eHSM
HSM
Add flash-less device support e.g. for S32V200
CSE3
CSE2
CSE1
CSEc
CSE SHE compliant security module
CSE enhanced by additional security features
S32K security; SHE compliant cost-effective security solution
2010
2011
2012
2013
2014
2015
2016
2017
2018
Time

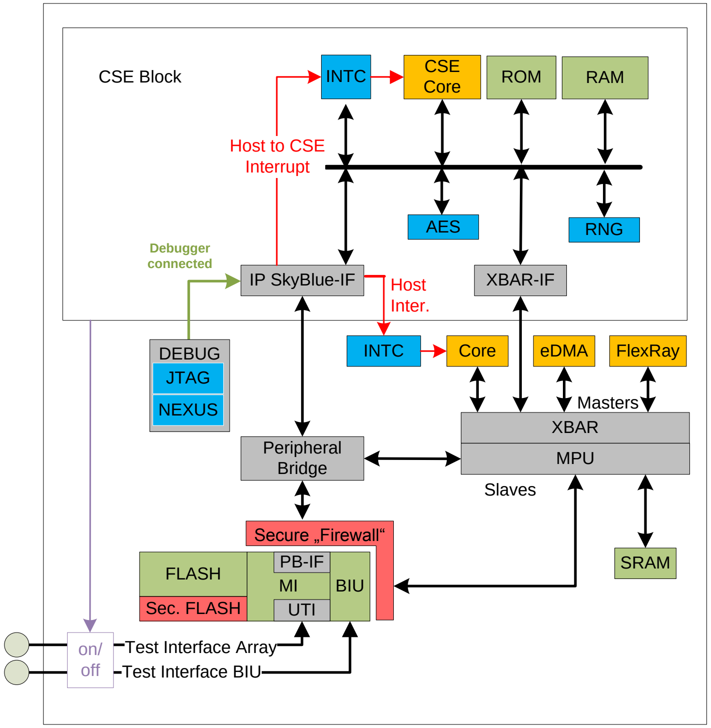
Security on MPC5777C

Security Concepts in MPC5777C

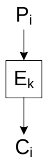
Concepts	Description	HW Implementation
Security versus Testability	Possibility to enable/disable security features according to customer needs	Device Life Cycle
Secure System Configuration	All the critical security-related data are protected against manipulation	Configuration Records parsed by System Config Module
Secure Boot	“root of trust“ (e.g. Key unwrapping, Flash integrity check, etc.) establish at boot time	Boot Assist & CSE2 code execution
External access protection	Protection against access to internal resources from external tools	Debug access protection, Serial Boot protection
Flash memory protection	Protection against Flash memory access and modification	PASS & TDM modules, Flash Sealing,
End of life protection	Protection against re-use of module after failure analysis	No cryptographic services at ‘Failure Analysis’ lifecycle state
Cryptographic functionalities	Availability of a HW cryptographic accelerator for AES-128 algorithms	CSE2
Secure Key Storage	Isolated unit in the MPC5777C, with its own Flash/RAM memory, handles all key management	CSE2 module, ROM secret keys

Cryptographic Services Engine (CSE)

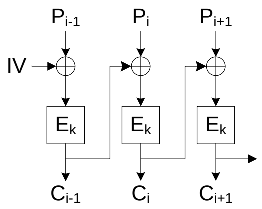
- **CSE module implements the official SHE-Specification (Version 1.1), a HIS standard**
- **32-bit secure core working at up to 132 MHz**
- **AES-128**
  - Supported crypto modes: ECB & CBC
  - Throughput 100 Mbit/sec
  - Latency 2µs per one encoding/decoding ops
- **CSE module interfaces:**
  - Crossbar master interface
  - Configuration interface
- **Secure flash blocks assigned to the CSE module. Accesses from other masters are impossible.**
- **PRNG seed generation via TRNG**
- **CSE Core not programmable by customer**



ECB



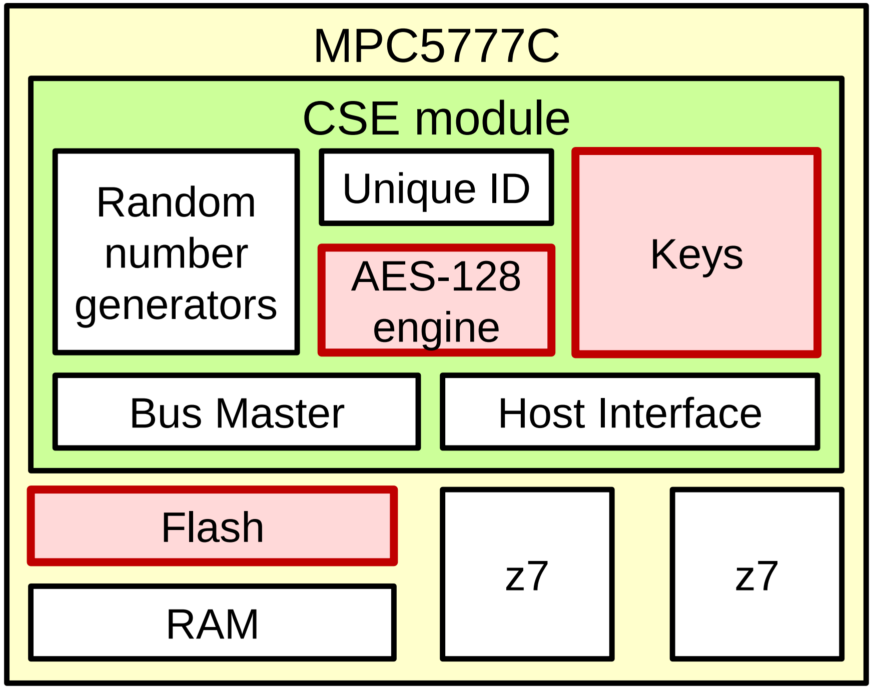
CBC



Security Use-Cases with CSE

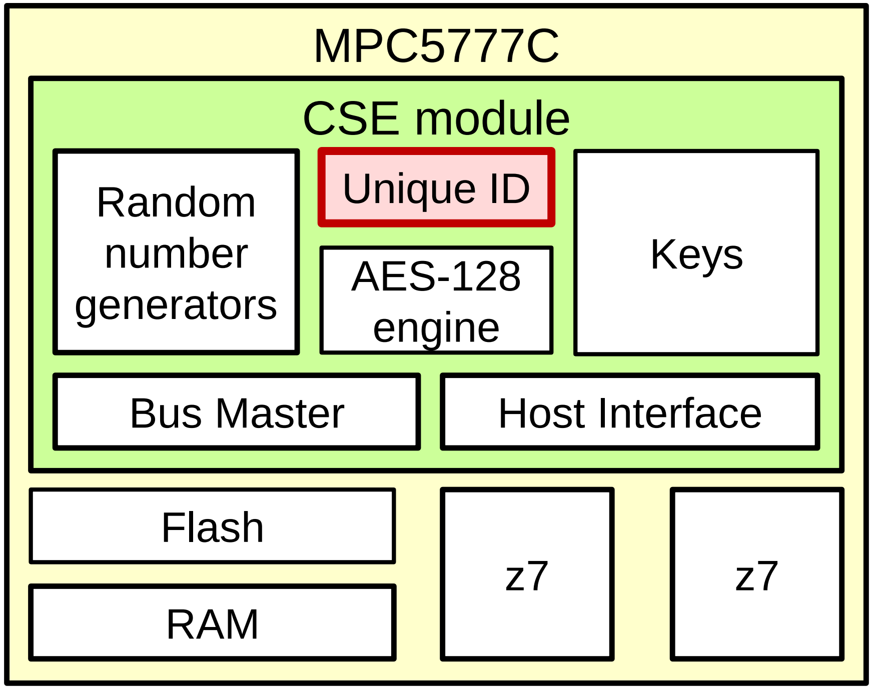
MPC5777C – Secure Boot, Chain of Trust

- Secure Boot:
  Detect modification of boot loader
- Chain of Trust:
  Detect modification of remaining flash content
- Based on AES-128 engine and secret key storage
- Provides integrity and authenticity of flash content
- Protects against firmware modification



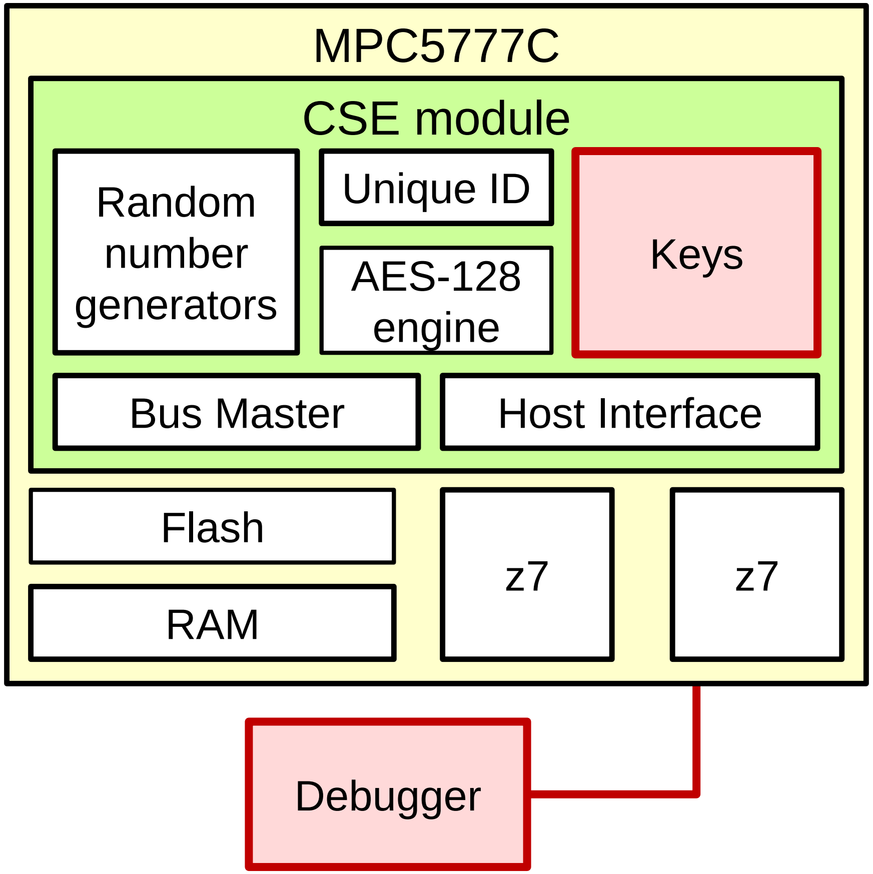
MPC5777C – Component Protection

- Detect replacement of component (ECU) in the car
- Required by OEMs as:
  - Cars are stolen just to resell their parts/components (higher prize than “complete” car)
  - Insurance rates increased due to increased car thefts
- Based on unique device ID in CSE module
- Provides authenticity of ECU/device
- Protects against reselling of “stolen” ECU. Reduces car thefts



MPC5777C – Debug Detection

- CSE module detects debugger, connected to the system
- Reaction (depending on Lifecycle State):
  - CSE module blocks keys
  - No crypto services available
- CSE module flags detected debugger in register of host interface
  - Customer application (on z7 core) can take actions
- Provides confidentiality
- Protects against tamper attacks



MPC5777C – Other Security Use Cases

- Secure Communication:
  Add CMAC to messages on network (CAN, LIN,...), enable authenticity between sender and receiver.
- Data Privacy:

  Encrypt message on network
- Mileage Protection
- Secure Flashing:
  Ensure that only original unmodified firmware (e.g., from OEM/Tier1) is accepted by MPC5777C
- Feature Activation:
  Ensure that only original unmodified feature (e.g., from OEM) is accepted by MPC5777C

Other MPC5777C Security Features

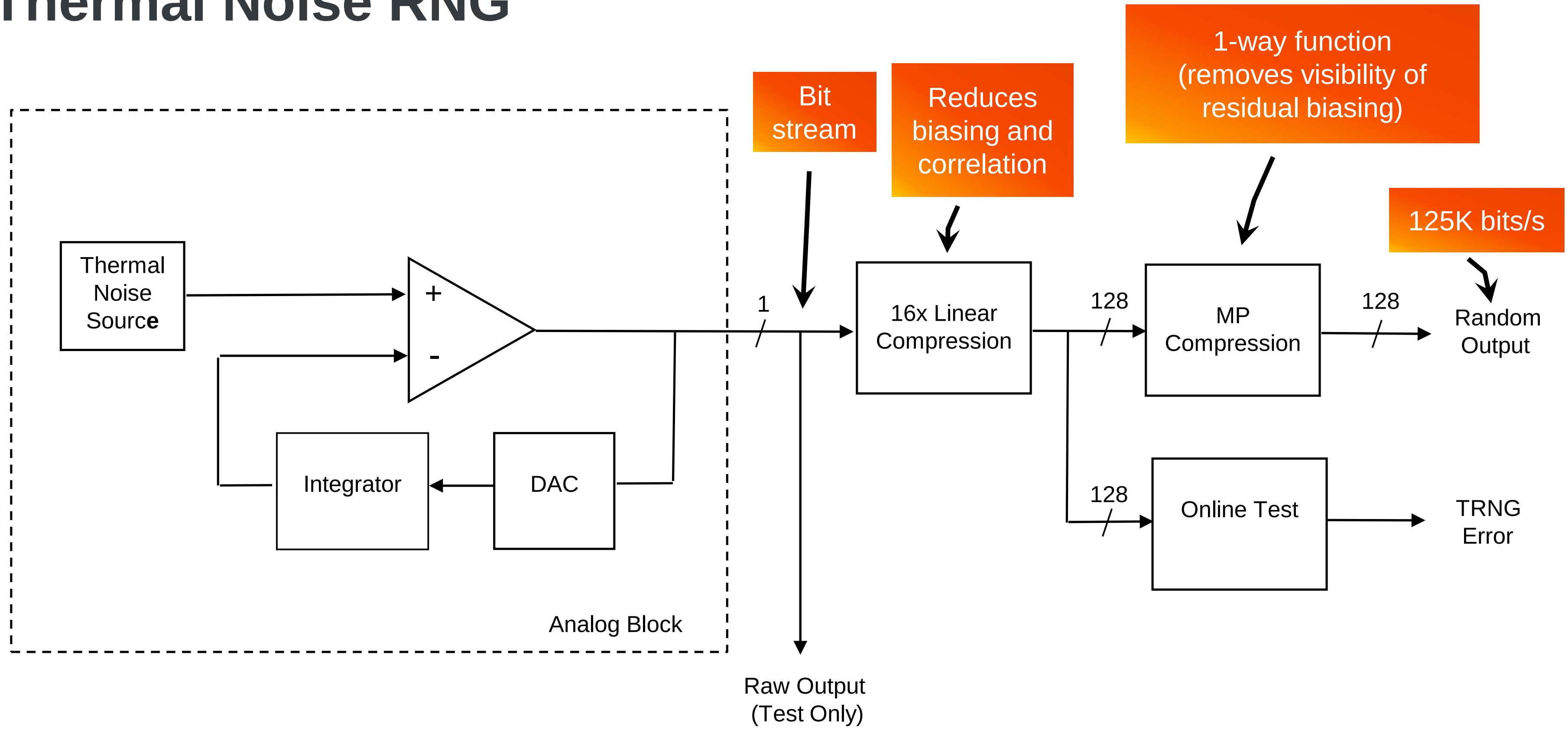
Random Number Generators

- Use cases : replay attack countermeasure, session key generation

- Analog entropy source is often a thermal noise generator
  - May fail silent, so needs to be continuously checked
  - Bias eliminated by post-processing bit stream (e.g. compression)

- Entropy generator data rate may be insufficient
  - Often used as seed to PRNG, which can then produce random numbers at a very high data rate

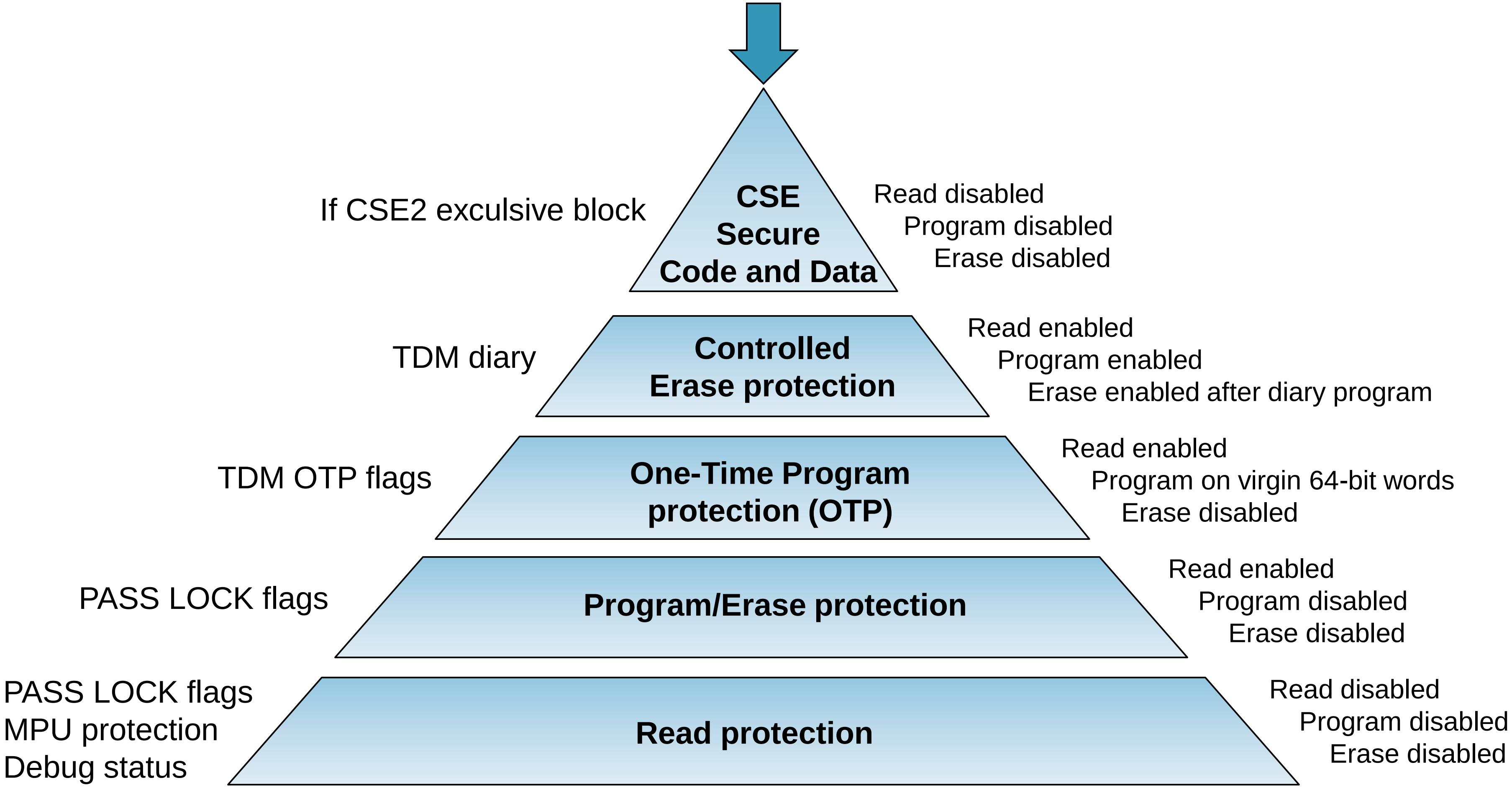
Thermal Noise RNG



- The TRNG analog block generates a random bit stream by sampling amplified thermal noise.
- Two stages of digital compression are applied to the raw analog output to increase entropy per bit, eliminate one/zero bias and eliminate correlation between bits.
- On CSE module, a statistical online test is run (1/0 bias and correlation of bits) to ensure TRNG is still functional and randomness is valid

Flash Memory Protection Levels

Flash access request from debugger or core



If CSE2 exculsive block

CSE Secure Code and Data

Read disabled
Program disabled
Erase disabled

TDM diary

Controlled Erase protection

Read enabled
Program enabled
Erase enabled after diary program

TDM OTP flags

One-Time Program protection (OTP)

Read enabled
Program on virgin 64-bit words
Erase disabled

PASS LOCK flags

Program/Erase protection

Read enabled
Program disabled
Erase disabled

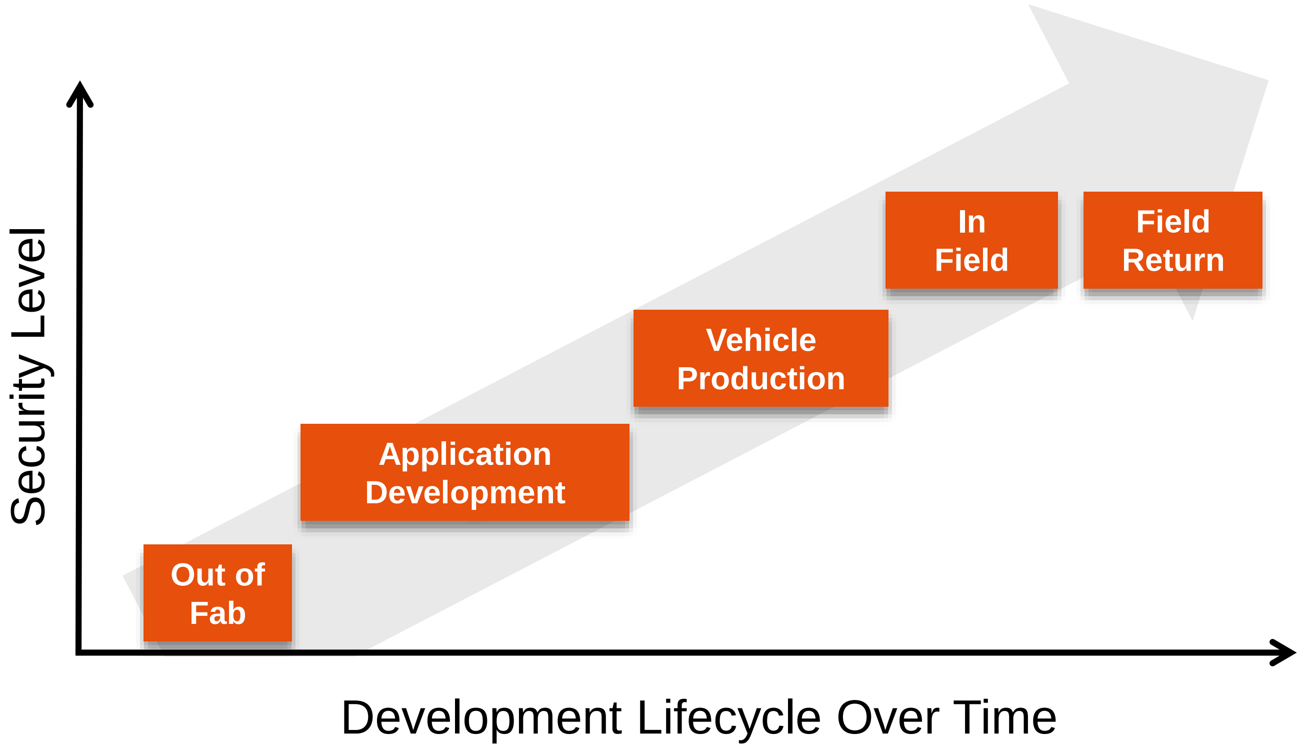
PASS LOCK flags
MPU protection
Debug status

Read protection

Read disabled
Program disabled
Erase disabled

Security for the Development Lifecycle

- Increased security level required at each stage of the development lifecycle – non-reversible, non-revocable
- Ensures application can be safely developed, debugged and validated without compromising security in the production vehicle
- Protects customer software IP in field returns

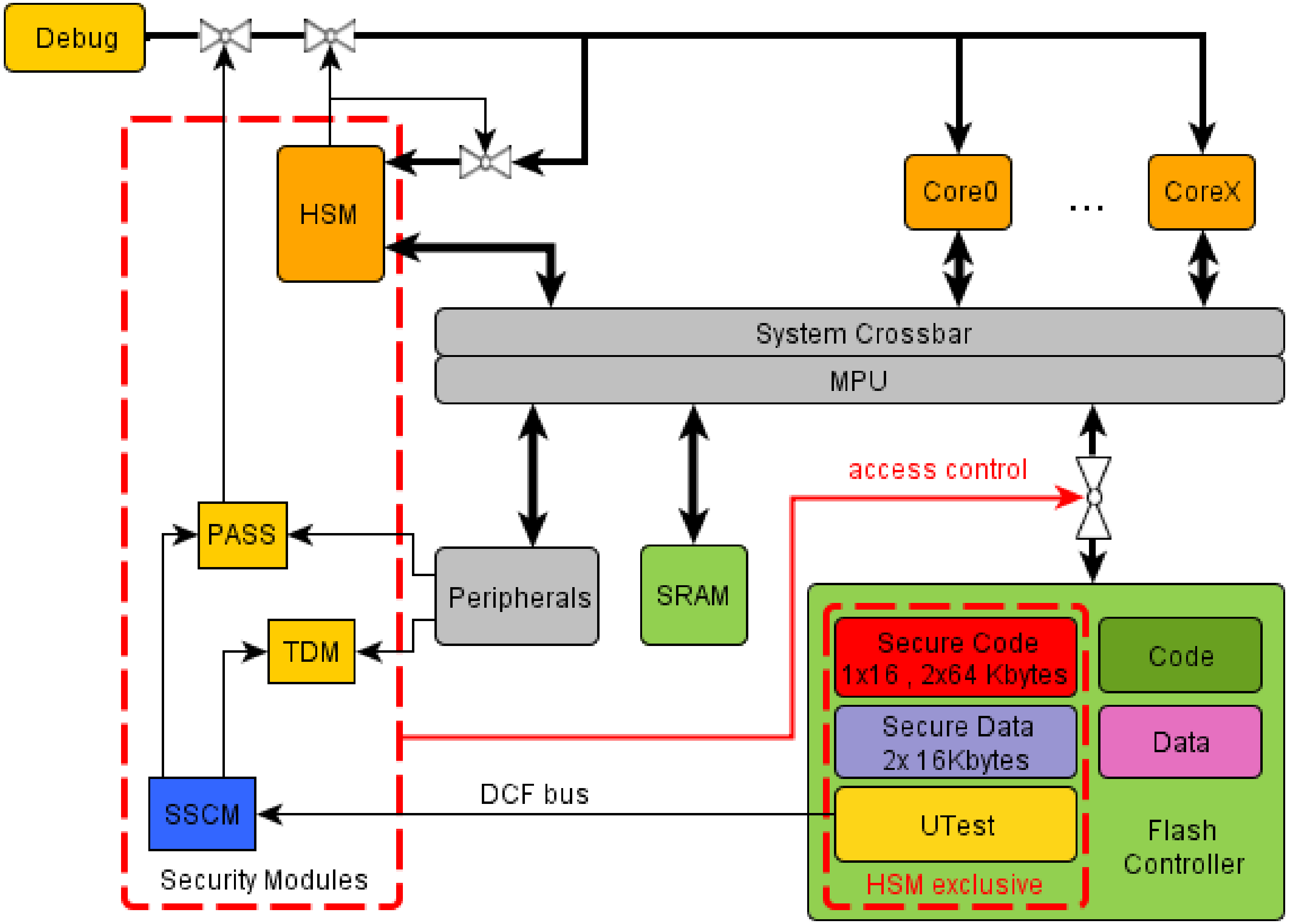


Lifecycle State for MPC5777C

	Pre-Delivery	Customer delivery	OEM production	In field	Failure analysis
Device & Flash test interface	Open	Closed	Closed	Closed	Open
BAF block	Not Programmed	Programmed and set as OTP	Programmed and set as OTP	Programmed and set as OTP	Programmed and set as OTP
UTest Block	Programmed during test	OTP	OTP	OTP	OTP
Flash Blocks Access	Erase/Program/Read	Based on PASS LOCK bits	Based on Censorship, PASS LOCK bits	Based on Censorship, PASS LOCK bits	Based on Censorship, PASS LOCK bits
Passwords	Not Programmed	Programmed /Readable	SSCM Access only	SSCM Access only	SSCM Access only
PASS LOCK register	n/a	Without password	Upon password matching	Upon password matching	Upon password
Cores Debug Interface	Open	Open	Based on Censorship, PASS LOCK bits	Based on Censorship, PASS LOCK bits	Based on Censorship, PASS LOCK bits
Boot	From internal Flash if a valid header is found, otherwise from Serial Boot	From internal Flash if a valid header is found, otherwise from Serial Boot	From internal Flash if a valid header is found, otherwise from Serial Boot	From internal Flash	From internal Flash

MPC5777M / MPC5748G Security Concepts and Features

Security Architecture for MPC5777M

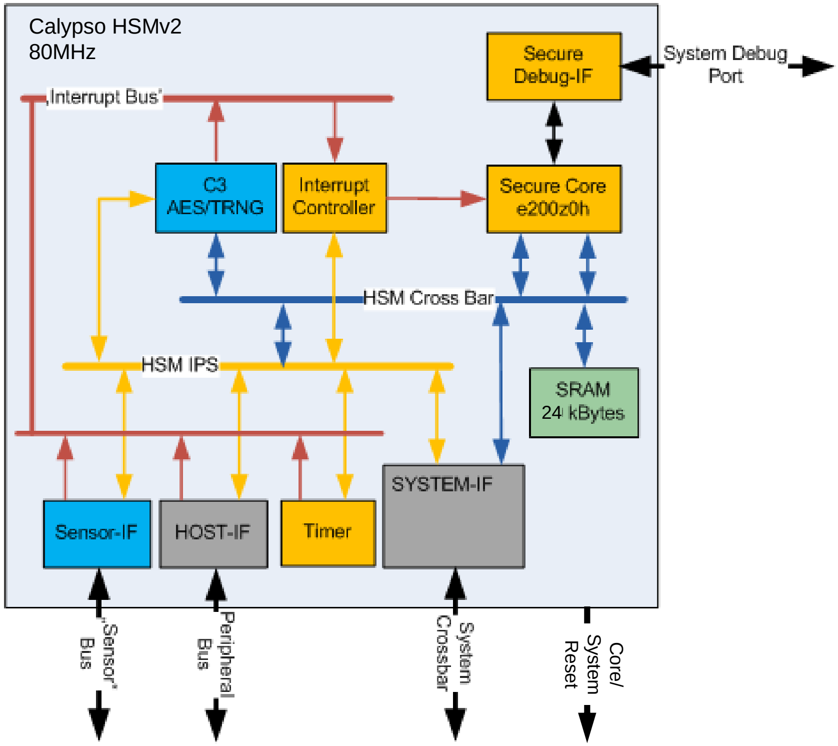


SSCM: System Status Configuration Module
PASS: Password And Device Security Module
TDM: Tamper Detection Module
HSM: Hardware Security Module
MPU: Memory Protection Unit
DCF: Device Configuration Format

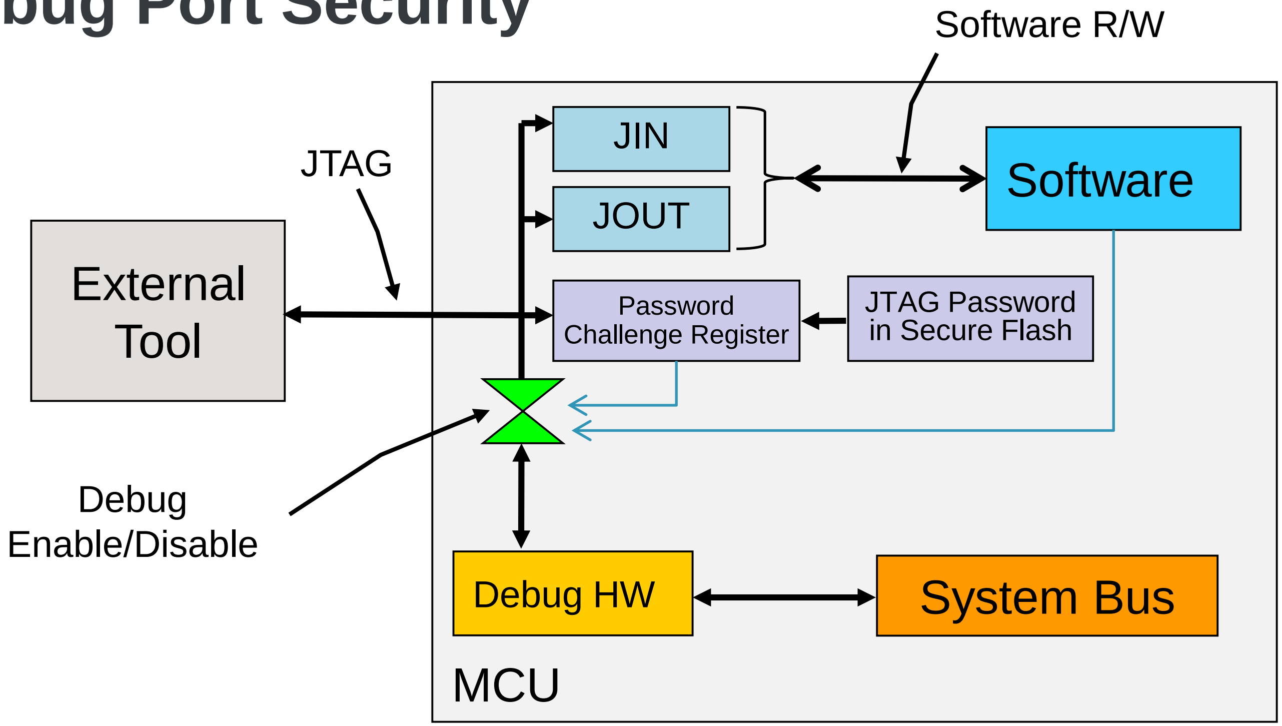
Hardware Security Module (HSMv2) MPC5748G

HSMv2

- e200z0h core @ 80MHz
- Crossbar with MPU
- Interrupt controller (32 x HOST to HSM)
- Memory
  - 24KByte internal SRAM
  - Flash
    - Data: 2x 16KBytes
    - Code: 2x 64 KBytes; 1x 16KBytes
- Cryptographic Core (C3)
  - AES-128
  - Random Number Generator
  - DMA functionality



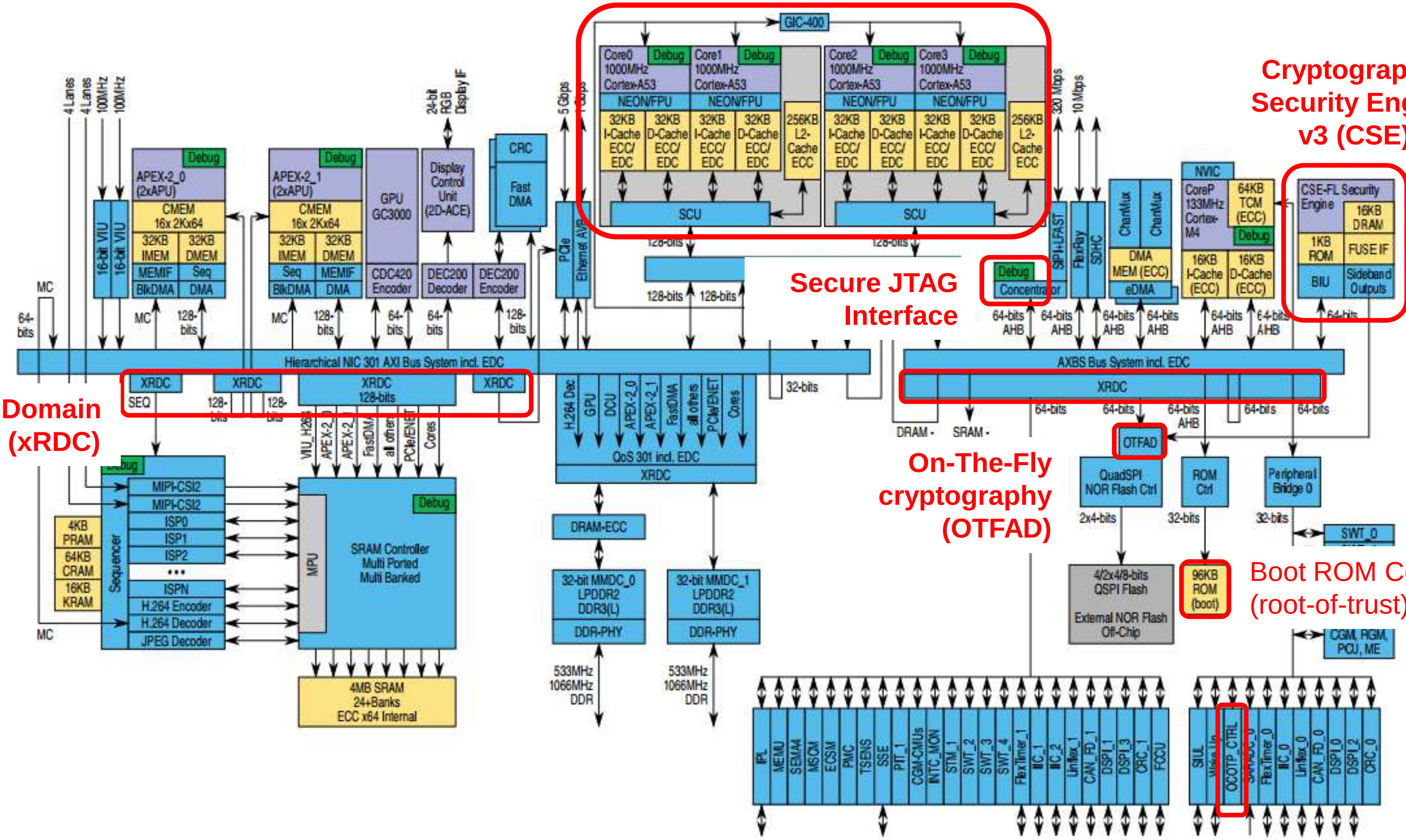
Debug Port Security



- JTAG Interface to External Tool & Software Interface to Host CPU
- Provides two methods of enabling debug access
  - a software method using cryptography services (e.g. challenge/response)
  - a direct method where external tool provides password challenge
- Option to disable read access to some areas of memory when a debugger is present
- Option to disable cryptography services after debugger connect

Security Features in S32V200

S32V200 – Security Relevant Features



ARM Trust Zone architecture

Cryptographic Security Engine v3 (CSE)

Secure JTAG Interface

Resource Domain Controller (xRDC)

On-The-Fly cryptography (OTFAD)

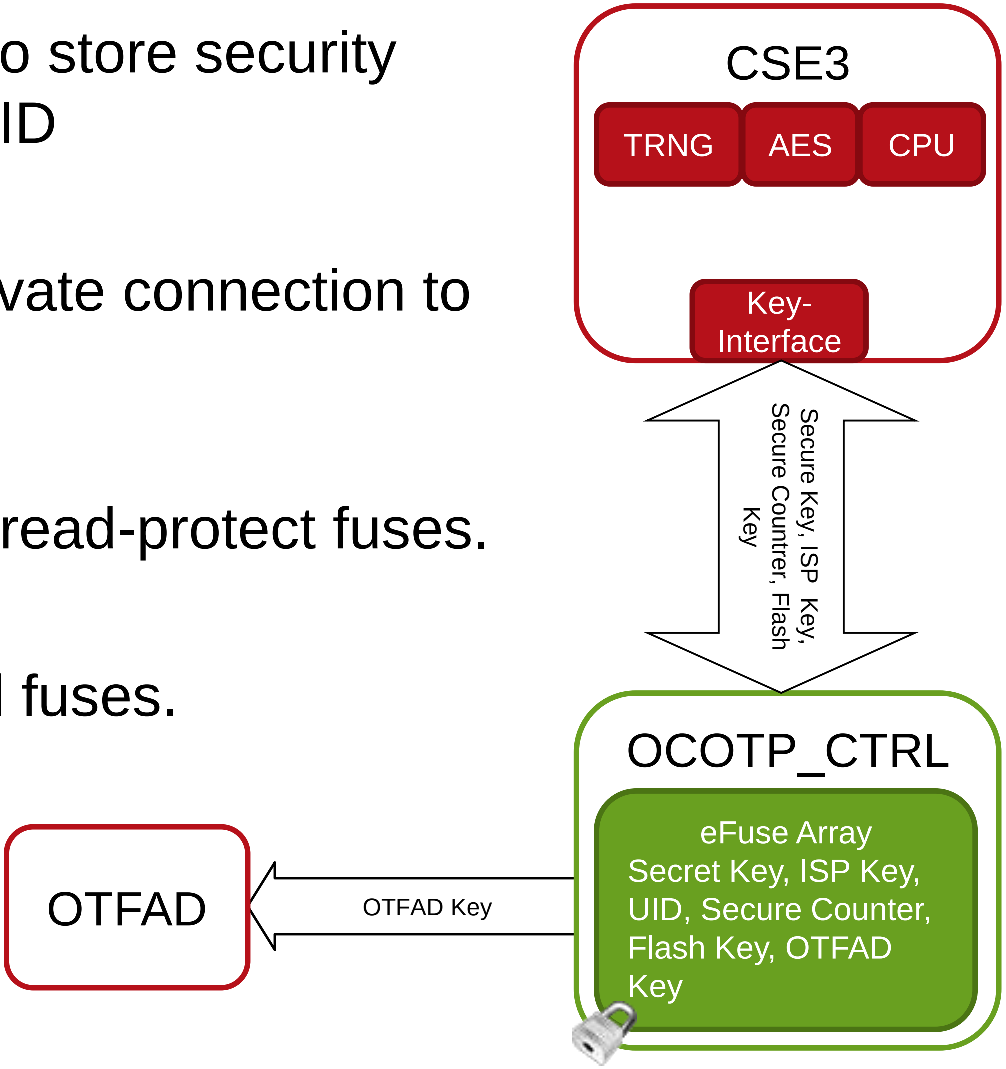
Boot ROM Code (root-of-trust)

On-chip One Time Programmable (OCOTP) Controller

freescale™

On-chip One Time Programmable (OCOTP)

- On-chip electrical fuse array to store security related keys and unique chip ID
- Program interface for SW, private connection to security blocks
- Provide program-protect and read-protect fuses.
- CRC32 testing of read-locked fuses.


CSE3
TRNG
AES
CPU
Key-Interface
Secure Key, ISP Key, Secure Countrer, Flash Key
OCOTP_CTRL
eFuse Array
Secret Key, ISP Key, UID, Secure Counter, Flash Key, OTFAD Key
OTFAD
OTFAD Key

TrustZone Architecture & xRDC

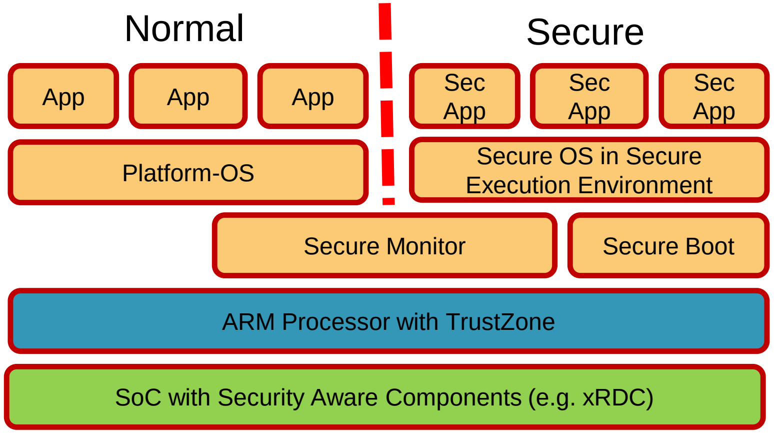
- TrustZone virtualises the core & interrupt controller in two “domains” secure/non-secure

- Core mode visible on every bus access

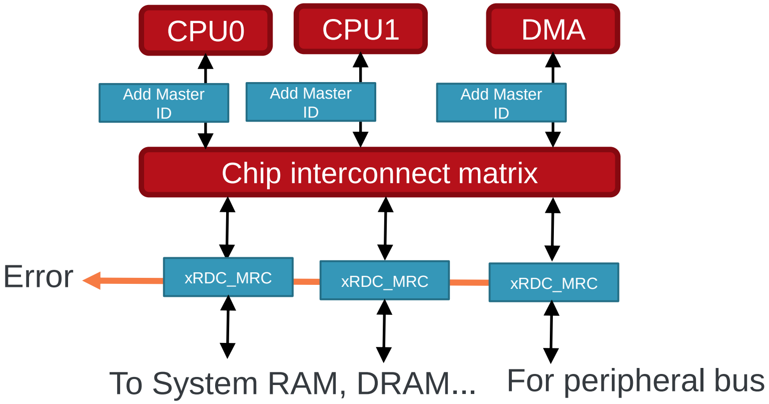
- xRDC use this information plus the bus master-ID to implement an access scheme.

  Example: CAN bus module is only accessible, if the core is in secure domain and in supervisor mode.

TrustZone Software Architecture

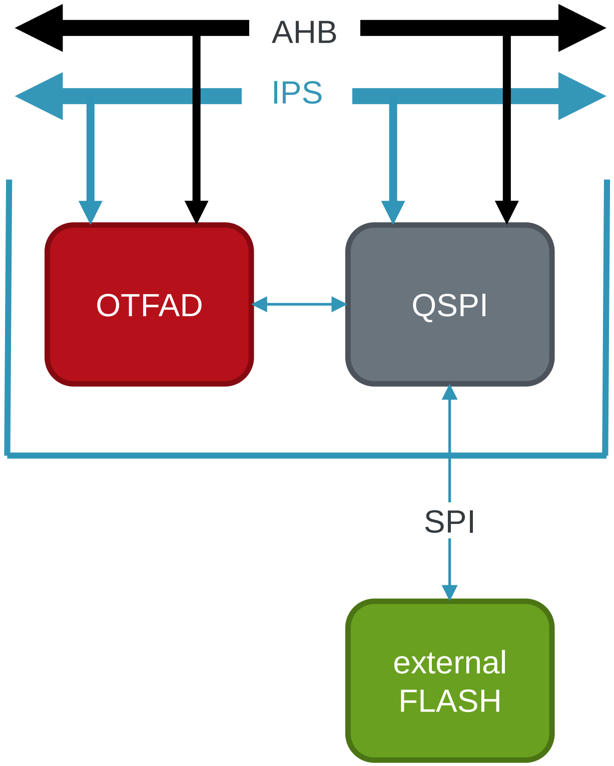

Normal
Secure
App
App
App
Sec App
Sec App
Sec App
Platform-OS
Secure OS in Secure Execution Environment
Secure Monitor
Secure Boot
ARM Processor with TrustZone
SoC with Security Aware Components (e.g. xRDC)

xRDC: Concept Overview



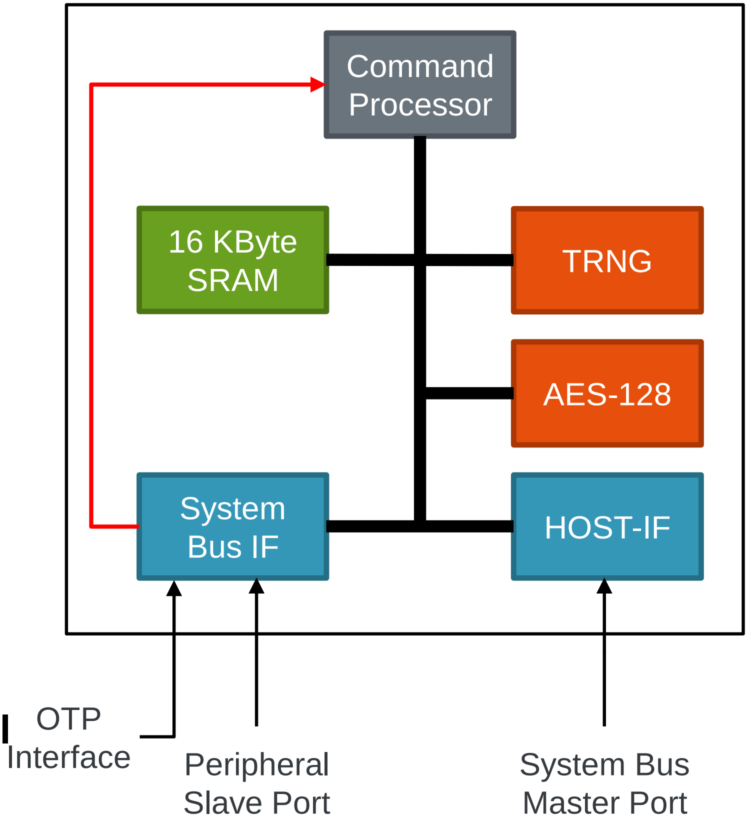
On-the-Fly AES Decryption Module (OTFAD)

- Decrypt data from external NOR QSPI-Flash
- Allows code execution from an encrypted image
- Pipelinig reduce (up to 0ws) latency to decrypt code & data fetching
- Support of AES-128 with counter chipher mode
- Support of 4x decryption segments
- Hardware support for unwrapping "key blobs“ (as defined by RFC3394)



Cryptographic Services Engine v3 (CSE3)

- **CSE module implements main elements of the HIS SHE-Specification**
- **32-bit secure core working at 133 MHz**
- **AES-128**
  - Supported crypto modes: ECB & CBC
  - Throughput ~100 Mbit/sec
  - Latency 2μs per one encoding/decoding ops
- **CSE module interfaces:**
  - System master interface
  - Configuration interface
- **PRNG seed generation via TRNG**
- **CSE Core not programmable by customer**
- **Encrypted code and key image are stored in external memory**
- **Several tamper detect inputs and a tamper detect enable**



i.MX Security Features

i.MX Security Features

TrustZone

- Trusted execution environment for security-critical SW
  - Secure & Normal Worlds (processor modes, timers, Interrupt. Controller)
  - Hardware access permissions gaskets to all memories

High Assurance Boot:

- Security library embedded in immutable on-chip ROM
- Authenticating Secure boot process: protects against unauthorised SW
  - Signature Verification leveraging public key based infrastructure (PKI)
  - RSA-1024/2048/3072/4096 anchored to OEM Public Key (Super Root)
- System HAB Run every time chip is reset.
- Encrypted Boot

Secure Storage:

- Programmable TrustZone and Domain protected regions On and Off chip memories
- On-chip zeroizable Secure RAM: 32 KB i.MX7D, 64-128KB i.MX8QMax
- Off-chip storage protected using AES-256 and chip’s unique and secret HW-only key

i.MX Security Features (continued)

HW Cryptographic Accelerators

- Certifiable RNG: TRNG entropy source + Hash DRBG
- Symmetric: AES (128,256), 3DES
- Asymmetric:
  - Elliptic Curve (brainpool, NIST up to P-521)
  - RSA up to 4096 bit keys
- Hash SHA-1, SHA-256, SHA-512 (i.MX8) MD-5

HW-enforced Access Controls

- Control access from CPU & DMA peripherals to peripherals and memories
- Integrated with TrustZone

Resource Domain Separation (on some products)

- Ability to assign execution environments to individual domains
- Enforces isolation among domains for peripherals and memories
- Allows for hierarchical and non-hierarchical privileges levels

i.MX Security Features (continued)

Secure Real-Time Clock

- On-chip, self-powered real-time clock

Secure JTAG

- Configurable protection against unauthorised JTAG manipulation
- Three security levels + complete JTAG disable

Tamper Detection

- 5 Active or 10 Passive Tamper

Lifecycle Device Configurations

- Open: non-secure products
- Closed: secure products
- Field Return: OEM-authorized test paths re-opened

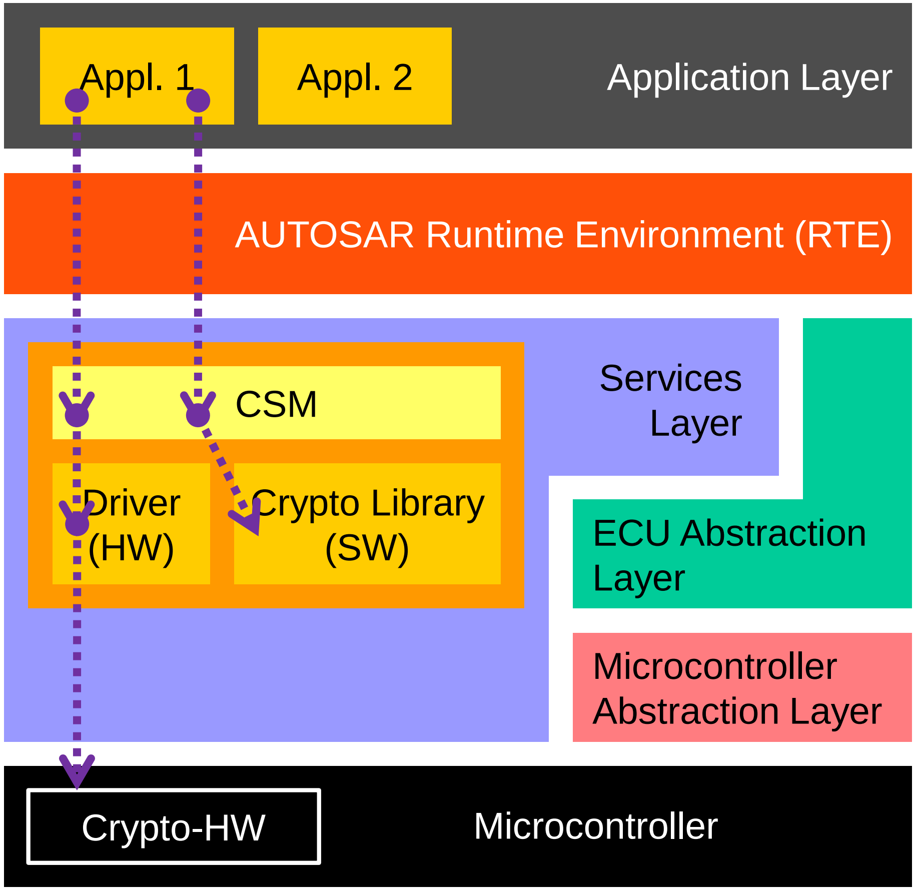
Software Support for Automotive Cyber Security

AUTOSAR 4.0 - Crypto System Services

- Crypto Service Manager (CSM)
  - Access to cryptographic services for applications and system functions
  - Cryptographic services:
    - Hash computation
    - Asymmetrical signature verification
    - Symmetric encryption

- Crypto library (CAL)
  - Provides cryptographic algorithms
  - SW or HW, e.g., CSE module of MPC5646C

- Freescale + Elektrobit
  - Include CSE module in AUTOSAR



Semiconductor Industry Drivers Affects Security Implementations for Automotive

Semiconductor Industry Trends

- The fixed cost for microcontrollers is increasing exponentially while the variable cost of adding extra logic and features is decreasing
- Highest performance automotive processors won't have embedded NVM
  - Manufacturing process for logic is available long before NVM fabrication process
  - Adding flash memory significantly increases the number of manufacturing steps for a micro – putting NVM on-chip is only cost effective if it represents a large percentage of the die
  - Certain applications have a much larger code footprint than the amount of flash memory that can be implemented on-chip
- Automotive represents <10% of total semiconductor market

Impact of Semiconductor Industry Drivers on Automotive Security

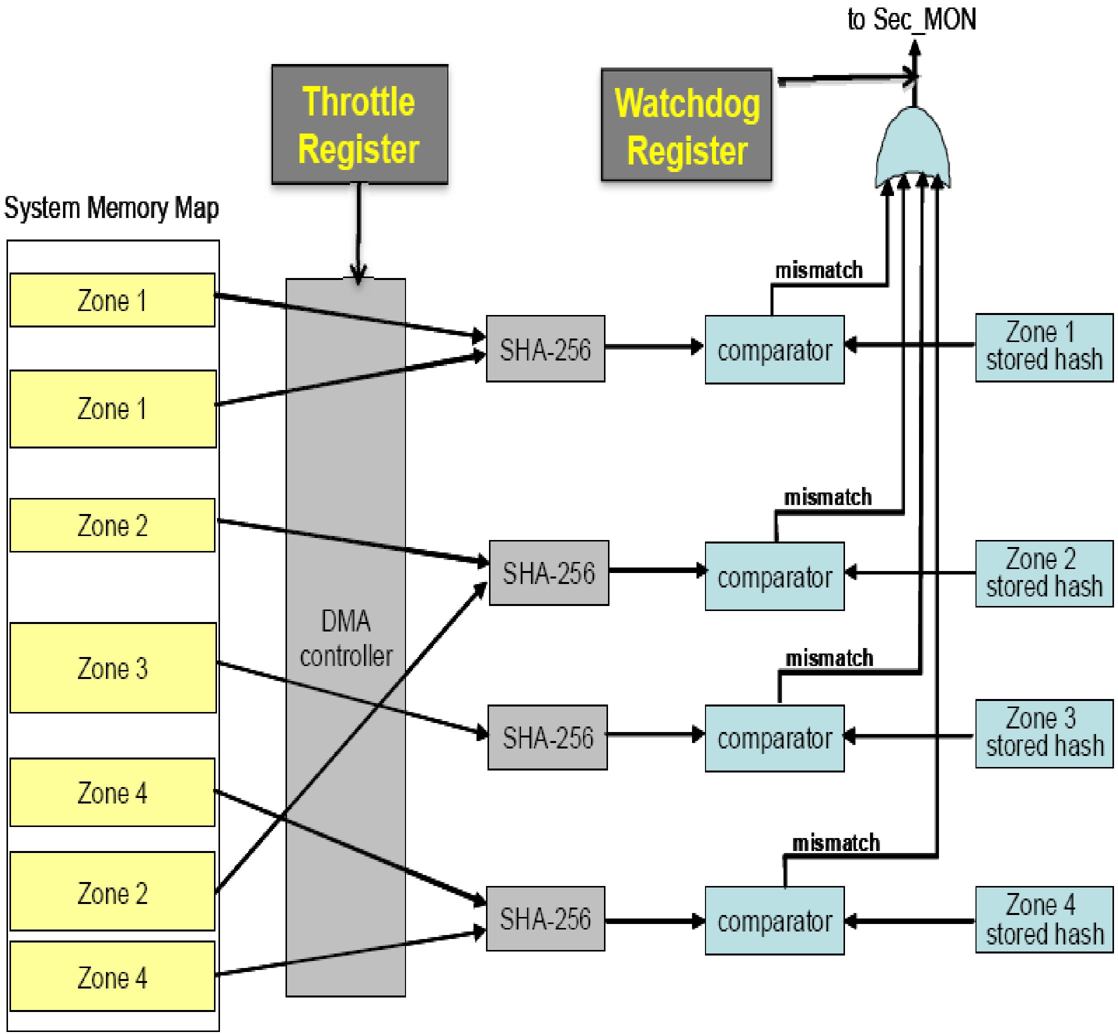
- Fewer processors variants means that each part will need to support multiple applications and multiple security standards
  - Standards should scope requirements, not implementation
  - Flexible on-chip security implementation will be highly desirable

- Automotive security requirements should not prohibit external flash memory (at least for some applications)
  - It is possible to use a security element external to the main processor, but this may increase implementation cost and increase system response latency

Security Features Used Outside Automotive

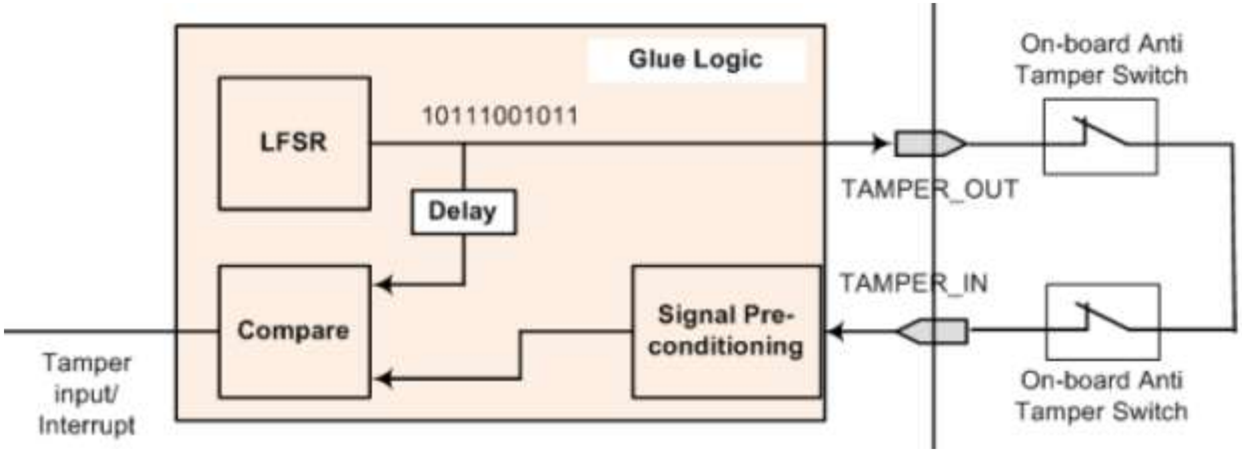
Run Time Integrity Checker

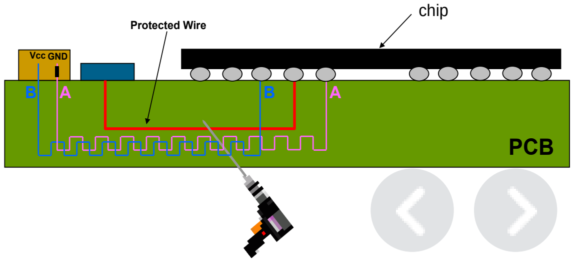
- Executes in parallel with the application code, and shares memory bus bandwidth with the application
- Burst mode DMA capability can minimize bus contention
  - SHA-256 execution rate in the order of 100M bytes/second
- Performs continuous authentication of static memory image
  - e.g. Flash program and calibration space
- Signals a fault condition if memory content appears to have changed



Active Physical Tamper Detection

- How it works:
  - Each of the active tamper output pins will output a pseudo-random value that can changes periodically (1-2000 Hz).
  - The input pin expects to see the associated active tamper output signal (with some propagation delay allowed for a glitch filter).





Side Channel Attacks

Side Channel Attacks & Countermeasures

- Fault Injection (Active Attacks)
  - Low voltage manipulation, voltage glitching
  - Overclocking, clock glitching
  - Heating / cooling (either localized or general)
  - Can retrieve crypto keys with small number of iterations
  - Exist on many known ciphers – AES, RSA, ECC

- Passive Attacks
  - SPA : Simple Power Analysis
  - DPA : Differential Power Analysis
  - Timing analysis

Reverse Engineering Attacks & Countermeasures

- The standard countermeasures taken against reverse engineering attacks include the following:
  - Memory encryption
  - Encryption of data
  - Scrambled logic (especially no hard macros)
  - No logic relevant to security in top metal layers

- Recent New Feature
  - Physical Unclonable Functions (PUFs)
    - Arbiter PUFs (based on race conditions)
    - SRAM-based PUFs

Power Supply Fault Injection

- Voltage manipulation can influence the behavior of code execution
  - e.g. Change a “BNE” instruction to “BEQ”
  - Could take less than 5 minutes per attack (Barenghi et al, FDTC 2009)
  - FDTC is an annual conference on Fault Diagnosis & Tolerance in Crypto
- Voltage manipulation can corrupt data reads and writes
- Might require installation of specific software to continuously exercise the crypto algorithm
- Addition Low Voltage Detection (LVD) circuits might be an acceptable countermeasure
  - Provided response time is matched to characteristics and behavior of chip implementation
- Redundant decision logic should also protect against this attack

Clock Glitch Injection

- Requires access to device clock input
- Glitch could appear as a transient overclocking of the device.
- Generally causes either a corruption of the fetched instruction, or a repeated execution of the previous instruction
- Attack seems most successful on multi-cycle instructions
  - Balasch et al, FDTC 2011
- Installation of glitch detection circuits or clock monitor circuits could provide countermeasures
- Best countermeasure may be to use only internal clock source for cryptographic unit engine

SPA & DPA

- Extracts cryptographic information by analyzing the power profile or EM spectrum emitted by the device during cryptographic operations

- Might require installation of specific software to continuously exercise the crypto algorithm

- Information can be extracted using selective filtering of the power spectrum, and a knowledge of algorithm's arithmetic operations

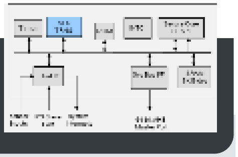
- DPA uses signal processing and statistical analysis to extract crypto keys from noisier signals than SPA is capable of

- Countermeasures can be integrated into the design of the hardware algorithm to evenly distribute the power profile
  - Could result in 30-50% increase in implementation size
  - Techniques include hiding, masking, shielding, etc.

Summary

Freescale Hardware Auto Security Options

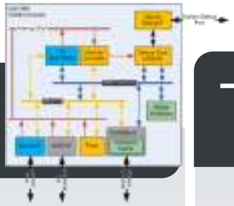
CSE



Cryptographic Security Engine

- MPC564xB/C
- MPC5777C
- Turn-key solution
- SHE Compliant
- AES-128
- Secure Key Storage

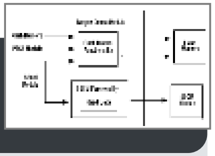
HSM



Hardware Security Module

- MPC5746M
- MPC5777M
- User programmable
- Secure debug
- Supports CSE functional requirements
- Secure sensor interface
  - Voltage, temperature and clock monitoring

TDM



Flash Tamper Detection Module

- MPC5777M/C
- Records all attempts to modify flash memory
- Detects unauthorized re-programming of application code
- Protects manufacturers' investment

HAB

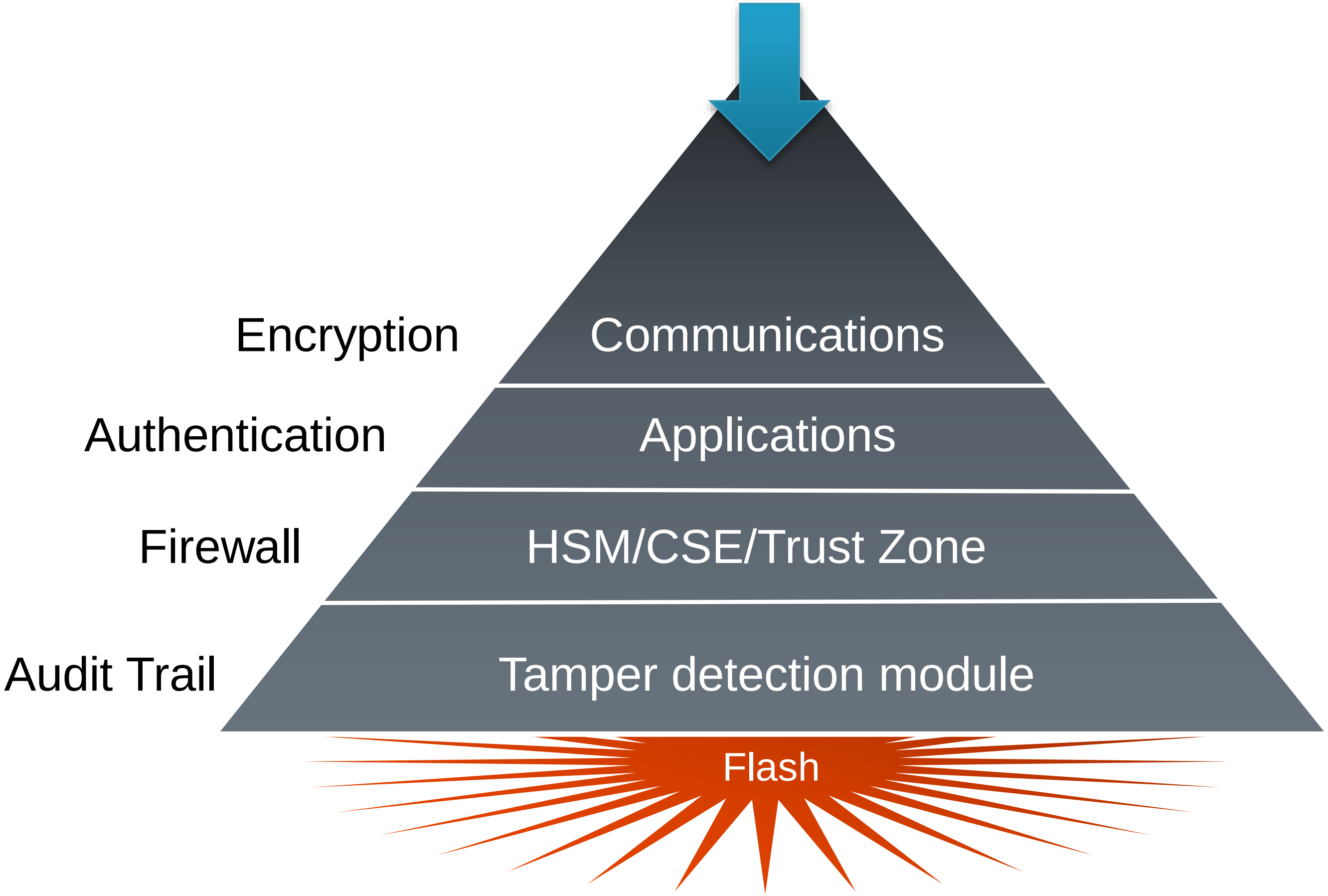
High Assurance Boot

- i.MX Processors
- Supports ARM TrustZone®
- Physical tamper detection
- AES-128, AES-256, 3DES, ARC4
- SHA-1, SHA-256, MD-5

Freescale Security Architecture

Multi-layered approach strengthens overall vehicle security

Protects against HW and SW theft, tuning, parts cloning, mileage manipulation and personal data theft



www.Freescale.com