FTF 2016
TECHNOLOGY FORUM

# MAXIMIZING SECURITY USING THE SECURE MCU FEATURES

## FTF-AUT-N1810

JUERGEN FRANK
SR. SYSTEM ENGINEER
FTF-AUT-N1810
MAY 17, 2016

PUBLIC USE

# AGENDA

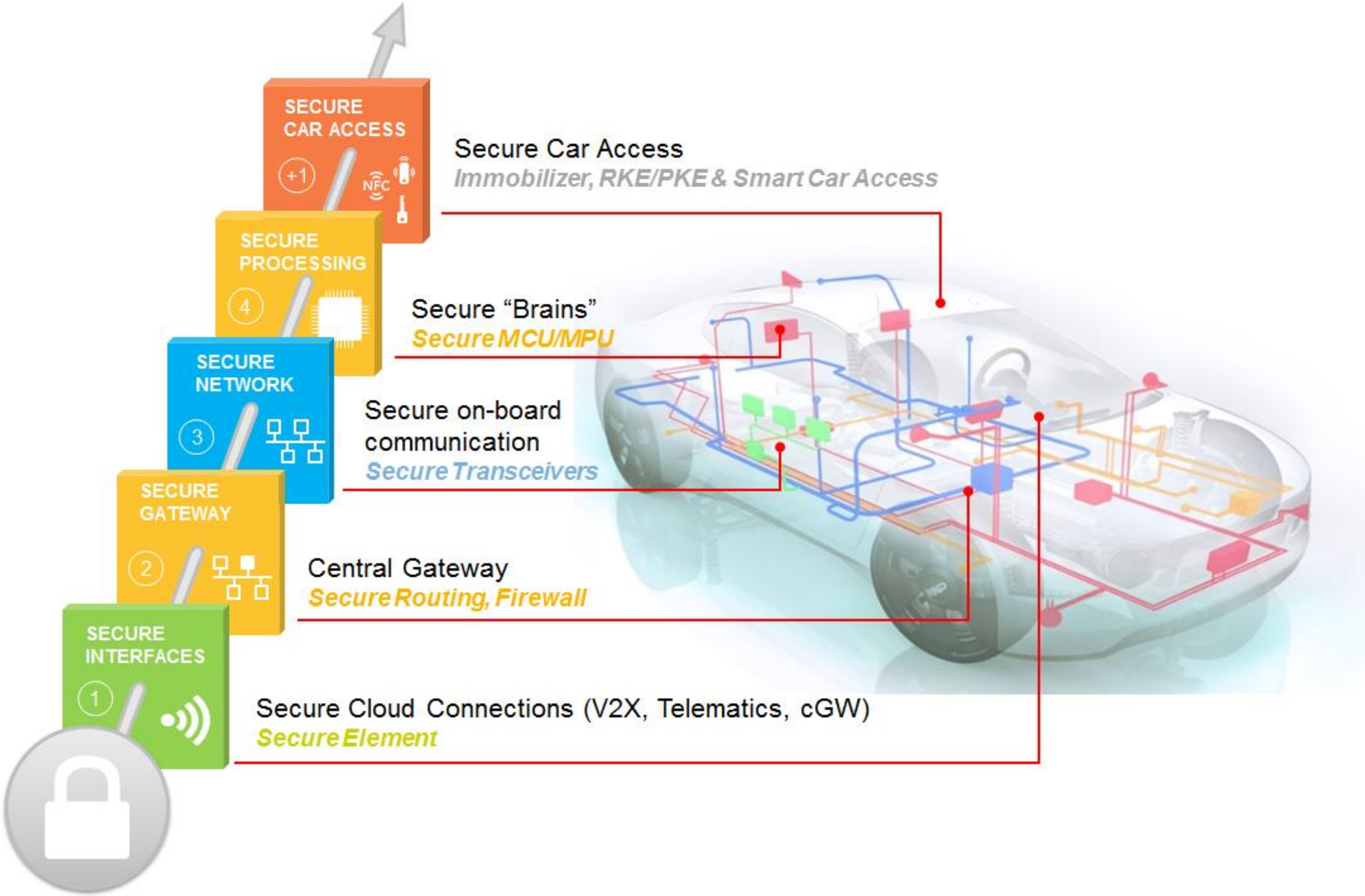
- Security Use-Cases & Attacks
- Automotive Specifications
- NXP Automotive MCU – Security Features
  - Secure Start-Up & Secure Boot
  - Flash Protection
    - PASS
    - TDM
  - Security Modules
    - CSE
    - HSM

# FTF-AUT-N1810

## TITLE: Maximizing Security using the Secure MCU Features

This presentation will cover the Hardware Security Module (HSM) and how to use software kits NXP published for it (HSM Security Firmware and HSM SDK). Other device security features offered by modules like PASS or TDM and their configuration will be discussed, too.

# NXP Automotive Vehicle Security Architecture (4 +1 Solution)



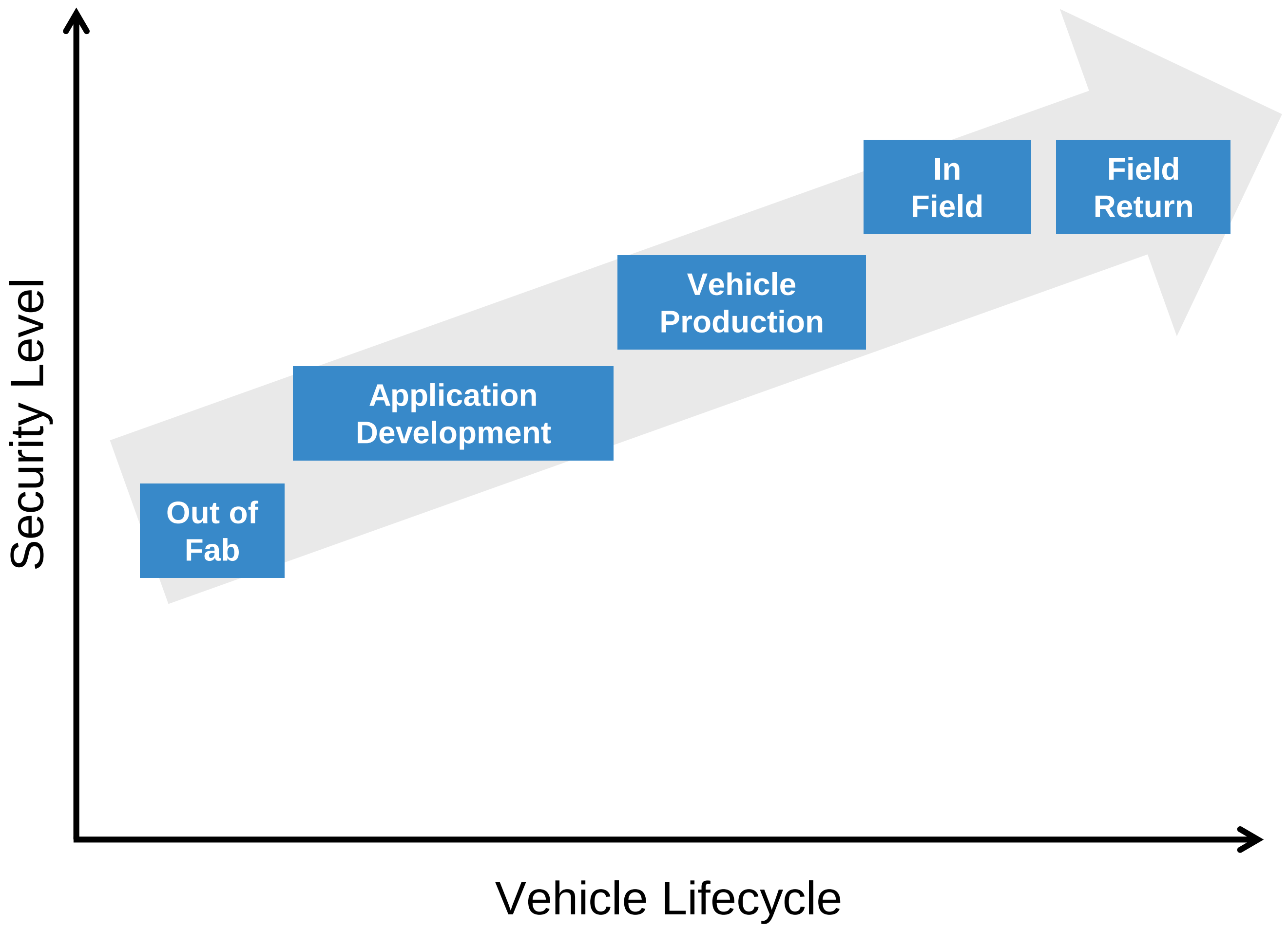
- **NXP #1 in Auto HW Security**
- **4-Layer Cyber Security Solution**
- **Plus 'Best In Class' Car Access Systems**
- **Recognized Thought & Innovation Leader**
- **Partner of Choice for OEMS, T1s & Industry Alliances**

# Hardware Security is a Must

- **Crypto accelerators**, to guarantee strict performance requirements
  - E.g. V2X message authentication, CAN authentication, secure boot, …
- **Hardware-enforced isolation**, to protect against software attacks
  - E.g. system vs. user mode, TrustZone, SHE/HSM, …
- **Tamper-resistant hardware**, to protect against advanced, physical attacks
  - E.g. Secure Elements

# Security Throughout the Entire Lifecycle

- Increased security level at each stage of the development lifecycle
- Non-reversible, non-revocable
- Enable application development, debugging and failure analysis
- Without compromising security in the production vehicle



# Proven History in Driving Automotive Security

**Mid 1990s**
- Censorship
- Infrastructure

**Early 2000s**
- Enhanced Censorship
- Infrastructure

**Mid 2000s**
- High Assurance Boot
- Fault detection sensors

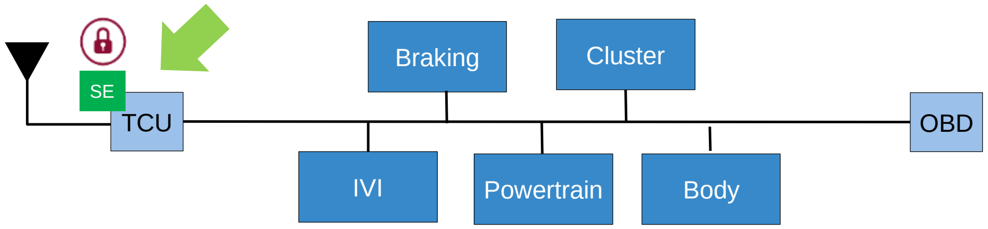
**Late 2000s**
- Crypto Services Engine (SHE)
- Active shields

**2010s +**
- Hardware Security Module (HSM)
- Secure Elements (SE)
- Gateway, IVN security

# 4 Layers to Securing a Car

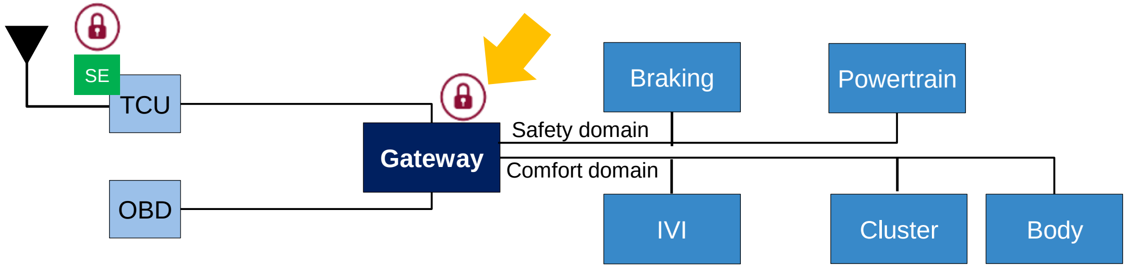
## Layer 1: Protect External Interface

Secure M2M authentication, secure key storage



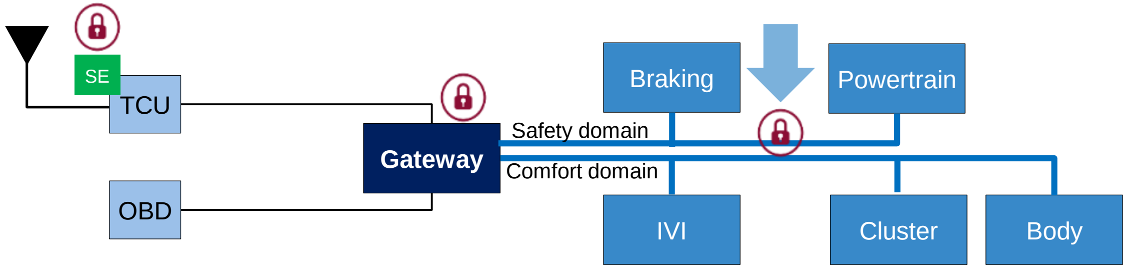
## Layer 2: Isolate Network

Domain isolation, firewall/filter, centralized intrusion detection (IDS)



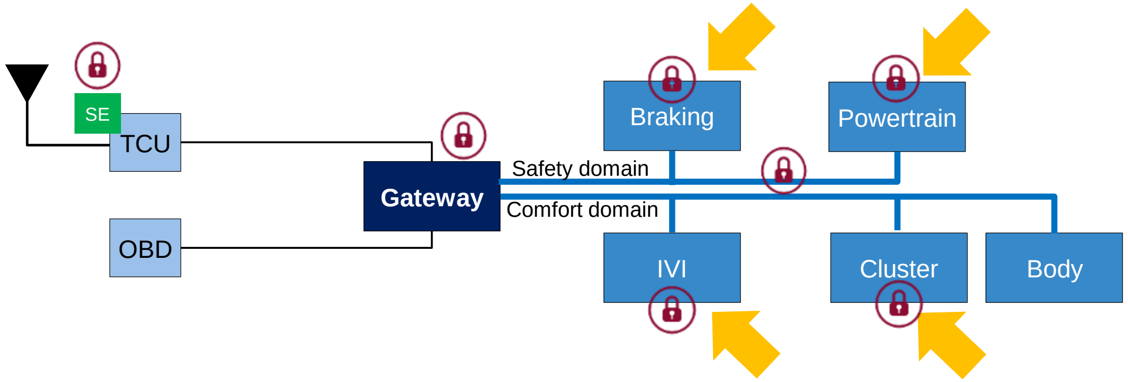
## Layer 3: Secure Network

CAN ID Killer, message authentication, distributed intrusion detection (IDS)



## Layer 4: Secure Processing

Secure boot, run time integrity, OTA updates



# SECURITY USE-CASES & ATTACKS

# Security Use Cases

## In-Vehicle Security

- Immobilizer / Component Protection
- Mileage Protection
- Secure Boot and Chain of Trust
- Secure Communication
- DRM for Batteries

## Connected Vehicle Security

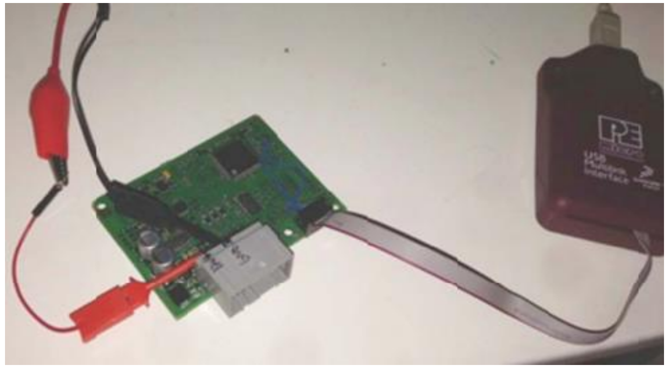
- Android application download
- DRM for content download/streaming
- Remote ECU firmware update
- Black-box for due government or insurance
- Car-to-Car communication

# Other Automotive Security Threats

NHTSA

Test Video of Counterfeit Air Bags
September 12, 2012

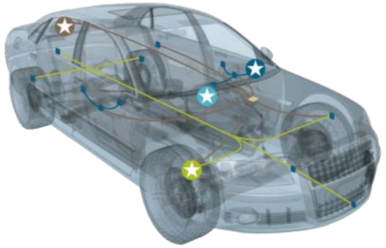
**Transportation Department Warns Against Counterfeit Air Bags**
October 10, 2012, NHTSA estimates it affects 0.1% of US Fleet, availability of such replacement systems traces back to 2003 (!)



**DARPA Funded Researchers Take Control Of Two Vehicles**
Using a Macbook connected to the On-Board Diagnostics Port Dr. Charlie Miller and Chris Valasek. July, 2013,  Defcon: Adventures in Automotive Networks and Control Units [http://illmatics.com/car_hacking.pdf]

**Mileage Manipulation (in Germany)**

- 2 million manipulated cars per year
- Average increases in value per car  ~3000€
- Total loss 6 billion euro



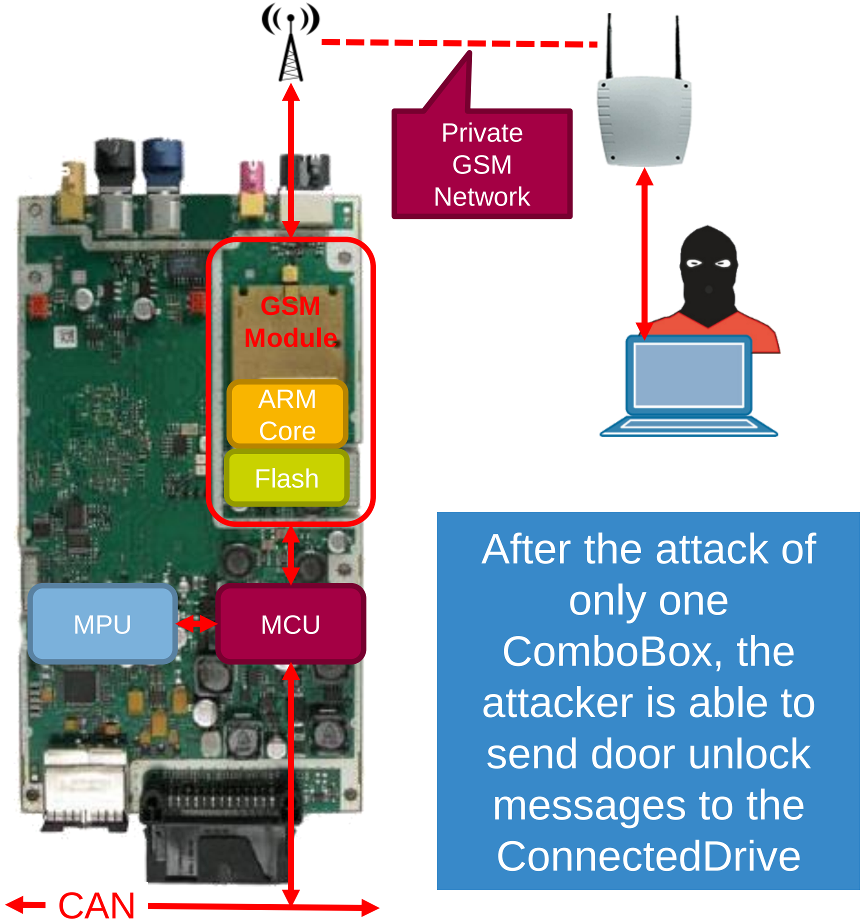
# The ConnectedDrive – Unlock the Doors

## Issue/Hack:

- No individual keys per car
- Keys stored in readable flash / Firmware readable
- Debug-port active
- Outdated or no encryption on some services
- No integrity check of the device configuration
- No authentication of the counterpart station
- ~ 2.2 million affected cars

## Security Requirements:

- Improve key management
- Use existing device features (e.g. disable debug port)
- Crypto modules with:
- Secure key storage
- Actual cipher algorithm (e.g. AES-128) support



After the attack of only one ComboBox, the attacker is able to send door unlock messages to the ConnectedDrive

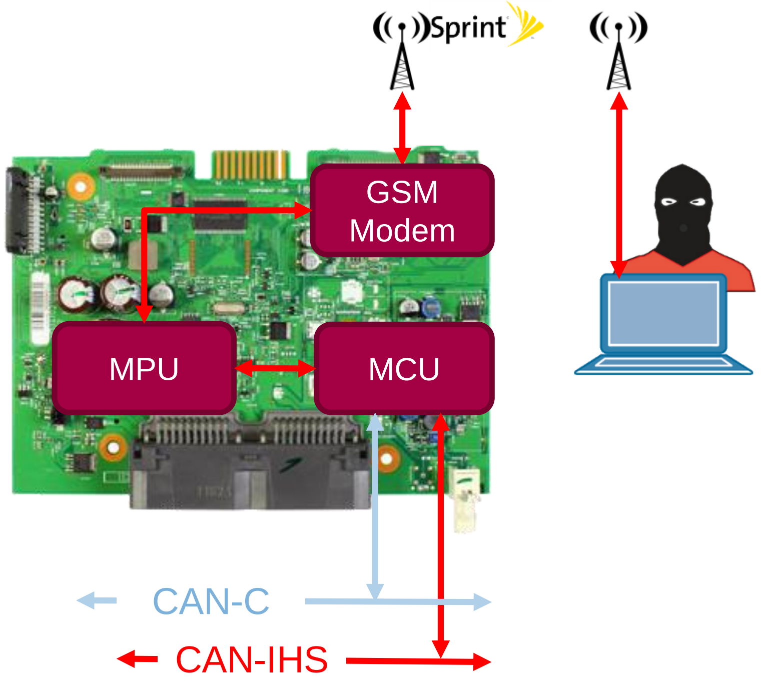
# Vehicle – Out of Control

**Issue/Hack:**

- Radio/Infotainment system is directly connected both CAN busses
- Weak Wi-Fi password system and network configuration (e.g. open D-Bus)
- Weak firmware update process
- Debug-port active
- No secure boot
- Flash content readable
- No encrypted firmware image, no signatures
- OEM has to recall 1.4 Million Cars Over Hacking

**Solution:**

- Improve network architecture
- Firmware image authentication during update
- Use Secure Boot
- Use Message Authentication for safety relevant messages (e.g. Break / Steering Wheel control)
- Use existing device features (e.g. disable debug port)



Due several weakness it‘s possible to execute code on the MPU remotely via the GSM network. Additional it‘s possible to modify the MCU firmware and send faked CAN messages via the MCU into the car network.
Finally it was possible to deactivate the breaks remotely!

# Automotive Security Specifications

- HIS – SHE Specification
  - Created by German OEMs, published as official HIS standard

- EVITA – Project → Hardware Security Module (HSM)
  - Defined three security modules of different complexity (low, medium, high) for different use-cases

- SAE J3061™ / J3101™
  - J3061™: CYBERSECURITY GUIDEBOOK FOR CYBER-PHYSICAL VEHICLE SYSTEMS
  - J3101™: Hardware Protected Security for Ground Vehicles

- Trusted Computing Group - Trusted Platform Module 2.0 (TPM) – automotive profile

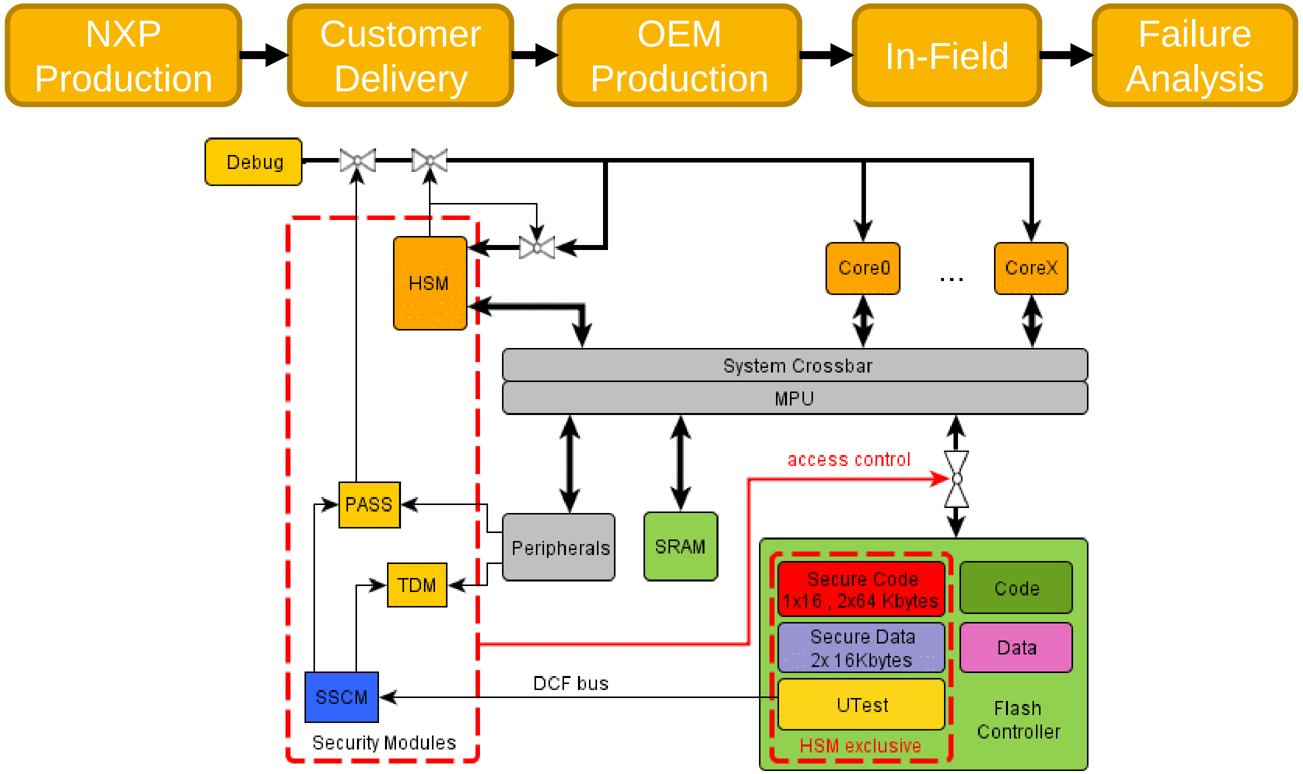
- Autosar Specifications
  - E.g. Secure Onboard Communication (Release 4.2.2)

# NXP MCU SECURITY FEATURES

# HSM Security Architecture

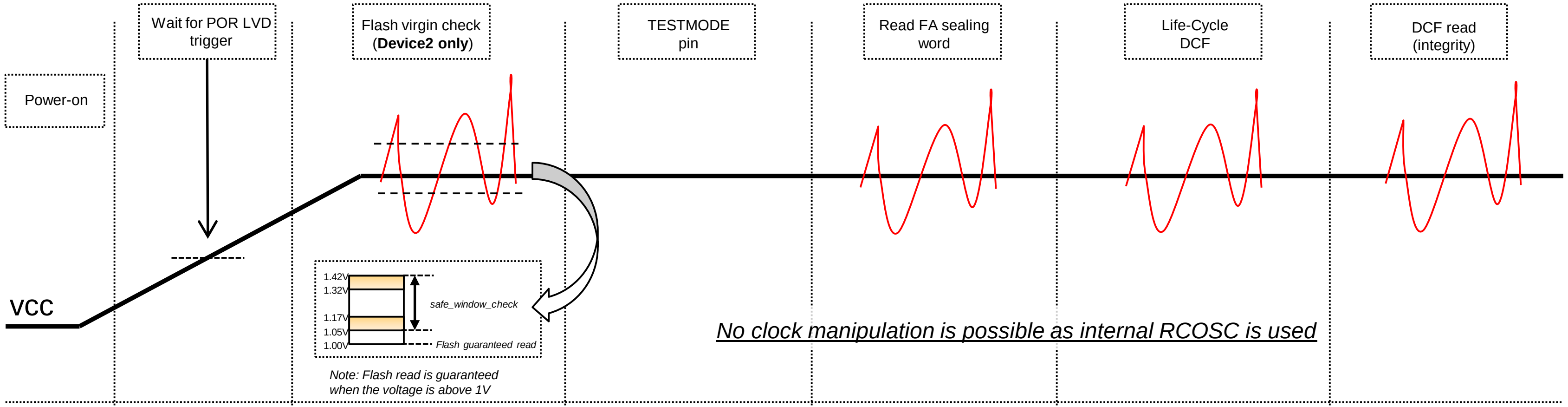
Features:

- Device life cycle scheme
- Unique ID for each device
- Debugger restrictions
- Flash Protection (TDM & PASS)
  - OTP
  - read / write & erase
  - diary to log erasing-steps



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

# Secure System Configuration – Side Attack



*Note: Flash read is guaranteed when the voltage is above 1V*

*No clock manipulation is possible as internal RCOSC is used*

| | | | | | | |
|---|---|---|---|---|---|---|
| Attack goal | No attack is possible | Create a fake Flash virgin status so that the Test Mode interface is open | Be able to manipulate the voltage and the temperature without any reaction from the internal protection mechanisms | Disable the FA sealing, so that secret data can be accessed in Test Mode when LifeCycle = FA | Revert the life cycle to an “older“ so that the security mechanism are open | Manipulate information read from the Flash during the reset |
| Attack method | - | Voltage or Temperature manipulation | Force TESTMODE pin | Voltage or Temperature manipulation | Read the 1st LIfeCycle DCF and the apply Voltage or Temperature manipulation | Voltage or Temperature manipulation |
| Effect | - | Corrupt the Flash Virgin check reading | Voltage and Temperature monitors cane be disabled | Corrupt the Seal word check reading | Only the 1st LifeCycle will be valid: protections are disabled | Corrupt the DCF value |
| Solution | The device will not exit the Reset phase | Flash = Virgin only if<br>1. Read word failed<br>AND<br>2. Seal pad + No fail from (non-maskable) Volt/Temp monitors | 1. Pre-Life cycle: the monitor disabling is applied only if a specific key is written Into the Flash<br>2. 4xDCF parallel reading | Voltage monitors disabling is protected by Pre-Life cycle<br>They can´t be disabled when „In Field“ | 1. Voltage monitors disabling is protected by Pre-Life cycle They can´t be disabled when „In Field“<br>2. 4xDCF LifeCycle are read in one shot | 1. Monitor protections<br>2. ECC check on each DCF reading<br>3. Validation of DCF reading between Destructive and Functional reset phases<br>4. One-time read DCF |

# UTest Memory Map

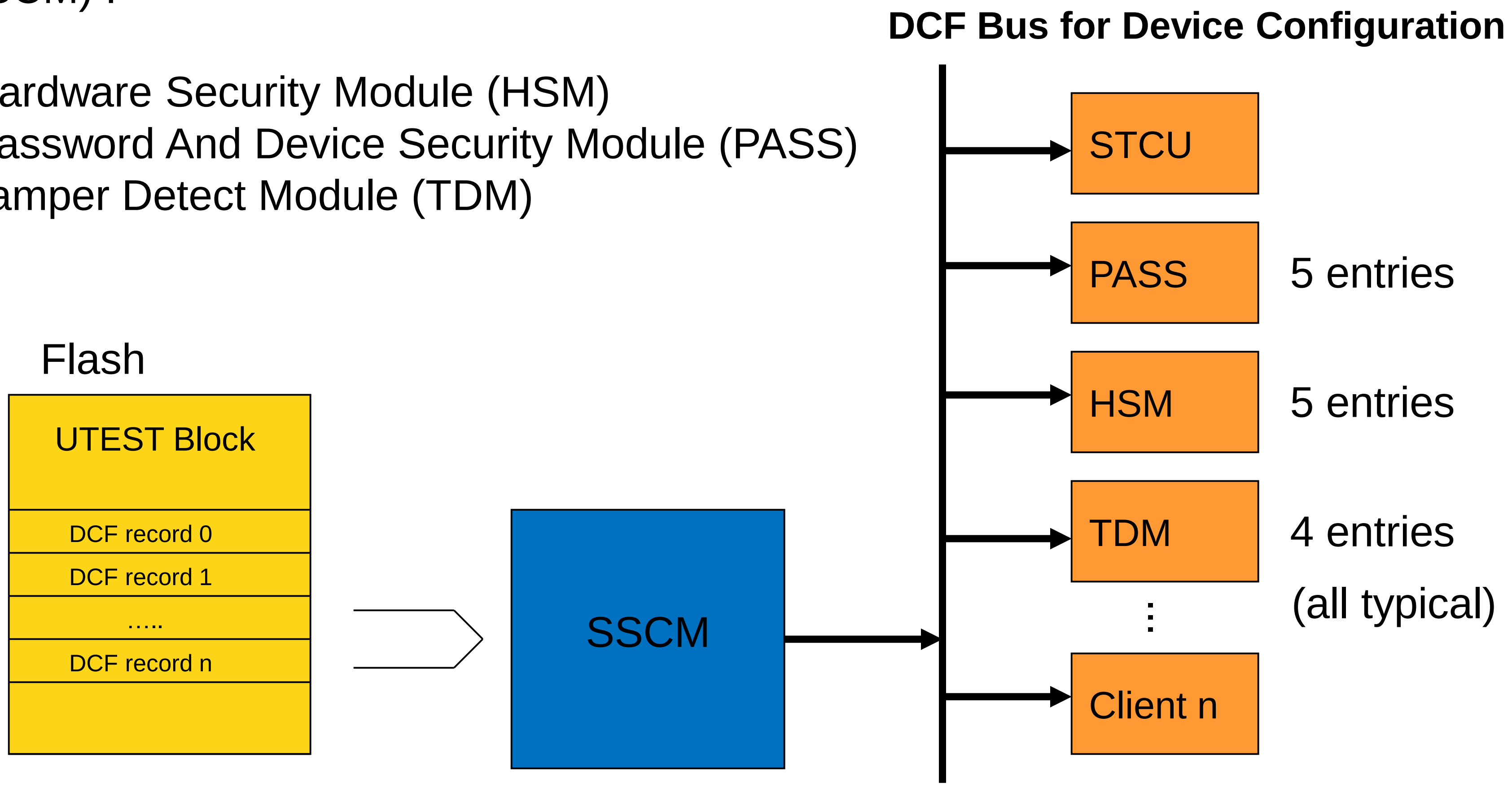
| Address | Size [Bytes] | Description |
|---|---|---|
| 0x00400000 | 2 | Sensor Calibration A |
| 0x00400002 | 2 | Sensor Calibration B |
| 0x00400004 | 2 | Sensor Calibration C |
| 0x00400006 | 2 | Sensor Calibration D |
| 0x00400008 | 4 | Reserved |
| 0x0040000C | 4 | Test Mode Disable Seal |
| 0x00400010 | 16 | Test Mode Disable Block Group A |
| 0x00400020 | 16 | Factory Erase diary Location |
| 0x00400030 | 16 | Test Mode Disable Block Group B |
| 0x00400040 | 32 | Customer Single Bit Correction Area |
| 0x00400060 | 32 | Customer Double Bit Detection Area |
| 0x00400080 | 32 | Customer EDC after ECC Area |
| 0x004000A0 | 32 | UID |
| 0x004000C0 | 4 | Soft DCF Record Start Address |
| 0x004000C4 | 4 | Reserved |
| 0x004000C8 | 56 | Reserved |
| 0x00400100 | 4 | Test Mode Override Passcode |
| 0x00400104 | 28 | Reserved |
| 0x00400120 | 32 | JTAG Password |

| Address | Size [Bytes] | Description |
|---|---|---|
| 0x00400140 | 32 | PASS Password Group 0 |
| 0x00400160 | 32 | PASS Password Group 1 |
| 0x00400180 | 32 | PASS Password Group 2 |
| 0x004001A0 | 32 | PASS Password Group 3 |
| 0x004001C0 | 32 | Reserved - PASS Password Group 4 |
| 0x004001E0 | 32 | Reserved - PASS Password Group 5 |
| 0x00400200 | 16 | Lifecycle slot 0 – FSL Production |
| 0x00400210 | 16 | Lifecycle slot 1 – Customer Delivery |
| 0x00400220 | 16 | Lifecycle slot 2 – OEM Production |
| 0x00400230 | 16 | Lifecycle slot 3 – In-Field |
| 0x00400240 | 16 | Lifecycle slot 4 – Failure Analysis |
| 0x00400250 | 176 | Reserved |
| 0x00400300 | 8 | DCF Start Record |
| 0x0040308 | 64 | DCF HSM ‘ROM’ keys |
| 0x00400348 | 3256 | DCF Records |
| 0x00401000 | 12288 | Reserved for custom OTP data |

# Secure System Configuration

During reset phase configuration data is moved from a special flash block (UTEST) to the security modules by the SystemStatusConfigurationModule (SSCM) :

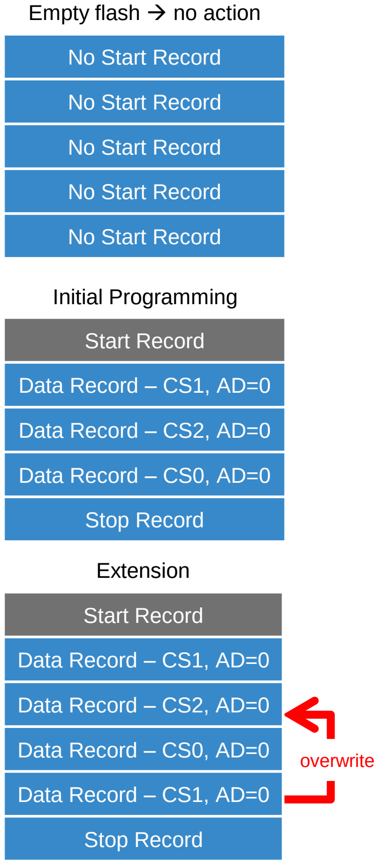
- Hardware Security Module (HSM)
- Password And Device Security Module (PASS)
- Tamper Detect Module (TDM)



# Device Configuration Format (DCF)

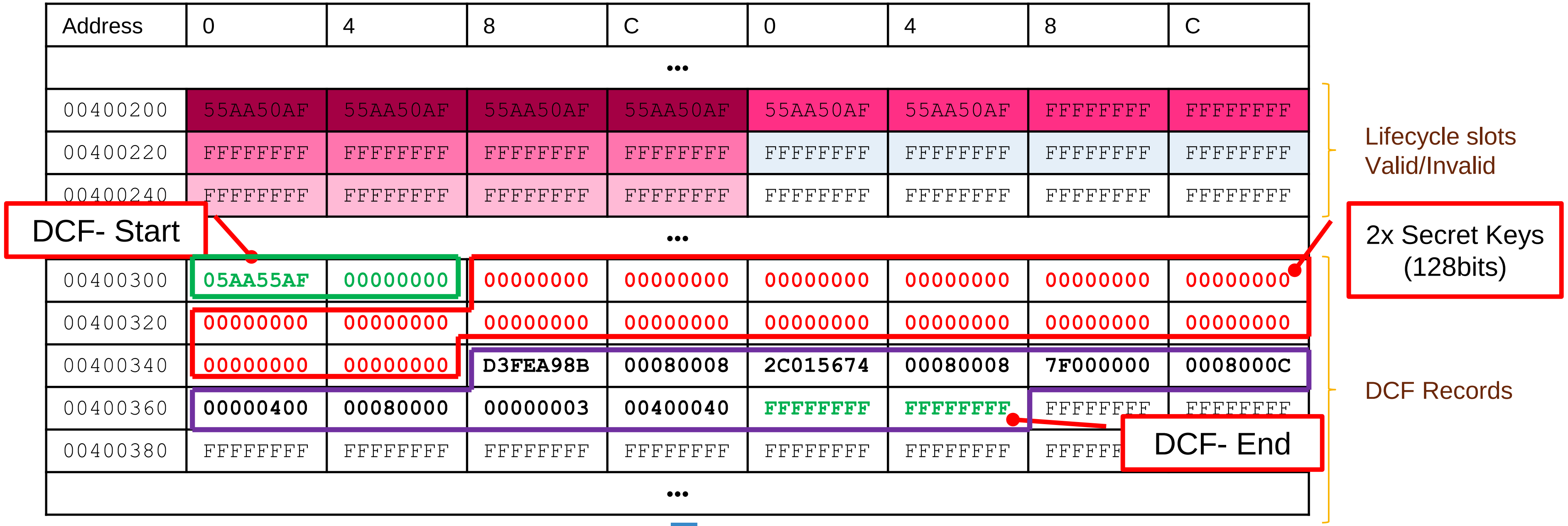
| | Word | DCF entry ( 2x 32bit words ) | | | |
|---|---|---|---|---|---|
| Data | 0 | WDATA[31:0] | | | |
| Destination Module/Register | 1 | Module [14:0] | Register [12:2] | Parity | Stop |

| Module | Client |
|---|---|
| CS2 | Self-Test Control Unit (STCU) |
| CS3 | Password and Device Security Module (PASS) |
| CS4 | Tamper Detection Module (TDM) |
| CS5 | Hardware Security Module (HSM) |
| CS7 | MISC |
| CS14 | BAF Soft Clients |



| Client Strategy | Description |
|---|---|
| None | No special DCF strategy is used. |
| Parity | Not implemented for DCF clients. Only used for TEST only DCF clients not accessible by the user. |
| Write Once | A register using the Write Once strategy can only be written once. The DCF client ignores subsequent writes. |
| Triple Voted | DCF clients that use the Triple Voted strategy have three copies of the register. The SSCM will write to all three registers in a single write cycle. The outputs of the 3 registers are majority voted together to determine the correct data value. Triple voting allows for a 'bit-flip' error to occur without changing the DCF client output data. |
| Triple Voted with second write | DCF clients that use the Triple Voted with 2nd write strategy have three copies of the register. The SSCM will write to all three registers in a single write cycle. The outputs of the 3 registers are majority voted together to determine the correct data value. During the second execution of Phase 3 of the reset sequence, the SSCM will attempt to write the DCF client again. At this time, the DCF client checks to see that the register contains the same data that is being written again. |
| Write 0 only | A bit in a DCF client can only be written from a logic 1 to a logic 0. An attempt to write a bit with this attribute to a logic 1 will be ignored. |
| Write 1 only | A bit in a DCF client can only be written from a logic 0 to a logic 1. An attempt to write a bit with this attribute to a logic 0 will be ignored. |

# UTest – Dump



| Address | 0 | 4 | 8 | C | 0 | 4 | 8 | C |
|---|---|---|---|---|---|---|---|---|
| ••• | | | | | | | | |
| 00400200 | 55AA50AF | 55AA50AF | 55AA50AF | 55AA50AF | 55AA50AF | 55AA50AF | FFFFFFFF | FFFFFFFF |
| 00400220 | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF |
| 00400240 | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF |
| ••• | | | | | | | | |
| 00400300 | 05AA55AF | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 |
| 00400320 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 |
| 00400340 | 00000000 | 00000000 | D3FEA98B | 00080008 | 2C015674 | 00080008 | 7F000000 | 0008000C |
| 00400360 | 00000400 | 00080000 | 00000003 | 00400040 | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF |
| 00400380 | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFFFFF | FFFFF | |
| ••• | | | | | | | | |

DCF- Start

DCF- End

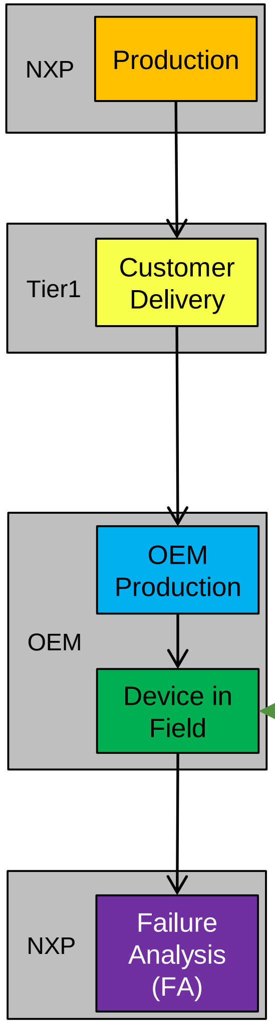
Lifecycle slots Valid/Invalid

2x Secret Keys (128bits)

DCF Records

| Data | Destination Module/Register | Module [14:0] | Reg [16:2] | Parity | Stop | Module & Register |
|---|---|---|---|---|---|---|
| D3FEA98B | 00080008 | 000_0000_0000_0100b | 0_0000_0000_0000_1000b | 0 | 0 | STCU.SKC |
| 2C015674 | 00080008 | 000_0000_0000_0100b | 0_0000_0000_0000_1000b | 0 | 0 | STCU.SKC |
| 7F000000 | 0008000C | 000_0000_0000_0100b | 0_0000_0000_0000_1100b | 0 | 0 | STCU.CFG |
| 00000400 | 00080000 | 000_0000_0000_0100b | 0_0000_0000_0000_0000b | 0 | 0 | STCU.RUN |
| 00000003 | 00400040 | 000_0000_0010_0000b | 0_0000_0000_0100_0000b | 0 | 0 | HSM.ENABLE_CONFIG |
| FFFFFFFF | FFFFFFFF | 111_1111_1111_1111b | 1_1111_1111_1111_1100b | 1 | 1 | DCF-Stop |

# Lifecycle Mechanism & States



Completely open, HSM can already be active

UTEST is OTP, Debug port open

UTEST is OTP, Passwords read/write protected, security mechanisms sharp

Most secure state

Device analysis possible, CAN & FlexRay disabled, bootloader and HSM disabled

| Lifecycle Slot (128bit) | | |
|---|---|---|
| **Valid Field(64bit)** | **Invalid Field (64bit)** | **Meaning** |
| erased | erased | erased |
| marked | erased | active |
| marked | marked | inactive |
| any other | | illegal |

| LC Slot 0 (Production) | LC Slot 1 (Customer Delivery) | LC Slot 2 (OEM Production) | LC Slot 3 (In Field) | LC Slot 4 (Field Analysis) | Resulting Lifecycle |
|---|---|---|---|---|---|
| active | inactive | inactive | inactive | inactive | Production (FSL) |
| erased | active | inactive | inactive | inactive | Customer Delivery (Tier1) |
| erased | erased | active | inactive | inactive | OEM Production (OEM) |
| erased | erased | erased | active | inactive | In Field (OEM) |
| erased | erased | erased | erased | active | Field Analysis (FSL) |

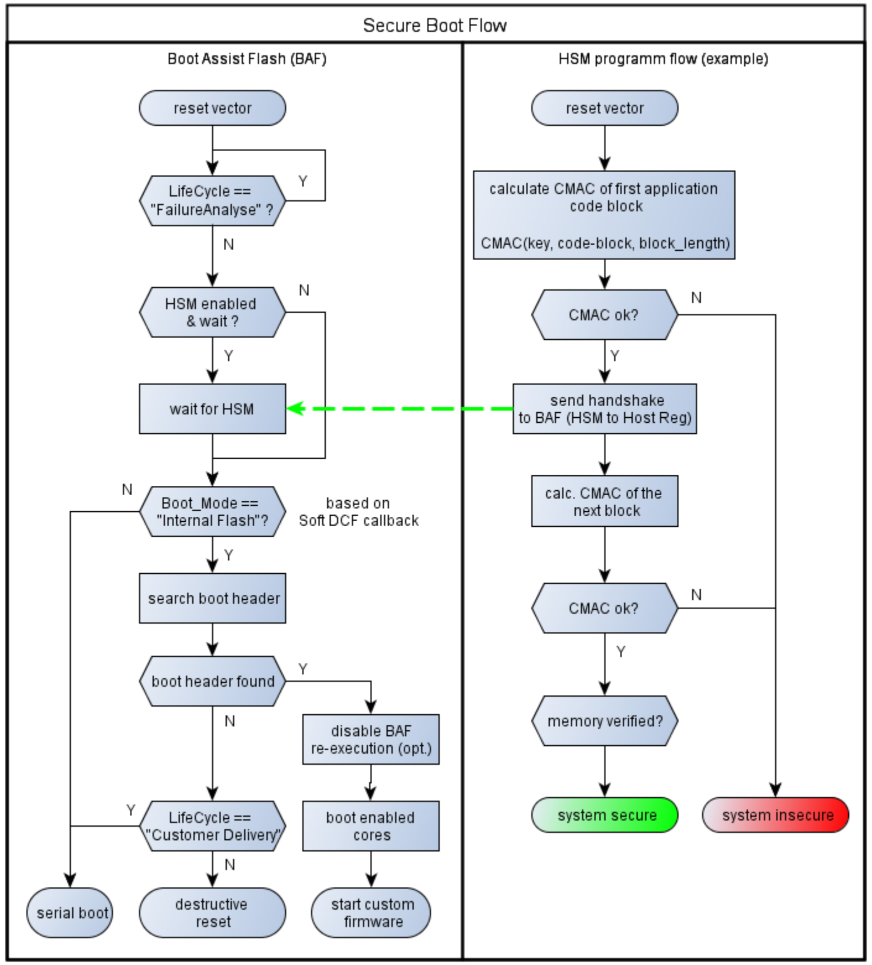
Erased: 0xFFFF_FFFF_FFFF_FFFF Marked: 0x55AA_50AF_55AA_50AF

# Secure Boot – Detect Code Manipulation

The BAF is located in a 16 KB block of flash that is mapped adjacent to the UTEST flash memory block. It is one time programmable (OTP) and is programmed during factory test.

## Functions:

- BAF is executed by CPU0
- Checks the life cycle of the device
- Run Secure Boot loop (optional)
- Execute SoftDCF clients (optional)
- Search boot header and boot options
- If no boot header is found, it downloads application code  via LINFlexD



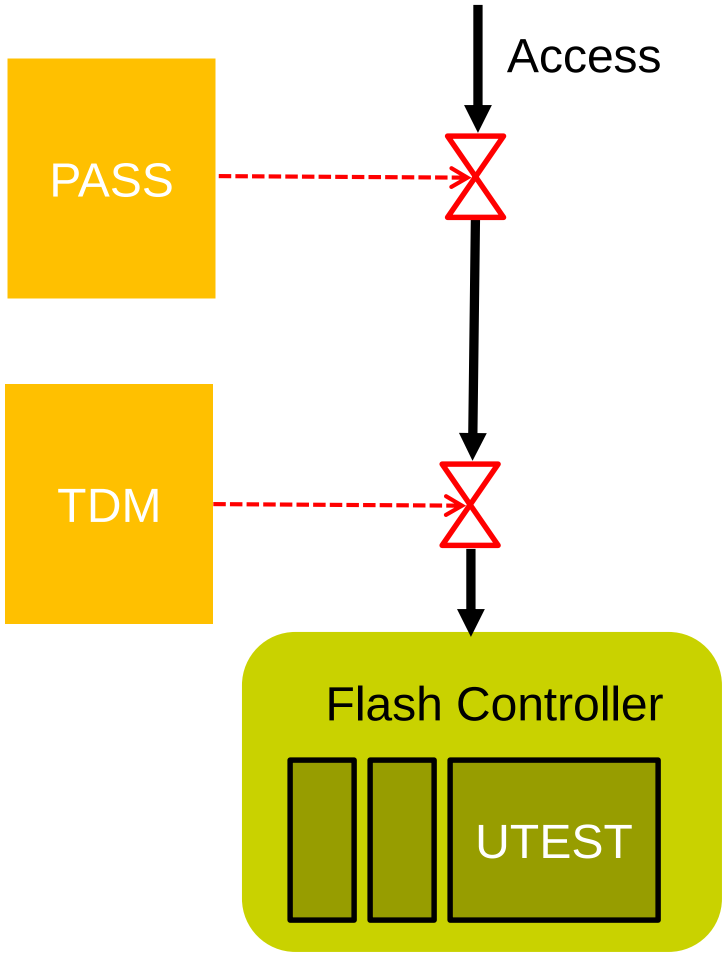
Secure Boot Flow
Boot Assist Flash (BAF)
HSM programm flow (example)
reset vector
LifeCycle == "FailureAnalyse" ?
Y
N
HSM enabled & wait ?
N
Y
wait for HSM
N
Boot_Mode == "Internal Flash"?
based on Soft DCF callback
Y
search boot header
boot header found
Y
N
disable BAF re-execution (opt.)
Y
LifeCycle == "Customer Delivery"
N
boot enabled cores
serial boot
destructive reset
start custom firmware
reset vector
calculate CMAC of first application code block
CMAC(key, code-block, block_length)
CMAC ok?
N
Y
send handshake to BAF (HSM to Host Reg)
calc. CMAC of the next block
CMAC ok?
N
Y
memory verified?
system secure
system insecure

# Flash Memory Protection

Non volatile flash memory consists of multiple blocks with different purpose and access possibilities:

- Read (location, master, lifecycle)
- Erase (location, master, lifecycle , OTP)
- Write (location, master, lifecycle, OTP)

The Password And Device Security Module (PASS) and the TamperDetectionModule (TDM) handle the access.



# PASS Overview

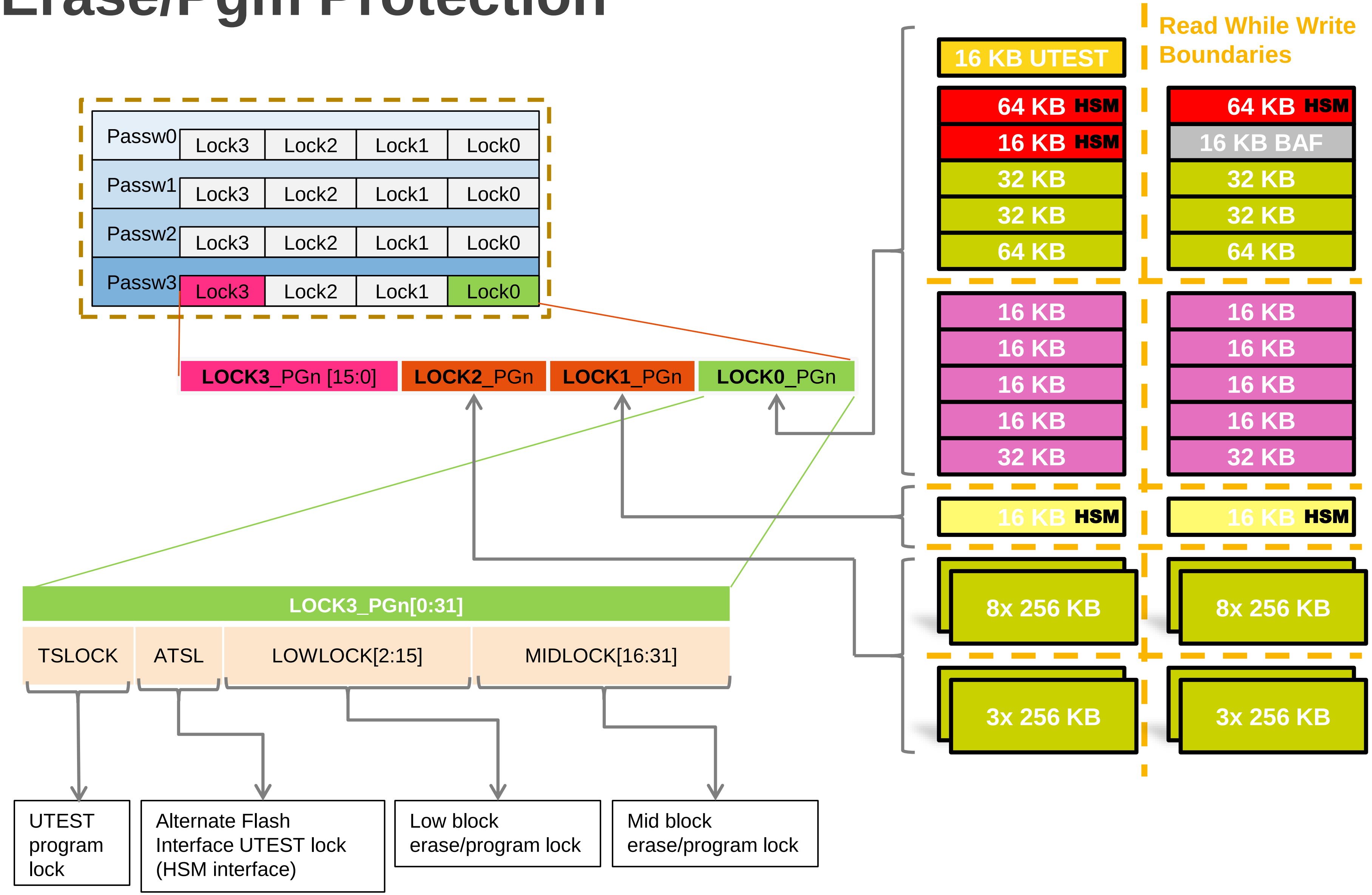
- The PASS module provide the following features:
  - Lock & JTAG passwords comparison (all 256bits long)
  - Life cycle status register

- Each Lock password correspond to a group of 4 configuration registers: Lock0/1/2/3.

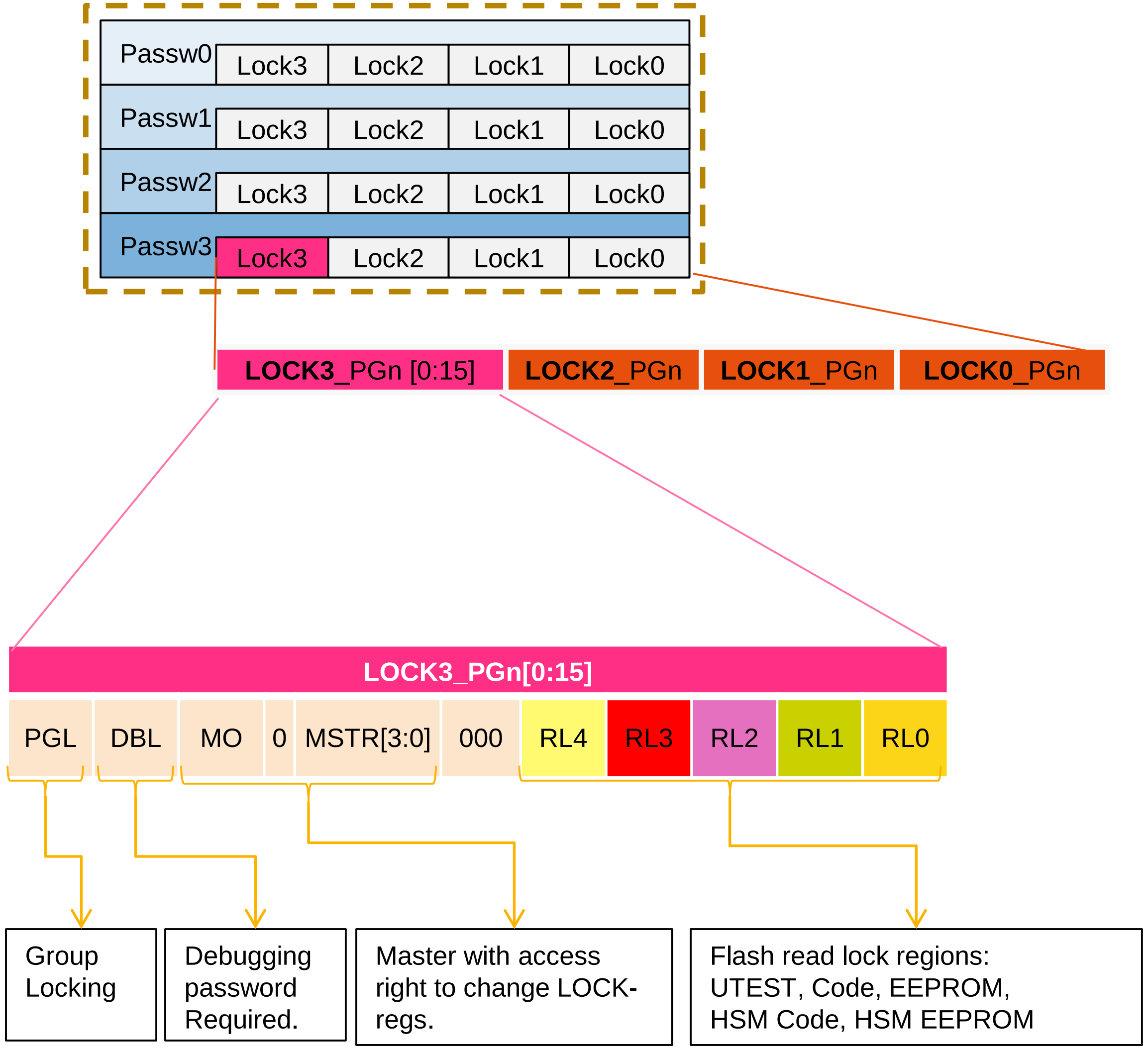
- On a successful Lock password comparison, write access is granted to the register corresponding to the password group

| | | |
|---|---|---|
| PWD0 | PWD group 0 | Lock0 |
| | | Lock1 |
| | | Lock2 |
| | | Lock3 |
| PWD1 | PWD group 1 | Lock0 |
| | | Lock1 |
| | | Lock2 |
| | | Lock3 |
| PWD2 | PWD group 2 | Lock0 |
| | | Lock1 |
| | | Lock2 |
| | | Lock3 |
| PWD3 | PWD group 3 | Lock0 |
| | | Lock1 |
| | | Lock2 |
| | | Lock3 |
| DEBUG | JTAG PWD | |

# PASS – Erase/Pgm Protection



# PASS – Read Protection



| | | | | |
|---|---|---|---|---|
| Passw0 | Lock3 | Lock2 | Lock1 | Lock0 |
| Passw1 | Lock3 | Lock2 | Lock1 | Lock0 |
| Passw2 | Lock3 | Lock2 | Lock1 | Lock0 |
| Passw3 | Lock3 | Lock2 | Lock1 | Lock0 |

| | | | |
|---|---|---|---|
| **LOCK3**_PGn [0:15] | **LOCK2**_PGn | **LOCK1**_PGn | **LOCK0**_PGn |

**LOCK3_PGn[0:15]**

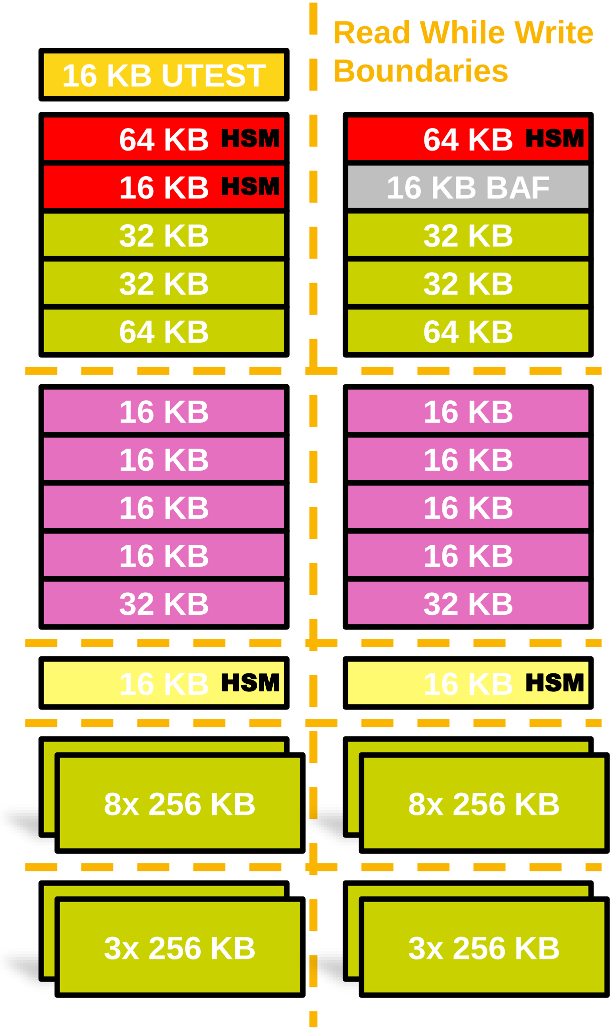
| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| PGL | DBL | MO | 0 | MSTR[3:0] | 000 | RL4 | RL3 | RL2 | RL1 | RL0 |

Group Locking

Debugging password Required.

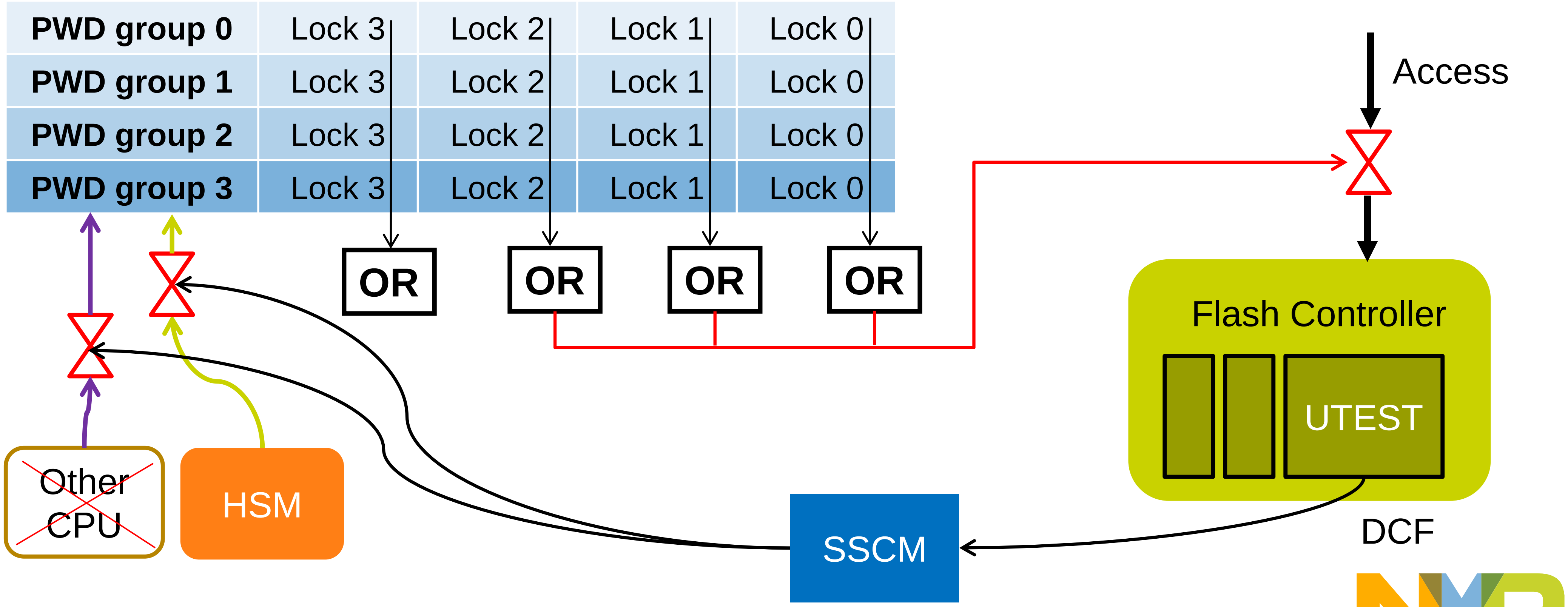
Master with access right to change LOCK-regs.

Flash read lock regions: UTEST, Code, EEPROM, HSM Code, HSM EEPROM



# PASS Lock Registers

The resulting lock status of a Flash block is determined by the logical ORing of the block lock bits in all password groups. If a block is locked in multiple groups, then all lock bits for the block need to be cleared (by writing the corresponding lock register bit) before program and erase is possible.

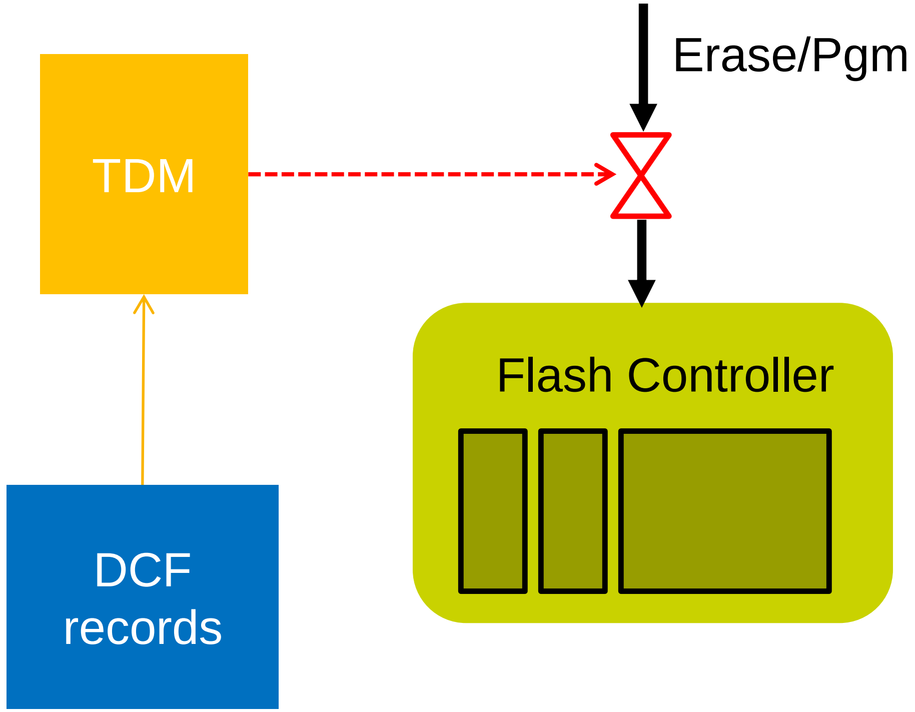


| | | | | |
|---|---|---|---|---|
| **PWD group 0** | Lock 3 | Lock 2 | Lock 1 | Lock 0 |
| **PWD group 1** | Lock 3 | Lock 2 | Lock 1 | Lock 0 |
| **PWD group 2** | Lock 3 | Lock 2 | Lock 1 | Lock 0 |
| **PWD group 3** | Lock 3 | Lock 2 | Lock 1 | Lock 0 |

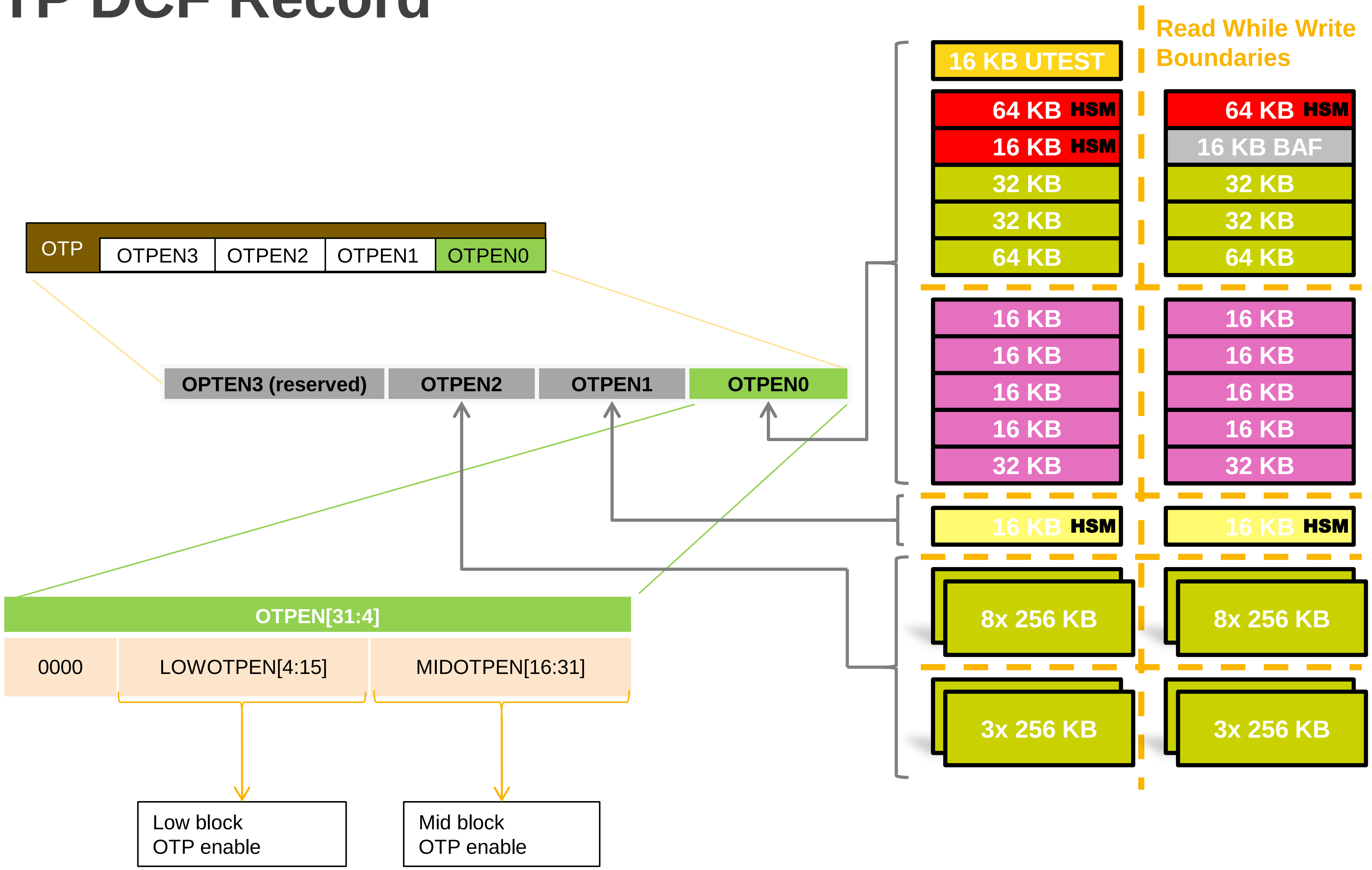
# TDM - One Time Programable

## One Time Programable (OTP) definition:

- A Flash block assigned as OTP cannot be erased.
- Programming can only be done on an erased location.
- Overprogramming is not possible.



# TDM – OTP DCF Record

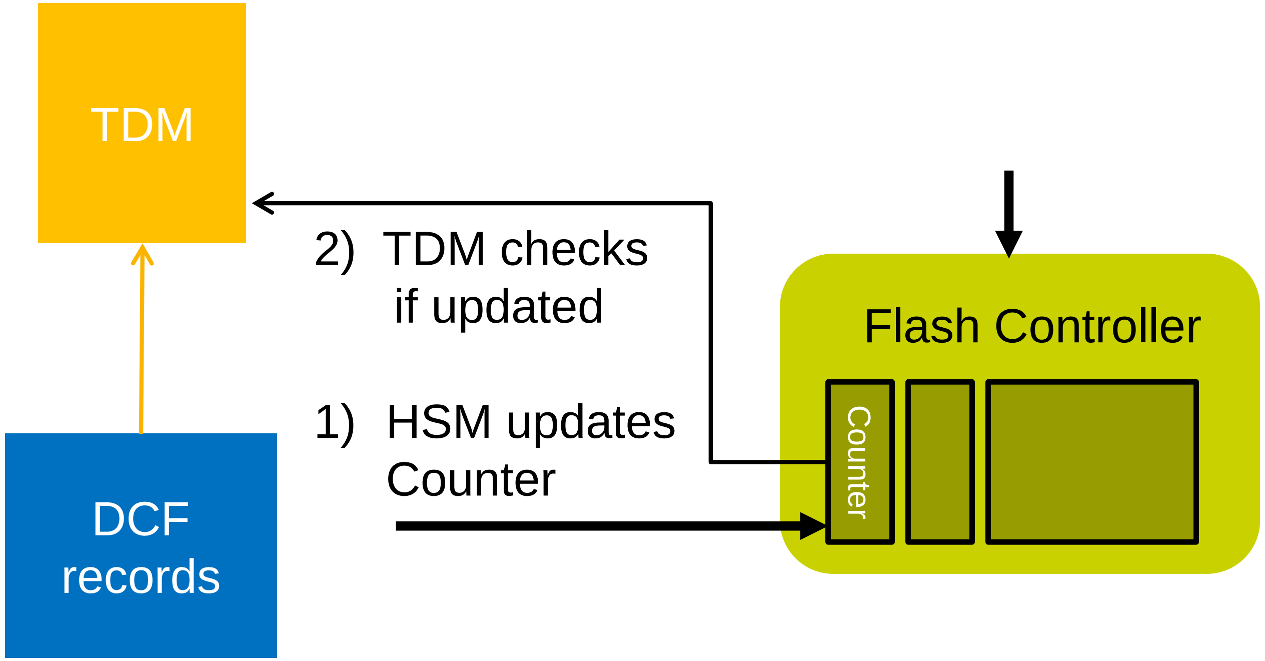


# TDM – Diary

Erase cycles are permanently recorded in the diary. OEM can compare erase cycles between OEM database and ECU and as such detect tamper events.

Every erase event requires a diary update before actual execution. Maximum 6 diary regions are defined by DCF records.

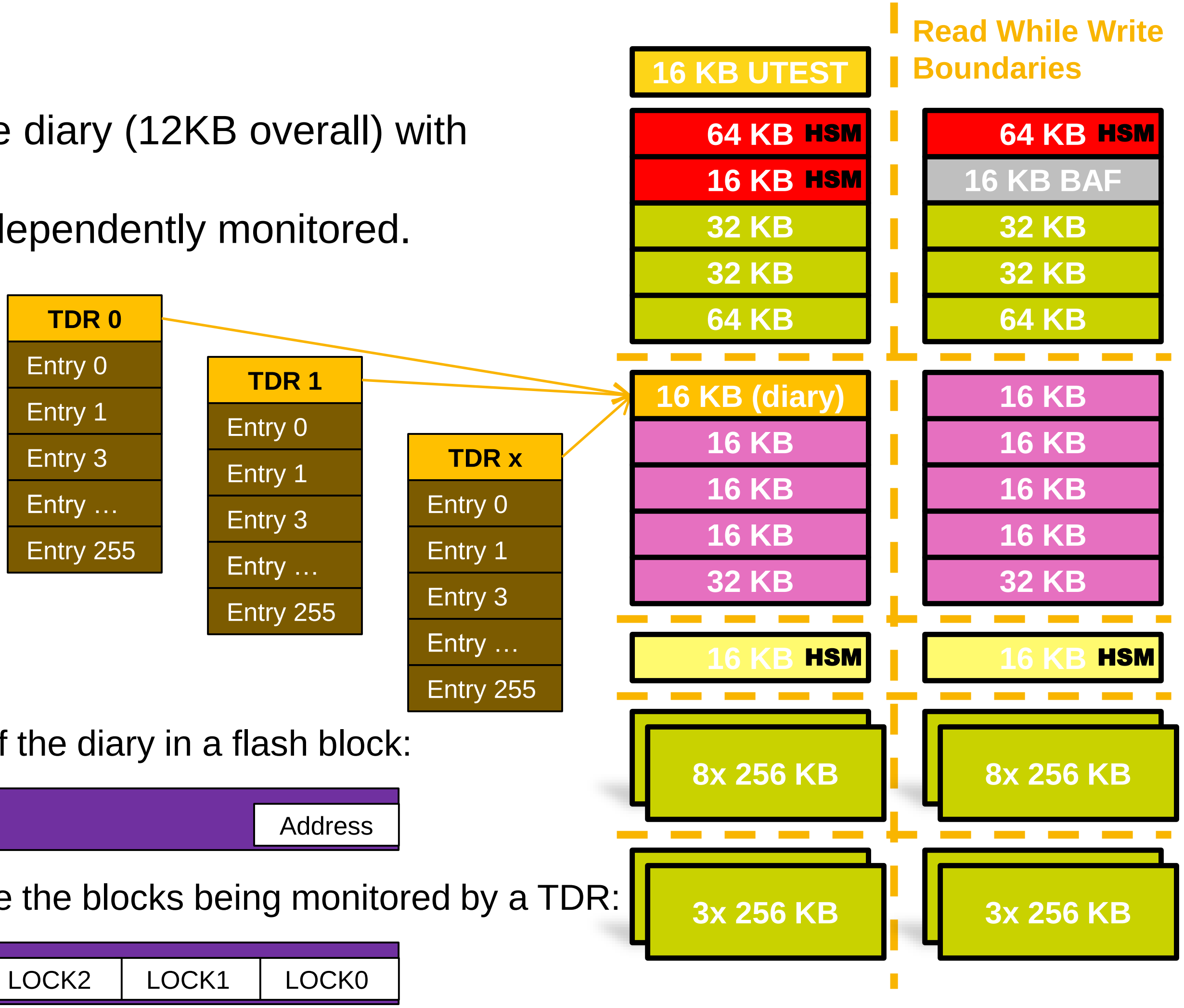
Before a flash block assigned to a diary region can be erased an update to the diary has to be made which is supervised by the TDM.



# TDM – Diary Configuration

There are 6 tamper detect regions (TDR) in the diary (12KB overall) with each having 256 x 8 bytes (2KB).
For every region specific flash blocks can be independently monitored.

One entry in a TDR (for example a counter) is 8 bytes long and can hold any data.



## Set of DCF Records:

Start address(aligned on 4KB) of the diary in a flash block:

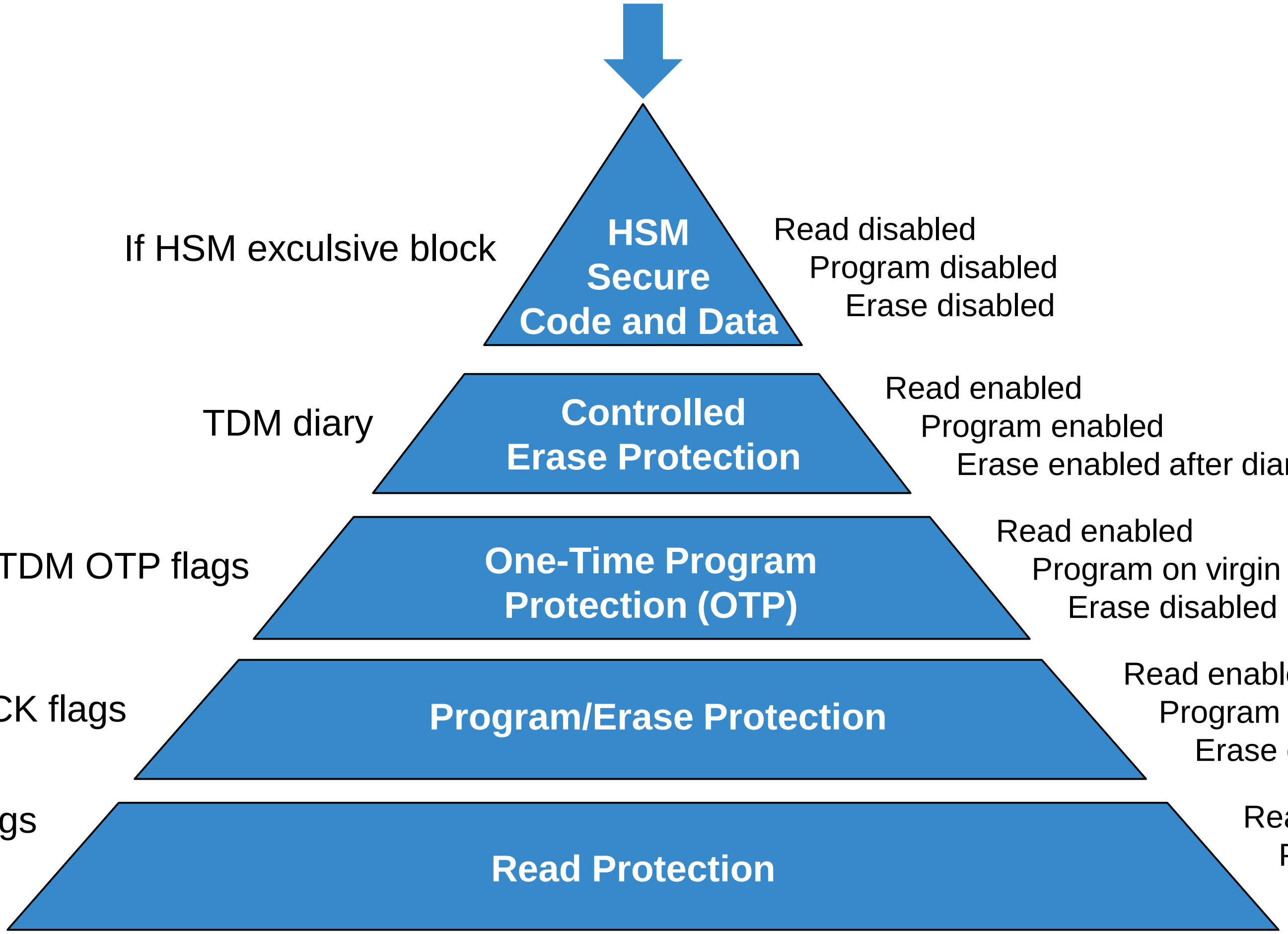
| DCF_TDR_DIARY_BASE | Address |
|---|---|

4 DCF records per TDR to define the blocks being monitored by a TDR:

| DCF_TDR_LOCKx | LOCK3 | LOCK2 | LOCK1 | LOCK0 |
|---|---|---|---|---|

# Flash Memory Protection Levels

**Flash access request from debugger or core**



If HSM exculsive block

**HSM 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

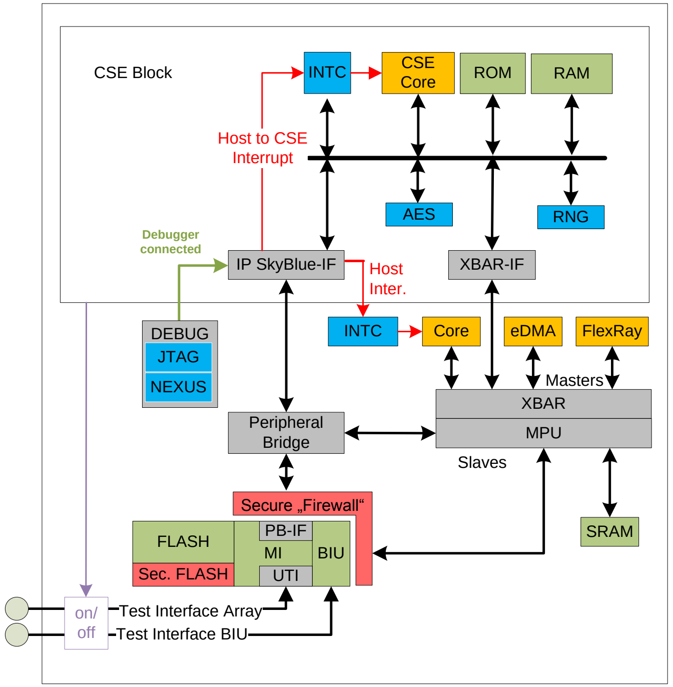
**Read Protection**

Read disabled
Program disabled
Erase disabled

# Cryptographic Services Engine (CSE)

## e.g. MPC564xB/C

- CSE module implements the official HIS SHE-Specification
- 32-bit secure core working at 120 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



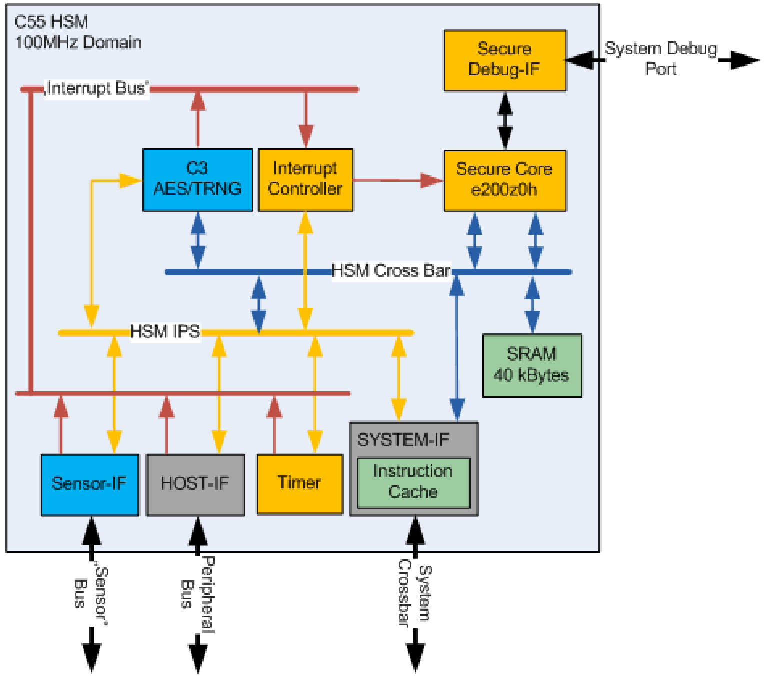
# Hardware Security Module (HSM)

## v1: MPC5746M / MPC5777M & v2: MPC5748G / MPC5746C

**HSM is free programmable by the customer, additional security algorithm could implemented in software**

**Features:**

- e200z0h core (v1: 100MHz / v2: 80 MHz)
- 4Kbytes Instruction cache
- Secure Debugger Interface
- Cryptographic Modules with AES-128, Random Number Generator, DMA
- Sensor Interface – monitor for voltage, temperature and clock (v1)
- Memory
  - SRAM (v1: 40 Kbytes / v2: 32 Kbytes)
  - Flash
    code: 2 x 64 Kbytes + 1 x 16KBytes
    data : 2 x 16 Kbytes



juergen.frank@freescale.com

# SHE Firmware

- Release 1.0 is available for MPC574xG (3M & 6M)
- Firmware implements the CSE2 feature set
  (SHE firmware + Global-B requirements) on the HSM
- Firmware „emulates“ the CSE register interface, to simplify porting of existing SW stacks (e.g. Elektrobit)
- Firmware is delivered pre-programed in the device
  - No SHE firmware programming and DCF configuration required by customer

# Security SDK Feature Set

- HSM startup code
- Configurable user interface, which helps application access security features implemented in HSM from HOST Application cores
- Services to expose HSM platform feature for Application development like Cache & Interrupt Controller APIs, SMPU Configuration APIs, CMU APIs, Timer APIs (Watch dog & PIT), Host Register Interface APIs, Flash Programming interfaces
- Support functions to manage secure key area
- True & Pseudo Random number generator handling
- Debugger Activation protocol support
- FSL Crypto Library
  - Symmetric cryptography support.
    - AES-128 Encryption & Decryption
    - Confidentiality mode: ECB, CBC, CFB, OFB,CTR, XTS
    - Authentication modes: AES-128 based CMAC
    - Confidentiality + Authentication modes: GCM
  - Asymmetric Cryptography support:
    - RSA, ECC based encryption & Decryption
  - Hashing Algorithm : SHA2/SHA3
- The SDK is intended to be ported to next HSM generation

# Attack and Protection Schemes - Summary

| Attacker Method | Protection Scheme | NXP Solutions |
|---|---|---|
| Flash Modification | • Secure Boot (e.g. like SHE)<br>• Protect FLASH blocks against modifications | • CSE & HSM offers full secure boot support<br>• PASS module implements password-based read/write protection<br>• TDM provides a mechanism for configuring individual flash memory blocks as One Time Programmable (OTP) |
| Read FLASH content | • Disable the debugger interface<br>• FLASH Read Protection<br>• Read crypto keys | • Censorship / Life-Cycle offers a debug disable feature (with/without password)<br>• PASS module implements password-based read protection<br>• CSE & HSM offers a secure key storage<br>• CSE & HSM can en-/decrypt firmware/data |
| Car network without access | • Encryption for information hiding<br>• Signatures for message authentication | • CSE & HSM offers via AES-128 a standard algorithm with CMAC support |
| Replay attacks on car networks | • Usage of challenge-response process | • CSE & HSM offers a TRNG/PRNG system to generate a random number (challenge) |
| Replacing an ECU with a another one | • Usage of secure communication and unique ECU Ids (UID) | • CSE & HSM devices offers a UID programmed by Freescale |
| Physical attacks via out-off-spec execution | • Monitors for voltage / temperature / frequency<br>• Glitch-Resistent design | • Devices has sensor for several environ conditions<br>• Device configuration modules are reviewed and hardened against glitch attacks |
| Side channel attacks | • Increase the overall power-noise | • On c55 devices customer can configure random noise during secure boot and encryption |

# Summary

- NXP overs since years innovative automotive security solutions
- Crypto modules alone didn’t support all customer use-cases
- NXP offers security solutions for all 32bit-MCU segments

| NXP Security Solution for Automotive MCU | | | |
|---|---|---|---|
| | Device | Platform | Module |
| MCU ( internal flash) | MPC564xB/C | PowerPC e200 | CSE |
| | MPC5746M / MPC5777M | | HSMv1 |
| | MPC5748G / MPC5746C | | HSMv2 |
| | MPC5777C | | CSE2 |
| | Radar MCU | | CSE2 |
| | MAC57D54H | ARM Cortex-A5/M4 | CSE2 |
| MPU (flash-less) | S32V243 | ARM Cortex-Ax/Mx & ARM9/11 | CSE3 / OTFAD/ TrustZone |
| | VFxxx | | Trust Zone + CAAM |
| | i.Mx | | |

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

# ATTRIBUTION STATEMENT