

M2351 Security Architecture

TrustZone® Technology for Armv8-M Architecture

Outline

NuMicro® M2351 Security Architecture



TrustZone® for Armv8-M

Processor Core, Interrupt Handling, Memory Partitioning, State Transitions.



TrustZone Implementation on M2351

IDAU / SAU, Secure Configuration Unit (SCU), Security Configurations.



M2351 Security functions

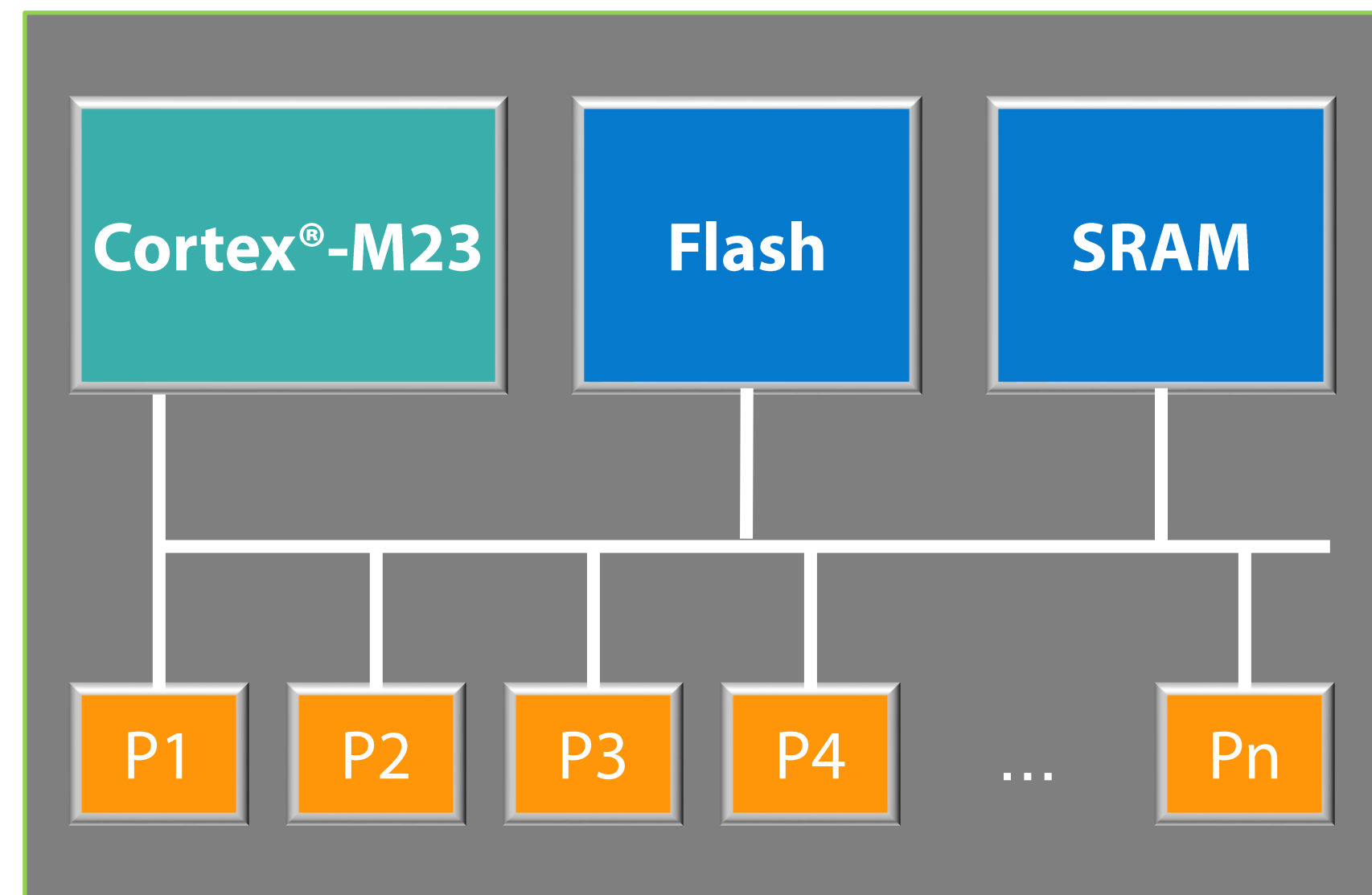
Crypto Accelerator, Secure bootloader, KPROM, XOM, Flash Lock, Secure Debug and Tamper Detector.

TrustZone[®] for Arm[®]v8-M

*Processor Core, Interrupt Handling, Memory Partitioning,
State Transitions.*

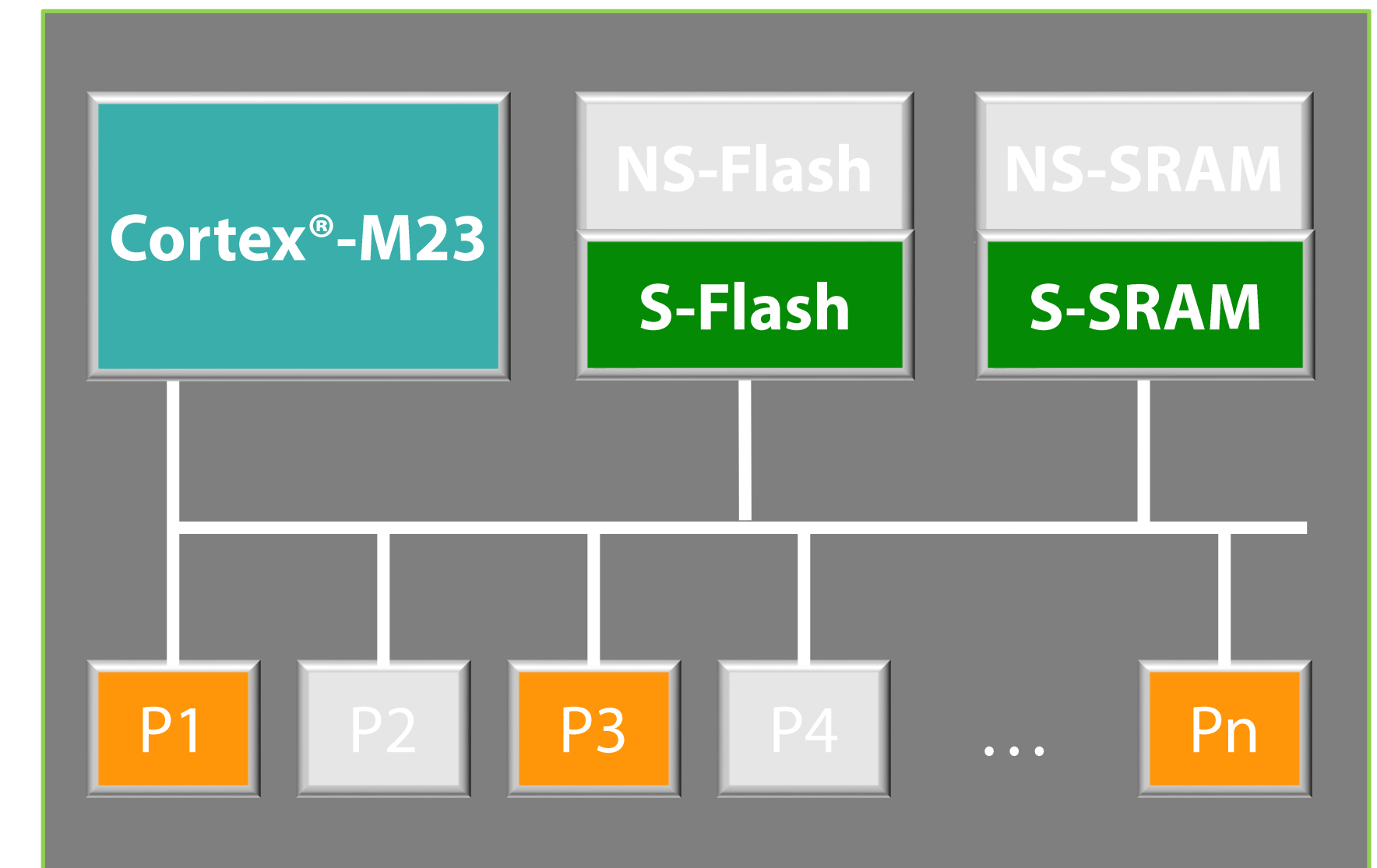
- The memory and peripherals can be grouped into **Secure World** and **Non-secure World** according to the **memory address**.
- The processor supports Secure and Non-Secure operating states.

Microcontroller

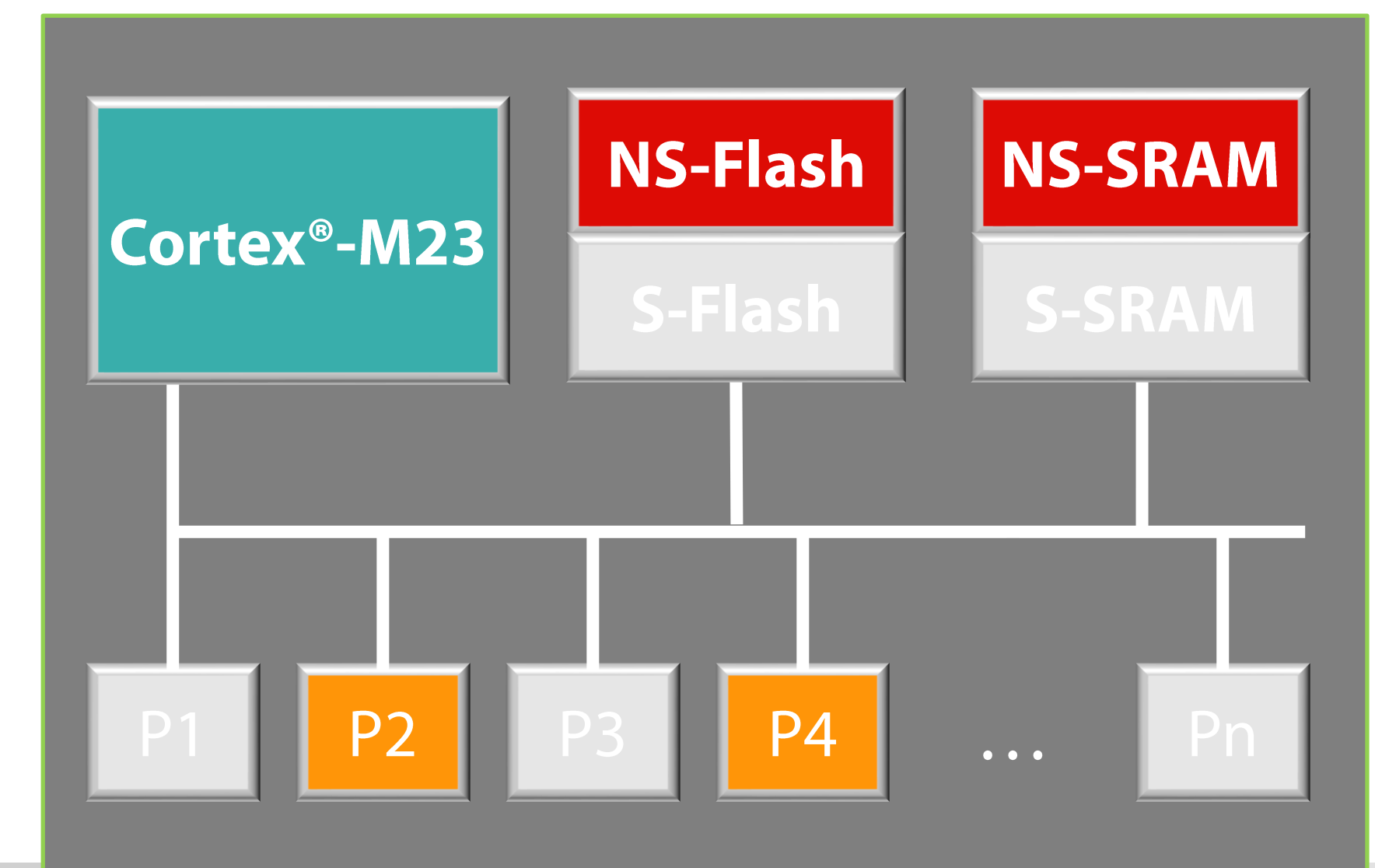


TrustZone !

Secure World



Non-secure World



TrustZone®
for
Armv8-M

Processor
Core

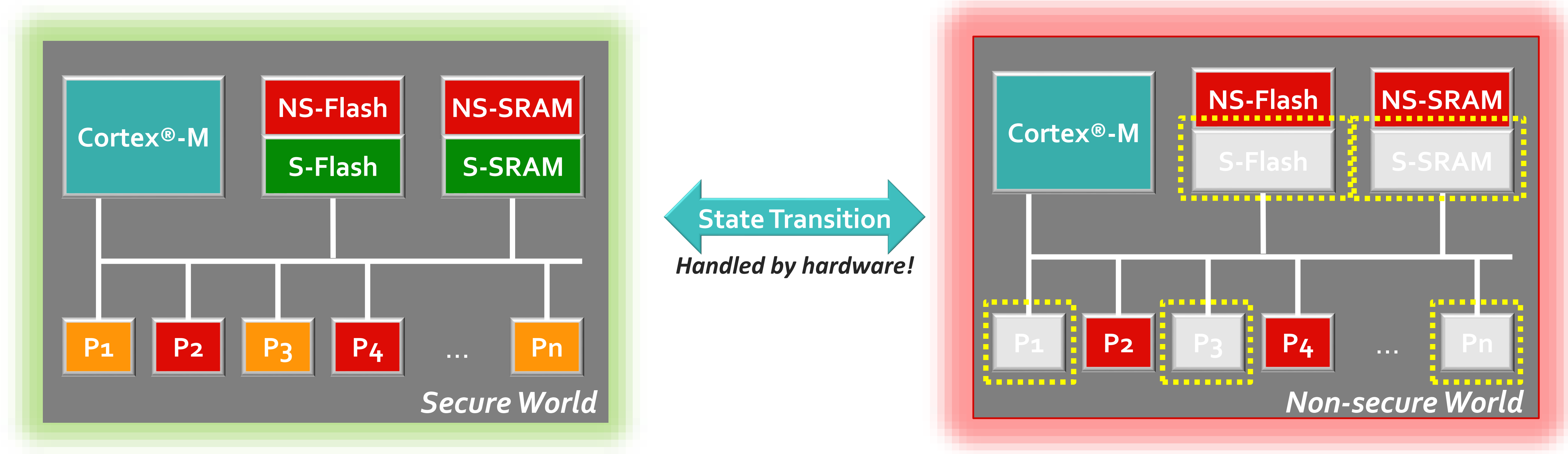
Interrupt
Handling

Memory
Partitioning

State
Transitions

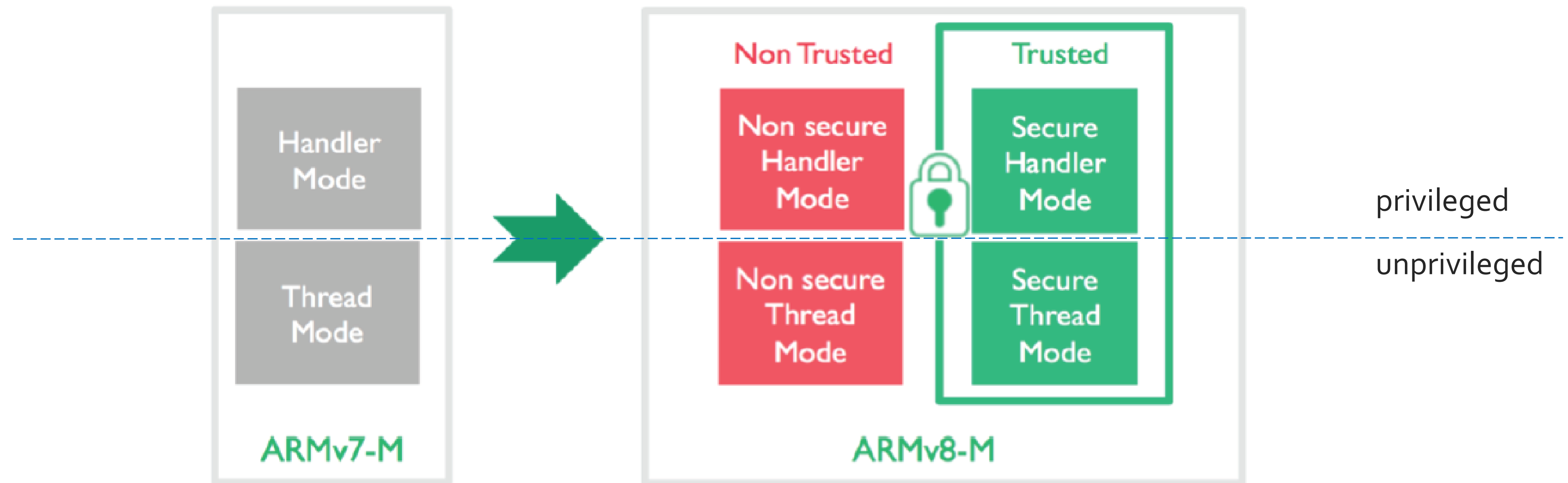
TrustZone® for ARMv8-M

- **Secure code** and **Non-secure code** can run on the same microcontroller
 - **Secure world** is an **isolated execution environment** protected by hardware.
 - State transition is handled by hardware!



Processor Core

- **Processor states**
 - **Secure** and **Non-secure** states that are orthogonal to the existing Thread and Handler modes



Source: "Introducing ARM Cortex-M23 and Cortex-M33 Processors with TrustZone for ARMv8-M"

• Separate hardware resources for **secure** and **non-secure** states

- SysTick timer
- MPU configuration registers

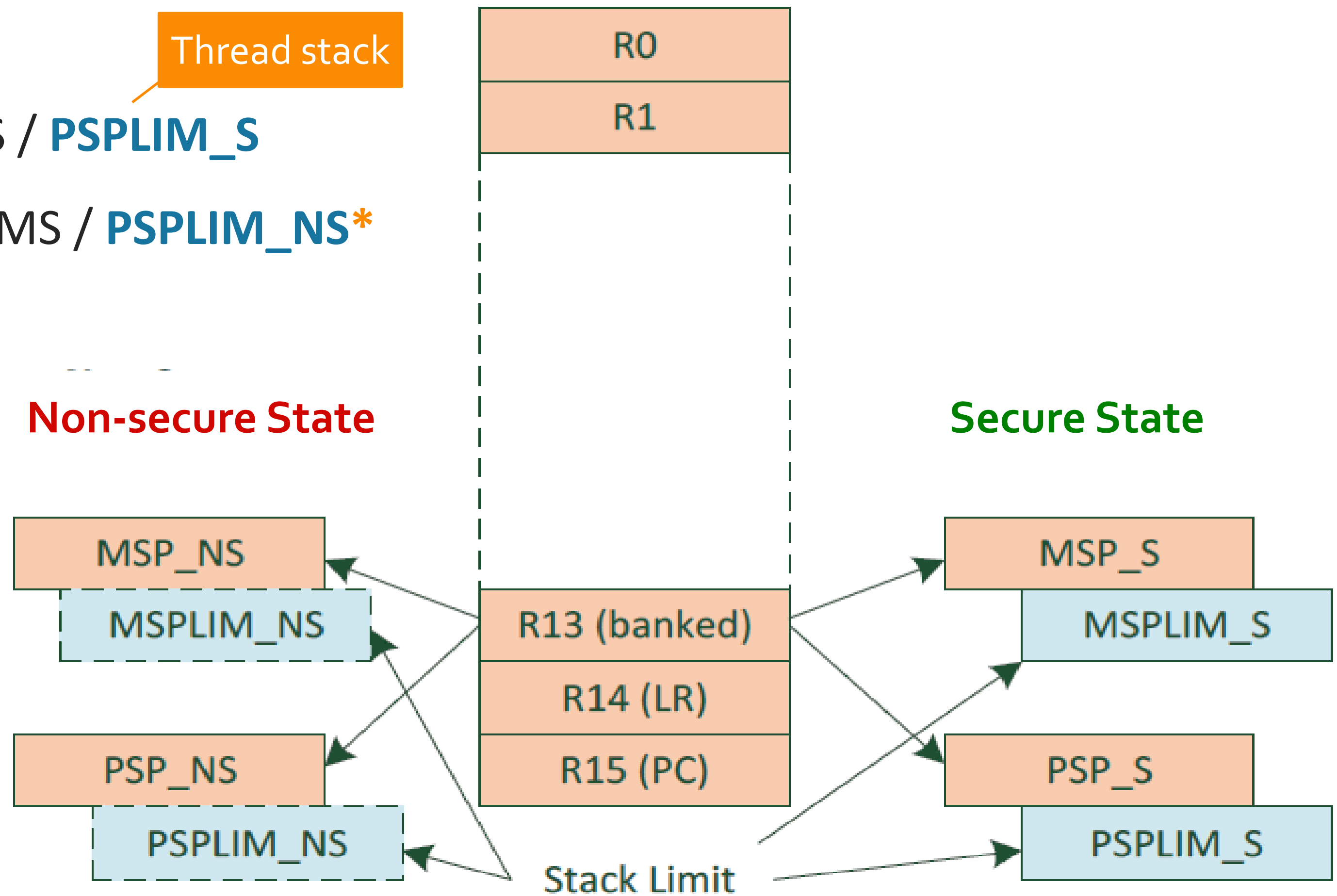
- Stack register (R13)

Main stack

Thread stack

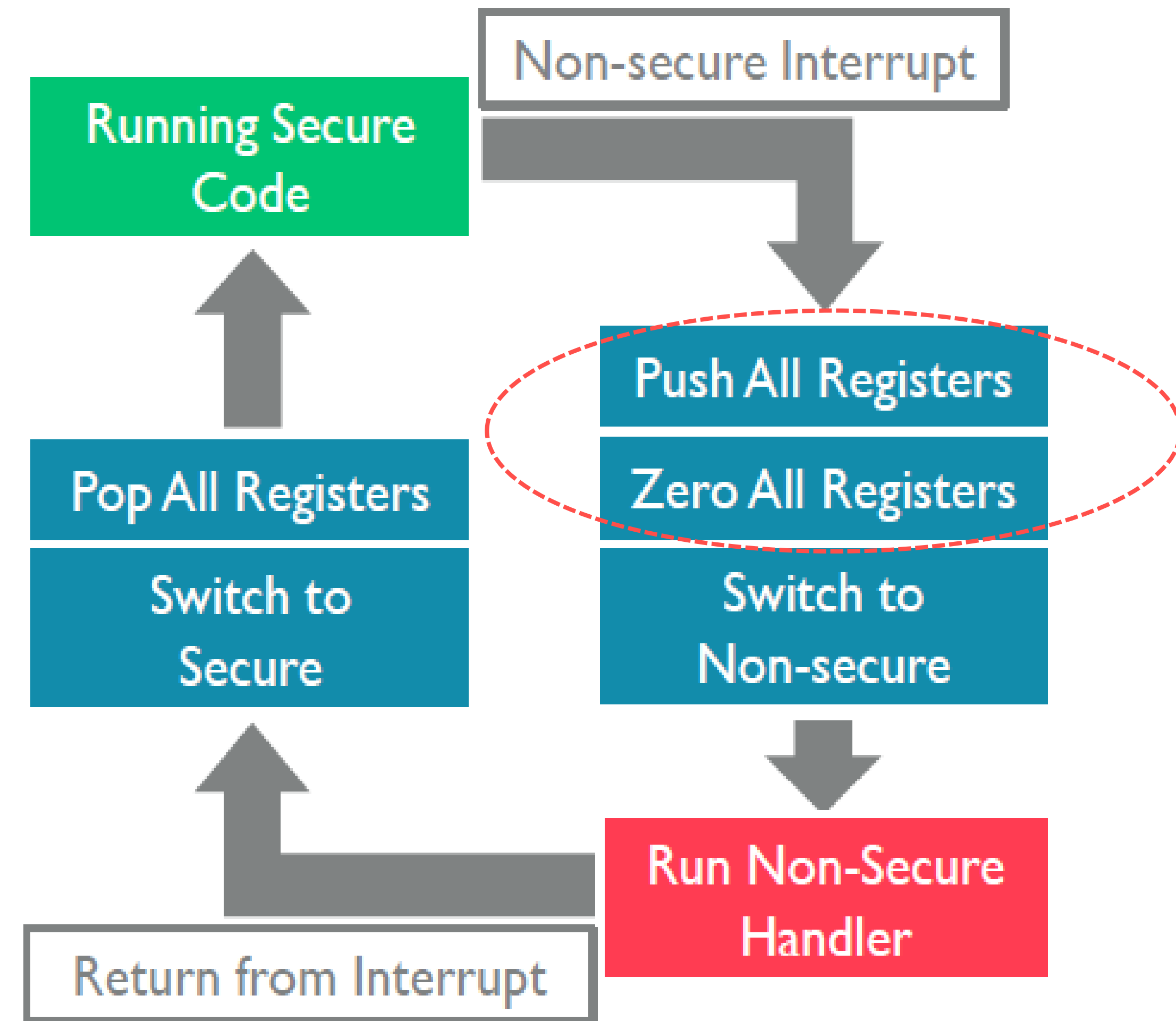
- MSP_S / **MSPLIM_S**, PSP_S / **PSPLIM_S**
- MSP_NS / **MSPLIM_NS***, PSP_MS / **PSPLIM_NS***

(* is not supported in Cortex®-M23)



Interrupt Handling

- Interrupt management mechanism is similar to ARMv7-M.
- Support separated exception vector tables for the **Secure** and **Non-Secure** exceptions
 - Can share the same priority level, or can force non-secure interrupts to use lower half priority range.

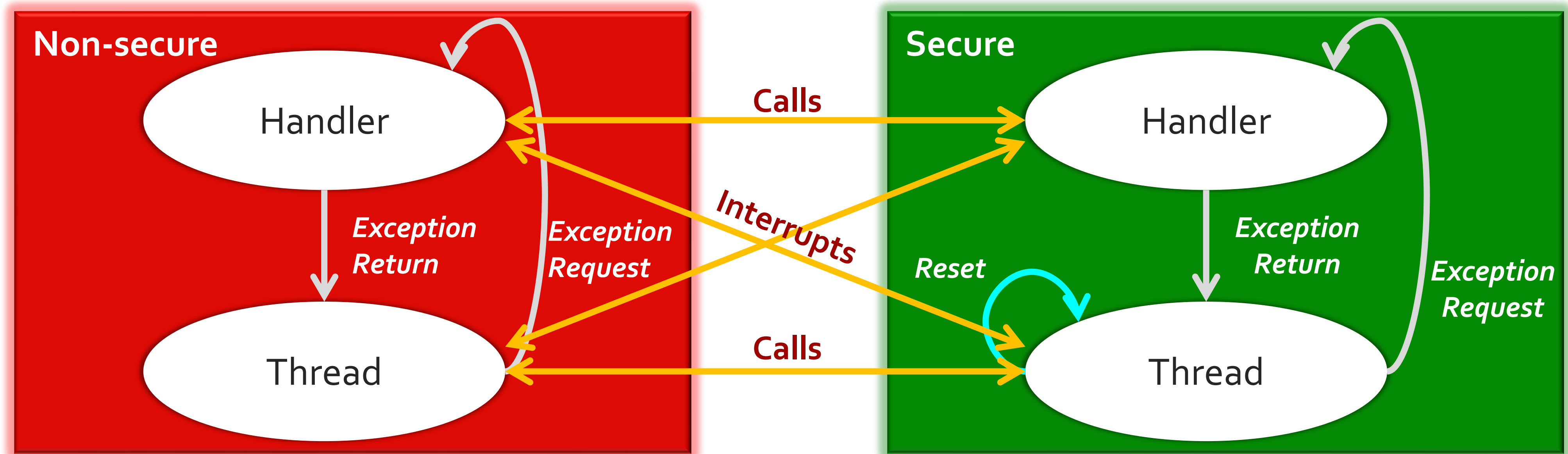


Memory Partitioning

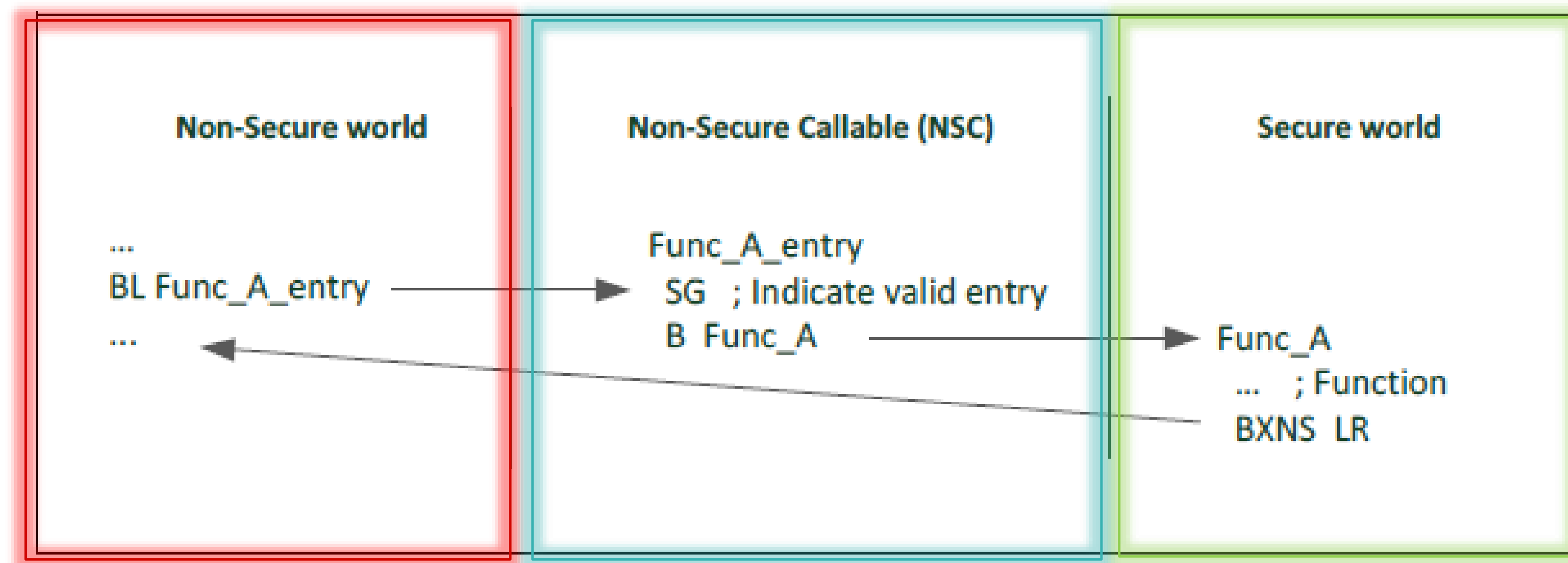
- The 4GB memory space is partitioned into **Secure (S)** and **Non-secure (NS)** memory regions
 - Only **secure code** can access **secure memory** and **peripherals**.
 - Support optional secure MPU and non-secure MPU
- **Non-Secure Callable (NSC)**
 - This secure memory area contains valid entry points for secure APIs
 - First instruction in API must be **SG** (Secure Gateway)

State Transitions

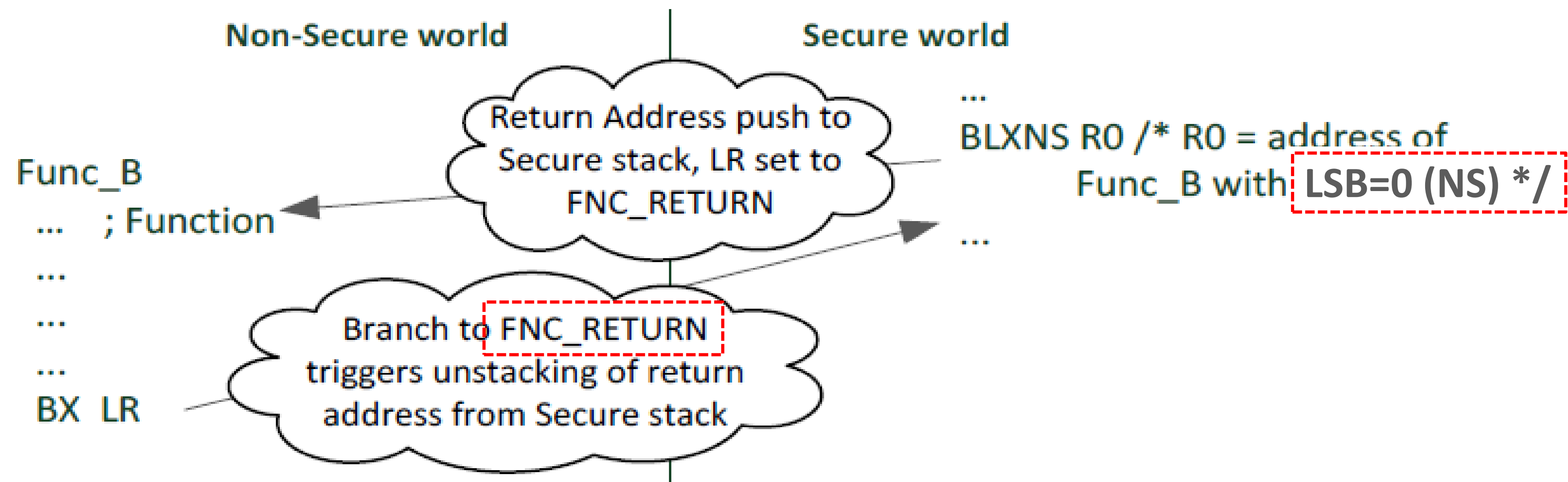
- The processor's secure state is determined by the program address
 - Instructions from secure memory executed in the secure state
 - Boot into secure state
 - Direct function calls between states
 - Interrupts directly taken to target state



- **Non-secure code to secure function**
 - **Non-secure code** can call a function in secure memory where
 - The entry point is in a **NSC** region
 - The first instruction is **Secure Gateway (SG)**
 - The LSB of **R14** will be cleared to 0



- **Secure code to non-secure function**
 - **Secure code** can call a function in **non-secure memory** by using **BLXNS** instruction
 - Return address and part of the PSR is pushed to the current Secure stack
 - **FUN_RETURN** is assigned to Link register (R14)





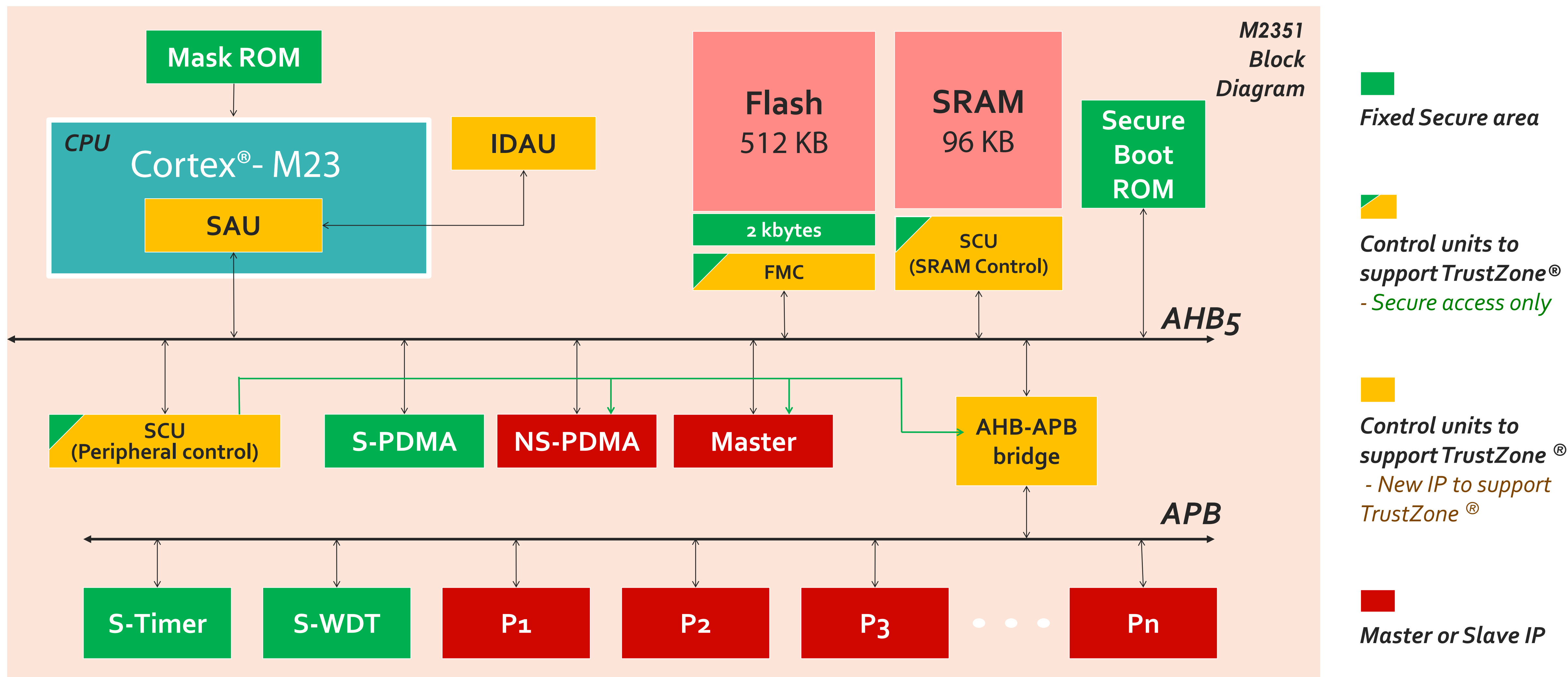
TrustZone[®] Implementation on M2351

*IDAU / SAU, Secure Configuration Unit (SCU), Security
Configurations.*

TrustZone® Implementation on M2351

*IDAU / SAU, Secure Configuration Unit (SCU), Security
Configurations.*

- Arm® Cortex®-M23 core @ 64MHz, 512KB/ 96KB Flash and SRAM.
- Support TrustZone® for Armv8-M.



TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

Security
Configurations

Security
Configuration
of Flash

Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral

Implementation

Defined

Attribution

Unit

IDA U

Non-programmable, defines
static address partitioning

• Implementation Defined Attribution Unit

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

Security
Configurations

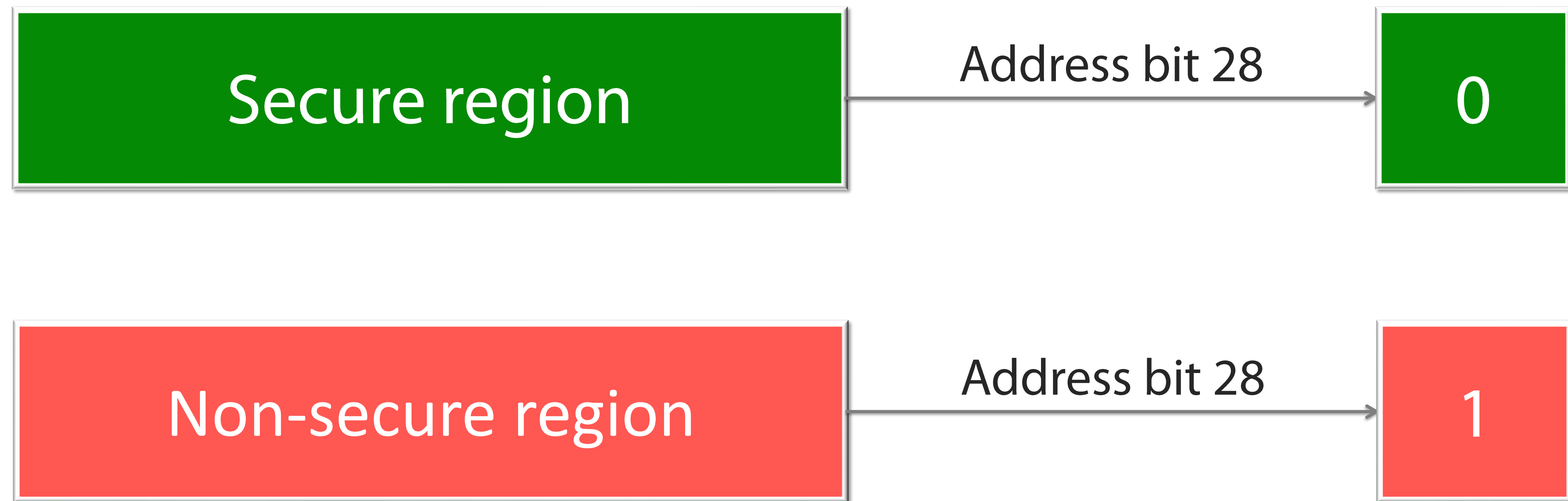
Security
Configuration
of Flash

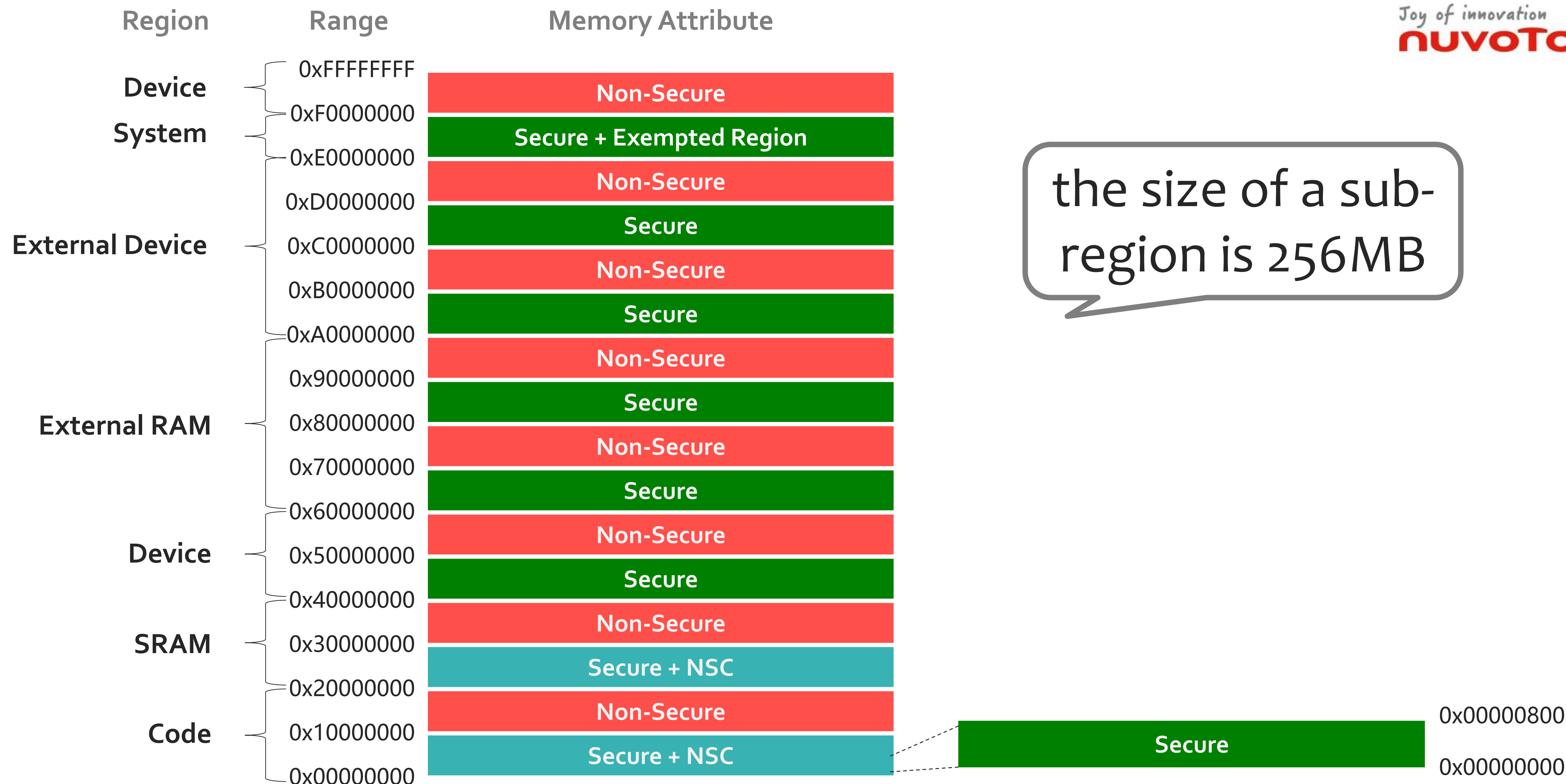
Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral

- **Address Bit 28** is used to partition **secure** and **non-secure** memory region.





Default Address Map

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

Security
Configurations

Security
Configuration
of Flash

Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral

Security Attribution Unit

SAU

Programmable,
provides dynamic
address partitioning.

• Security Attribution Unit

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

Security
Configurations

Security
Configuration
of Flash

Security
Configuration
Unit

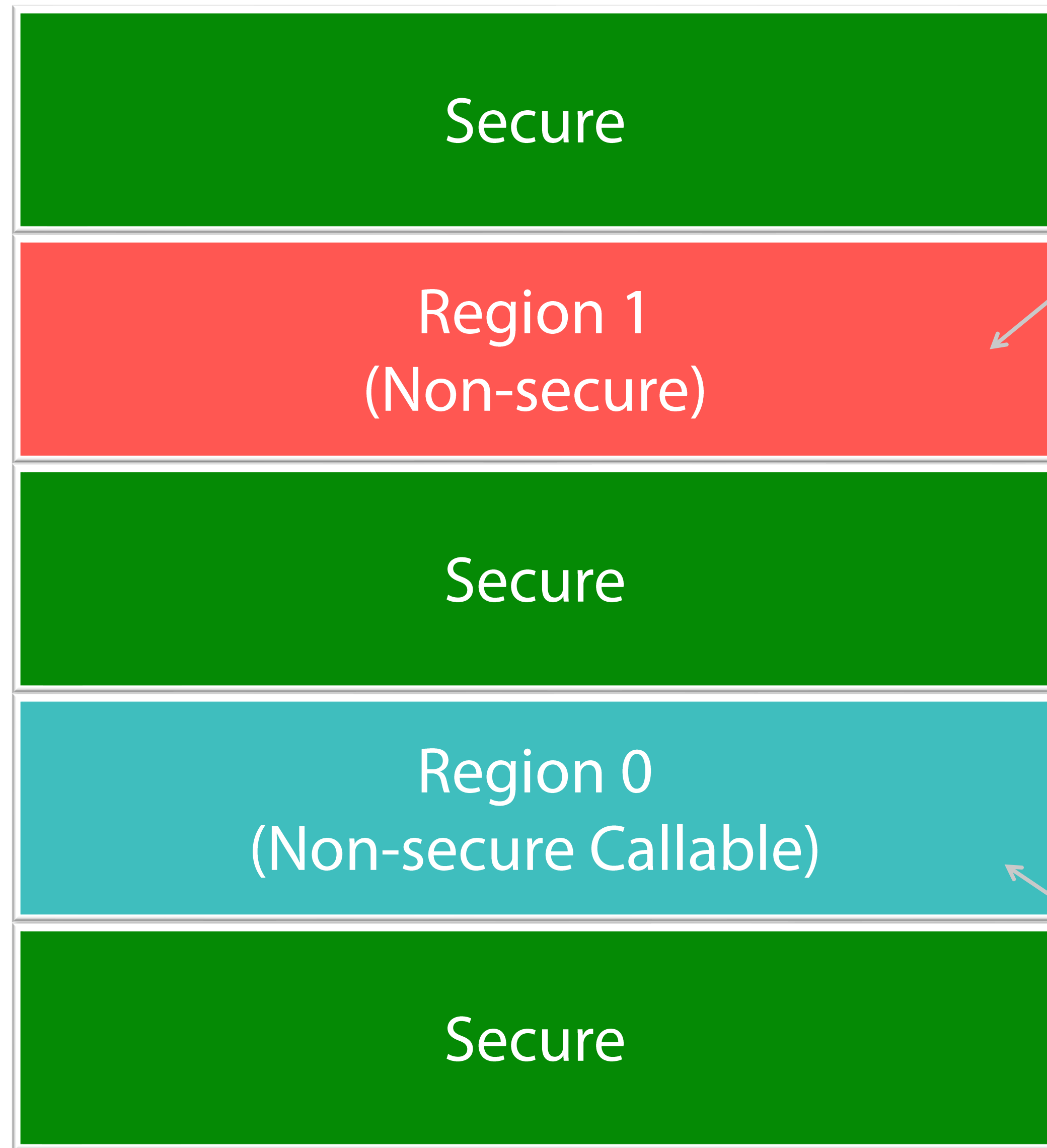
Security
Configuration
of SRAM

Security
Configuration
of Peripheral

- Up to 8 memory regions can be defined by programming its control registers.

Address	Register	
0xE00EDD0	SAU_CTRL	Control Register
0xE00EDD4	SAU_TYPE	Number of SAU region (read only)
0xE00EDD8	SAU_RNR	Region Number Register
0xE00EDDC	SAU_RBAR	Region Base Address Register
0xE00EDE0	SAU_RLAR	Region Limit Address Register

**used to
define
a SAU region.**



#1 SAU_RLAR.NSC = 0

A memory region defined by SAU is either **Non-secure** or **Non-secure Callable**.

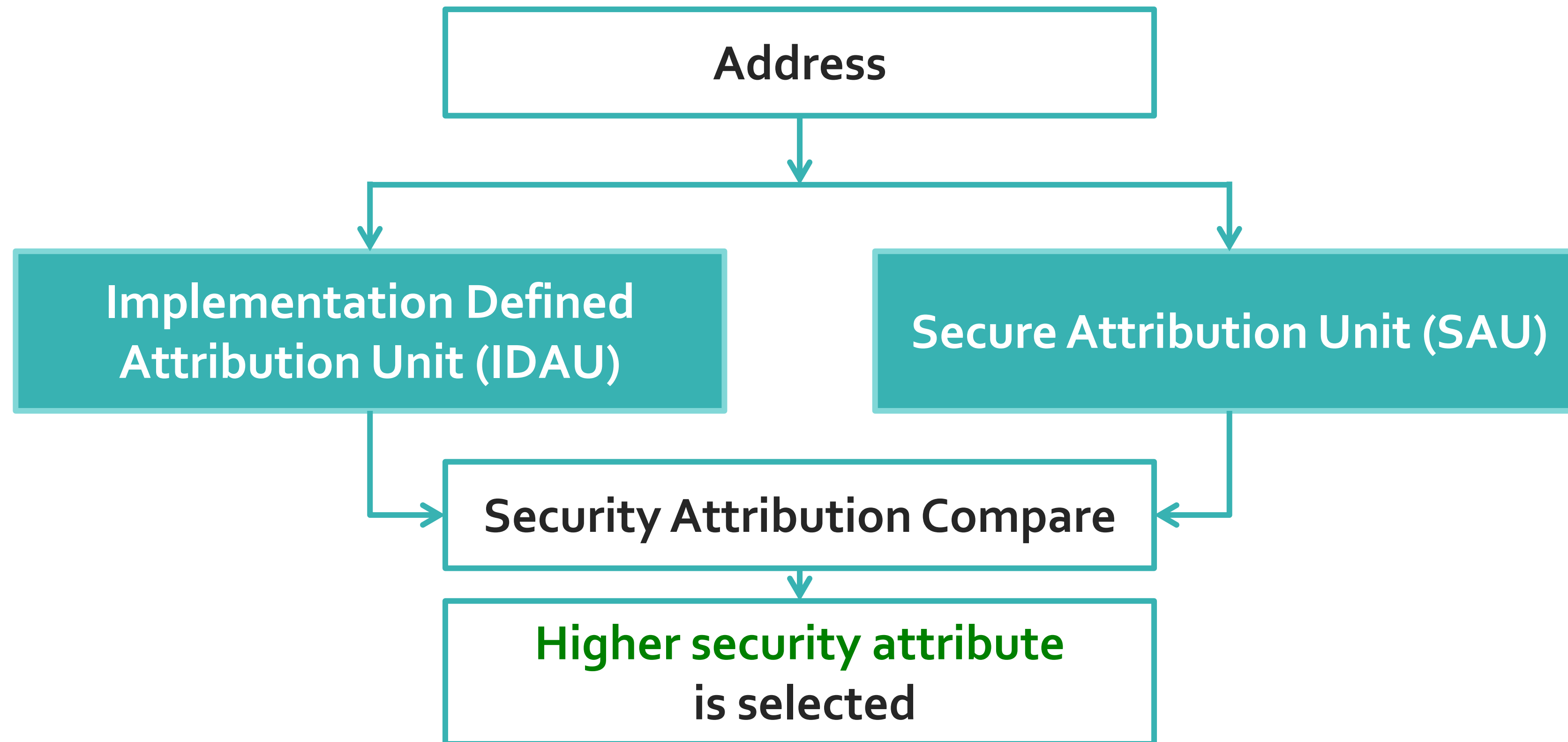
#0 SAU_RLAR.NSC = 1

IDA U

V.S.

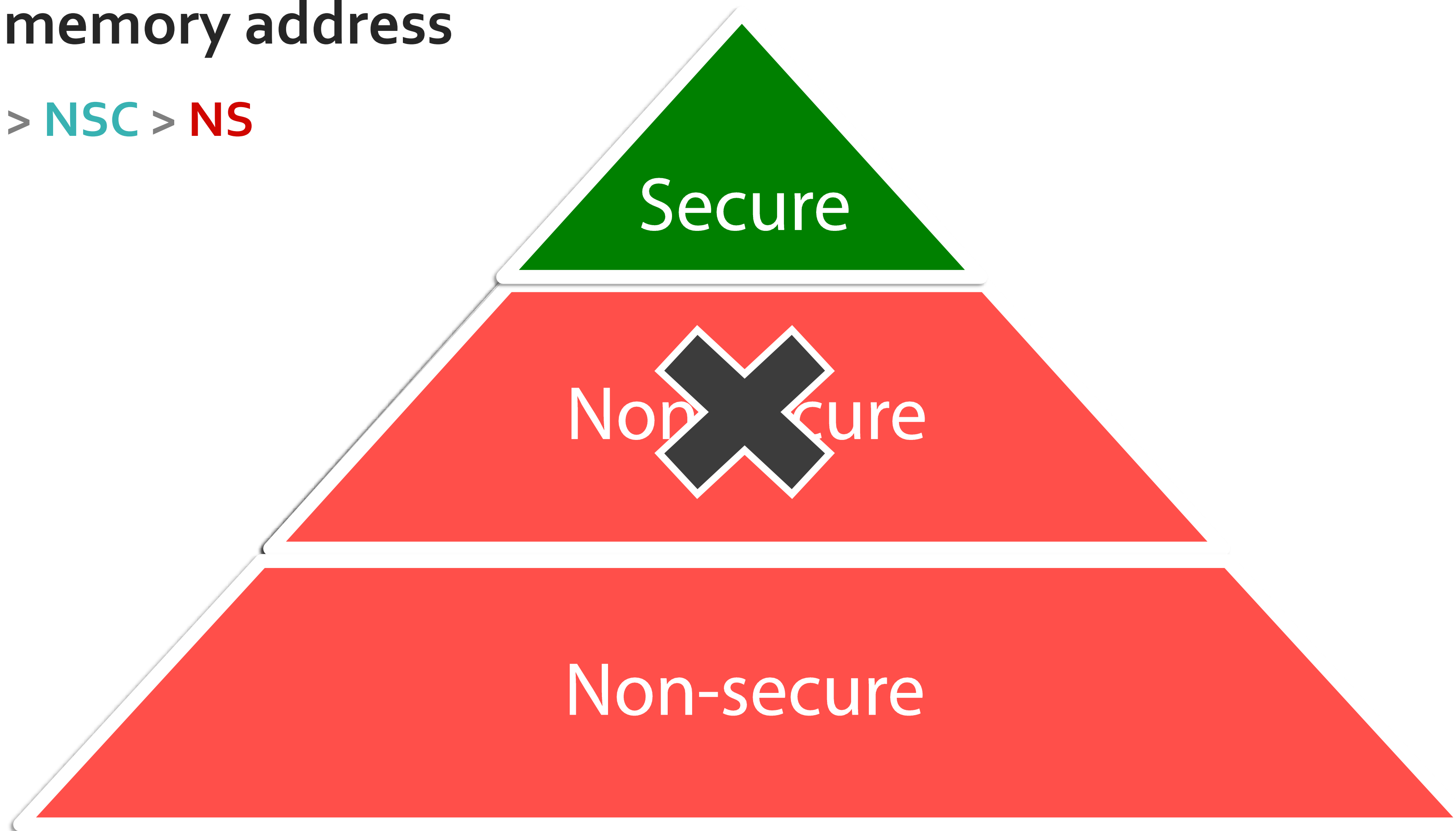
SAU

- The address space partitioning is completed by IDAU and SAU together
- Compare IDAU and SAU definition, **higher security attribute** is selected for a memory address
 - **S** > **NSC** > **NS**



- The address space partitioning is completed by IDAU and SAU together
- Compare IDAU and SAU definition, **higher security attribute** is selected for a memory address

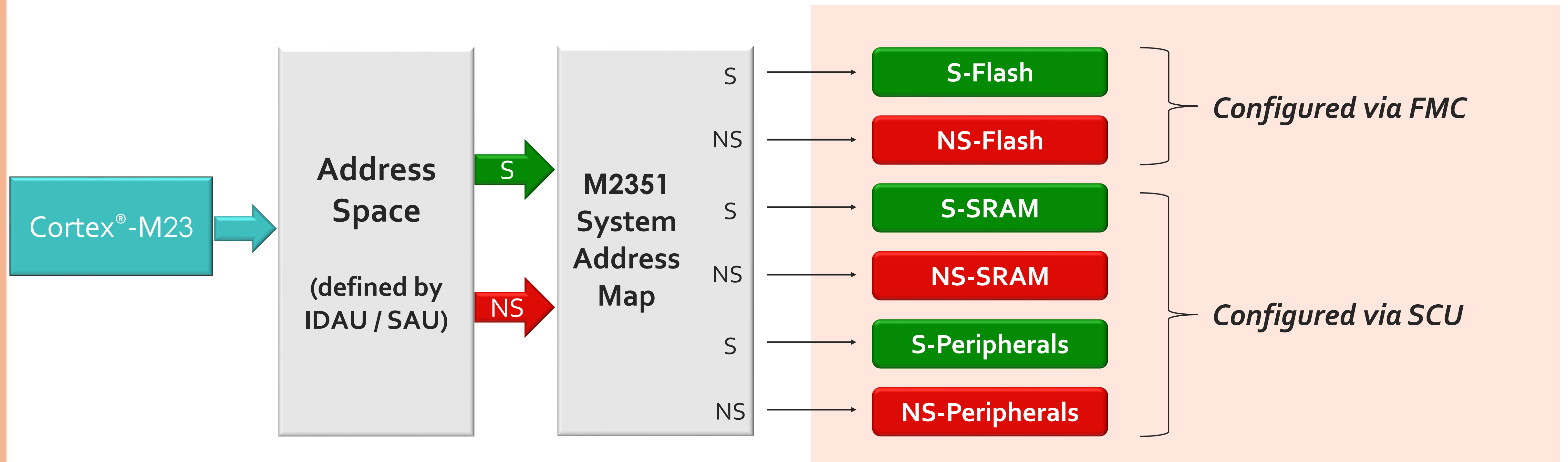
- **S** > NSC > NS



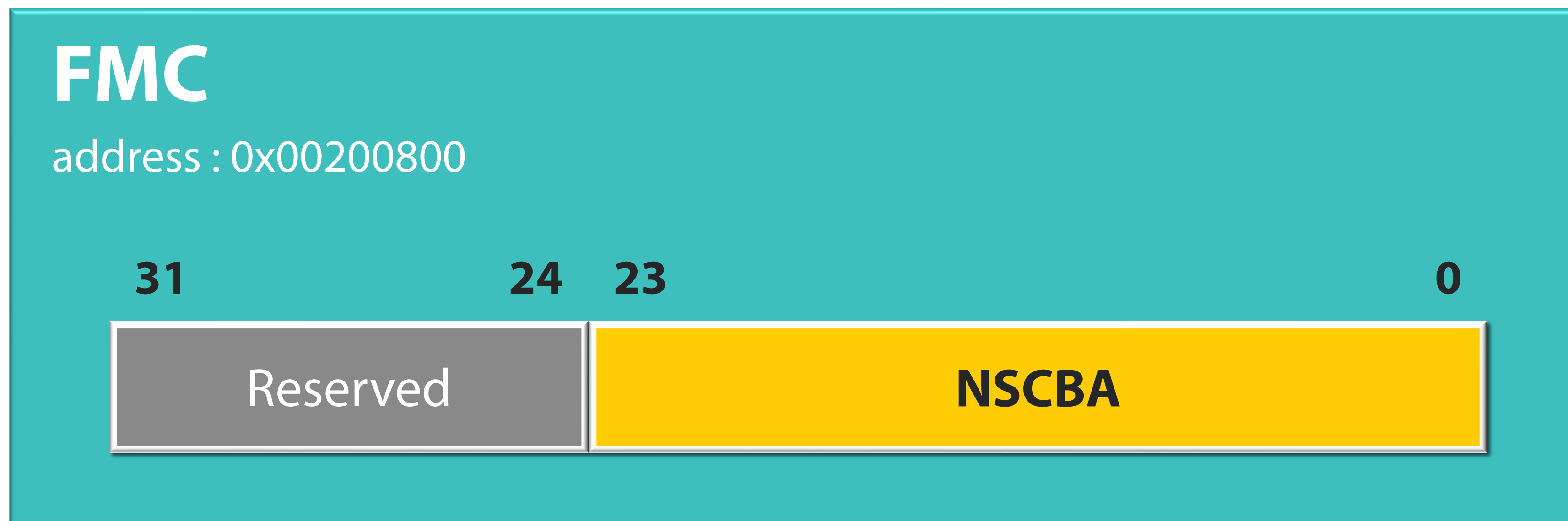
Security

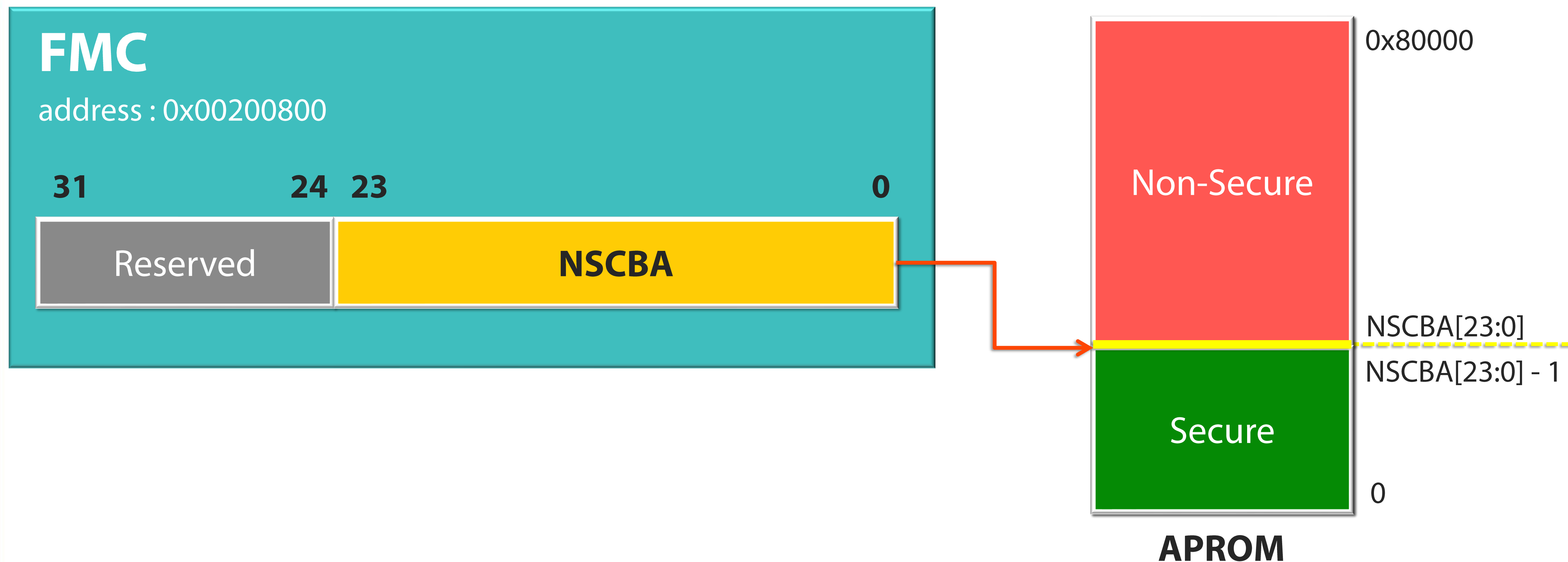
Attribute Configuration

- If the **security state** of a hardware resource is changeable, both **secure** and **non-secure** address range are allocated for it.
- Once assigned to be **non-secure** by system initialization code, the hardware resource will only respond to **non-secure** address.



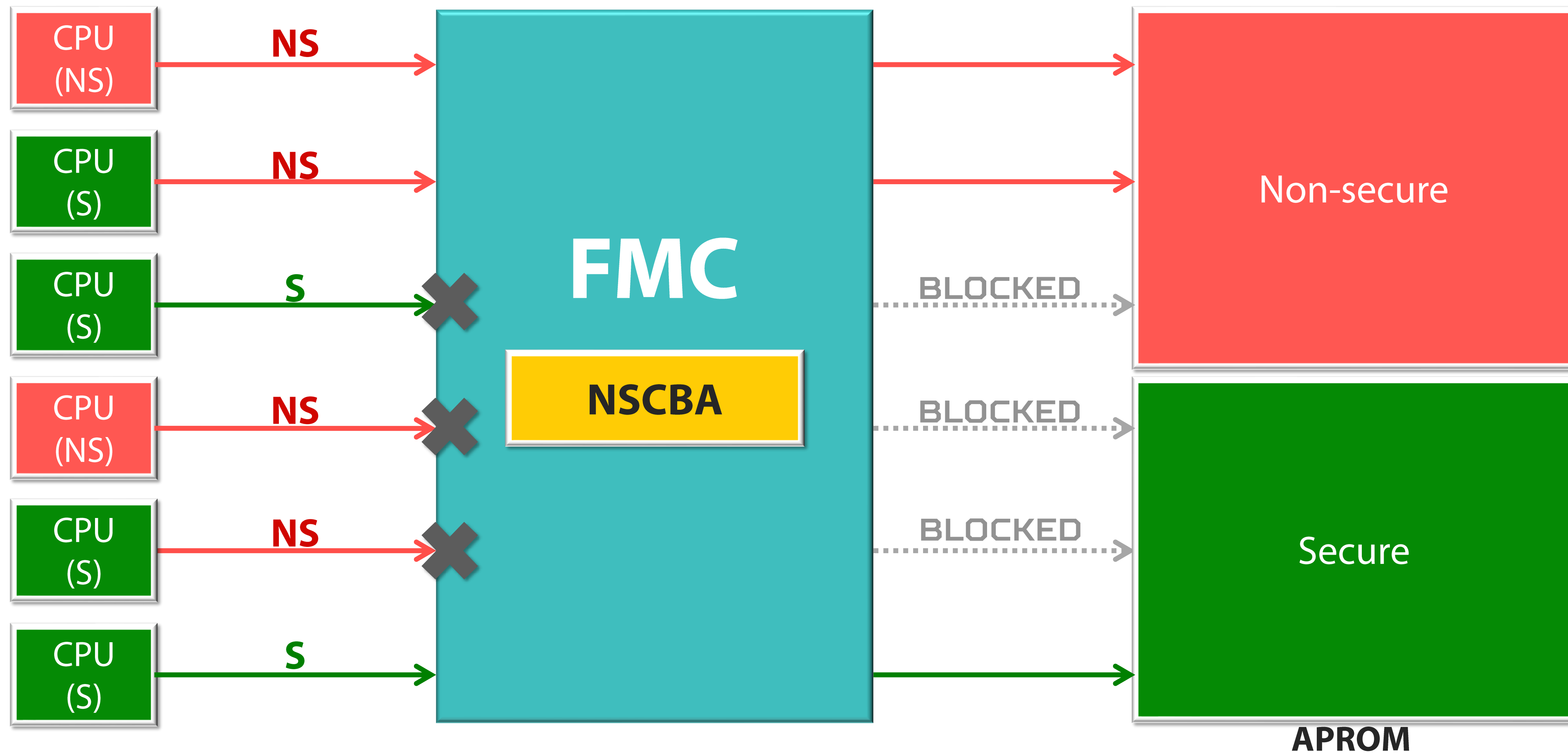
- Most of the M2351 Flash areas are always **secure** and cannot be changed.
- Only APROM area can be changed to be **non-secure**.
 - NSCBA[23:0] indicates the starting address of **non-secure** APROM, which should align with Flash page size.





- **FMC can block unsecure access to flash.**

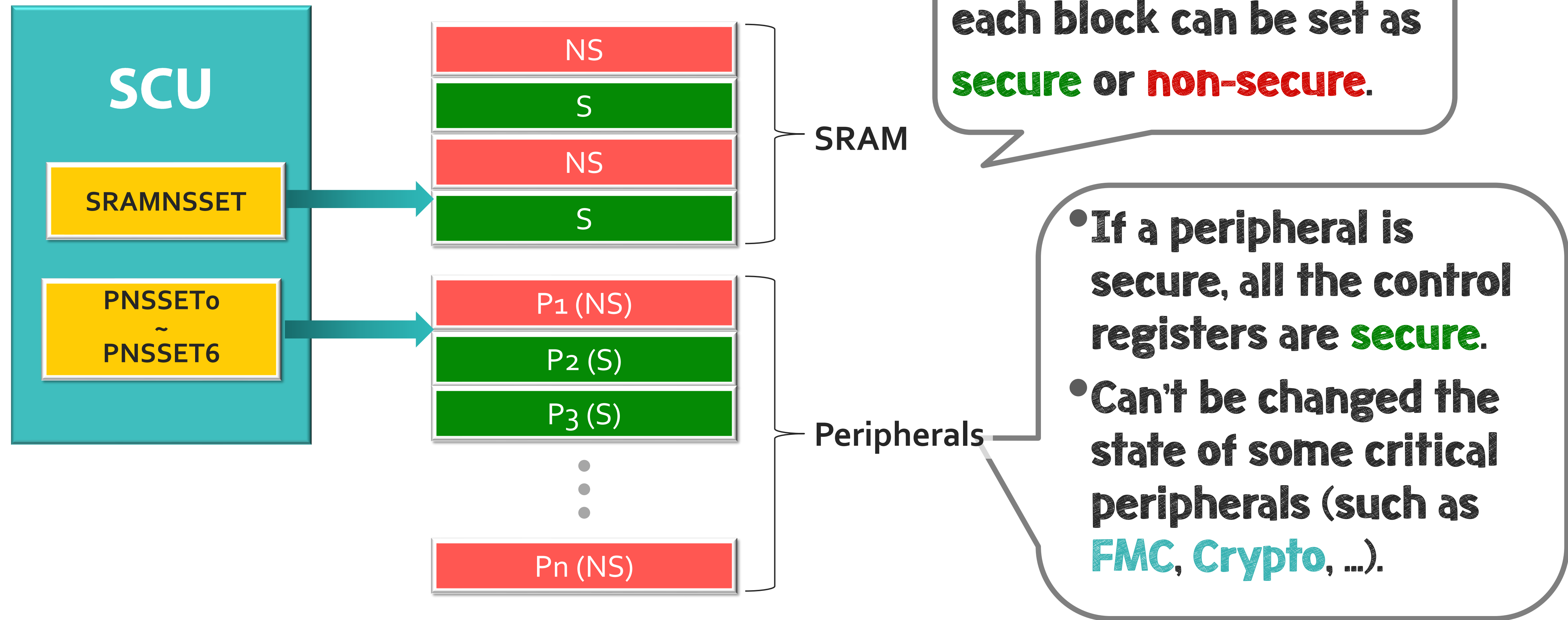
- Secure processor uses **secure address** (address bit 28 = 0) to access **non-secure APROM**.
- Secure processor uses **non-secure address** (address bit 28 = 1) to access **secure APROM**.
- **Non-secure processor** uses **non-secure address** (address bit 28 = 1) to access **secure APROM**.



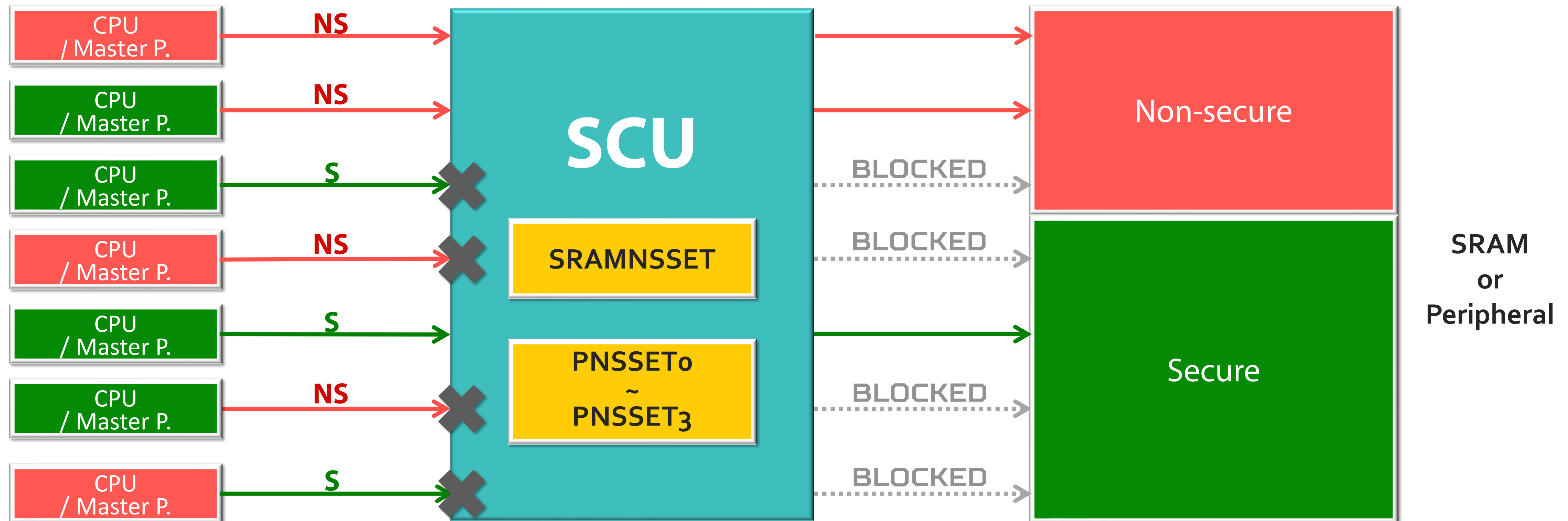
Secure Configuration Unit

SCU

- Used to configure the security attribute of SRAM and peripherals.



- **SCU can block unsecure access to SRAM or peripherals.**
 - **Secure** processor or master peripheral
 - Uses **secure address** (address bit 28 = 0) to access **non-secure SRAM** or **non-secure Peripheral**.
 - Uses **non-secure address** (address bit 28 = 1) to access **secure SRAM** or **secure Peripheral**
 - **Non-secure** processor or master peripheral uses **non-secure address** to access **secure SRAM** or **secure Peripheral**.
 - **Non-secure** master peripheral tries to access a **secure address** (address bit 28 = 0) .



SRAM is in **secure state** after reset.

- SCU - SRAM Security Configuration

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

Security
Configurations

Security
Configuration
of Flash

Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral

**Register SRAMNSSET
in SCU is used to
set SRAM block to
non-secure state.**

• SCU - SRAM Security Configuration

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

Security
Configurations

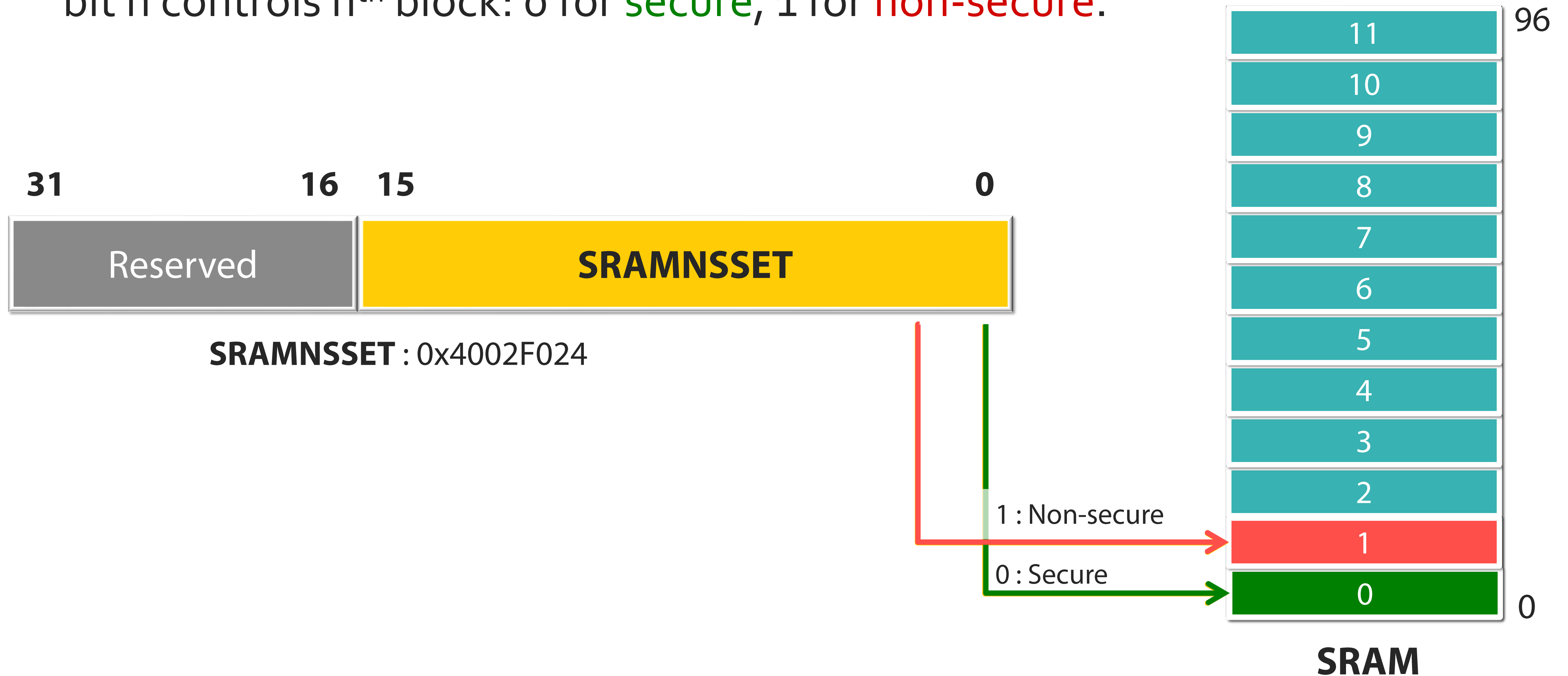
Security
Configuration
of Flash

Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral

- each block is 8KB.
- bit n controls nth block: 0 for **secure**, 1 for **non-secure**.



All peripherals
are in **secure state**
after reset.

- SCU - Peripheral Security Configuration

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

Security
Configurations

Security
Configuration
of Flash

Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral

The **secure state** of each configurable peripheral is controlled by a corresponding bit in registers **PNSSET0 ~ PNSSET6**

• SCU - Peripheral Security Configuration

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

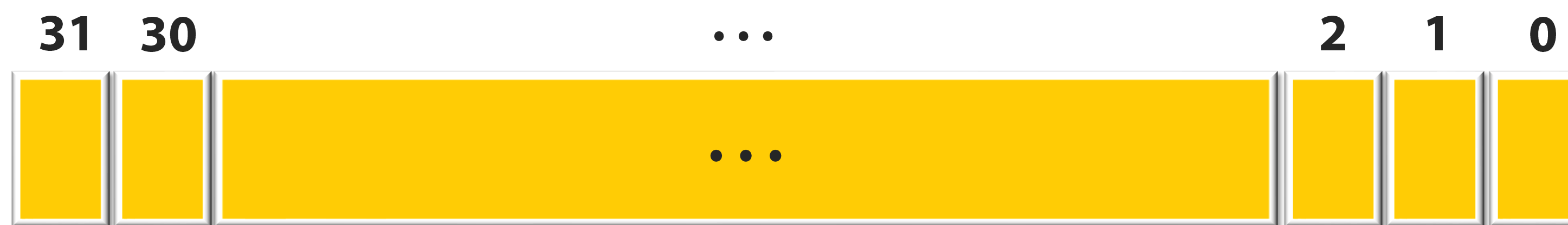
Security
Configurations

Security
Configuration
of Flash

Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral



PNSSETx : $0x4002F000 + 4 * x$

0 : Secure

1 : Non-secure

Register IONSSET is
used to configure
secure state of
individual GPIO port.

• SCU - Peripheral Security Configuration

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

Security
Configurations

Security
Configuration
of Flash

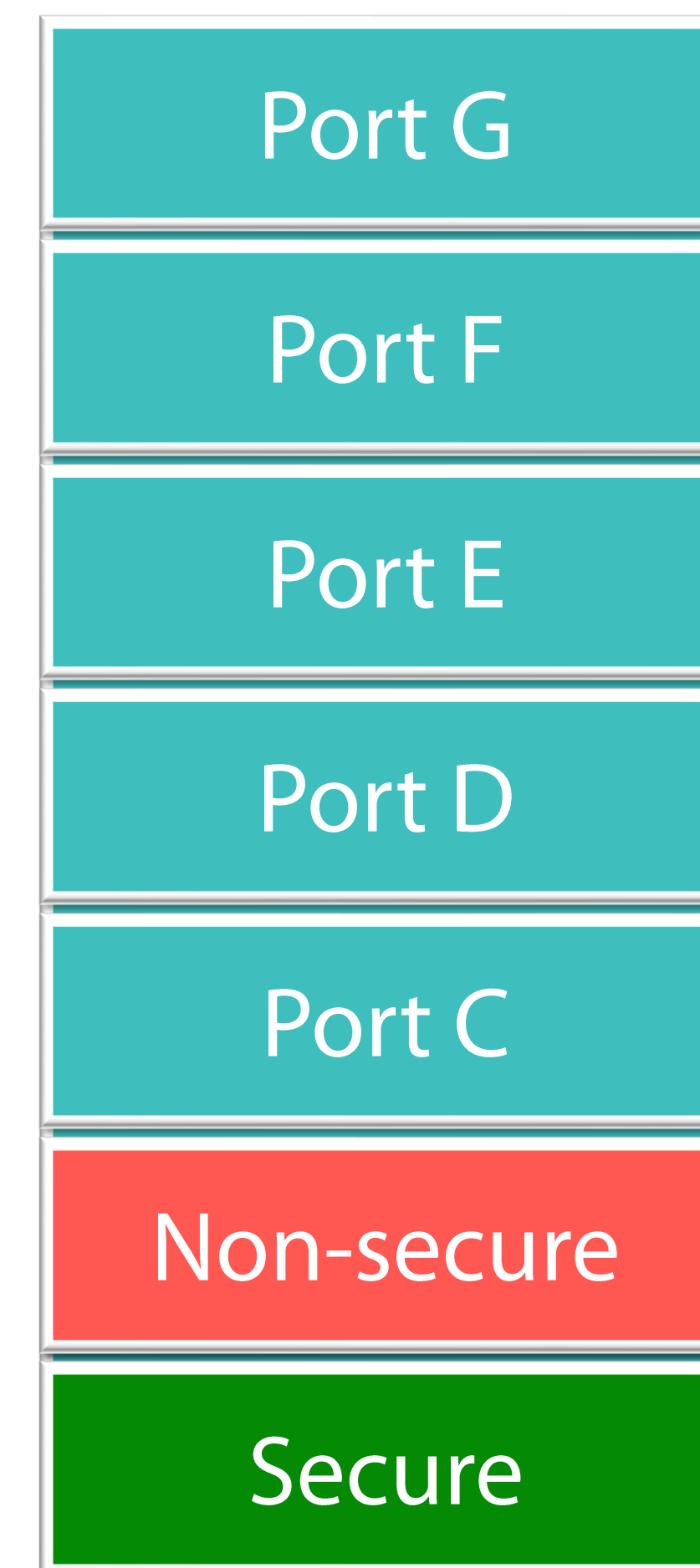
Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral



IONSSET : 0x4002F020



GPIO

TrustZone®
Implementation
On M2351

M2351
Block
Diagram

IDAU

SAU

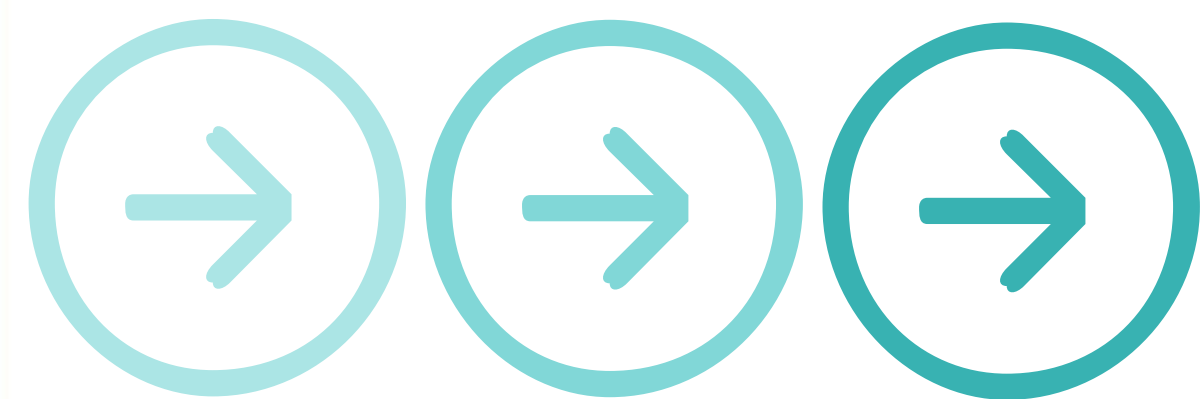
Security
Configurations

Security
Configuration
of Flash

Security
Configuration
Unit

Security
Configuration
of SRAM

Security
Configuration
of Peripheral



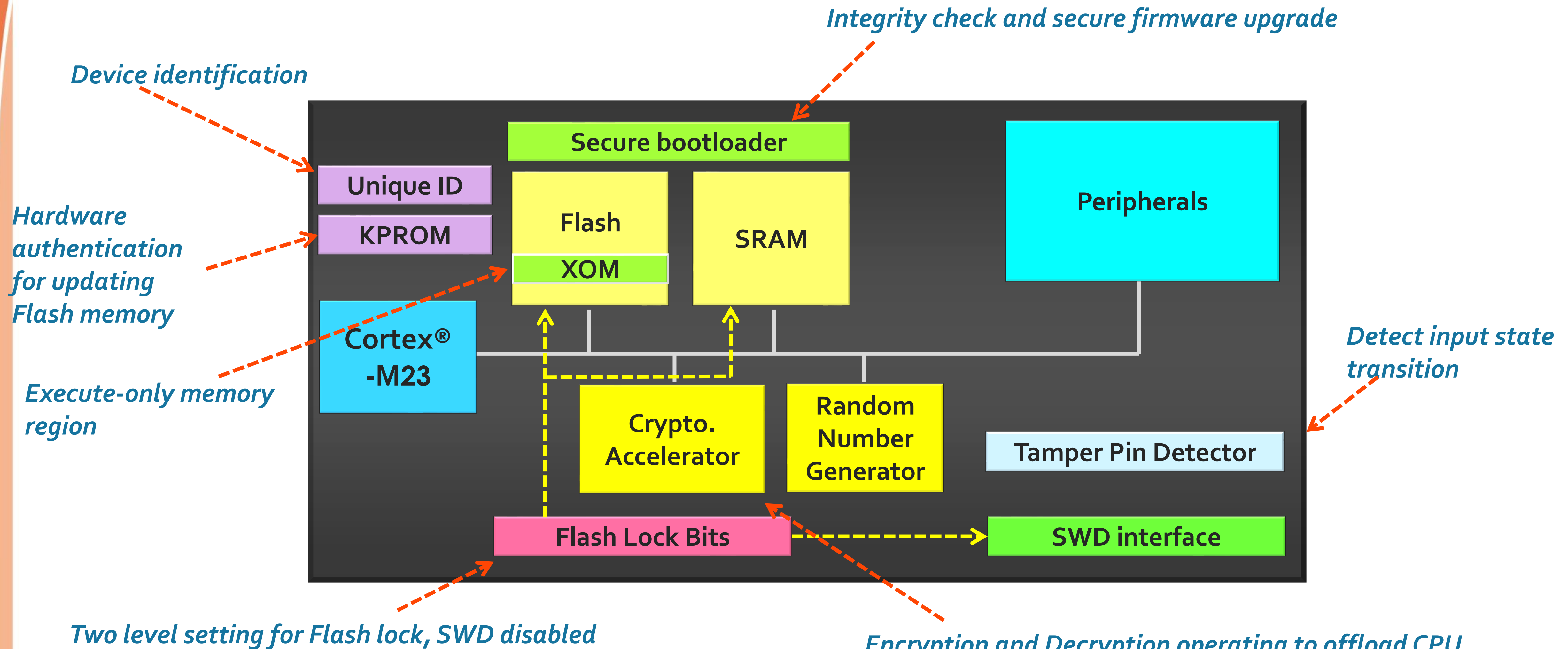
M2351 Security Functions

*Crypto Accelerator, Secure bootloader, KPROM, XOM,
Flash Lock, Secure Debug and Tamper Detector.*

M2351 Security Functions

*Crypto Accelerator, Secure bootloader, KPROM, XOM,
Flash Lock, Secure Debug and Tamper Detector.*

M2351 Security Functions



M2351
Security
Functions

Crypto
Accelerator

Secure
Bootloader

KPROM

XOM

Flash
Lock Bits

Secure
Debug

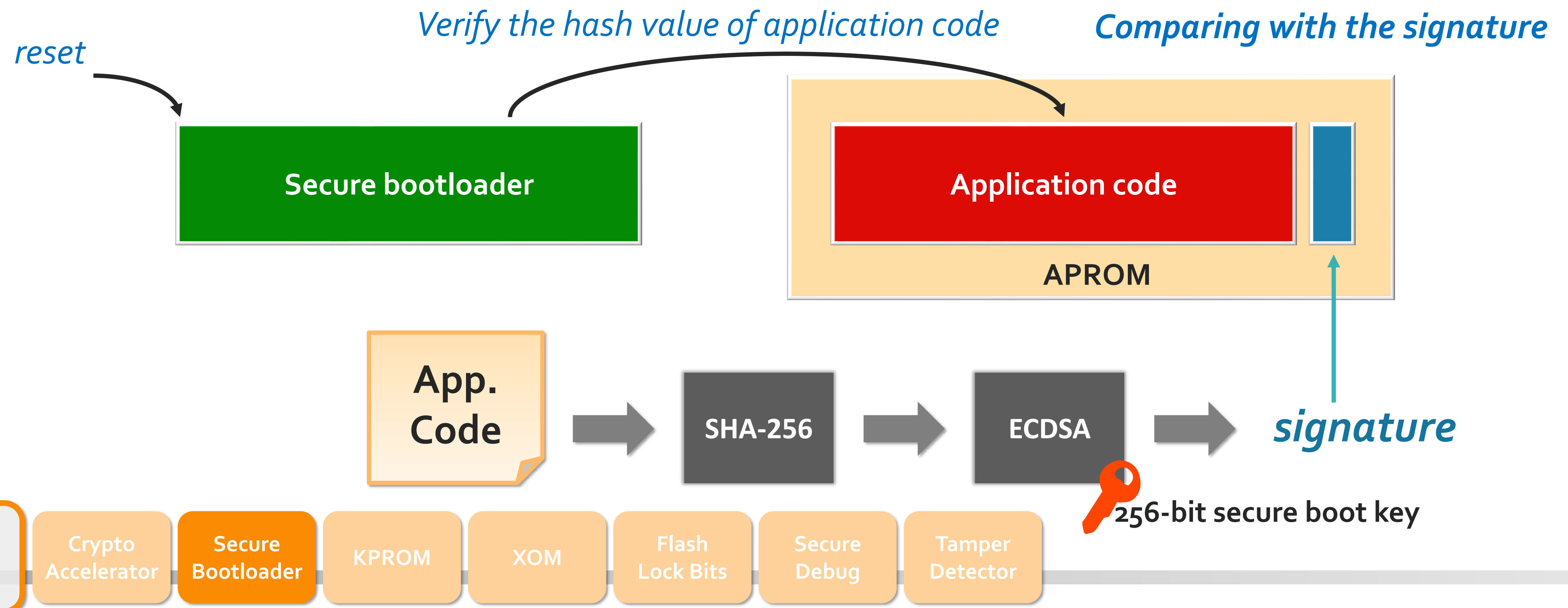
Tamper
Detector

Crypto Accelerator

- **Support cryptographic operations for ciphering and message integrity**
 - Elliptic Curve Cryptography (ECC)
 - DES, 3DES in ECB, CBC, CFB, OFB and CTR mode
 - AES 128-, 192-, and 256-bit
 - ECB, CBC, CFB, OFB, CTR, CBC-CS1, CBC-CS2, and CBC-CS3 mode
 - SHA-160/224/256/384
 - TRNG for key generation
 - 64, 128, 192 and 256-bit random number

Secure Bootloader

- An immutable ROM code resident in execution-only region
 - Assures application code in flash memory has not been tampered.

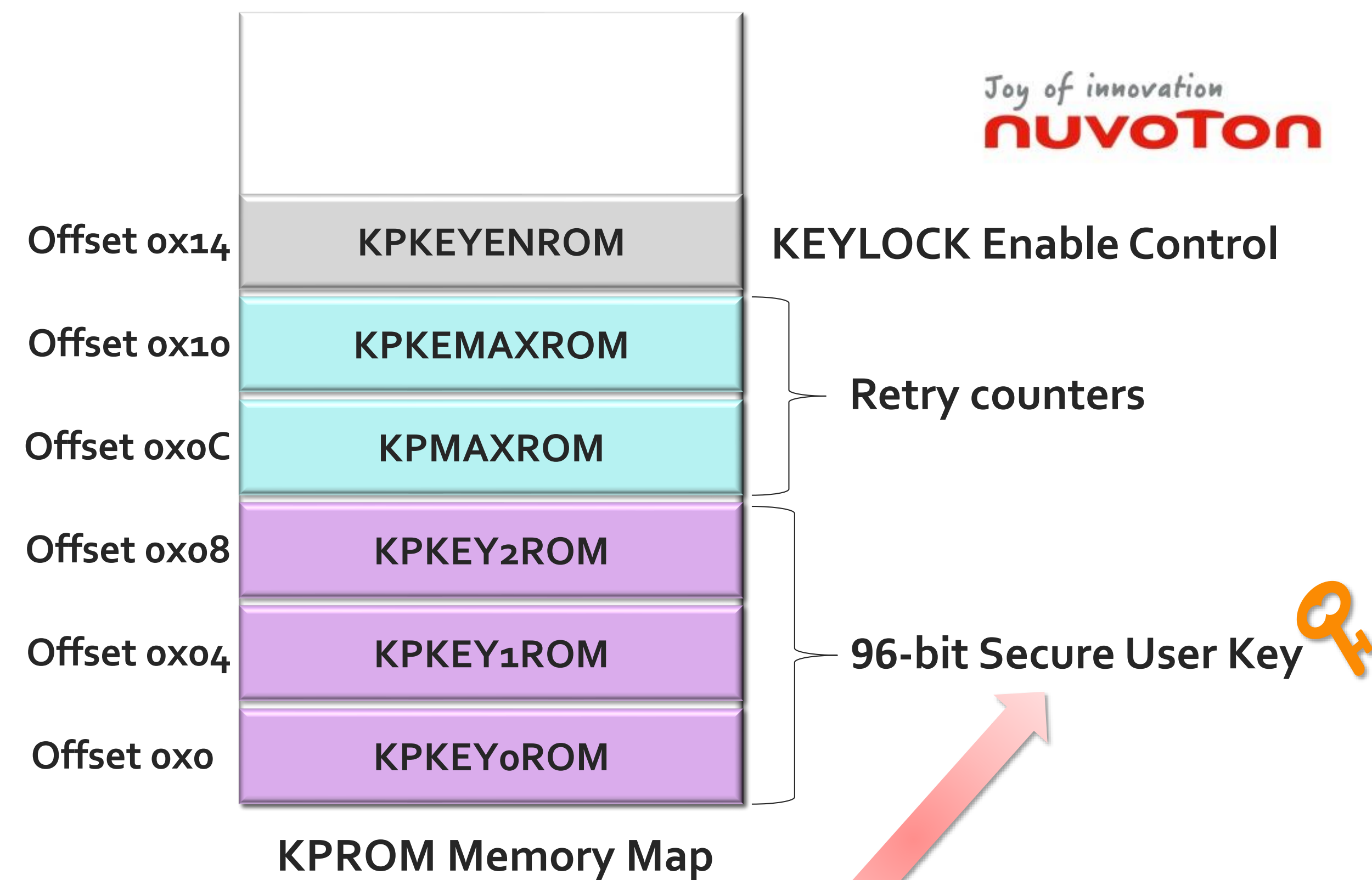


KPROM

- **4 Kbytes flash to store 96-bit Secure User Key and Secure User Key Retry Limitation**

- The 96-bit Secure User Key cannot be read directly and only can be verified by hardware.

- LDROM, APROM and KPROM are write-protected once KPROM is enabled.



96-bit Secure User Key Compare

Flash Write or Erase

Success
Fail

LDROM
APROM
KPROM

M2351
Security
Functions

Crypto
Accelerator

Secure
Bootloader

KPROM

XOM

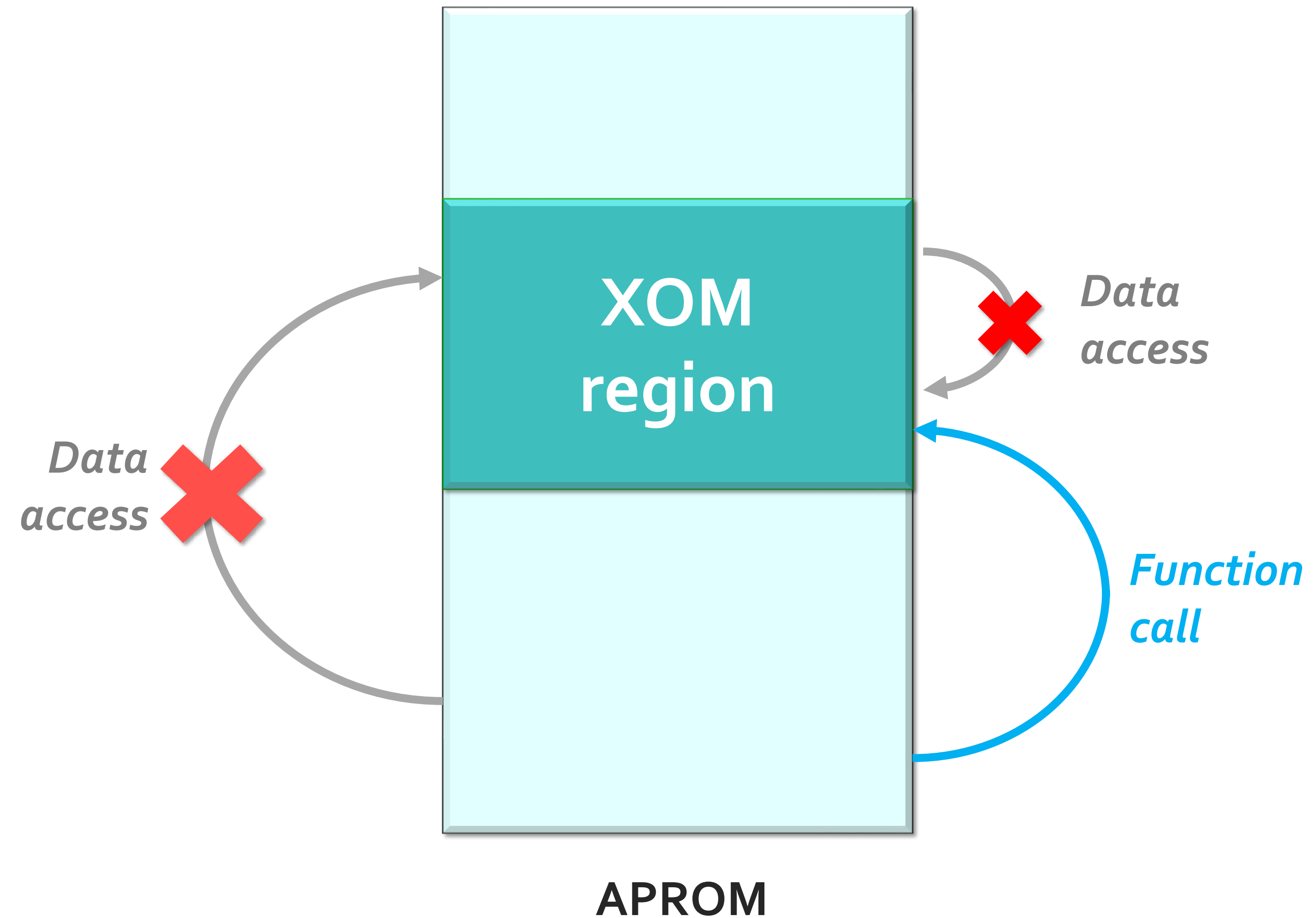
Flash
Lock Bits

Secure
Debug

Tamper
Detector

eXecution-Only Memory (XOM)

- Up to 4 XOM regions can be defined in APROM
- Execution-only, data access is not allowed.
(PC-relative data access is not allowed).



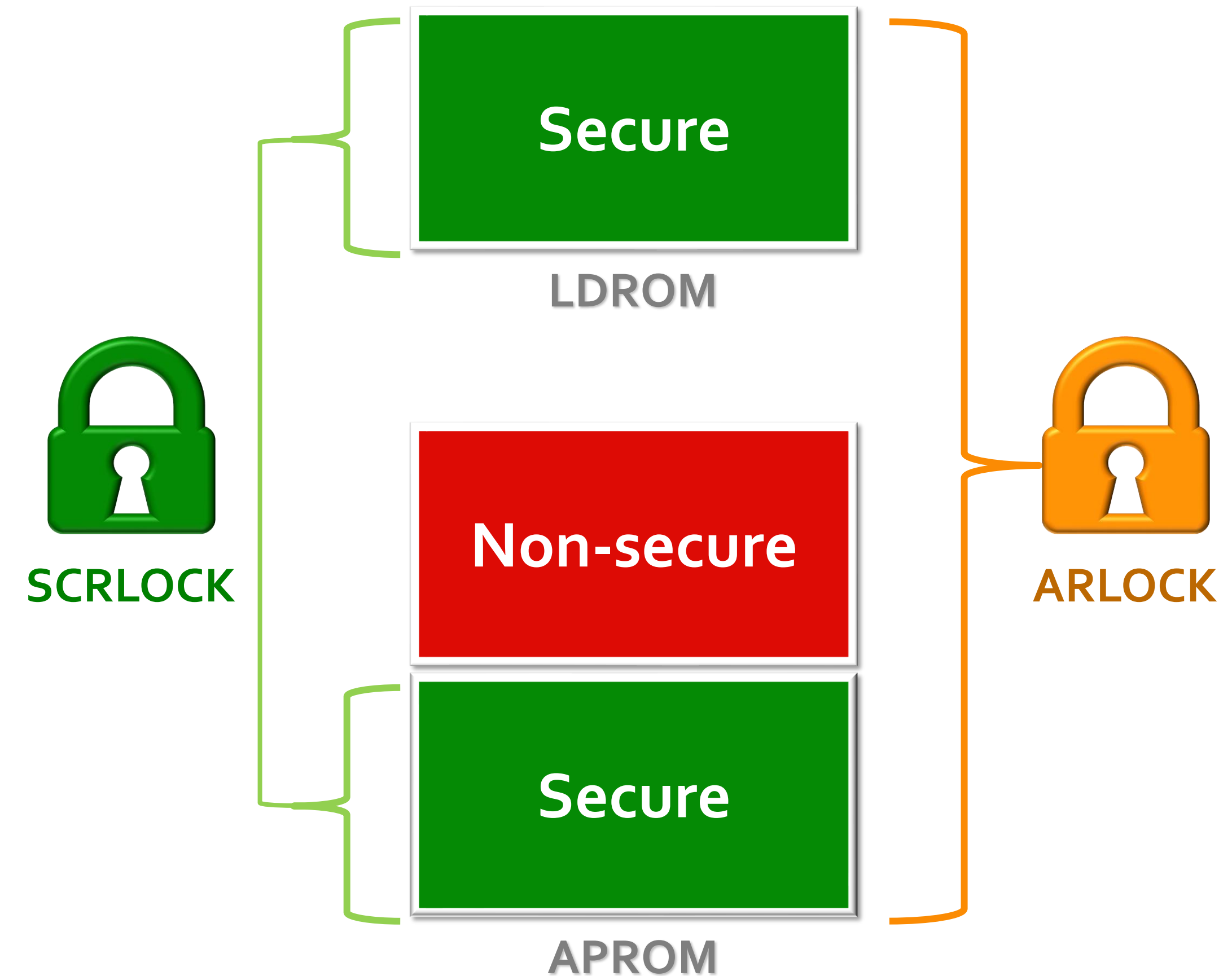
Flash Lock Bits

- **SCRLOCK**

- When SCRLOCK is set, external read and write access to secure Flash regions (LDROM, secure APROM region) are denied.





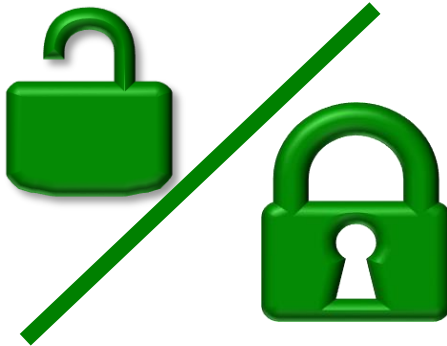

- **ARLOCK**

- When ARLOCK is set, external read and write access to Flash regions (LDROM, entire APROM) are prohibited.



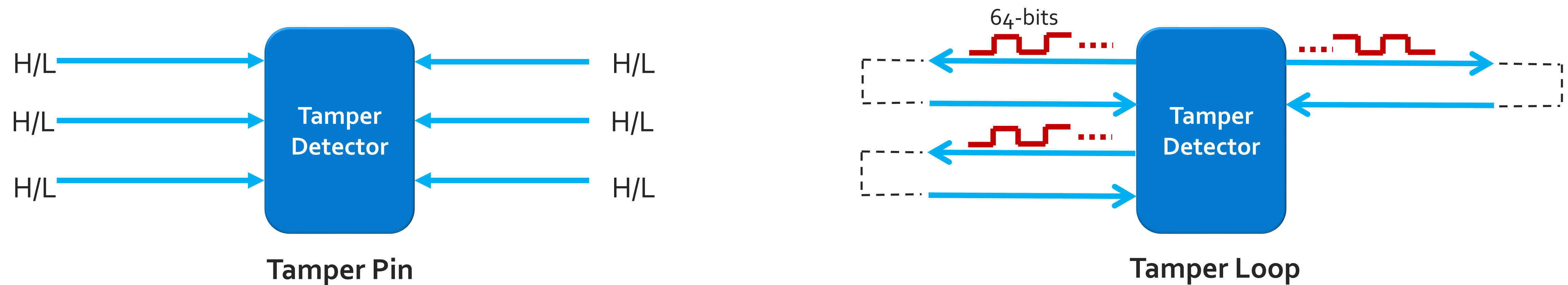
Secure Debug

- Debug interface (SWD) is controlled by the status of SCRLOCK and ARLOCK

SCRLOCK	ARLOCK	Debug Capability
		Can debug and trace any software code.
		Only can debug and trace non-secure software code.
		Debug interface is disabled, cannot debug and trace any software code.

Tamper Detector

- Tamper pins can be configured as six individual inputs or 3 tamper loops.



- When the defined transition condition is detected
 - A tamper alarm interrupt will be triggered.
 - The RTC spare registers (80 bytes) will be cleared.

Summary

M2351 is equipped with hardware functions to improve system security.

