STM32L5 MCU series

Excellence in ultra-low-power with more security

life.augmented

ST Restricted

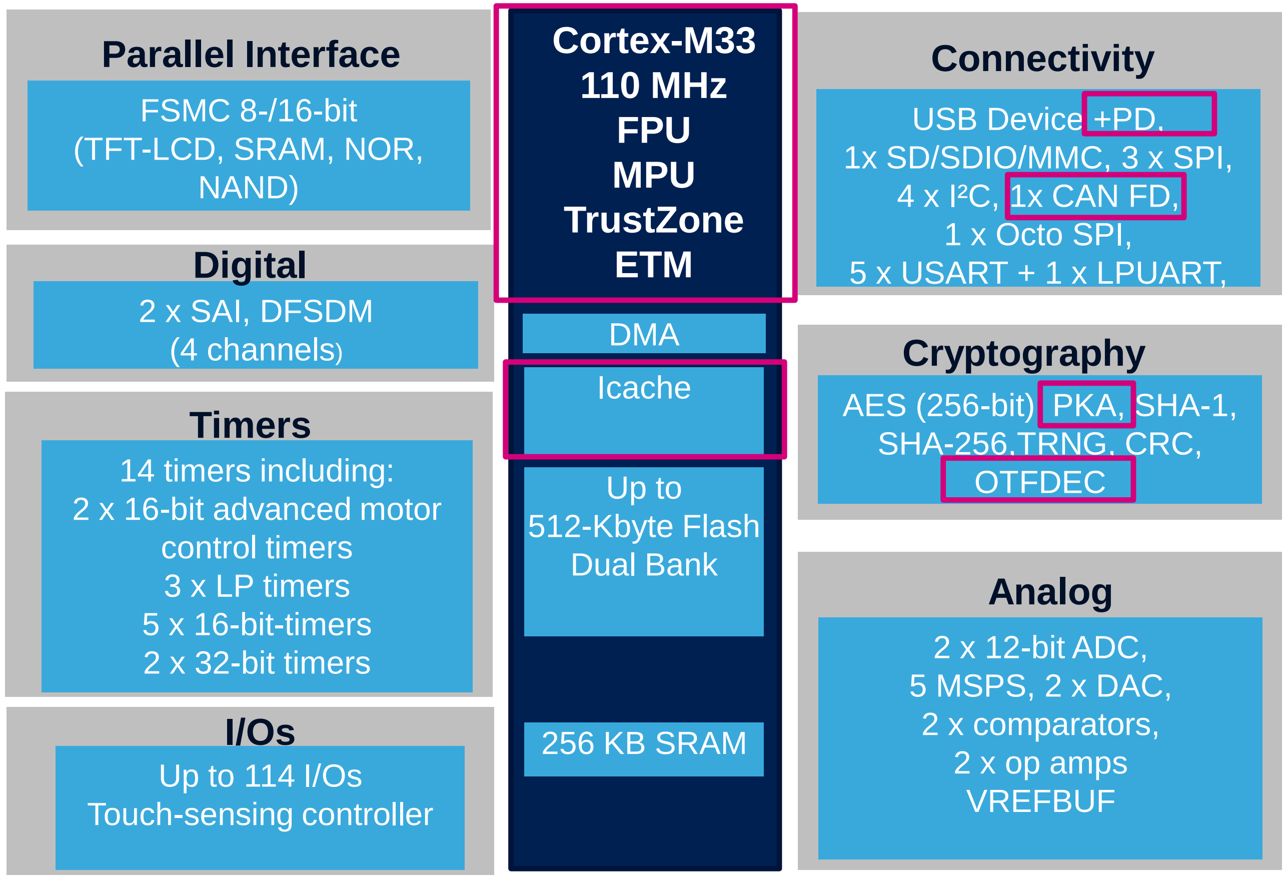
First STM32 Based on Cortex-M33

STM32L5 is the answer

- More security with TrustZone and ST security implementation
  - **HW to resist to Logical and board level attack**
- Lower Power consumption
  - **STM32 ultra-low-power technology**
- Integration, Size, performance
  - **More performance, high memory size and wide portfolio**

STM32L5 block diagram

- Up to 110MHz, 165DMIPS
- 512 KB Flash / 256KB SRAM
- Security TrustZone ARM v8M
- ART acceletor: Instruction Cache 8 KB, for internal and external memories
- 1xOctoSPI



Parallel Interface

FSMC 8-/16-bit (TFT-LCD, SRAM, NOR, NAND)

Digital

2 x SAI, DFSDM (4 channels)

Timers

14 timers including:
2 x 16-bit advanced motor control timers
3 x LP timers
5 x 16-bit-timers
2 x 32-bit timers

I/Os

Up to 114 I/Os
Touch-sensing controller

Cortex-M33
110 MHz
FPU
MPU
TrustZone
ETM

DMA

Icache

Up to 512-Kbyte Flash Dual Bank

256 KB SRAM

Connectivity

USB Device +PD, 1x SD/SDIO/MMC, 3 x SPI, 4 x I²C, 1x CAN FD, 1 x Octo SPI, 5 x USART + 1 x LPUART,

Cryptography

AES (256-bit) PKA, SHA-1, SHA-256,TRNG, CRC, OTFDEC

Analog

2 x 12-bit ADC, 5 MSPS, 2 x DAC, 2 x comparators, 2 x op amps VREFBUF

Extend the Battery Life Time

- STM32L5 reuses the STM32L4/L4+ technology achieving **best-in-class** power consumption

- STM32L5 integrates an optional **SMPS** (DC/DC buck voltage regulator) which can be enabled/disabled on the fly to optimize the energy.

- Proven by EEMBC test results:

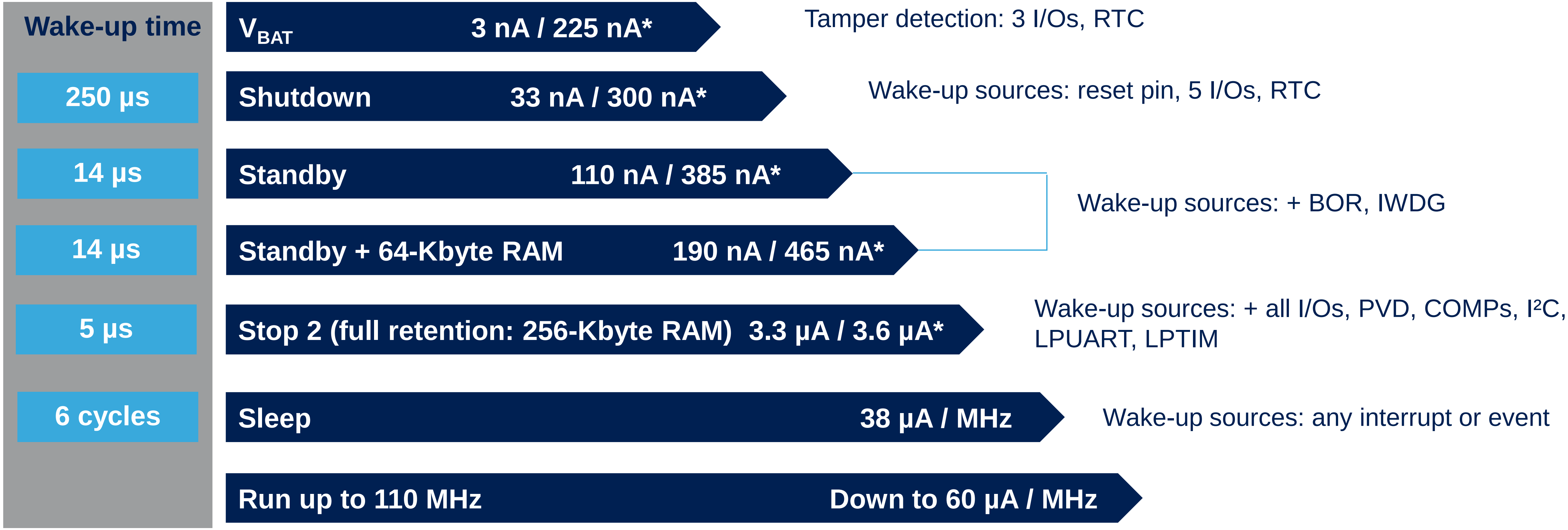
ULPBENCH™ An EEMBC Benchmark **402 ULPMark-CP**

ULPBENCH™ An EEMBC Benchmark **60 ULPMark-PP**

ULPBENCH™ An EEMBC Benchmark **27400 SecureMark-TLS**

Ultra-low-power Modes

Best power consumption numbers with full flexibility



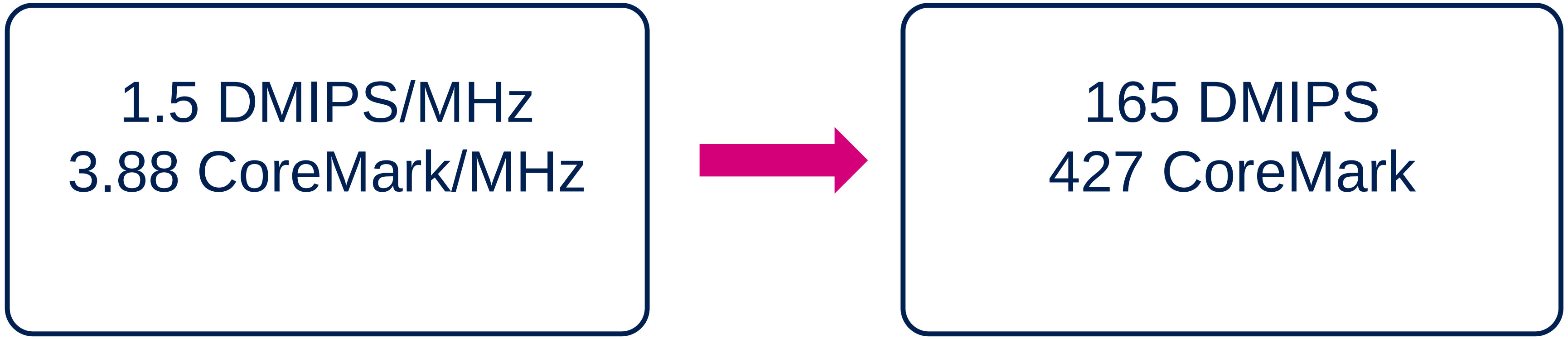
Wake-up time	Mode	Consumption	
	V_{BAT}	3 nA / 225 nA*	Tamper detection: 3 I/Os, RTC
250 µs	Shutdown	33 nA / 300 nA*	Wake-up sources: reset pin, 5 I/Os, RTC
14 µs	Standby	110 nA / 385 nA*	Wake-up sources: + BOR, IWDG
14 µs	Standby + 64-Kbyte RAM	190 nA / 465 nA*	
5 µs	Stop 2 (full retention: 256-Kbyte RAM)	3.3 µA / 3.6 µA*	Wake-up sources: + all I/Os, PVD, COMPs, I²C, LPUART, LPTIM
6 cycles	Sleep	38 µA / MHz	Wake-up sources: any interrupt or event
	Run up to 110 MHz	Down to 60 µA / MHz	

Note : * without RTC / with RTC

More Performance

Better responsiveness of the application

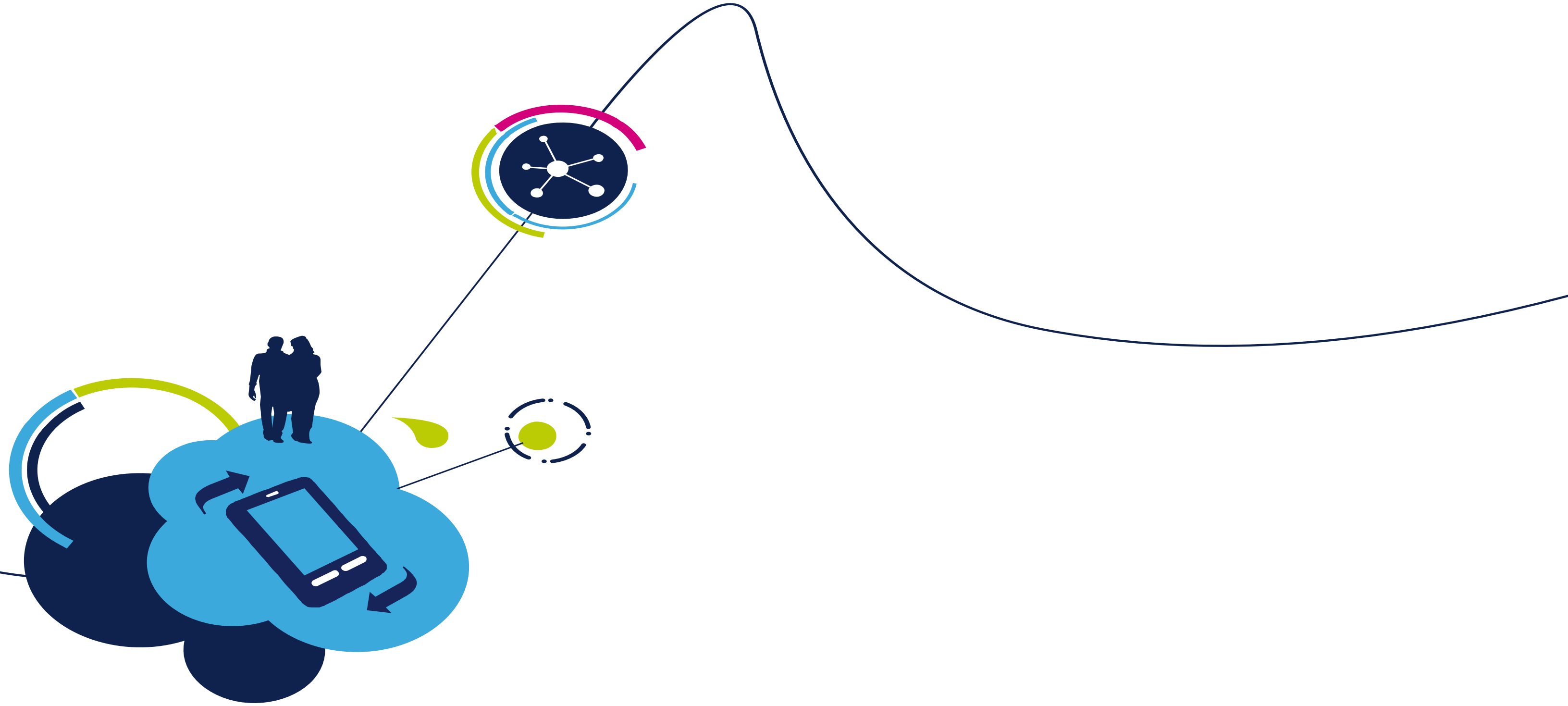
- **New** Arm® Cortex®-M33 performance: **+20%** versus Cortex-M4



1.5 DMIPS/MHz
3.88 CoreMark/MHz

165 DMIPS
427 CoreMark

- **New** ST ART Accelerator™: working both on internal and **<u>external</u>** Flash
  - 8 Kbytes of instruction cache



Series/Packages/Pinout

ST Restricted

STM32L5 series

Cortex M33 (DSP + FPU) – 110 MHz

- ICACHE

- USART, SPI, I^{2}C
- 16 and 32-bit timers
- SAI + audio PLL

- SHA, TRNG, PKA
- On-the fly descryption

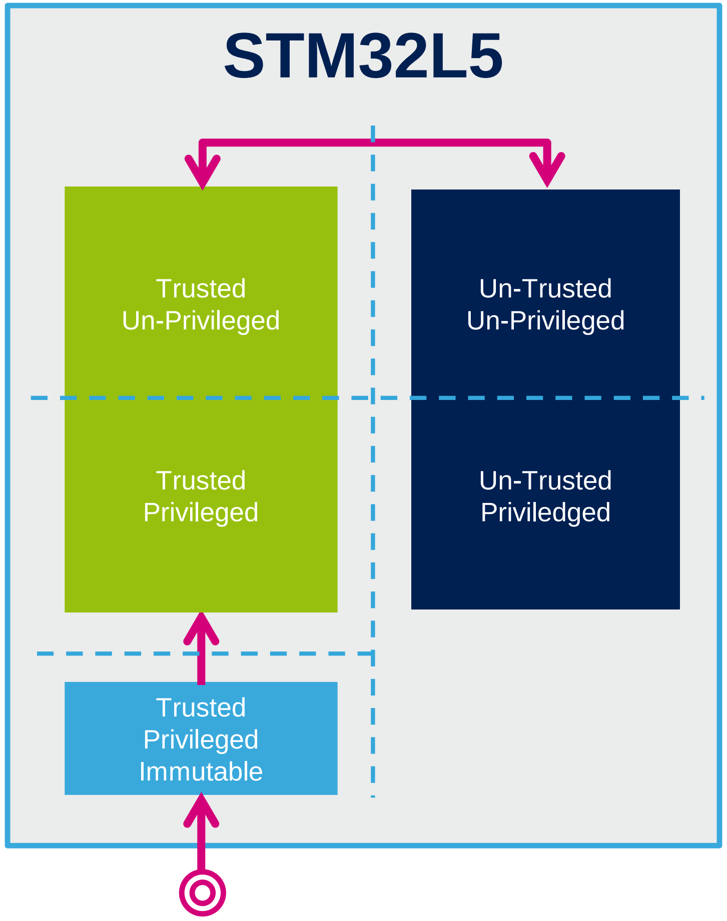
- 2x 12-bit DAC
- Temperature sensor

- Low voltage 1.71V to 3.6V
- VBAT Mode
- Unique ID
- Capacitive Touch sensing

Product line	FLASH (KB)	RAM (KB)	Memory I/F	2 x Op-Amp	2 x Comp.	4ch / 2x Sigma Delta Interface	12- bit ADC 5 Msps 16 bit HW oversampling	USB2.0 Device XTAL-less	CAN-FD	AES 128/256-bit	PKA	OTFDEC
STM32L552 USB Device & CAN-FD	512 to 256	256	SDMMC FSMC Octo SPI	●	●	●	2	●	●			
STM32L562 USB Device & CAN-FD & AES, PKA, OTFDEC	512	256	SDMMC FSMC Octo SPI	●	●	●	2	●	●	●	●	●

STM32L5 TrustZone Isolations

Up to 5 security domains – PSA isolation level 3



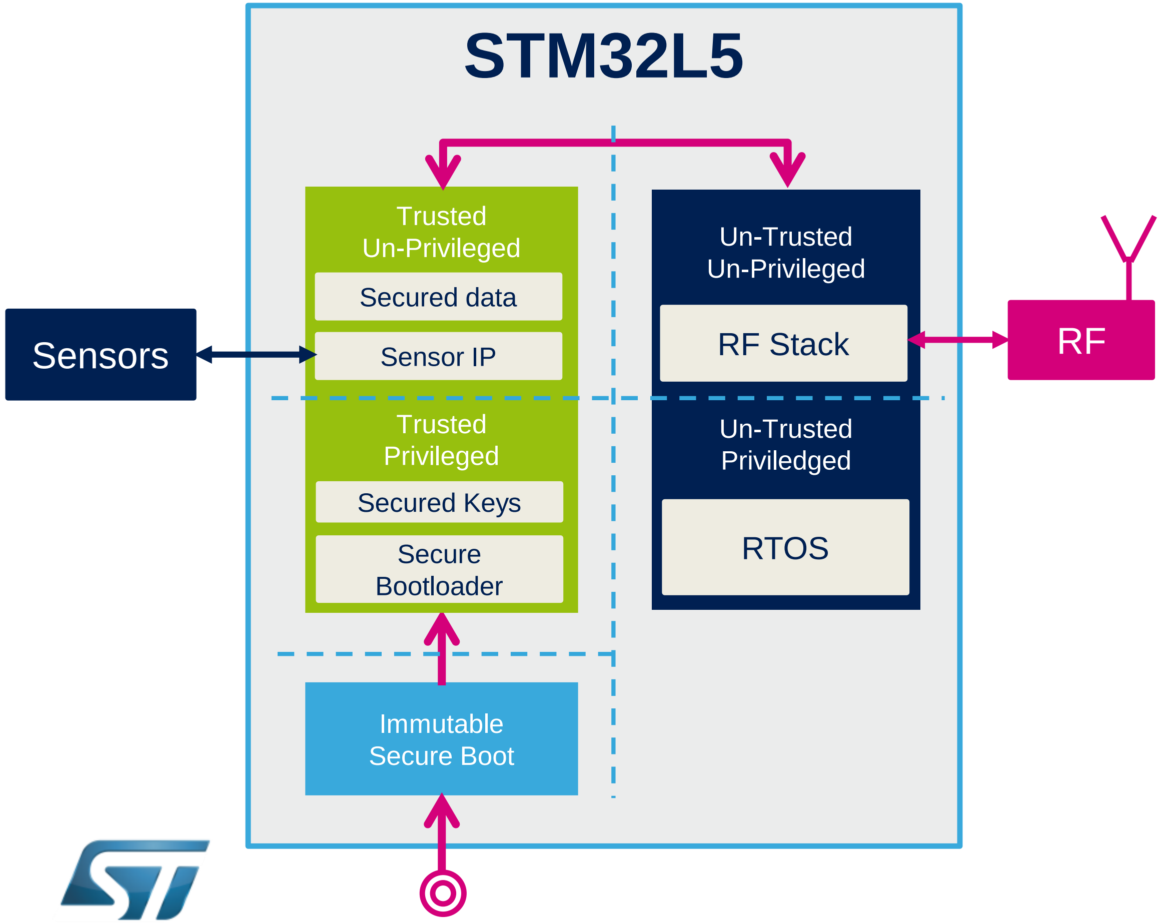
Un-Trusted area with code isolation
RTOS & applications

Trusted area with code isolation
Secure OS and services

Trusted Privileged Immutable area
Customer RoT / Secure Boot code

STM32L5 TrustZone Implementation

High granularity of Isolation



Each GPIO, DMA channel, part of memory, etc... can be affected to 1 domain

Fine granularity adjustment of memory size and peripherals for each domain

Full Hardware Isolation on each domain

A Full Set of Security Resources

STM32L5

Private Key (PKA) acceleration
ECC - RSA

AES
acceleration
up to 256

Hash

Up to SHA-256

Active and Static tamper detection

On-The-Fly Decryption

TRNG

A Full Set of Security Resources

STM32L5

TrustZone

Unique Boot Entry

HDP (Hide Protect)

Memory protection Unit (MPU)

OTP memory

Unique ID

Security Certification Compliant

STM32L5

Industrial Security Level Capable

Arm PSA security Level 1 Certified

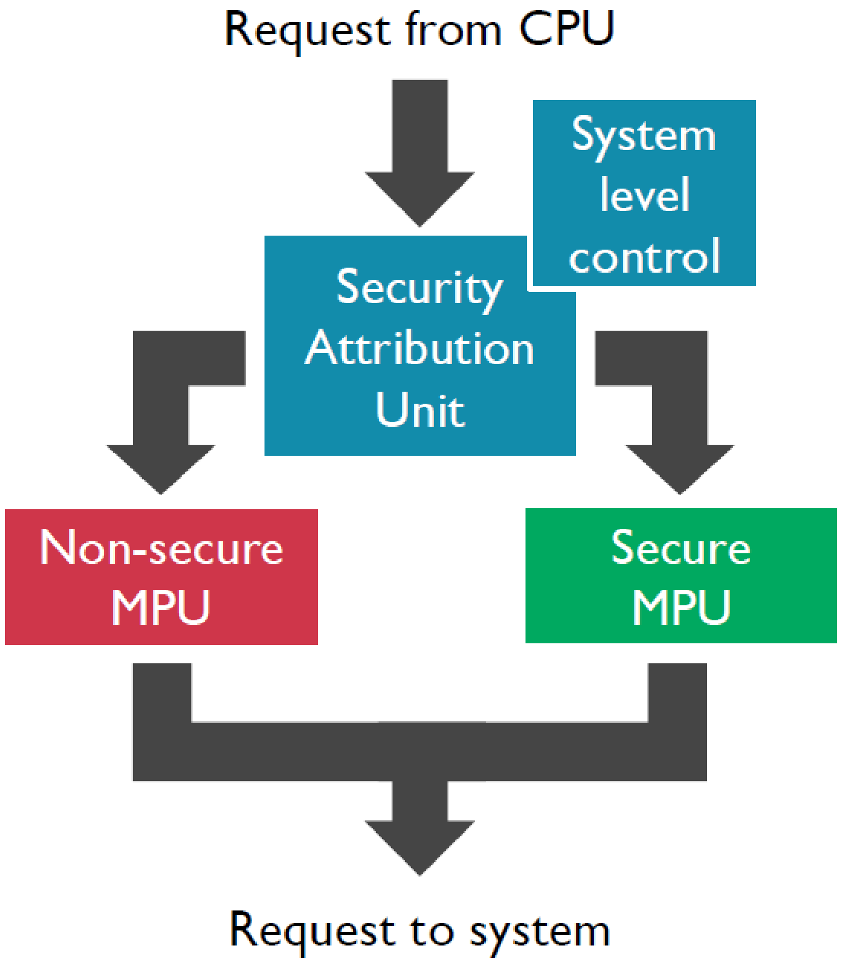
Arm PSA security Level 2 Ready

STM32L5 TrustZone architecture

TrustZone Security architecture

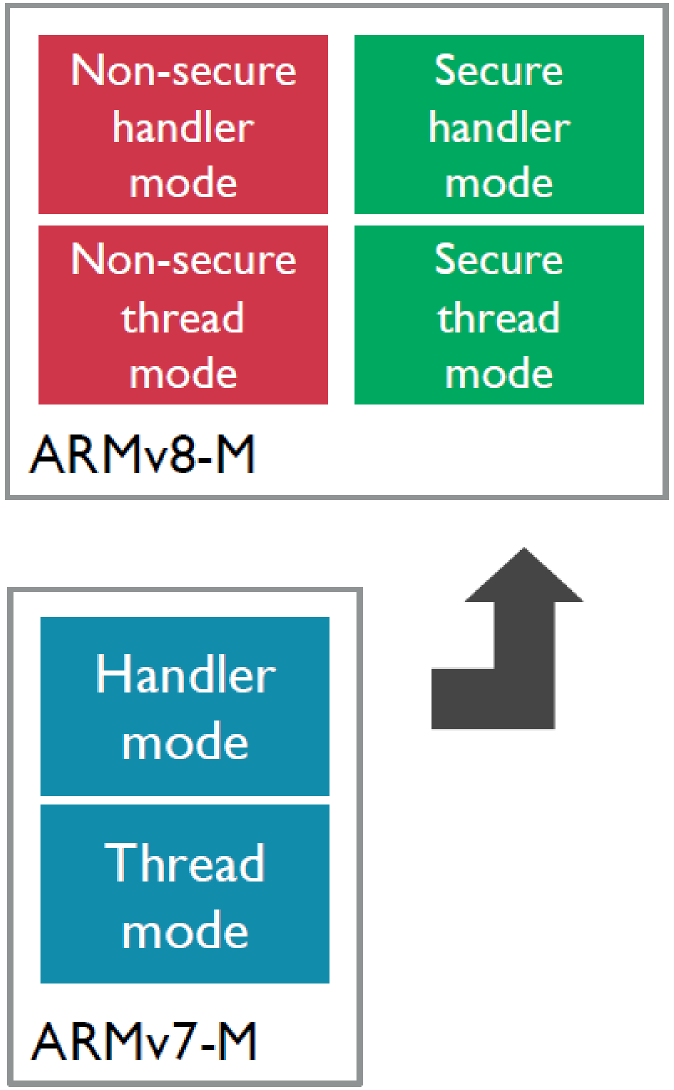
- Security architecture is based on Arm® TrustZone® with the ARMv8-M Main Extension

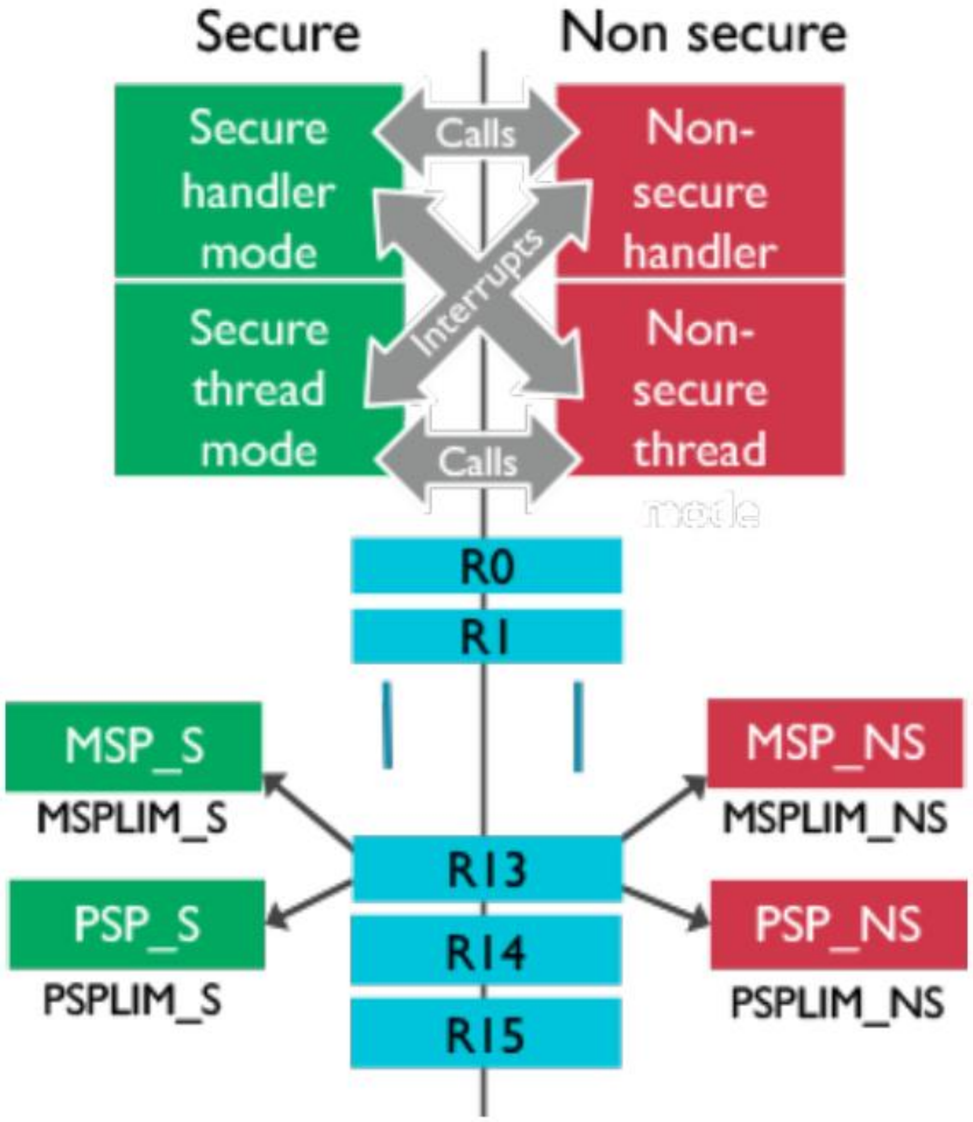
- When the TrustZone is enabled, the SAU (security attribution unit) and IDAU (implementation defined attribution unit) define the access permissions based on secure and non-secure state.
  - IDAU: It provides a first memory partition as non-secure or non-secure callable attributes. The IDAU memory map partition is not configurable and fixed by hardware implementation.
  - SAU: Up to eight SAU configurable regions are available for security attribution.
  - The security state is selected based first on IDAU security attribute, then combined with SAU security attribution

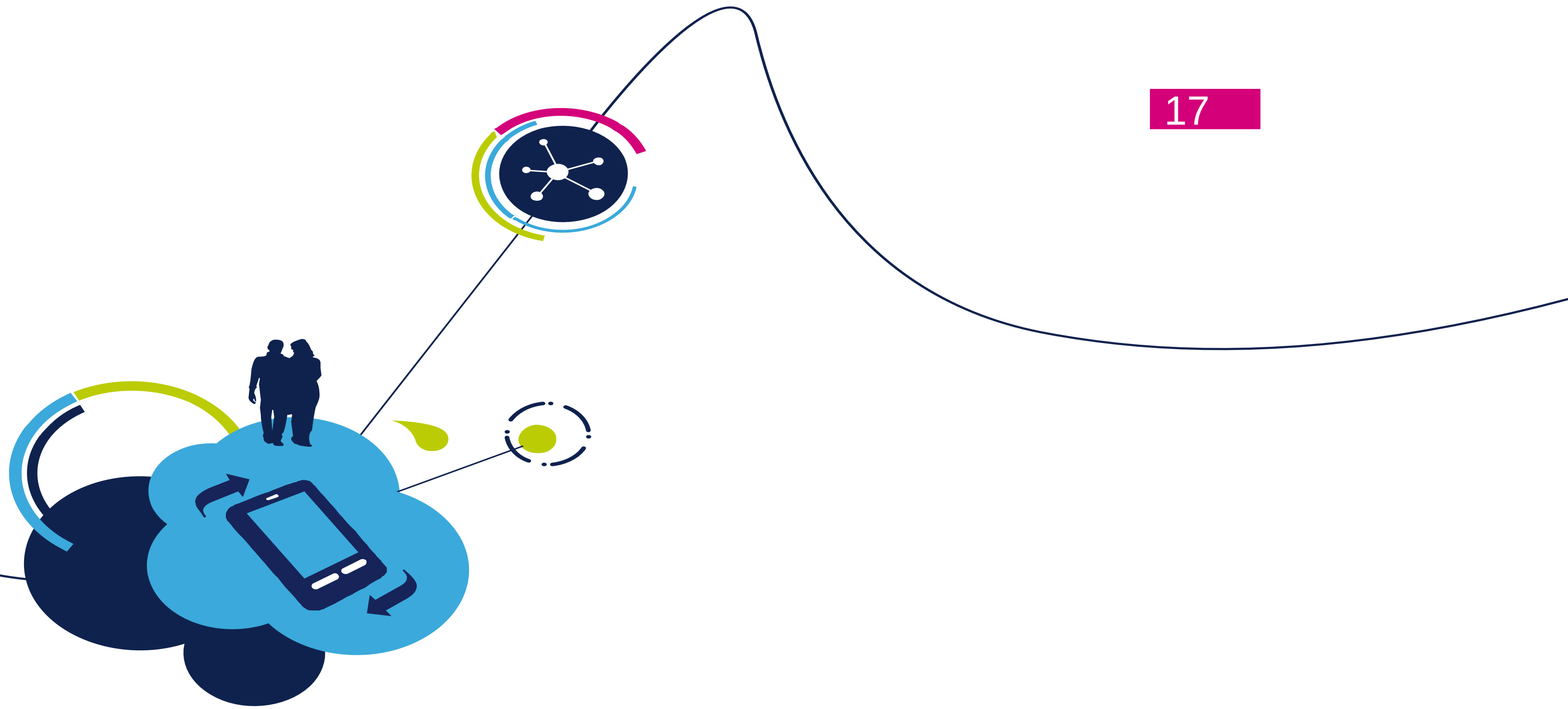


ST Restricted

Additional states in ARMv8-M

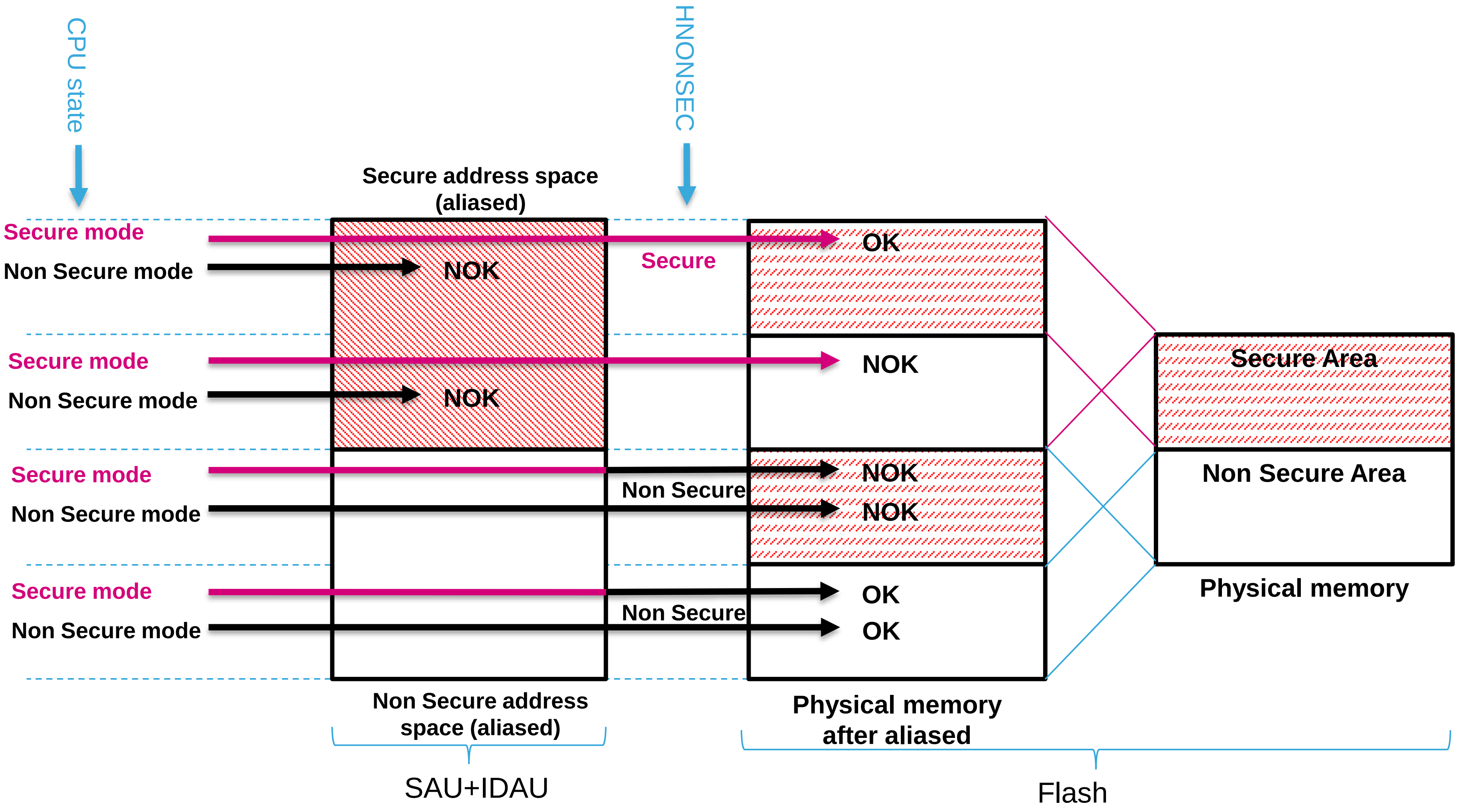






ARM v8-M Trustzone access rules

General picture



TrustZone peripheral classification (1/2)

- When the TrustZone security is active, a peripheral can be either Securable or TrustZone-aware

- Securable peripheral:
  - a peripheral is protected by an AHB/APB firewall gate that is controlled from TZSC controller to define security properties.

- TrustZone-aware:
  - a peripheral connected directly to AHB or APB bus and is implementing a specific TrustZone behavior such as a subset of registers being secure.

TrustZone peripheral classification (2/2)

- List of TrustZone-aware peripherals

Bus	Peripherals
AHB2	GPIOA..GPIOH
AHB1	MPCBBx MPCWMx TZIC TZSC EXTI Flash memory RCC DMAMUX DMA2 DMA1
AHB2	OTFDEC
APB2	SYSCFG
APB1	PWR RTC

- The remaining peripherals are Securable.

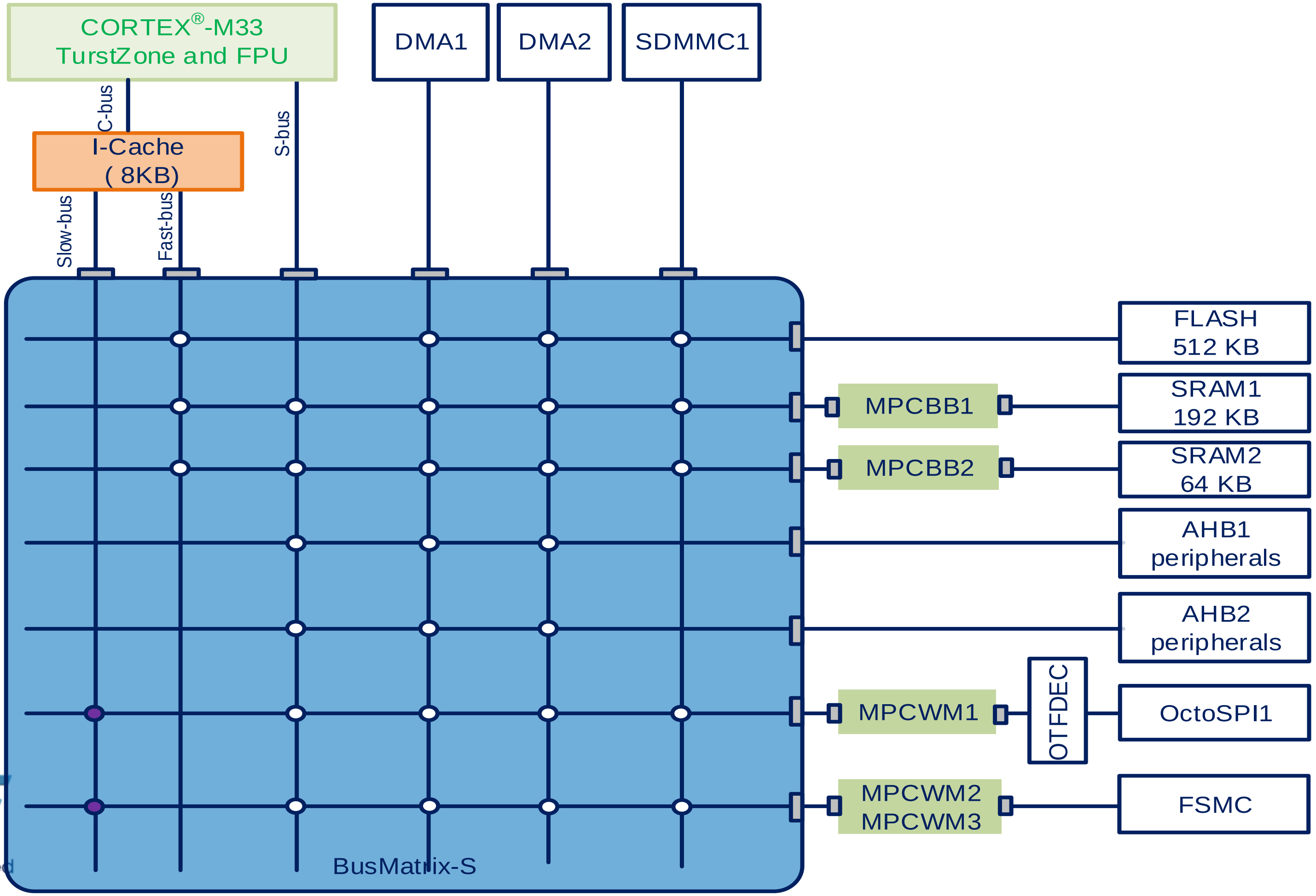
ST Restricted

STM32L5 System Architecture

ST Restricted

STM32L562xx/52xx System Architecture

32-bit multilayer AHB bus matrix, 6 Masters, 7 Slaves

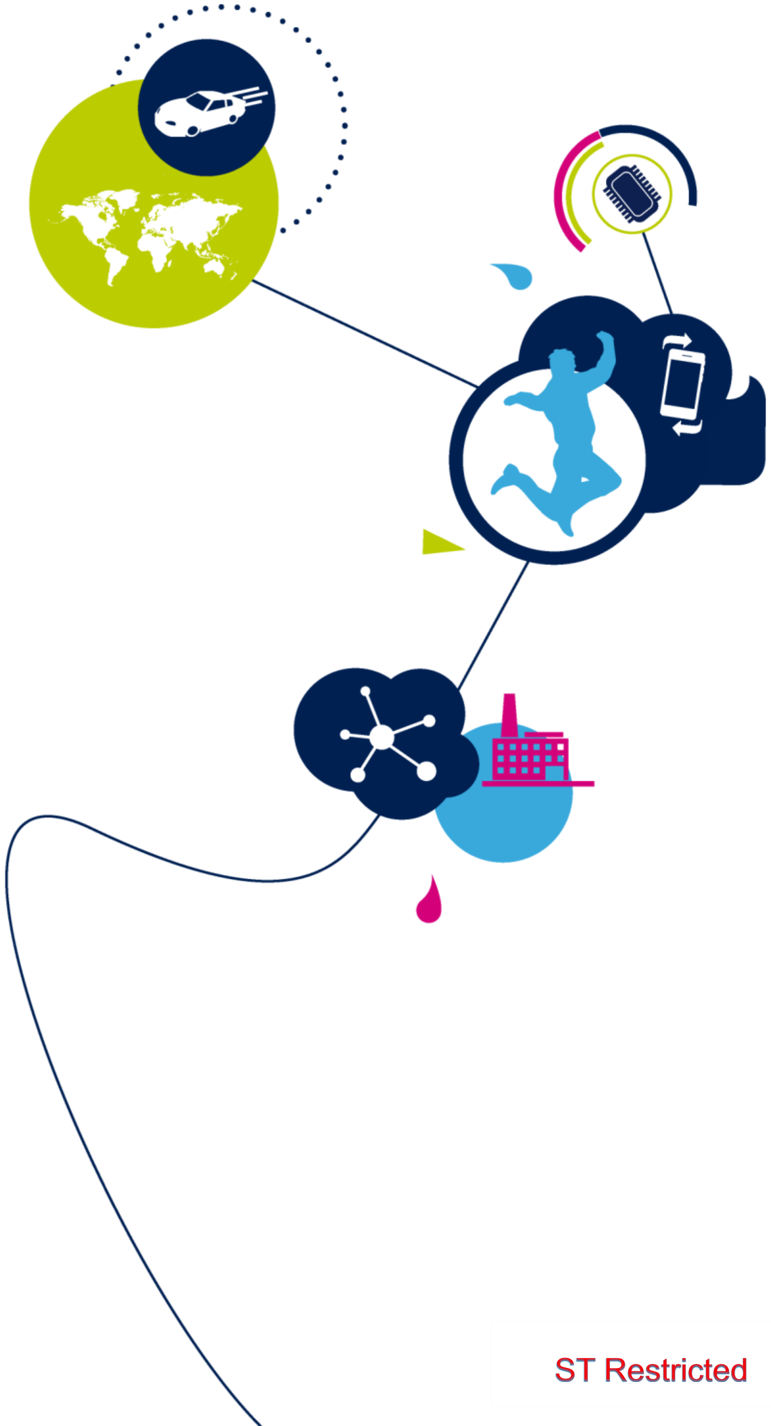


- ICACHE is a 8KB instruction cache, on C-AHB Code bus of Cortex®-M33 to improve performance when fetching instruction (or data) from internal or external memories.
- Remapping logic allows any internal or external memory range to be cached.

MPCBBx: Memory protection controller bloc based
MPCWMx: Memory protection controller Watermark

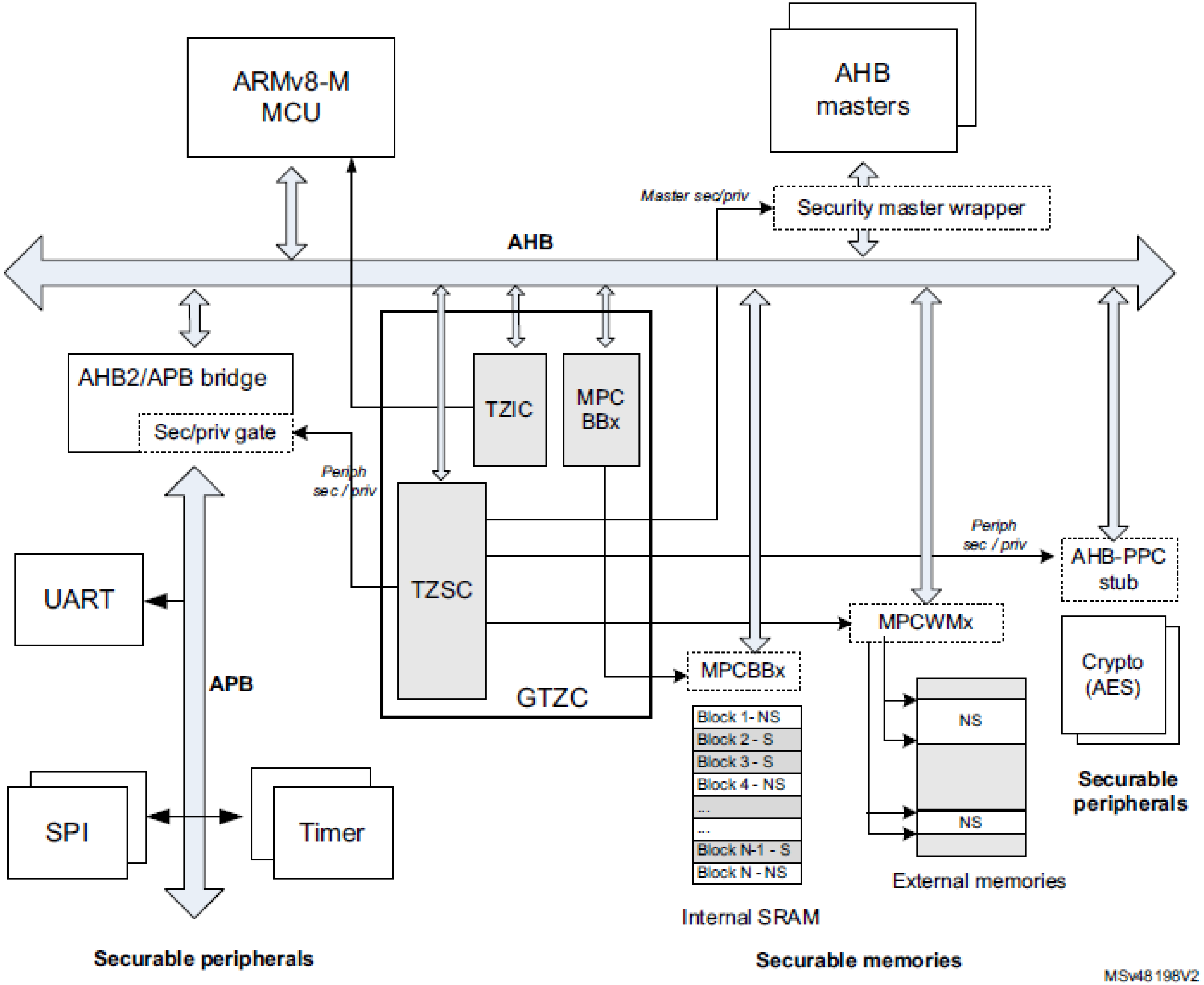
GTZC

TZSC / MPC-BB / TZIC

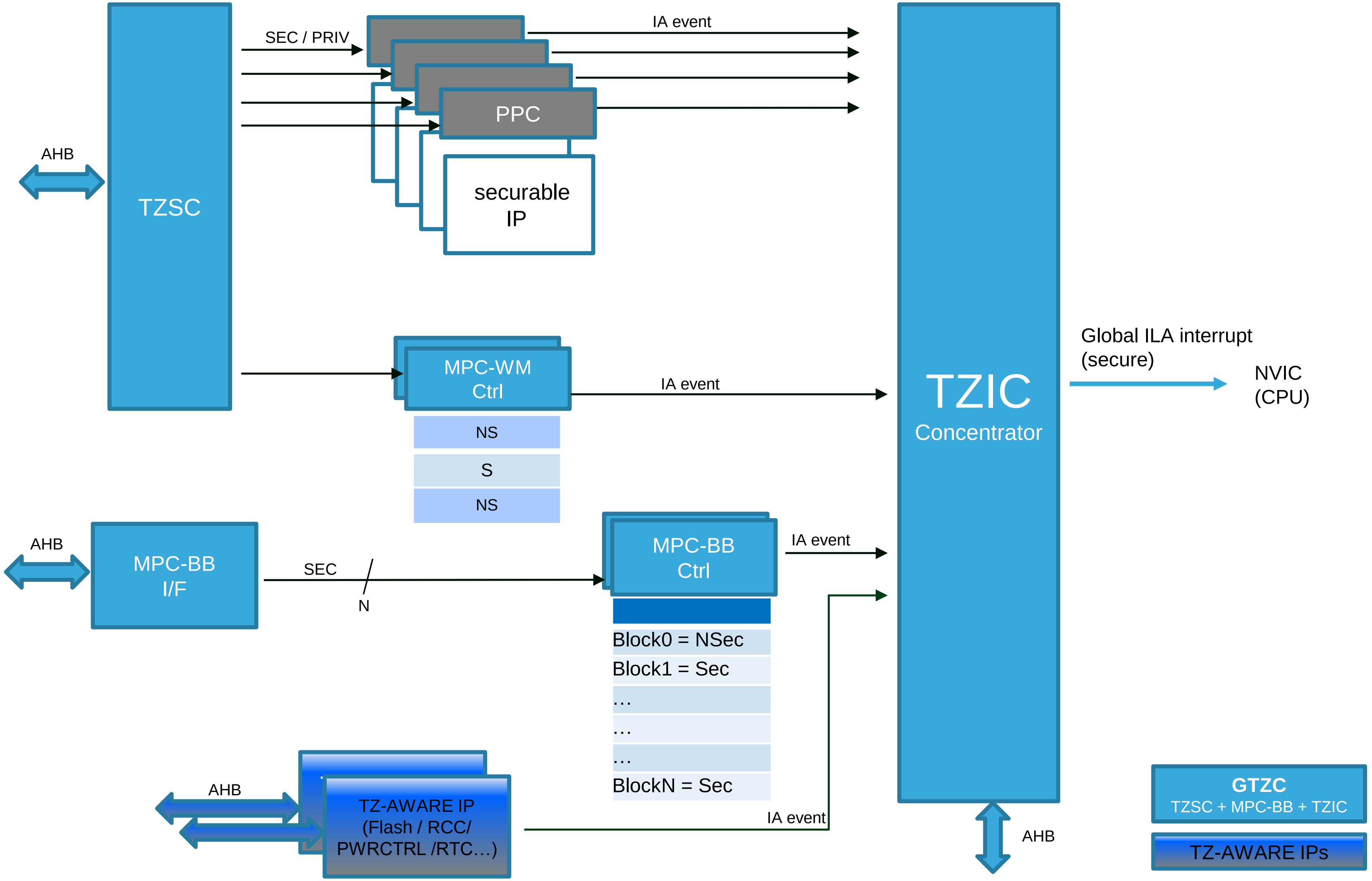


life.augmented

GTZC in ARMv8-M subsystem block diagram



GTZC – MPCBB – TZ aware



Embedded FLASH

Flash memory : Features

- Up to 512 Kbytes : 128pages
  - Single Bank: Page size = 4 Kbytes,
  - Dual Bank: Page size = 2 Kbytes
- 512 bytes OTP (one-time programmable)
- Flash memory read operations with two data width modes:
  - Single bank mode DBANK=0: read access of 128 bits
  - Dual bank mode DBANK=1: read access of 64 bits
- TrustZone security support
  - Flash security area is defined by watermark user options or block based configuration register

Flash memory : TrustZone Security

- Secure watermark-based area by option bytes
  - Single Bank: 2 secure watermarked areas
  - Dual Bank: 1 secure watermarked area **per bank**
- Secure or non-secure block-based areas
  - Any page can be configured as secure /non secure
- Erase/program in secure and non-secure mode
  - Non-secure and Secure register
- Secure and non-secure interrupts

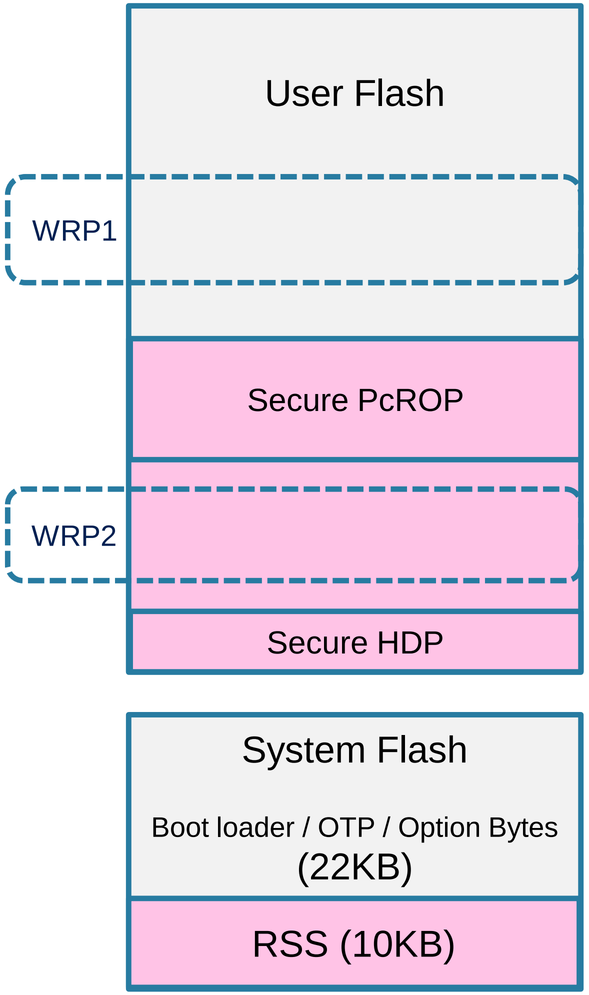
New

STM32L5
FLASH I/F

ST Restricted

FLASH features overview

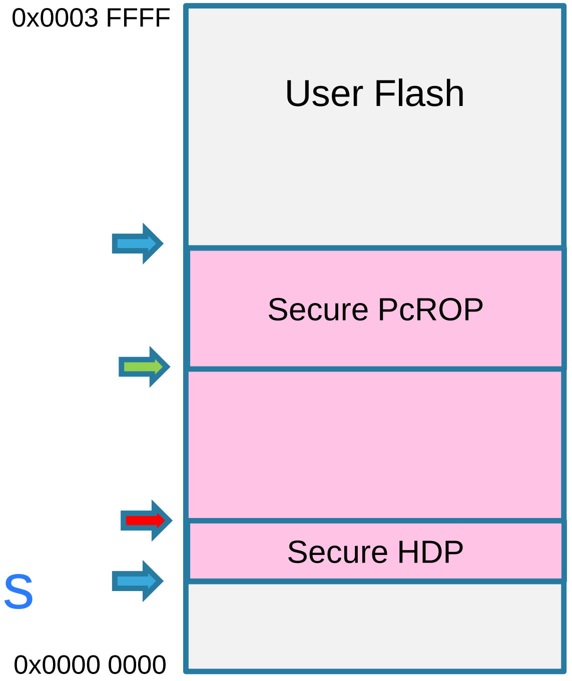
- Up to 512 KB with dual bank (RWW)
- Memory Organization
  - dual bank
  - main memory: up to 512MB (128 x 2KB pages)
  - System memory: 32KB (16 x 2KB pages)
- 2 write protection area per bank (n x2KB)
- Trustzone support
  - 1 secure area per bank including:
    - 1 secure PcROP area
    - 1 secure HDP area
  - Block based security attribute (volatile)
- Bank swapping
- ECC support (SECDED)
  - 8 bits per 64-bits double word



Secure areas (WM) - non-volatile settings (option bytes)

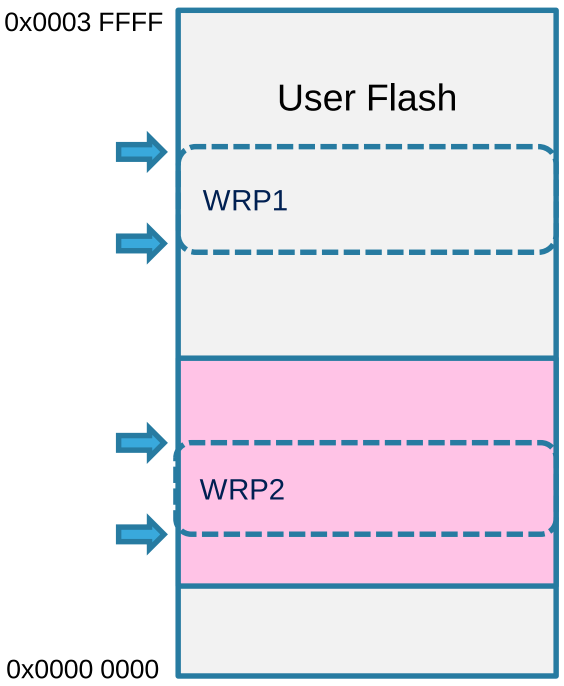
- Secure watermark area
  - Start and End addresses defined in secure option bytes
- Secure PcROP area
  - Start @ defined in secure option bytes
  - End @ same as Secure area
- Secure Hide protection area
  - Start @ same as Secure area one
  - End @ defined in secure option bytes

All area definition are aligned on number of pages



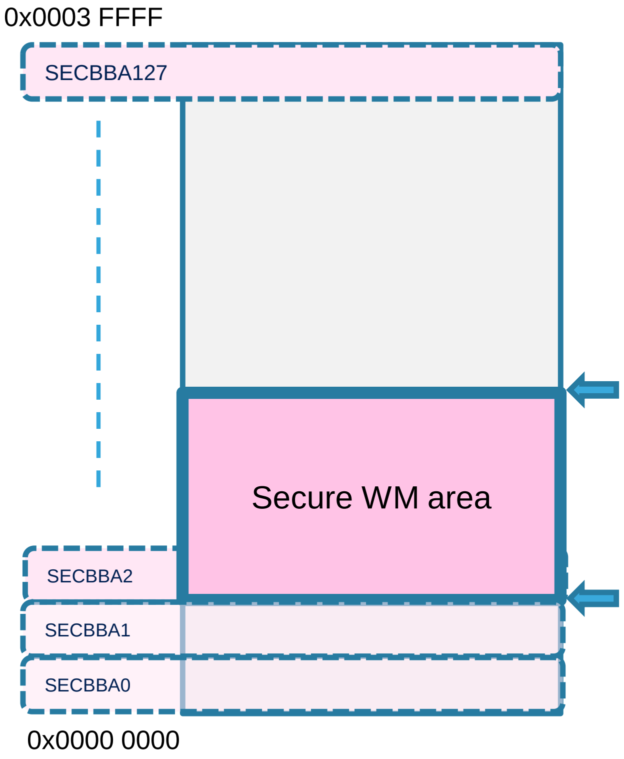
Write protection areas - non volatile settings (option bytes)

- 2 independent WRP areas
  - Start and End addresses defined in option bytes
  - Always aligned on number of pages
  - Write protection attribute orthogonal to other settings (Secure / HDP / PcROP)



Bloc based security attribute – volatile settings

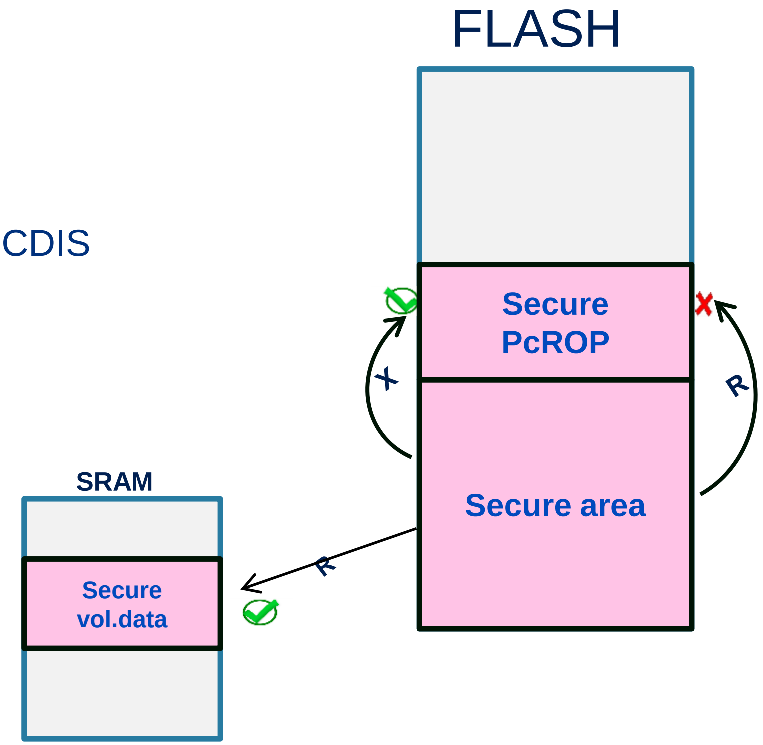
- Any 2KB flash page (bloc) can be set as secure/non-secure thanks to dedicated secure registers in the flash interface (SECBBXA/Bn)
- At reset all SECBBA/Bn registers are cleared (non-secure)
- Setting a page as secure, which already belongs to the secure watermark area, will have no effect



PcROP

- PcROP Properties
  - Only secure fetch/execute access permitted
  - PCROP area is activated by setting the PCROPEN option bit
  - PCROP size and PCROPEN can only be modified while HDP1_ ACCDIS register bit is reset
- Benefits
  - FW IP protection
  - Mutual protection of secure FW IPs
- constraints
  - Specific compilation option required

    (no literal pool / execute only)
  - Small impact on Code size & performance



Hide Protection area (aka sticky)

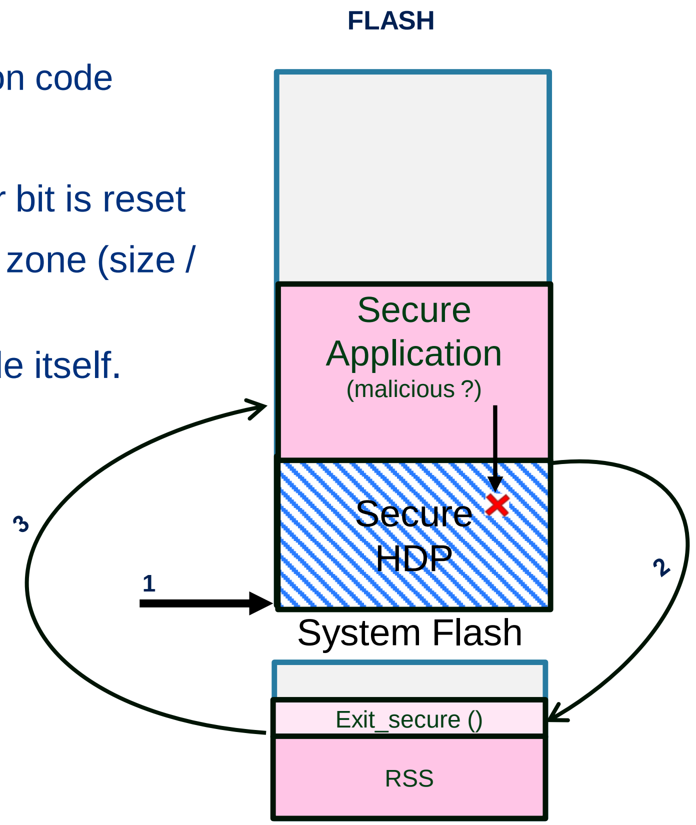
- SECURE HDP Memory Properties
  - Enable isolation of secure boot code & data (secrets) from (secure) application code
  - HDP area is activated by setting the HDPEN option bit
  - HDP size and HDPEN can only be modified while HDP1_ ACCDIS register bit is reset
  - Once the HDP1_ ACCDIS is set, no more operation are permitted on HDP zone (size / R / W / Erase)

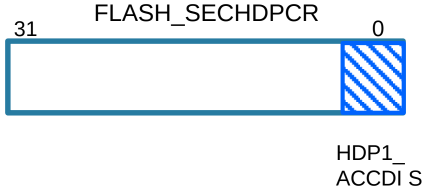
  => Any page belonging to the HDP area can only be erased by the HDP code itself.

- How it works ?

  1. System Boots and execute HDP area (sensitive code)
  2. Call HDP exit function (immutable in RSS lib)
     → Disable / Hide secure HDP area until next reset
  3. Exit function will branch to (secure) application code
  4. (secure) FW can not access any more securable HDP area

- Benefits
  - Easy & Efficient boot code/secrets isolation





ST Restricted

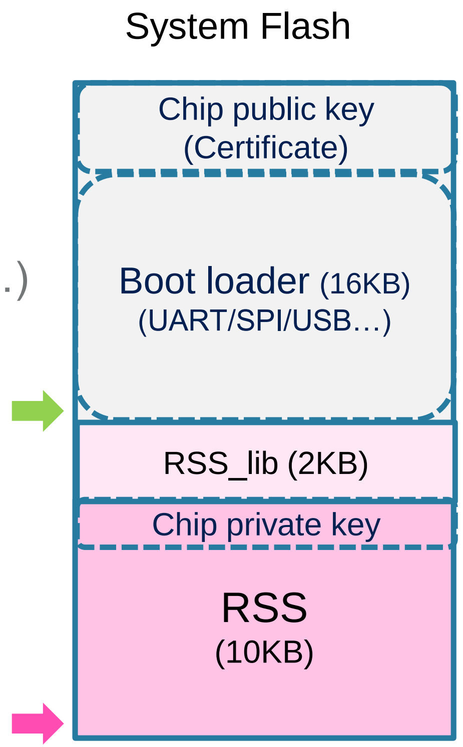
RSS – Root Security Services

RSS

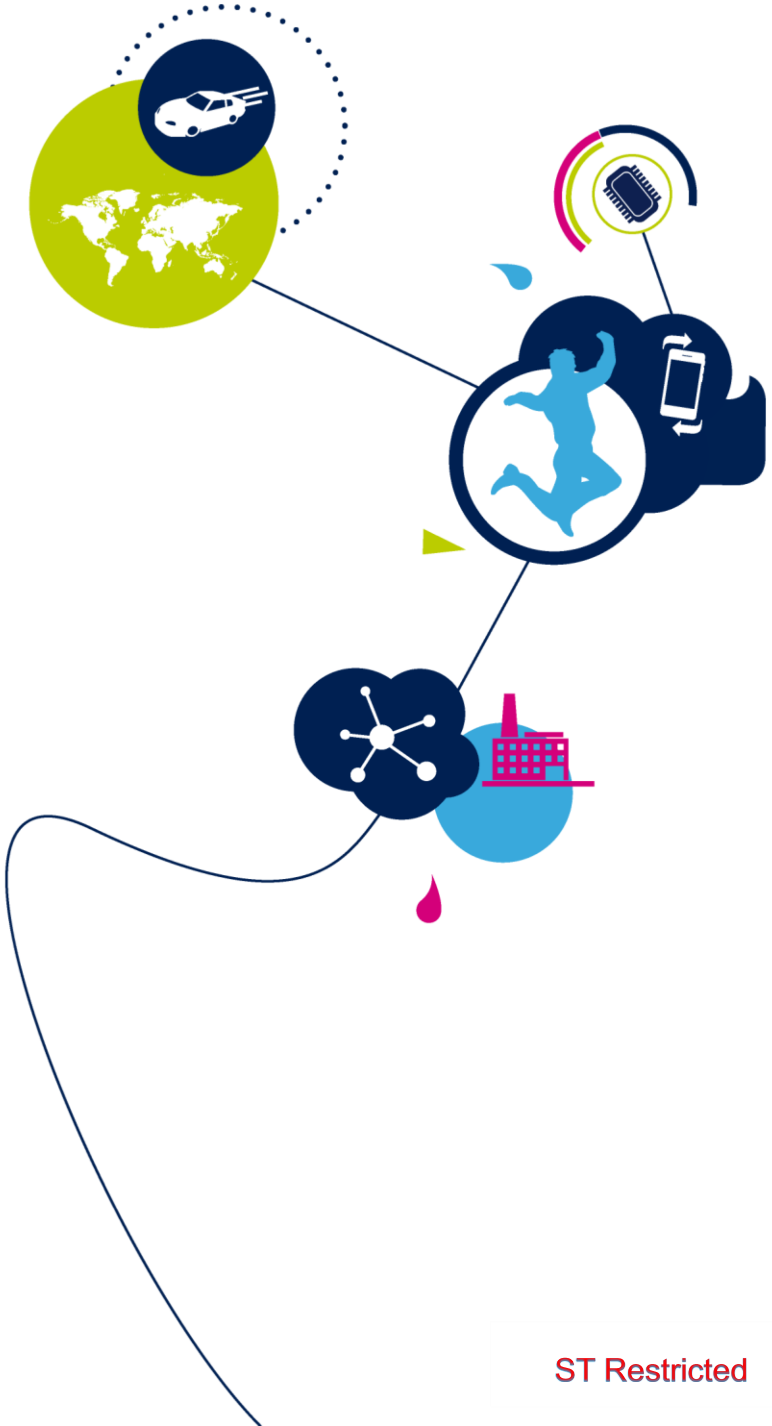
- SYSTEM FLASH (aka Information bloc)
  - Immutable (=ROM)
  - Root Security Services

    A) RSS_boot (sticky property- HDP like)
    - Unique entry point
    - Provide set of security services available at reset (SFI / SMI / …)

    B) RSS_lib
    - Multiple entry points (Trusted ST APIs)
    - Provide set of security services callable by User code
  - Boot Loader
    - Unique entry point
    - Classic bootloader functions
  - Provisionning
    - Pair of chip public/private key
    - Certificate (genuine STM32) + UID


System Flash
Chip public key (Certificate)
Boot loader (16KB) (UART/SPI/USB…)
RSS_lib (2KB)
Chip private key
RSS (10KB)

STM32L5
Device Life Cycle (RDP)

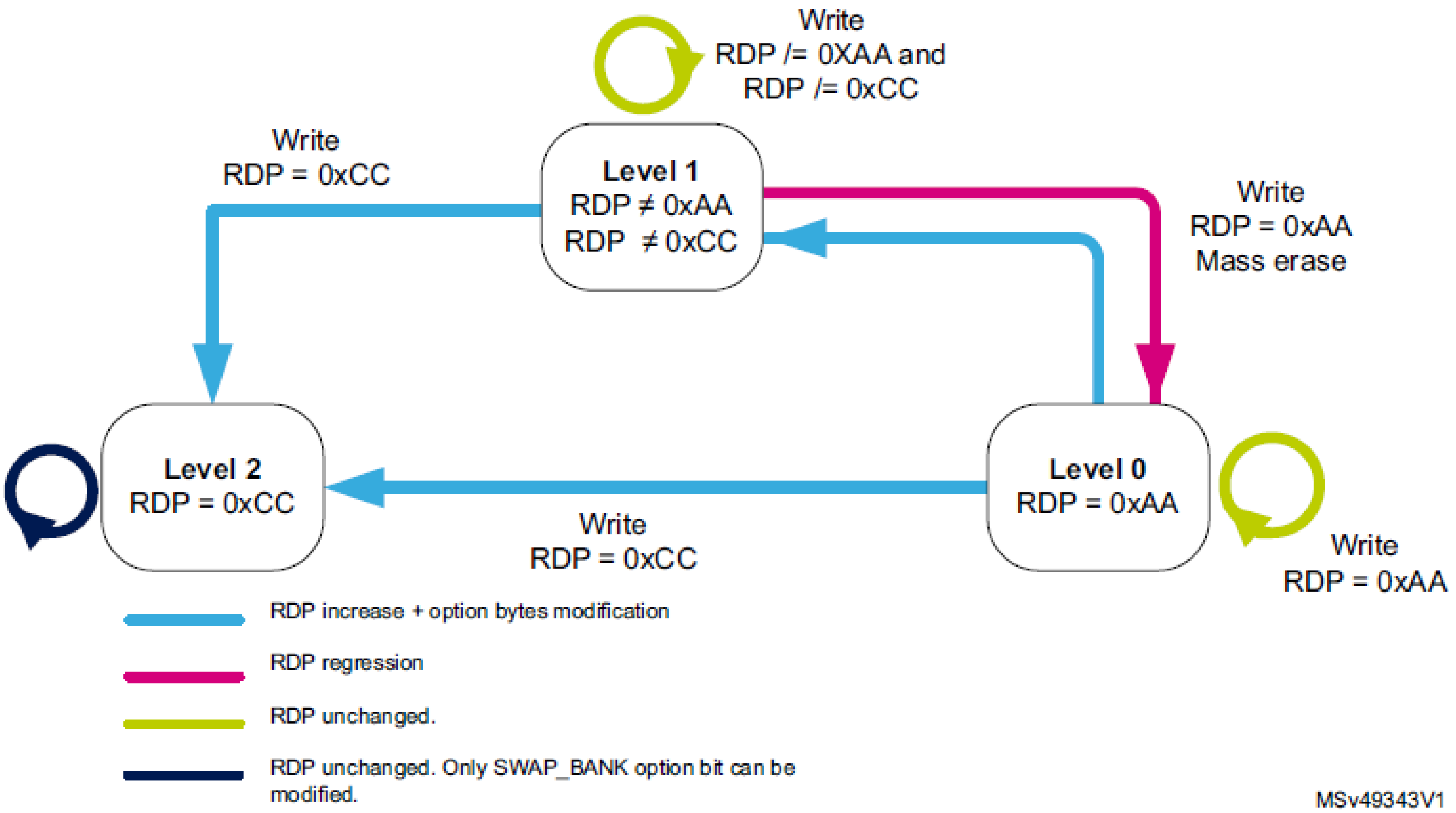


life.augmented

ST Restricted

TZEN =0

- Legacy mode



Write
RDP /= 0XAA and
RDP /= 0xCC

Write
RDP = 0xCC

Level 1
RDP ≠ 0xAA
RDP ≠ 0xCC

Write
RDP = 0xAA
Mass erase

Level 2
RDP = 0xCC

Level 0
RDP = 0xAA

Write
RDP = 0xCC

Write
RDP = 0xAA

🟦 RDP increase + option bytes modification

🟥 RDP regression

🟩 RDP unchanged.

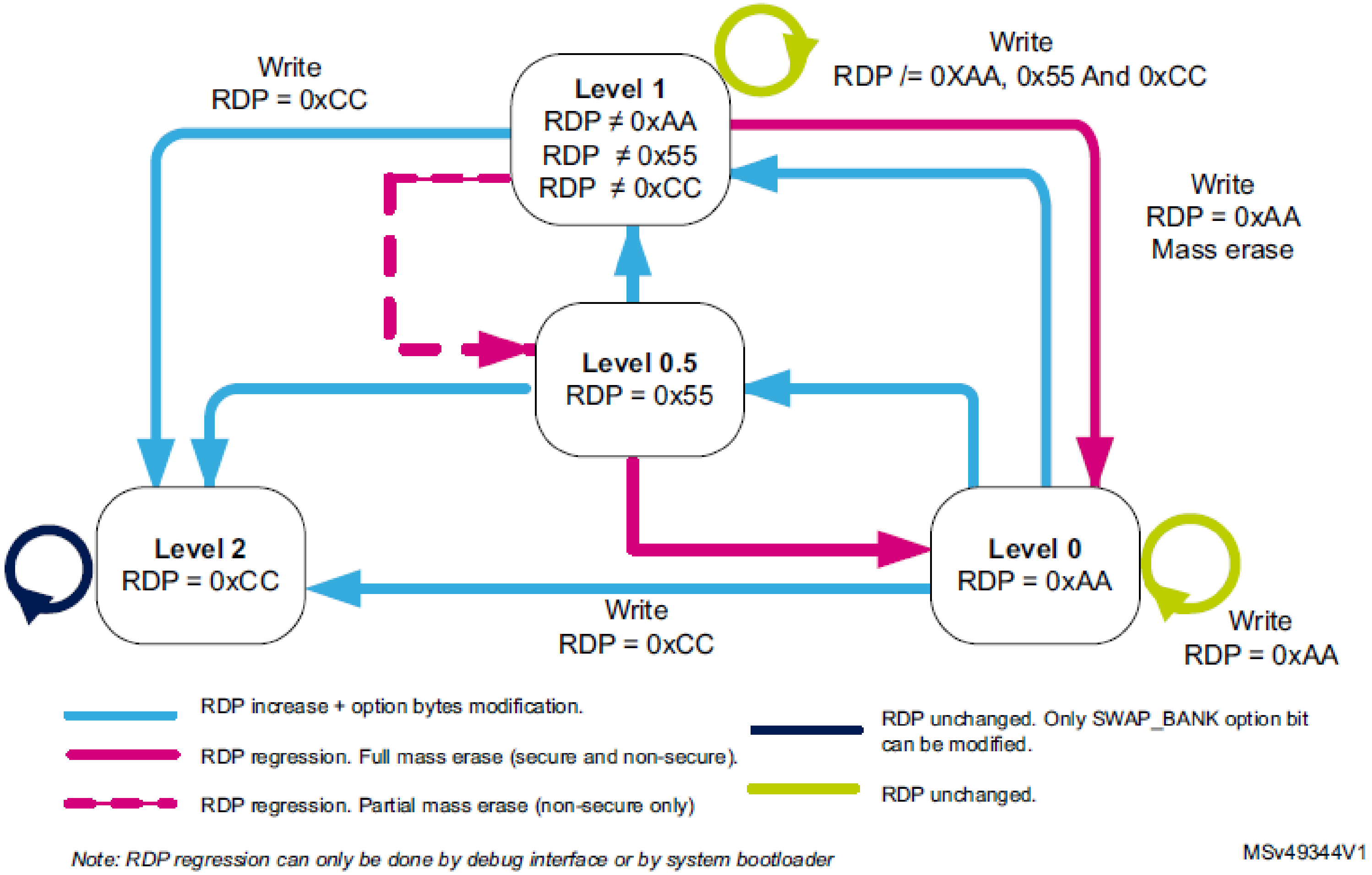
⬛ RDP unchanged. Only SWAP_BANK option bit can be modified.

MSv49343V1

ST Restricted

TZEN =1

- Trustzone enabled mode
  - Additional RDP level


Level 1
RDP ≠ 0xAA
RDP ≠ 0x55
RDP ≠ 0xCC
Write
RDP = 0xCC
Write
RDP /= 0XAA, 0x55 And 0xCC
Write
RDP = 0xAA
Mass erase
Level 0.5
RDP = 0x55
Level 2
RDP = 0xCC
Level 0
RDP = 0xAA
Write
RDP = 0xCC
Write
RDP = 0xAA
RDP increase + option bytes modification.
RDP regression. Full mass erase (secure and non-secure).
RDP regression. Partial mass erase (non-secure only)
RDP unchanged. Only SWAP_BANK option bit can be modified.
RDP unchanged.
MSv49344V1

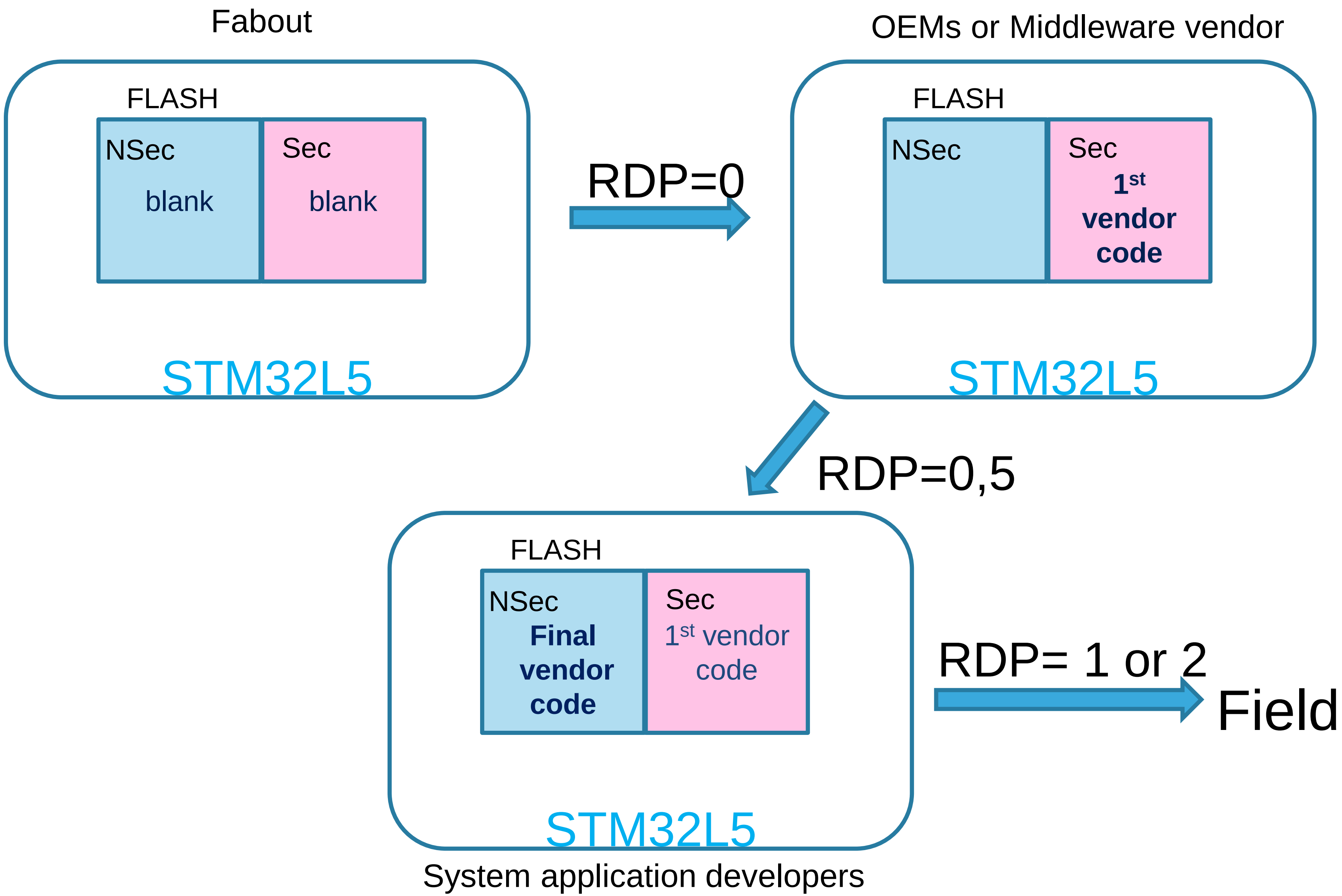
Note: RDP regression can only be done by debug interface or by system bootloader

RDP level summary TZEN=1

Protection Level	Properties	Comments
Level 0	**DEVICE OPEN**	- No debug restriction (secure and non-secure) - Boot @ must target a <u>secure</u> area - Boot on secure SRAM, FLASH, SYSTEM FLASH (RSS) possible
Level 0,5	**DEVICE PARTIALLY CLOSED** **NO SECURE DEBUG**	- Non-secure debug only - NS-Flash access allowed (w\ debug connection) - Boot @ must target secure user flash - Boot on SRAM not permitted
Level 1	**DEVICE MEMORIES PROTECTED** **NO SECURE DEBUG** **FLASH + SRAM2 + Backup_Reg PROTECTED**	- Non-secure debug only - Flash access **<u>not allowed</u>** (w\ debug connection) - Boot @ must target secure user flash
Level 2	**CLOSED DEVICE** **(No JTAG)** **NO OPTION BYTE CHANGE**	- No debug (JTAG fuse) - Boot @ in secure user flash

Debug = invasive and non-invasive debug

Protection of a first 3rd party vendor from a final one



Encryption/ Decryption Authentification

Encryption/ Decryption Authentification

- The STM32L5 embeds:
  - True random number generator
  - 96-bit unique ID
  - Encryption hardware accelerator: AES(128/256-bit key)
  - HASH processor, fully compliant of the secure hash algorithm (SHA-1, SHA-224, SHA-256), the MD5 hash algorithm and the HMAC
  - Public Key Acceleration (PKA): acceleration for RSA, Diffie-Hellmann or ECC (Elliptic Curve Cryptography)
  - OTFDEC (On-the-fly decryption engine)

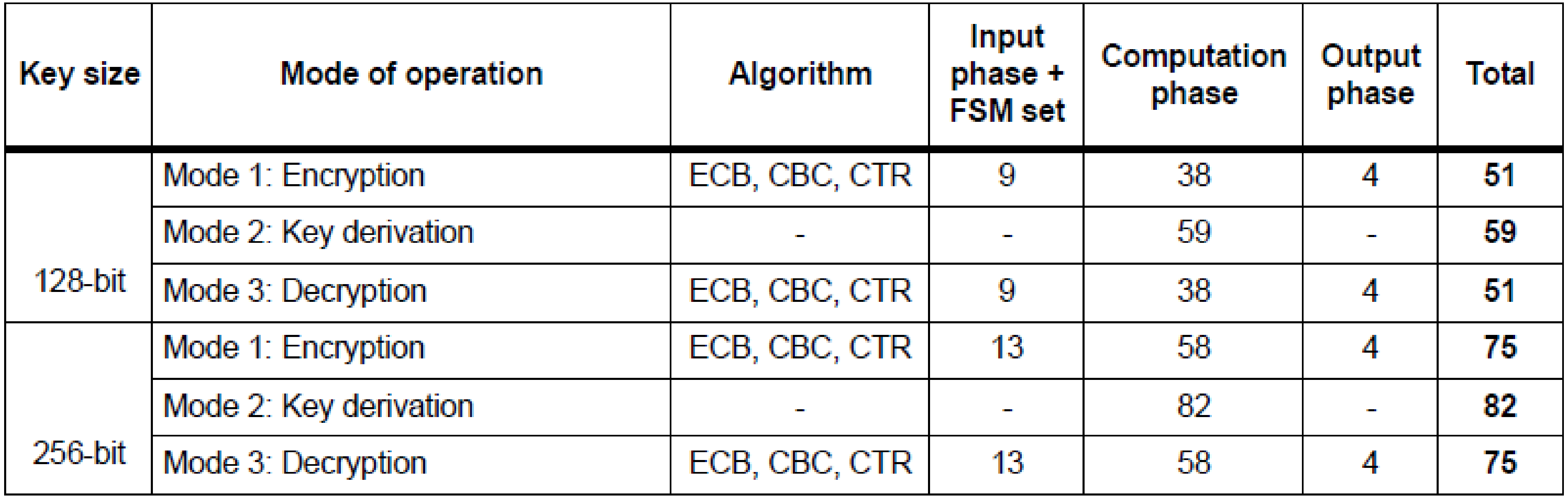
New

AES HW accelerator

- 128-bit data block processing
- Support for cipher key lengths of 128-bit and 256-bit
- Multiple chaining modes are supported
  - ECB, CBC, CTR, GCM, GMAC, CCM
- The AES accelerator is a 32-bit AHB peripheral. It supports DMA single transfers for incoming and outgoing data
- 51 or 75 clock cycle latency in ECB mode for processing one 128-bit block of data with, respectively, 128-bit or 256-bit key

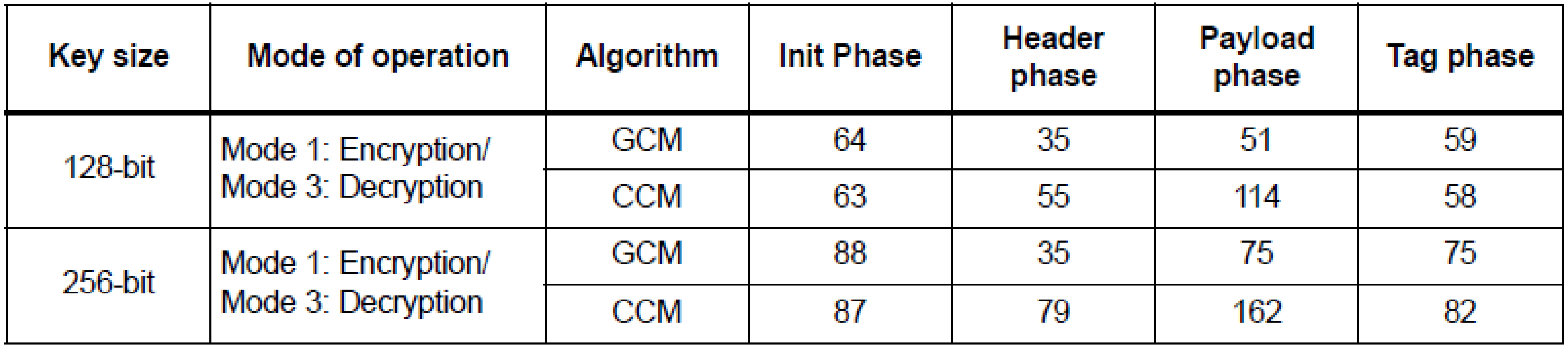
AES processing latency

Table 205. Processing latency (in clock cycle) for ECB, CBC and CTR



Key size	Mode of operation	Algorithm	Input phase + FSM set	Computation phase	Output phase	Total
128-bit	Mode 1: Encryption	ECB, CBC, CTR	9	38	4	**51**
	Mode 2: Key derivation	-	-	59	-	**59**
	Mode 3: Decryption	ECB, CBC, CTR	9	38	4	**51**
256-bit	Mode 1: Encryption	ECB, CBC, CTR	13	58	4	**75**
	Mode 2: Key derivation	-	-	82	-	**82**
	Mode 3: Decryption	ECB, CBC, CTR	13	58	4	**75**

Table 206. Processing latency for GCM and CCM (in clock cycle)

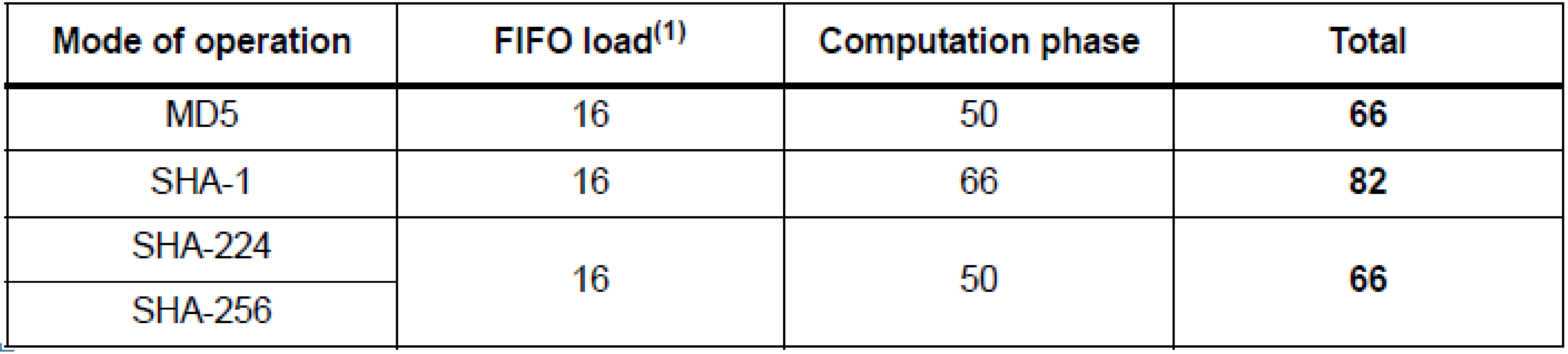


Key size	Mode of operation	Algorithm	Init Phase	Header phase	Payload phase	Tag phase
128-bit	Mode 1: Encryption/ Mode 3: Decryption	GCM	64	35	51	59
		CCM	63	55	114	58
256-bit	Mode 1: Encryption/ Mode 3: Decryption	GCM	88	35	75	75
		CCM	87	79	162	82

Hash processor

- Fully compliant of the secure hash algorithm
  - SHA-1 and SHA-2 family
  - MD5
  - HMAC

- Fast computation of SHA-1, SHA-224, SHA-256, and MD5



Mode of operation	FIFO load[1]	Computation phase	Total
MD5	16	50	**66**
SHA-1	16	66	**82**
SHA-224	16	50	**66**
SHA-256			

life.augmented

Public key accelerator (PKA)

- Acceleration of RSA, DH and ECC over GF(p) operations, based on the Montgomery method for fast modular multiplications.
  - RSA modular exponentiation
  - RSA Chinese Remainder Theorem (CRT) exponentiation
  - ECC scalar multiplication, point on curve check
  - ECDSA signature generation and verification
- Capability to handle operands up to 3136 bits for RSA/DH and 640 bits for ECC.
- Arithmetic and modular operations such as addition, subtraction, multiplication, modular reduction, modular inversion, comparison, and Montgomery multiplication.
- Built-in Montgomery domain inward and outward transformations.

ST Restricted

PKA computation times

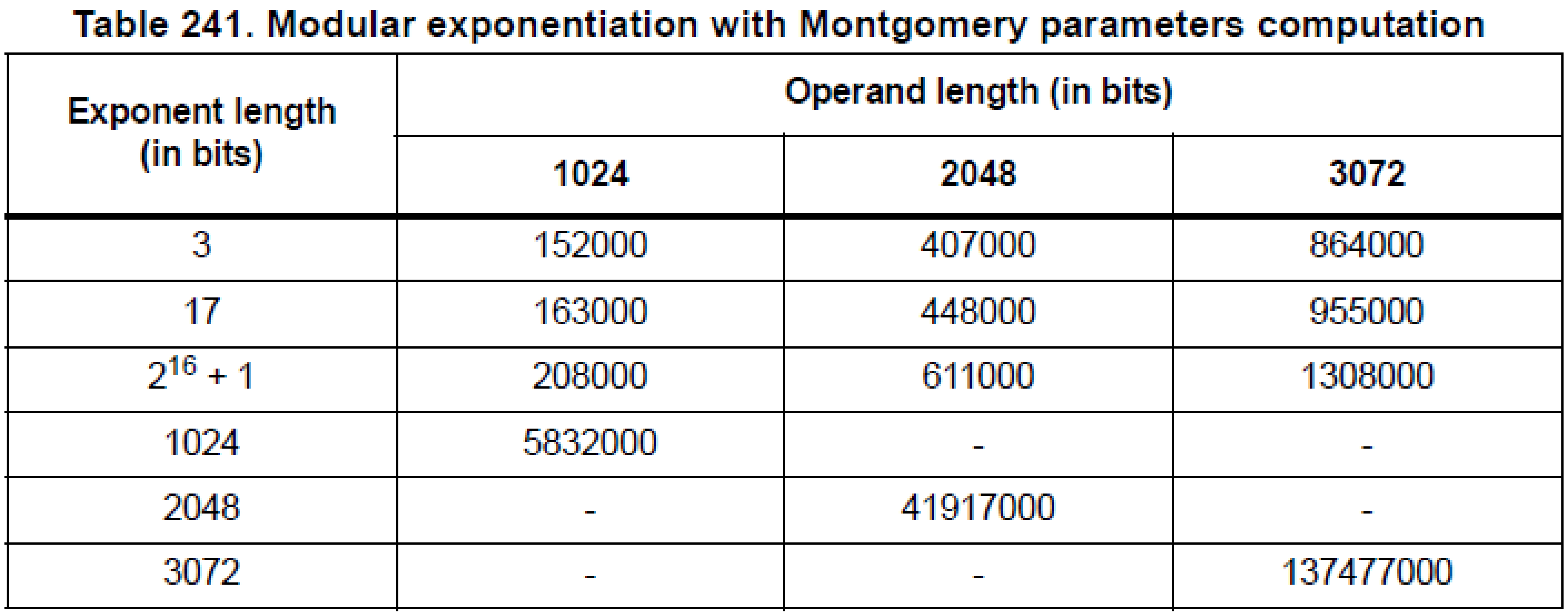


Table 241. Modular exponentiation with Montgomery parameters computation

Exponent length (in bits)	Operand length (in bits)		
	1024	2048	3072
3	152000	407000	864000
17	163000	448000	955000
$2^{16} + 1$	208000	611000	1308000
1024	5832000	-	-
2048	-	41917000	-
3072	-	-	137477000

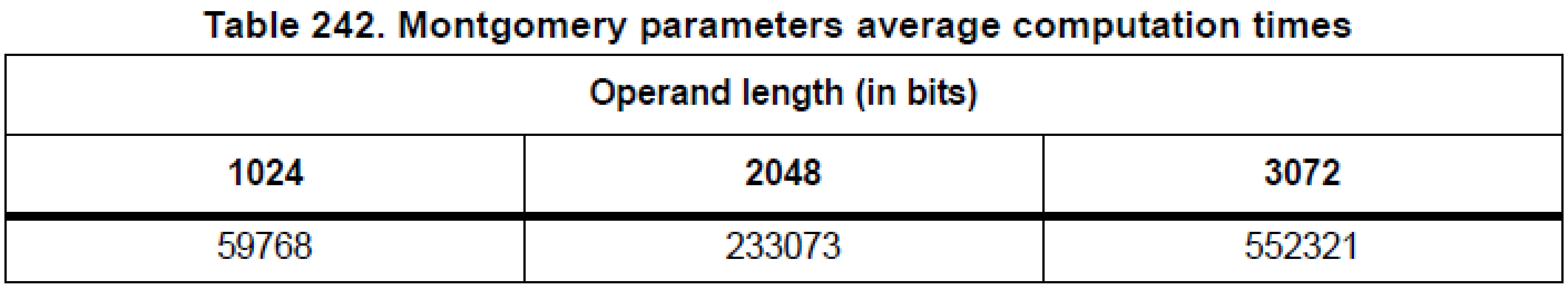


Table 242. Montgomery parameters average computation times

Operand length (in bits)		
1024	2048	3072
59768	233073	552321

PKA computation times

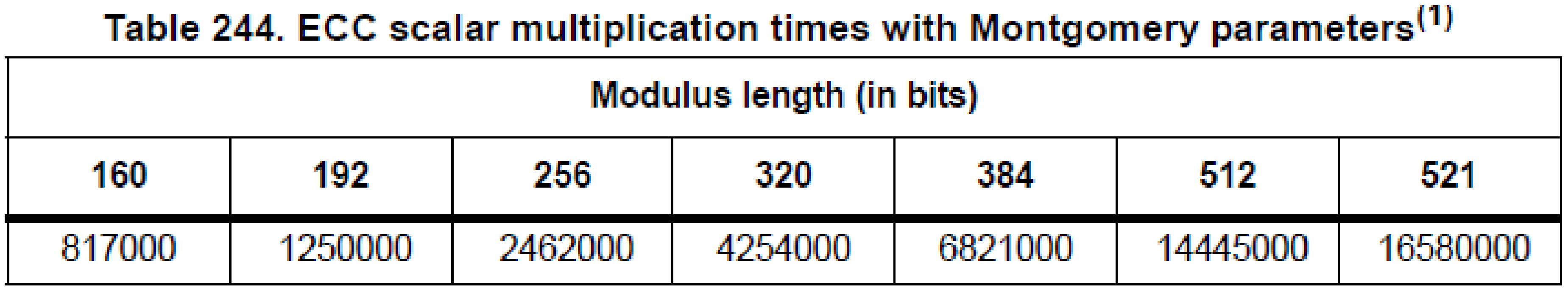


Table 244. ECC scalar multiplication times with Montgomery parameters[1]

Modulus length (in bits)						
160	192	256	320	384	512	521
817000	1250000	2462000	4254000	6821000	14445000	16580000

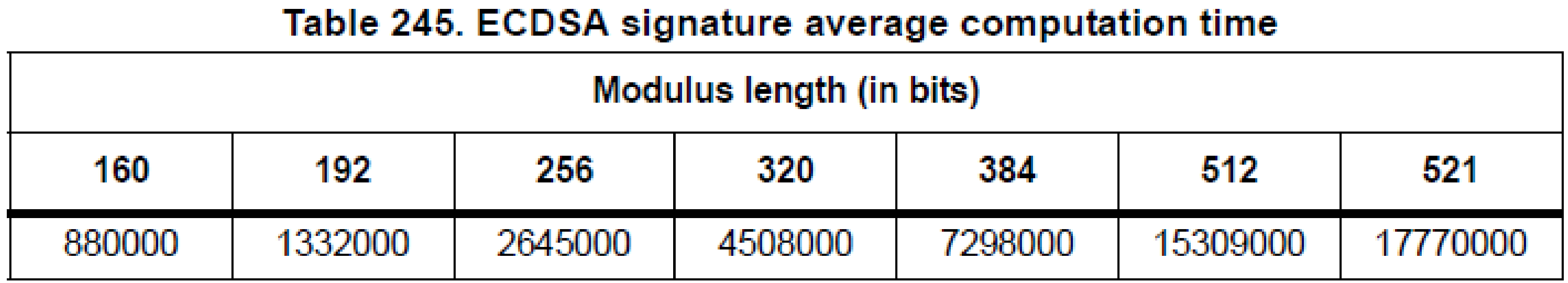


Table 245. ECDSA signature average computation time

Modulus length (in bits)						
160	192	256	320	384	512	521
880000	1332000	2645000	4508000	7298000	15309000	17770000

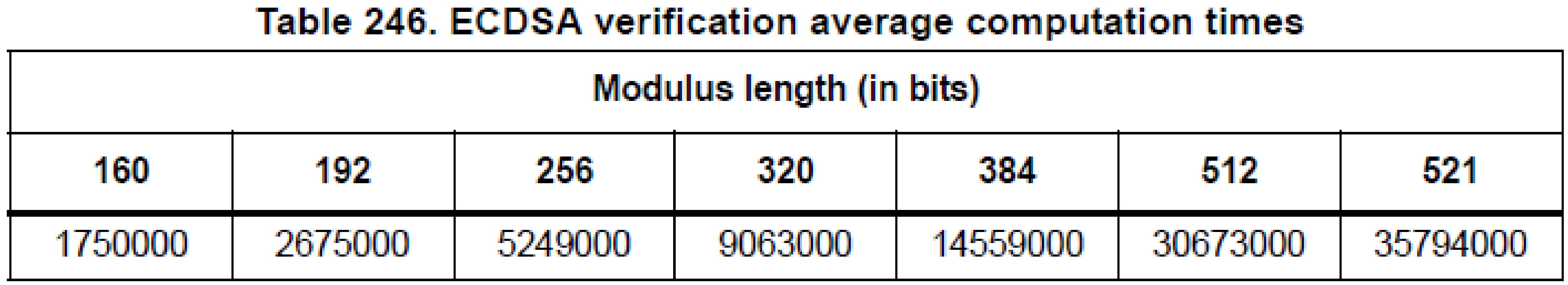


Table 246. ECDSA verification average computation times

Modulus length (in bits)						
160	192	256	320	384	512	521
1750000	2675000	5249000	9063000	14559000	30673000	35794000

On-the-fly decryption engine (OTFDEC)

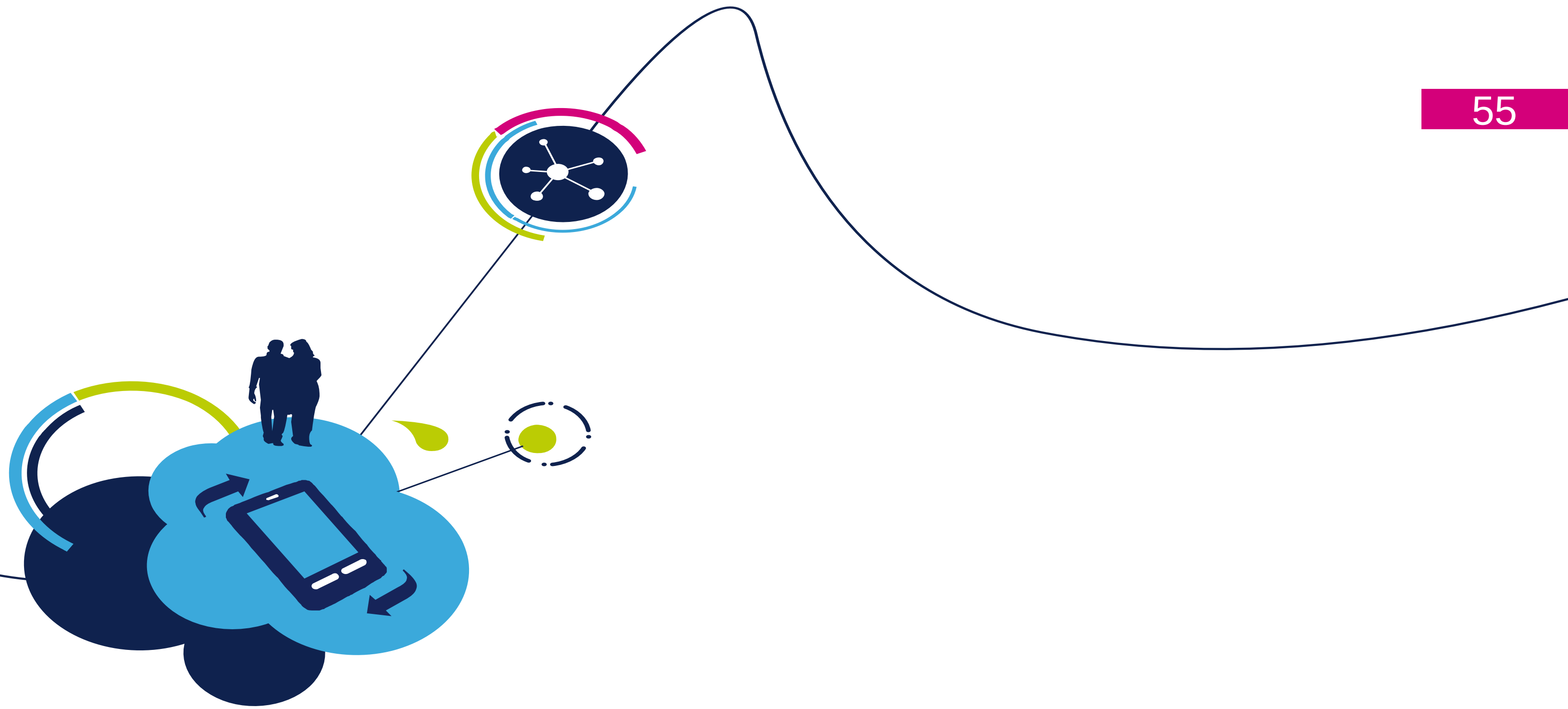
- The embedded OTFDEC decrypts in real-time the encrypted content (AES) stored in the external OctoSPI memories used in Memory-mapped mode
- 2 modes:
  - Standard AES
  - Enhanced

New

DMA

DMA

- 2 x DMA with 2 x 8 channels,
- Privileged/unprivileged mode
  - Support of privileged/unprivileged DMA transfers independently at a channel level
- TrustZone Security
  - Support of secure/non-secure DMA transfers independently at a channel level first and independently at source and destination address
  - TrustZone-aware AHB slave port, protecting any secure register from a non-secure software access
- DMAMUX TrustZone aware as DMA
- 2 interrupts entries
  - DMAMUX1_IRQHandler_S (Secure)
  - DMAMUX1_IRQHandler (Non-secure/Legacy)



EXTI

EXTI

- All EXTI features of STM32L4
- TrustZone security support
  - Each EXTI event can be configured as secure
    - Associated input event configuration and control bits can only be modified and read by a secure access
    - a non-secure write access is discarded and a read returns 0. RAZ and WI
- Privileged/unprivileged mode selection
  - Each EXTI event can be configured as privileged
    - associated input event configuration and control bits can only be modified and read by a privilege access,
    - an unprivileged write access is discarded and a read returns 0. RAZ and WI

GPIO

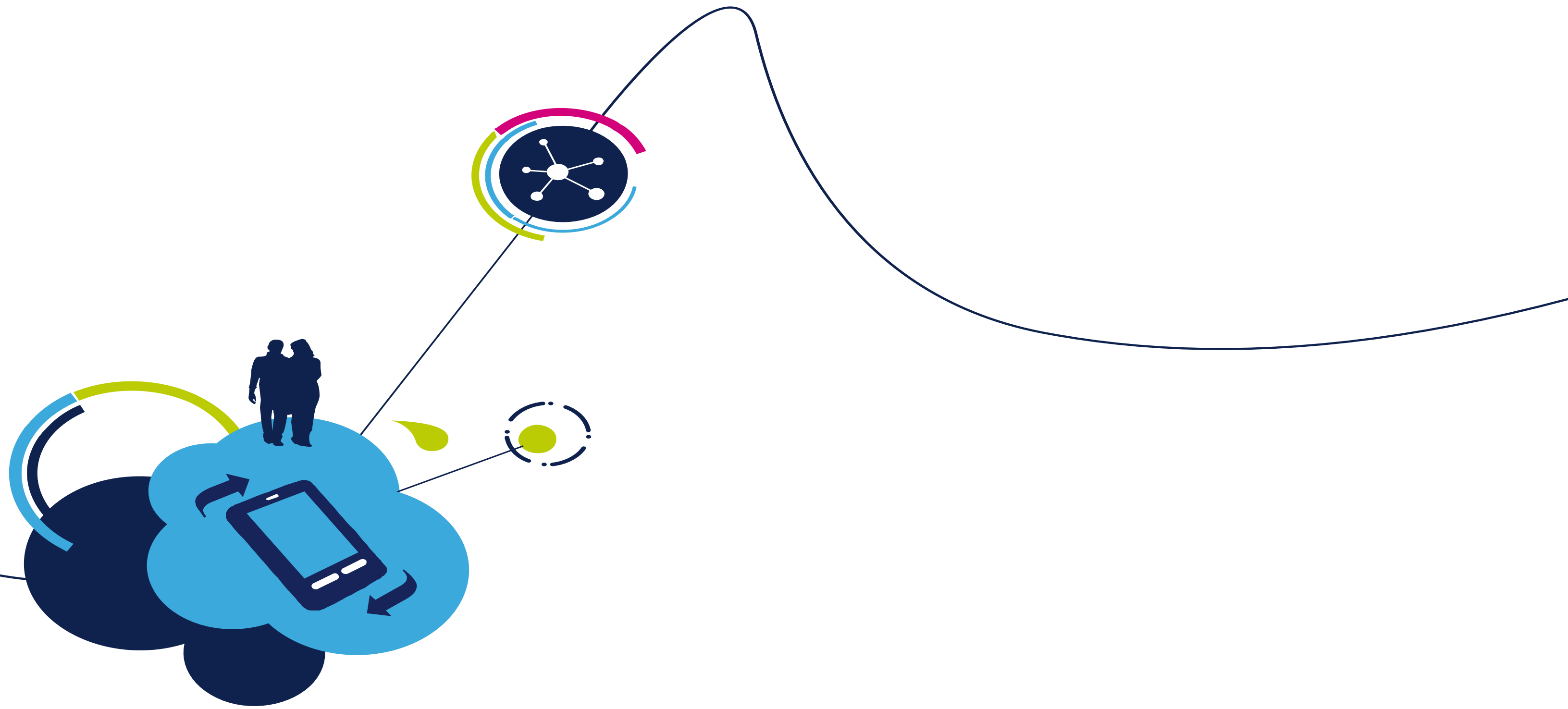
GPIO

- All GPIOs features of STM32L4
- TrustZone security support
  - Each I/O pin of GPIO port can be individually configured as secure/non-secure
  - After reset, all IOs of GPIO ports are secure
- Secure I/O pin
  - Alternate function AFI, AFO, mode selection configuration and I/O data are secure against a non-secure access
  - Input data are not redirected to another peripheral
  - Output data are not replaced by another peripheral
  - Secure I/O data can not be redirected to a non-secure I/O whatever the I/O is configured as alternate function or though peripherals as analog, USB, RTC, wakeup pins
  - Non-secure I/O data can not be redirected to a secure peripheral

ST Restricted

GPIO Privilege/Unprivileged mode

- All GPIO registers can be read and written by privileged and unprivileged accesses, whatever the security state secure or non-secure



Power Controller (PWR)

ST Restricted

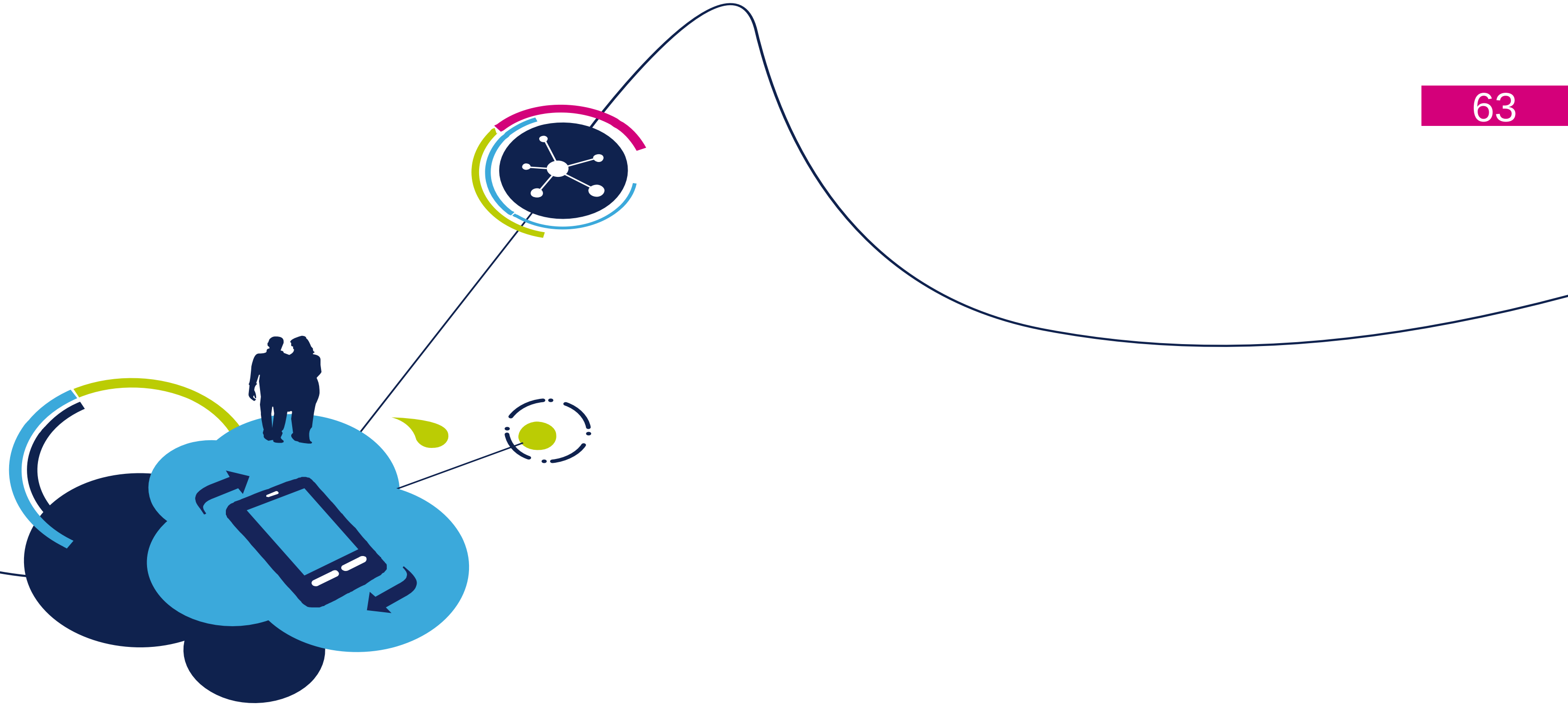
PWR: TrustZone Security

- Indedependant security bits to secure PWR fonctionalities:
    - Low-power mode
    - Wake-up (WKUP) pins
    - Voltage detection and monitoring
    - VBAT mode

- Additional PWR configuration bits are secure:
  - If System clock selection is secure in RCC secure it’s:
    - The voltage scaling (VOS) configuration **in PWR** is secure
  - If a GPIO is configured as secure
    - It’s corresponding bit **in PWR** for Pull-up/Pull-down configuration in Standby mode is secure
  - The RTC is secure,
    - The backup domain write protection DBP bit **in PWR** is secure.
  - The UCPD is secure,
    - The UCPD_DBDIS and UCPD_SDBY bits **in PWR** are secure.

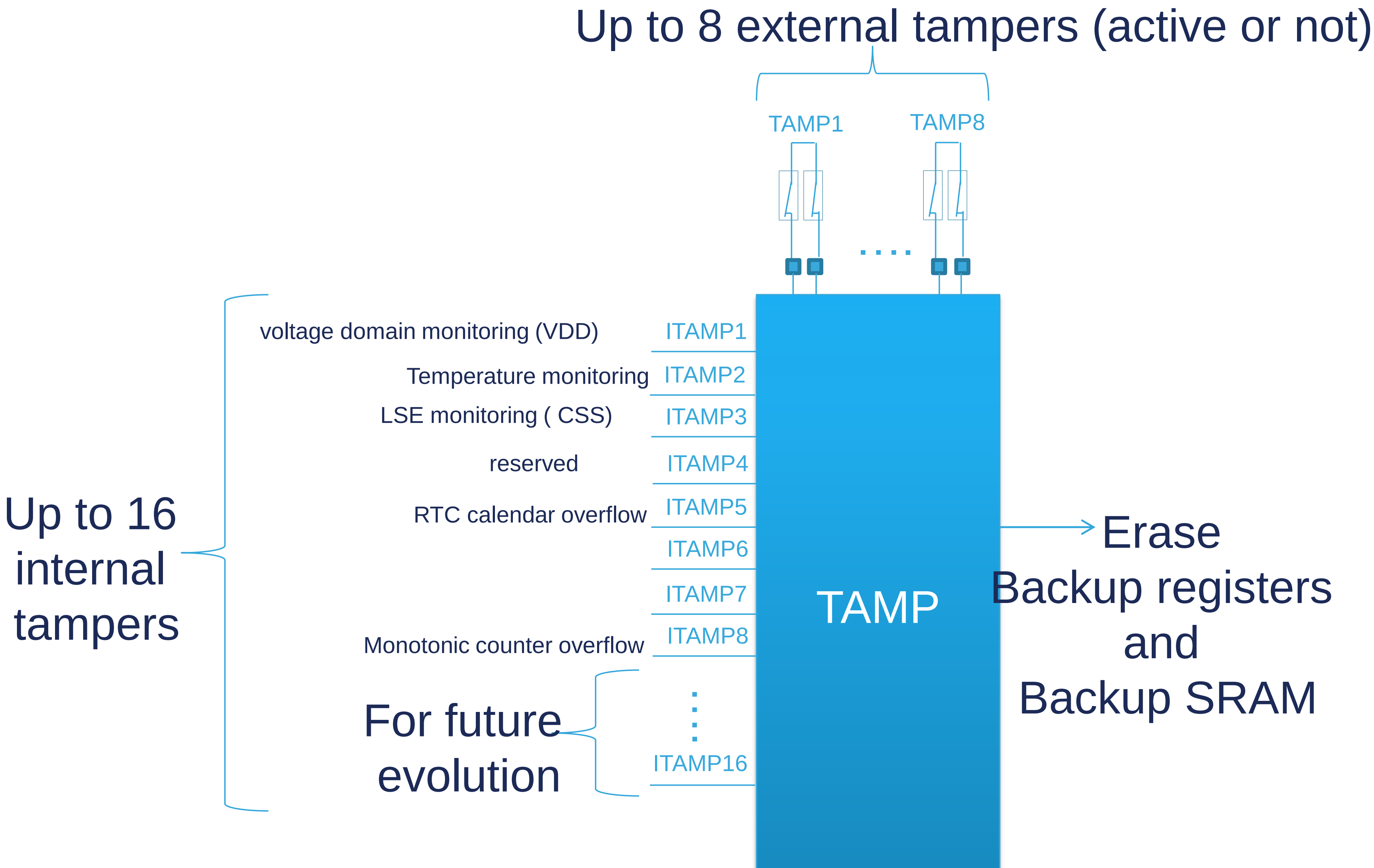
PWR Privilege mode

- Privilege/unprivileged mode
  - All PWR registres configuration can be set in Privilege mode
    - All PWR registers could be read and written by privileged access only except PWR_SR1, PWR_SR2 and PWR_SECFGR registers.
    - Unprivileged access to a privileged PWR registers is discarded. RAZ/WI.
    - If TrustZone is enabled, PRIV bit is secure.



RTC/TAMP

TAMP


Up to 8 external tampers (active or not)
TAMP1
TAMP8
....
Up to 16 internal tampers
voltage domain monitoring (VDD)
ITAMP1
Temperature monitoring
ITAMP2
LSE monitoring (CSS)
ITAMP3
reserved
ITAMP4
RTC calendar overflow
ITAMP5
ITAMP6
ITAMP7
Monotonic counter overflow
ITAMP8
For future evolution
ITAMP16
TAMP
Erase
Backup registers
and
Backup SRAM

RTC / TAMP

- RTC TrustZone support
  - Either RTC is fully securable
  - or RTC init, calibration, alarm A, alarm B, wakeup Timer and timestamp individual secure or non-secure configuration
- TAMP/Backup registers TrustZone support
  - Tamper secure or non-secure configuration
  - Backup registers configuration in 3 configurable-size areas:
    - 1 read/write secure area
    - 1 write secure/read non-secure area
    - 1 read/write non-secure area
- 2 interrupts entries for RTC (Alarm/Wake-up-timer)
  - RTC_IRQHandler_S (Secure) - gated by security state of RTC
  - RTC_IRQHandler   (Non-secure/Legacy)
- 2 interrupts entries for Tamper (Tamper)
  - TAMP_IRQHandler_S (Secure) - gated by security state of RTC
  - TAMP_IRQHandler   (Non-secure/Legacy)

Releasing Your Creativity

/STM32

@ST_World

community.st.com

life.augmented

www.st.com/STM32L5

ST Restricted