Hello, and welcome to this overview of security features present in the STM32MP13.

Key security features

Covered in this module

- Secure boot in ROM
- TrustZone protection controllers
  - Enhanced TrustZone Protection Controller (ETZPC)
  - TrustZone Address Space Controller (TZC)
- Hardware crypto features
- Enhanced life cycle management

Covered in another training modules

- Enhanced secure storage
  - STM32MP13 Enhanced key storage
- Cryptographic acceleration
  - STM32MP13 Secure AES coprocessor (SAES)
  - STM32MP13 Cryptographic processor (CRYP)
  - STM32MP13 Asymmetric crypto (ASYMCRYPTO)
  - STM32MP13 DDR Memory Cypher Engine (DDRMCE)
- Active tamper and protection against temperature, voltage and frequency attacks
  - STM32MP13 Enhanced anti-tamper (ANTITAMP)

life.augmented

2

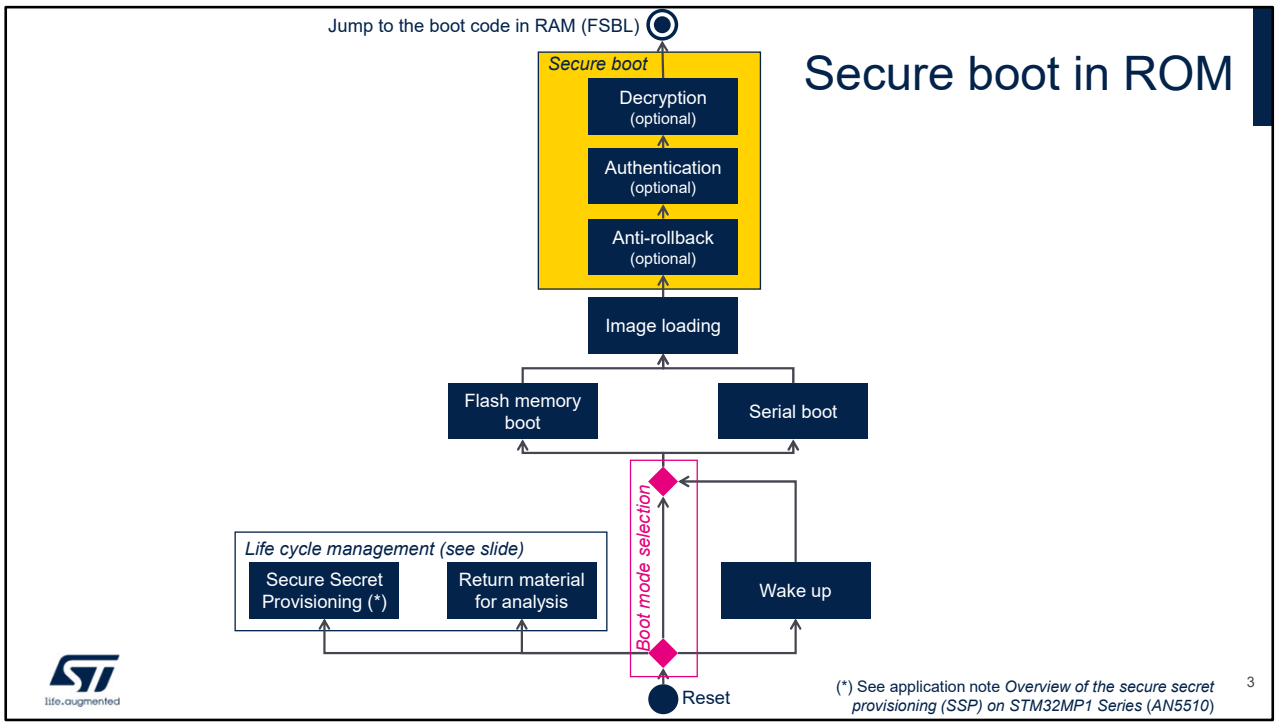
The STM32MP13 family of devices is designed with a comprehensive set of security features, some of which are based on standard Arm TrustZone technology. These security features simplify the process of evaluating IoT devices against security standards.

This module describes the following key security features:

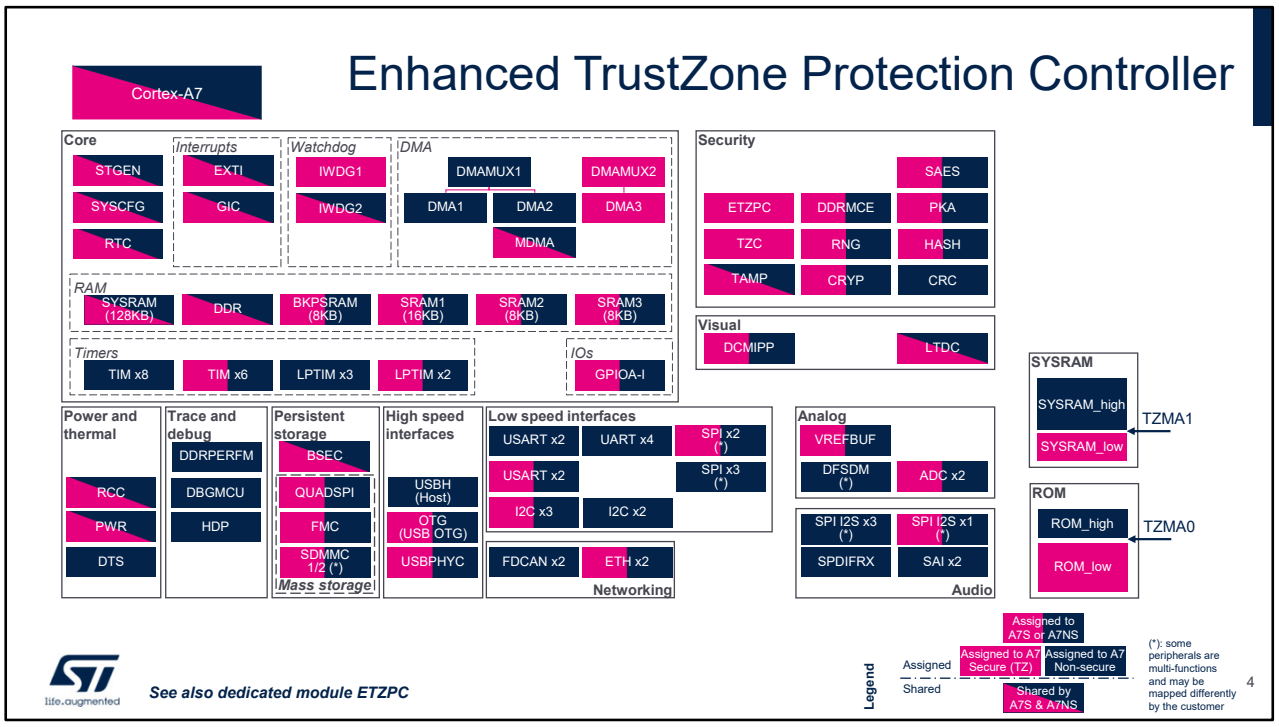
- Secure boot
- Resource isolation using TrustZone
- Hardware cryptographic features
- And Enhanced life cycle management

In other modules, you will find the following information:

- Enhanced secure storage
- Details on cryptographic acceleration
- And Active tamper and protection against temperature-, voltage- and frequency-attacks.



This slide summarizes the boot process implemented in the ROM code. The Secure boot part is only valid after provisioning secure boot information in OTP fuses, for example using the secure secret provisioning process.
The boot image, loaded in embedded SRAM, is downloaded either from flash memory or from a serial interface.
After the device goes to standby, ROM code manages wake-up of the device.



The Enhanced TrustZone Protection Controller (ETZPC) in the device is used to:

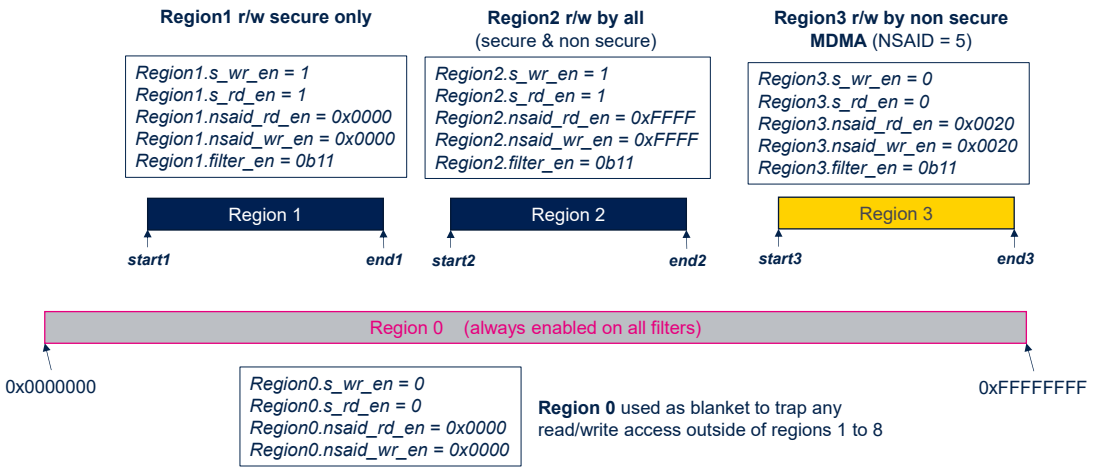
1) Configure TrustZone, the security for Securable IPs. Peripheral security mode can be:

- Secure: Read and Write access allowed only to secure world
- Write-secure: Write access allowed only to secure world, read allowed to any
- Non-secure: Read and Write access allowed to any

2) Configure the SYSRAM and ROM secure regions size. The Secure region is defined in a multiple of 4KB and at the bottom address.

And 3) Configure the MCU Isolation domain with a set of isolatable IPs allocated to this MCU domain.

TrustZone Address Space Controller



The TrustZone® Address Space Controller (TZC) is designed to filter DDR accesses . As an example, this slide portrays 3 non-overlapping regions:

- Region 1 is read- and write-accessible only by secure applications.
- Region 2 is a shared region read- and write-accessible by secure and non-secure applications.
- Region 3 is read- and write-accessible only by the non-secure MDMA engine (with NSAID=5).

Region 0 is always enabled and covers the full DDR address space. It is set as a blanket to trap any access outside of these regions, and is configured so that no access is allowed outside of the 3 defined regions.

STM32MP13 hardware crypto features

Crypto features		STM32MP13
Symmetric crypto	AES-128, 192 or 256 Modes ECB, CBC, CTR, GCM, CCM	**CRYP peripheral**
	AES-128 or 256 Modes ECB, CBC, CTR, GCM, CCM Side channel attack protection HW protected keys	**SAES peripheral** **Dedicated bus to share keys with CRYP peripheral**
Asymmetric crypto	Public key primitives for RSA, DH and ECC over GF(p)	**PKA peripheral**
Hash functions (+HMAC)	Digests: MD5, SHA-1	**HASH peripheral**
	Crypto hash: SHA2-224/ 256/ 384/ 512, SHA3-224/ 256/ 384/ 512, SHAKE-128/256, RawSHAKE-128/256	
Random numbers	FIPS 140-3 NDRNG (NIST SP800-90B certifiable)	**RNG peripheral** **Transparently used for side channel protections in PKA and SAES peripherals**
Memory encryption	AES-128 ECB + Key derivation, usable on one DDR-SDRAM region protected by TrustZone firewall	**DDRMCE peripheral**

life.augmented

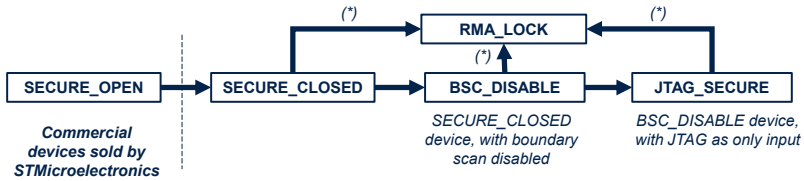
See also dedicated modules

6

This table sums up the available hardware cryptographic acceleration in the device.

Enhanced life cycle management

Lifecycle		Debug	Lifecycle overview
SECURE_OPEN	Root of trust not provisioned in fuses	Possible, but no secrets provisioned	**Boot on ROM without secrets in OTP** ➢ Debug possible in secure and non-secure after ROM execution ➢ OTP fuses for application are virgin
SECURE_CLOSED, BSC_DISABLE, JTAG_SECURE	Production device with secrets in fuses	Closed by default	**Boot on ROM with secrets in OTP** ➢ OTP fuses for application are no more virgin. Security options exist to limit boundary scan and JTAG capability (see below) ➢ Authenticated boot is enforced, using provisioned fuses ➢ Debug is disabled by default, with a possible enabling by application signed boot code (after hiding secrets).
RMA_LOCK	Return material for analysis device	Possible, but without secrets	**Boot on RAM with debugger** ➢ Debug possible in secure and non-secure after ROM execution ➢ Customer secrets stored in OTP fuse words 32 to 95 are permanently hidden



(*) Input of customer secret (max attempt: 3)

life.augmented

After leaving STMicroelectronics factories, the STM32 device hardware and ROM code manage the lifecycle of the device as described in this slide.

Thank you

life.augmented

Thank you for having attended this presentation!
You can now refer to the presentations that detail the operation of the STM32MP13's security modules:

- Symmetric cryptography.
- Asymmetric cryptography.
- Hash and random number generation.
- Enhanced anti-tamper.
- And Enhanced key storage.