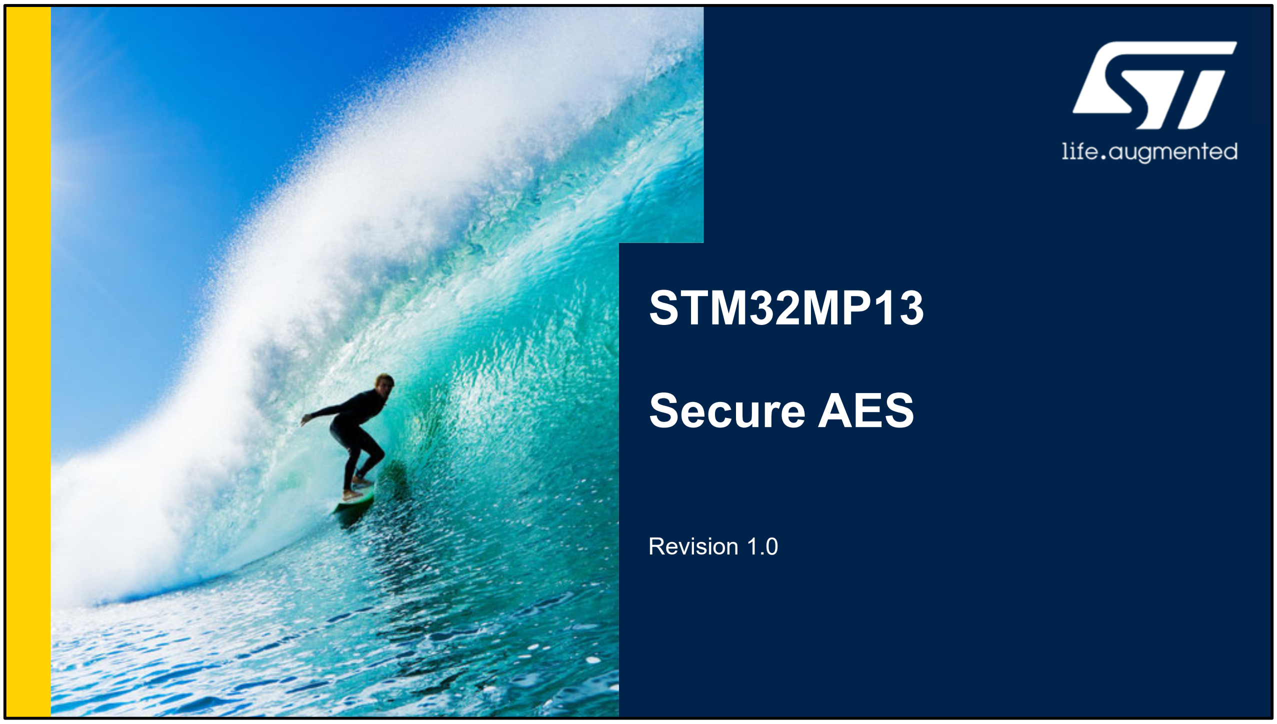


Hello and welcome to this presentation of the STM32MP13's secure AES.

SAES feature list

- AES chaining modes
  - Electronic codebook (ECB)
  - Cipher block chaining (CBC)
  - Counter (CTR) mode
  - Galois counter mode (GCM)
  - Galois message authentication code (GMAC)
  - Counter with CBC-MAC (CCM) mode
- Enhanced secure key storage
  - Hardware keys (DHUK, BHK)
    - Device-dependent, with DHUK
    - Application dependent, with BHK
  - Hardware secret key decryption (key unwrap)
  - Atomic key writing/loading enforcement
- Compliant AES operation modes on 128-bit data blocks, 128 or 256-bit keys
  - Encryption, Decryption (with associated key derivation mode)
- Key modes: normal, wrapped and shared key (loaded by faster CRYP engine)
- AHB slave with suspend/resume & DMA support (IN + OUT channels)
- Resistant to side channel attacks

Number of cycles required to process a 128-bit block

Key size	Encryption		Decryption	
	ECB	CBC	ECB	CBC
128b	480		480 [+145] (*)	
256b	680		680 [+230] (*)	

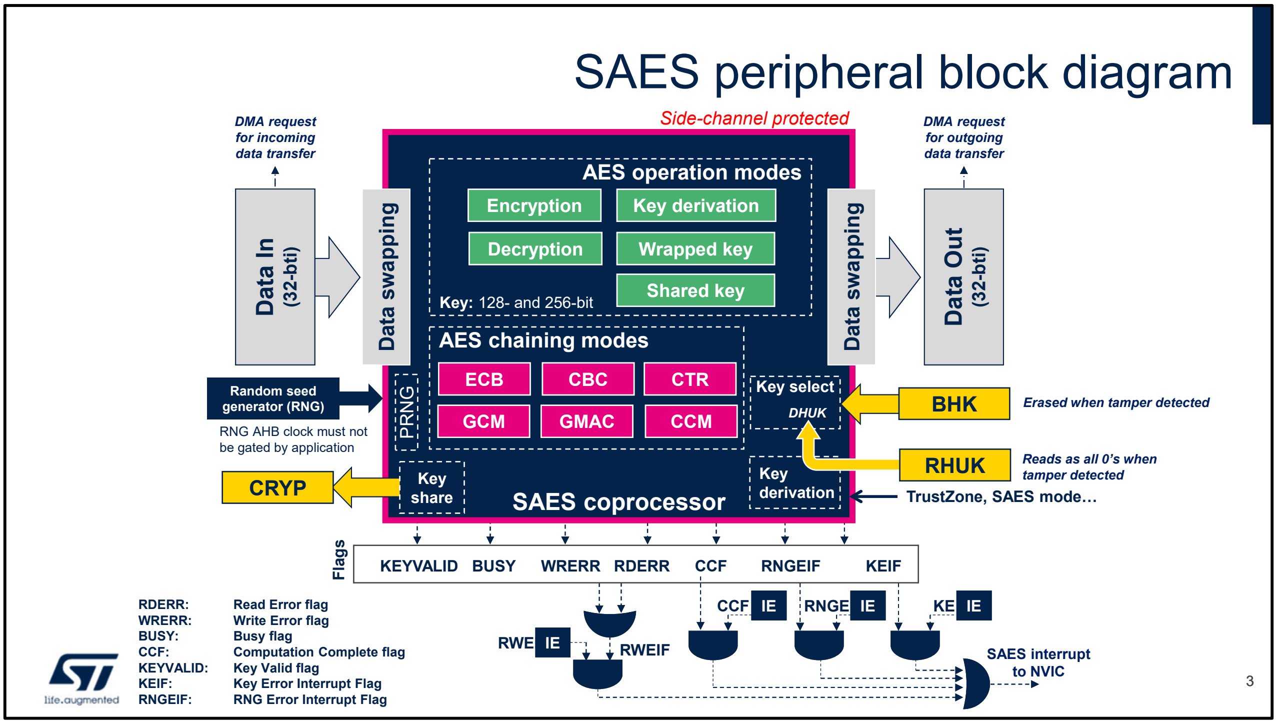
(*) For decryption you must add key derivation time, once

2

The SAES module supports the Advanced Encryption System (AES) in several operating modes described in the slide.
It processes 128-bit data blocks using an encryption key that is either 128 or 256 bits long, based on the selected chaining mode.
The table indicates the number of clock cycles required to process a block of data, according to the chaining mode and key size.

SAES peripheral offers the possibility to load secret keys by hardware (boot hardware key BHK and derived hardware unique key DHUK), usable but not readable by the application. It can also wrap (encrypt) and unwrap (decrypt) application keys using these hardware-secret keys DHUK, XOR-ed or not with the application key BHK. With this feature, AES keys can be made usable by application software without being exposed in clear-text (unencrypted).

A full data flow can be automated with the help of the Direct memory access controller (DMA).
The SAES module incorporates a protection against side-channel attacks (SCA), including differential power analysis (DPA). It can share decrypted keys to faster CRYP module. This procedure is controlled by SAES.



This simplified block diagram of the SAES module shows the data path from data in on the left to data out on the right.

The peripheral processes 128-bit data blocks using an encryption key with a length of either 128 or 256 bits, with or without a data swapping option.

The Computation Complete flag (CCF) is set by hardware when the computation is complete. An interrupt is generated if the CCF Interrupt Enable bit was previously set.

The SAES fetches random numbers from the RNG peripheral automatically after a module reset triggered in the RCC. The module also the has possibility to load the secret keys DHUK and BHK by hardware. These keys can be cleared / erased when a tamper is detected, making all secrets undecipherable by the attacker.

Encrypted keys in shared mode can be used by the CRYP module when SAES application activates the sharing function. DHUK and BHK can never be shared.

Thank you

life.augmented

For more details on the new enhanced secure key storage feature and wrap/share key modes, please refer to the Enhanced Secure Key Storage training module.