Hello, and welcome to this presentation on the STM32H5 security certification.

STM32H5 PSA L3 and SESIP3 Certified

- STM32H5 is compliant with Arm® Trusted Base System Architecture (TBSA) requirements and features Arm TrustZone® architecture
- STM32H57x is PSA Certified Level-3 and SESIP 3 confirming a substantial level of cyber protection
- PSA L3 is designed for IoT devices which require protection against physical attacks
  - PSA L3/SESIP3 allows key security applications
    - Suitable for Payment Card Industry Security Standards Council (PCI SSC)
    - All secure IoT devices and applications …

life.augmented

2

STM32H5 is PSA Certified Level-3 and SESIP Level 3, passing tests for logical, board, and basic physical resistance that confirm a substantial level of cyber protection.

- PSA Level 3 stands for Platform Security Architecture level 3. It establishes trust through a multi-level assurance program for chips containing a security component called a PSA Root of Trust (PSA-RoT) that provides trusted functionality to the platform. The multi-level scheme has been designed to help device makers and businesses get the level of security they need for their use case.
- SESIP Level 3 stands for Security Evaluation Standard for IoT Platforms. The SESIP, published by

GlobalPlatform, defines a standard for trustworthy assessment of the security of the IoT platforms, such that this can be re-used in fulfilling the requirements of various commercial product domains. SESIP Assurance Level 3 (SESIP3) is a traditional white-box vulnerability analysis. The evaluation is structured around a time-limited source code analysis combined with a time-limited penetration testing effort.

The STM32H5 is also compliant with ARM Trusted Based System Architecture, or TBSA, requirements and features of the ARM V8-M Trustzone technology that enable robust levels of protection at all cost points for IoT devices.
The technology reduces the potential for attack by isolating the critical security firmware, assets and private information from the rest of the application.

Security Certification Benefits

- What are the benefits of security evaluation and certification ?
  - Allows STMicroelectronics to progress and strengthen its expertise
  - Provides a measurable indicator and/or evidence of STM32 security robustness
  - Gains the confidence of customers dealing with security and eases their certification process
  - Establishes the STM32 as general purpose MCU reference in the IOT security world

life.augmented

3

The security certification brings a lot of benefits:

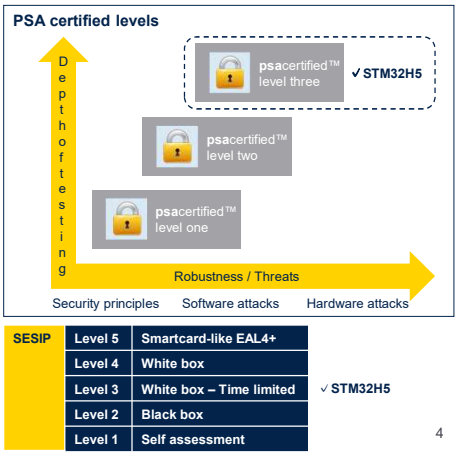
- Allows ST to progress and strengthen its expertise through standard certification procedures
- Proves the security robustness of the STM32
- Gains the confidence of customers dealing with security and eases their certification process
- Establishes the STM32 as a reference in terms of security features in the IoT security world.

PSA/SESIP L3 Security functions

10 PSA L3 Security Functions : 9 PSA L2 security functions + Physical attack resistance

14 SESIP3 Security Functions matching 9 PSA L2 security functions

- STM32H5 embeds a full set of security features allowing PSA/SESIP L3
  - Cryptographic accelerators, secure data storage, secure firmware installation, secure boot, and secure firmware update
  - Hardening of encryption of symmetric and asymmetric public-key accelerators (AES, PKA) against attacks with side-channel analysis (SCA)
  - A unique hardware key for secure data storage, and built-in active tamper detection
  - Internal monitoring (Tampers) erases secret data in the event of a perturbation attack
  - Full set of Hardware protection mechanisms (RDP, HDP, WRP ...)



SESIP		
	Level 5	Smartcard-like EAL4+
	Level 4	White box
	Level 3	White box – Time limited
	Level 2	Black box
	Level 1	Self assessment

✓ STM32H5

4

To pass PSA level 3 and SESIP level 3 certifications, the STM32H5 embeds multiple security features:

- General purpose cryptographic acceleration
- Secure storage
- Secure firmware installation
- Secure boot.

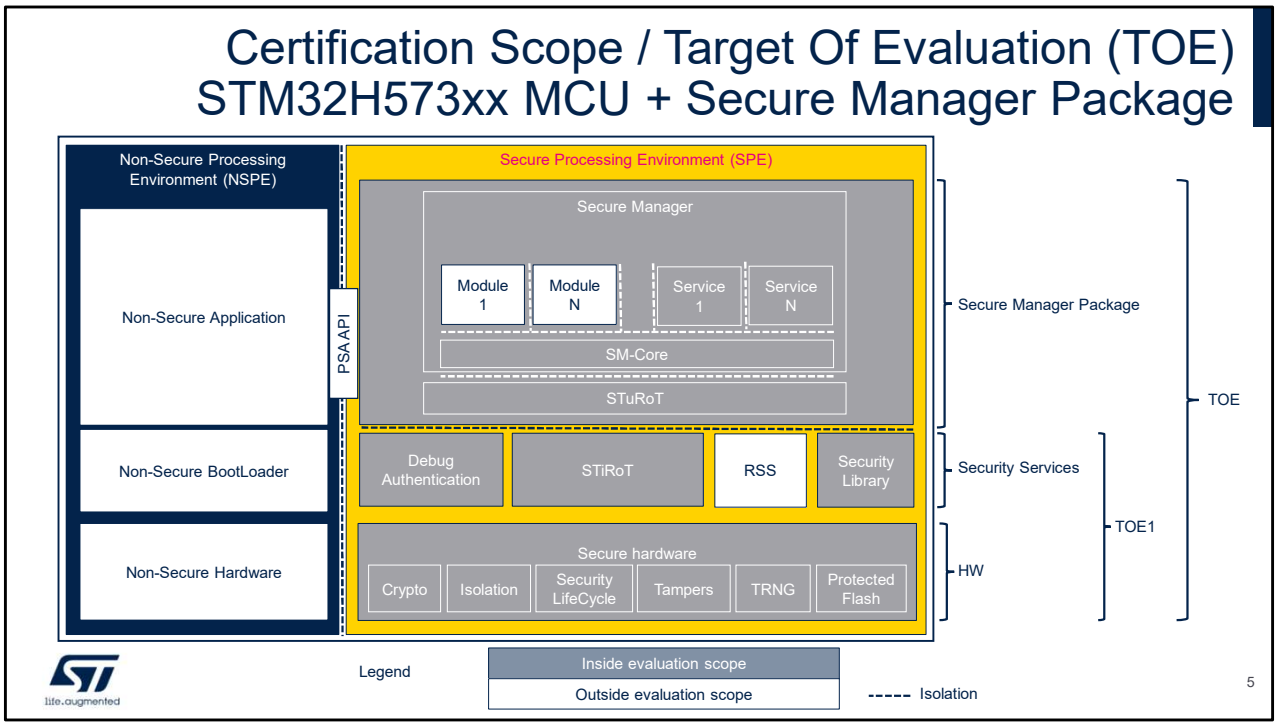
The secure AES 256-bit security co-processor supports side-channel counter-measures and mitigations.

The STM32H5 features an on-chip enhanced storage technology, using hardware secret non-volatile unique keys, and application-defined volatile hardware secret key. You can refer to the presentation entitled *KEYSTOR*.

The battery-powered volatile secure storage is automatically erased in the case of tamper. You can refer

to the presentation entitled ANTITAMP.
Multiple hardware protection mechanisms can be used to protect the contents of the flash memory:

- Encryption
- Temporal isolation
- Product life cycle.



The scope of a SESIP protection profile for PSA certified level3, or Target of Evaluation (TOE), is certified by composition.
This layered composition model uses STM32H573 MCU (TOE1) as base component and Secure Manager Package as Dependent component.

The platform components that are in the scope of the security evaluation are composed of the STM32H573 Security Services and the Secure Manager Package (SMP).
The SMP includes:

- ST Updatable Root of Trust (ST uRoT). It is responsible of Secure Boot and Secure Firmware Update of Secure

Manager, Secure Modules and non-secure Application.

- Secure Manager: software supplying Secure Services to non-secure application.
  - The secure manager is composed of:
  - Secure Monitor Core: responsible of core services, especially partition management to schedule Secure Services and Secure Modules
  - Secure Services: responsible of providing secure run-time services to non-secure Application, especially:
    - PSA Crypto services
    - PSA Internal Trusted storage services
    - PSA Attestation services
    - PSA Firmware update services

The STM32H573 Security Services are enabled by the secure hardware features resistant against physical attacks:

- ST Immutable Root of Trust (ST iROT): portion of immutable firmware that manages the secure boot and the secure firmware update of the STuRoT (code and/or related non-volatile data) installed in the integrated User Flash and option byte area
- Security Library: Portion of immutable firmware that manages the jump from ROT to boot loader or from iROT to the application
- Debug authentication: Portion of immutable firmware in charge of debug re-opening or regression (i.e erasing memories content).

Thank you

life.augmented

Thank you for attending this presentation!