Hello, and welcome to this presentation of the STM32U5 security certification.

STM32U5 PSA L3 and SESIP3 Certified

- STM32U5 is compliant with Arm® Trusted Base System Architecture (TBSA) requirements and features Arm TrustZone® architecture
- STM32U585 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 versus software attacks only for PSA L2 (case of STM32L5 Series)
  - 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

STM32U5 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 STM32U5 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 ST 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
  - Establisheds the STM32 as general purpose MCU reference in the IOT security world

life.augmented

3

The security certification brings a lot of benefits:

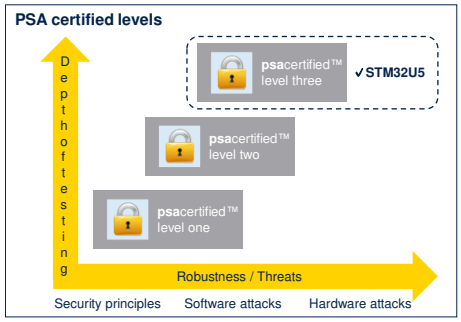
- Allows ST to progress and strengthen its expertise through standard certification procedures
- Proves the security robustness of the STM32
- Gains the confidence of customers dealing with security and eases their certification process
- Establisheds the STM32 as a reference in terms of security features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

- STM32U5 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

✓STM32U5

life.augmented

4

To pass PSA level 3 and SESIP level 3 certifications, the STM32U5 embeds multiple security features:
- General purpose cryptographic acceleration
- Secure storage
- Secure firmware installation
- Secure boot.

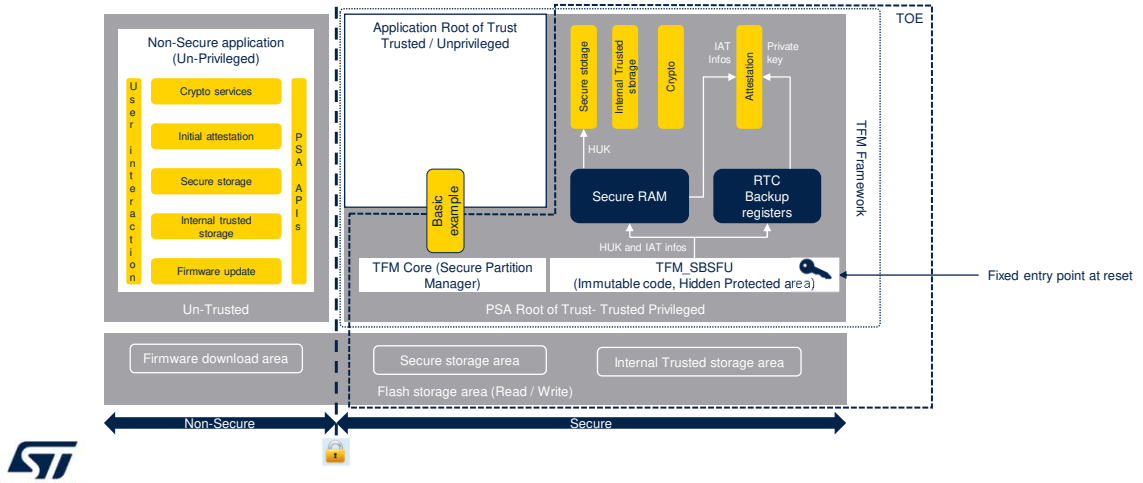
The secure AES 256-bit security co-processor supports side-channel counter-measures and mitigations.
The STM32U5 features an on-chip enhanced storage technology, using hardware secret non-volatile unique keys, and application-defined volatile hardware secret key. You can refer to the presentation entitled 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:

- Readout protection
- Secure hide protection
- Write protection.

Certification Scope / Target Of Evaluation (TOE)

TOE for PSA L3 & SESIP3: STM32U585 + Full TFM framework



life.augmented

5

The scope for a PSA Certified Level 3 Security evaluation, or Target of Evaluation (TOE), is the combination of the hardware and firmware components supporting a device compliant with PSA Certified specifications.
The platform components that are in the scope of the security evaluation are:

- PSA updateable Root of Trust, such as Software isolation framework, protecting more trusted software from less trusted software. This is based on generic services such as binding, initial attestation, generic cryptographic services, firmware update validation.
- PSA immutable Root of Trust, for example Boot ROM, Root secrets and IDs, Isolation hardware, Security lifecycle management and enforcement. This

component cannot be updated.

- Trusted Subsystems used by the PSA Root of Trust, such as security subsystems, trusted peripherals, which include both hardware and software components are also in the scope of evaluation.

The STM32U5 certification relies on the STM32 hardware and the software framework.

This software framework is based on Trusted Firmware for CortexM, or TFM, and ST Secure Boot and a Secure Firmware Update solution, also called SBSFU.

TrustZone on the STM32U5 includes more granular levels by combining trusted and privileged environments. For instance, the firmware will most likely be in a trusted and privileged environment while the sensitive part of an application will execute in a trusted but non-privileged area, and common programs stay in non-trusted and non-privileged systems. The modularity makes it easier to protect sensitive code in the case of an intrusion in one of the less secure environments.

Thank you

© STMicroelectronics - All rights reserved.
The STMicroelectronics corporate logo is a registered trademark of the STMicroelectronics group of companies. All other names are the property of their respective owners.

life.augmented

Thank you for attending this presentation!