STM32Trust

A security framework to protect embedded systems

Based on PSA and SESIP certifications, STM32Trust helps designers meet the requirements of their pre-defined security assurance levels

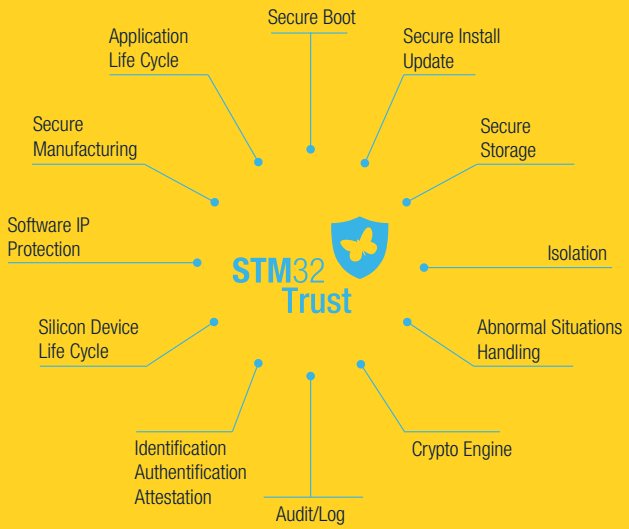
STM32Trust offers a robust multi-level strategy to enhance security in new product designs based on STM32 microcontrollers and microprocessors augmented with STSAFE secure elements.

STM32Trust is a security framework combining our knowledge, ecosystem, and security services. This solution offers developers a complete toolset to protect their design's valuable assets, such as software IP and data, and to ensure secure connectivity and system integrity.

With a set of 12 security functions offering hardware, software, and design services from ST and third parties, STM32Trust complies with the requirements of the major IoT certification schemes.

THE SECURITY FUNCTIONS

By providing services that cover 12 security functions, STM32Trust addresses developers' security needs.



www.st.com/stm32trust

1- Secure boot
Ability to ensure the authenticity and integrity of an embedded application

2- Secure Install/Update
Installation or update of firmware with initial integrity and authenticity checks before programming and execution

3- Secure Storage
Ability to securely store secrets like data or keys

4- Isolation
Isolation between trusted and non-trusted parts of an application

5- Abnormal situation handling
Ability to detect abnormal situations (both hardware and software) and to take adapted decisions such as removing secret data

6- Crypto Engine
Ability to process cryptographic algorithms, as recommended by security assurance schemes

7- Audit/Log
Keep trace of security events in an unchangeable way

8- Identification / Authentication / Attestation
Unique identification of a device and/or software, and ability to detect its authenticity, inside the device or externally

9- Silicon Device Lifecycle
Control states to securely protect silicon device assets through a constrained path

10- Software IP Protection
Ability to protect a section or the whole software package against external or internal reading. Can be multi-tenant

11- Secure Manufacturing
Initial device provisioning in unsecured environment with overproduction control. Possibility to personalize secure components

12- Application Life Cycle
Define unchangeable incremental states to securely protect application states and assets

CERTIFICATIONS

Security assurance levels are provided based on PSA and SESIP certifications.

For more details please visit www.st.com/stm32trust

Certifications

ARM PSA
- Level 1 (Self assessment)
- Level 2 (White box - Time Limited)
- Level 3 (Smartcard-like)

SESIP
- Level 1 (Self assessment)
- Level 2 (Black box)
- Level 3 (White box - Time Limited)
- Level 4 (White box)
- Level 5 (Smartcard-like EAL4+)

Available now

ARM PSA Level 1
- STM32L4
- STM32L5

ARM PSA Level 2
- STM32L5 (TFM)

ARM PSA Level 3
- STM32U5 (TFM)*

SESIP LEVEL 1
- STM32L4 (SBSFU)

SESIP LEVEL 3
- STM32L4 (SBSFU)
- STM32L5 (TF-M)
- STM32U5 (TF-M)*

CC EAL5+
- STSAFE-A110
- STSAFE-TPM
- ST4SIM

FIPS-140-2
- STSAFE-TPM

TCG
- STSAFE-TPM

GSMA
- ST4SIM

Evaluations

PCI POS
- Point of Sale application

Available now

- STM32L4

* U5 certification planned before September 2021

Order code: FLSTM32TRUST0721