STM32Trust

A security framework to protect embedded systems

STM32Trust helps designers meet the required security assurance levels, according to PSA and SESIP certifications.

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 combines our knowledge, ecosystem, and security services.

This security solution provides a complete toolset:

- to protect valuable assets, such as software IP and data
- to safeguard system integrity
- to ensure secure connectivity

STM32Trust complies with the major IoT certification schemes thanks to its 12 security functions that provide hardware, software, and design services from both ST and third-parties.

THE SECURITY FUNCTIONS

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

- Secure boot
- Secure install/update
- Silicon device lifecycle
- Isolation
- Secure storage
- Crypto engine
- Secure manufacturing
- Identification / Authentication / Attestation
- Software IP protection
- Abnormal situation handling
- Audit/Log
- Application lifecycle

www.st.com/stm32trust

1- Secure boot
Ability to ensure the authenticity and integrity of an application that runs inside a device.

2- Secure install/update
Installation or update of firmware with initial checks of integrity and authenticity before programming.

3- Silicon device lifecycle
Control states to securely protect silicon-device assets through a constrained path.

4- Isolation
Isolation between trusted and nontrusted parts of an application.

5- Secure storage
Ability to securely store secrets like data or keys (and to access them without them being visible externally).

6- Crypto engine
Ability to process cryptographic algorithms, as recommended by a security assurance level.

7- Secure manufacturing
Initial device provisioning in an unsecured environment with overproduction control. Potential secured personalization.

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

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

10- Abnormal situation handling
Ability to detect abnormal situations (both hardware and software) and to take adapted decisions like the removal of secret data.

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

12- Application lifecycle
Define unchangeable incremental states to securely protect application states and assets.

Simplify your security journey: discover the Secure Manager, the industry's first security solution at MCU level

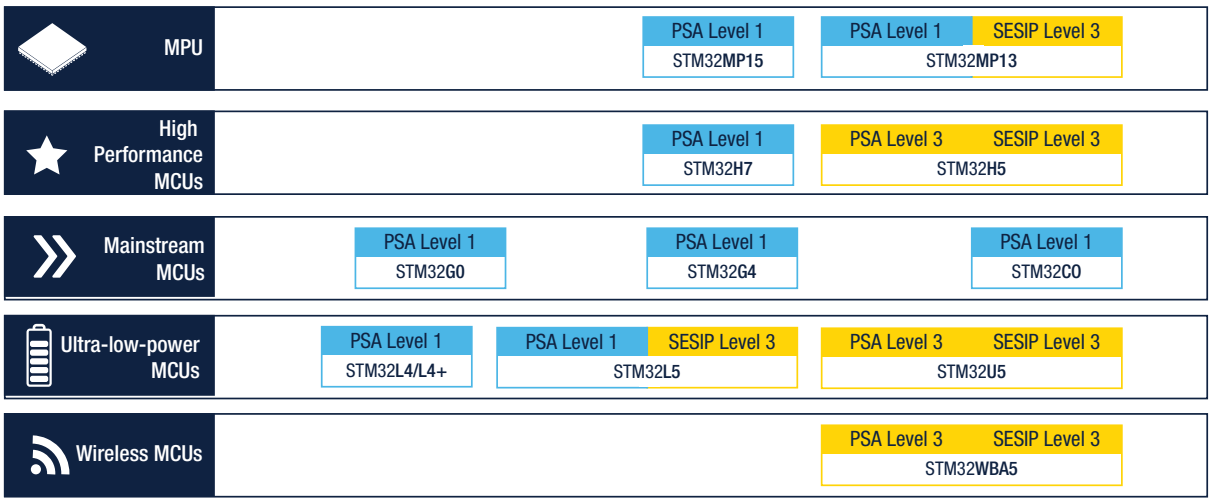
A trusted execution environment (TEE) integrating core security services at system level. It comes as a downloadable software package containing binaries, libraries, code implementations and documentation.

STM32 Trust TEE

Target certifications

Security assurance levels are provided based on PSA and SESIP certifications.
For more details, please visit www.st.com/stm32trust

psacertified™ SESIP™



Order code: FL2308STM32TRUST