life.augmented

STSAFE-TPM

Standardized solution for trusted devices

TCG-standardized platform expanding trust from personal computing to connected devices

STSAFE-TPM is a widely deployed, standardized Trusted Platform Module which is a key enabler of security in personal computers and servers. It is a perfect fit for ecosystems built on Windows and Linux operating systems.

Certified by Common Criteria, TCG and FIPS, all STSAFE-TPM secure elements meet security and regulatory requirements. Based on a ST33 hardware, the product portfolio is qualified for consumer, industrial and automotive applications.

KEY BENEFITS

- Integration with Linux and TCG TPM software stack
- Common Criteria-, TCG- and FIPS-certified
- Long lifetime products (up to 20 years)
- Delivered with keys and certificates already loaded

KEY APPLICATIONS

- Industrial and personal computing
- PC, servers and tablets
- Peripherals
- Network equipment
  - Routers and switches
  - Base stations and access points
- Home & building automation
  - Gateways
- Medical devices
- Automotive solutions

STSAFE-TPM is a proven solution offering standardized trusted computing services (ISO / IEC 11889) which is ideal for Windows or Linux-based platforms.

Key features

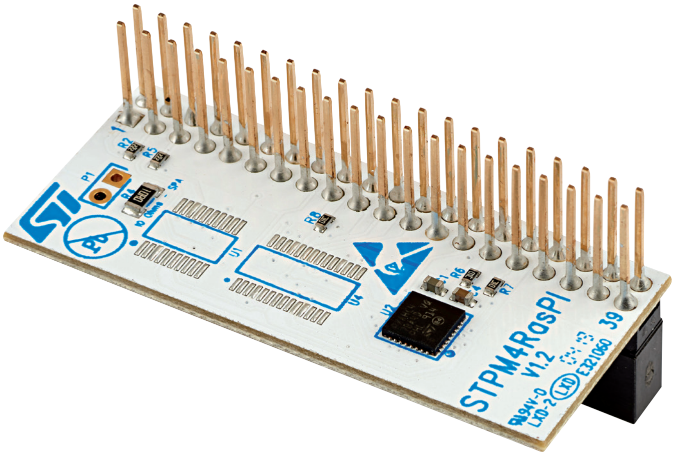
- Extended cryptography support for long lifecycle devices (ECC384, SHA2-384, SHA3, AES 256)
- TPM firmware upgrade possible through fault tolerant loading process
- TPM firmware and critical data self recovery (NIST SP800-193)
- Penetration tests conducted at the highest CC assurance level (AVA_VAN.5)
- Available with TCG compliant SPI or I^{2}C interface
- Consumer / AEC-Q100 / Industrial qualification
- Available in standardized and small footprint packages like WLCSP
- Extended operating temperature range (-40°c to 105°C)

Ecosystem

- A full development kit is available for easy integration
- Expansion board (STPM4RasPI) for Raspberry PI® and STM32MP1 MPU for both SPI and I^{2}C interfaces
- Software package with driver and utilities (communication driver and firmware upgrade)
- Smooth system integration thanks to Windows and Linux support, TCG Open Source or Third party TPM stacks

Certification

- First CC-certified TPM according to Trusted Computing Group protection profile augmented with resistance to high-potential attacks (AVA_VAN.5)
- FIPS 140-2 certificate level 2 with physical security level 3
- TCG certification



STPM4RasPI TPM Expansion Board

Product table

Product name	Application segment	OS support	Interface	Certification	Package options	Operating temperature range
ST33TPHF20/2E	TPM PC / server, network, printer, IoT	TPM 1.2 / TPM 2.0	TCG SPI (33MHz) TCG I^{2}C (400KHz)	CC EAL4+, TCG, FIPS 140-2	TSSOP28, VQFN32	-40 to +105°C
ST33TPHF2X		TPM 2.0		CC EAL4+ (high attack potential), TCG, FIPS 140-2	VQFN32	
ST33GTPMA	Automotive		TCG SPI (18MHz) TCG I^{2}C (200KHz)		TSSOP20	
ST33GTPMI	Industrial				WLCSP	

life.augmented

Order code: FLSTSAFETPM1120