ST33KTPM

New generation of TPM for Consumer and Industrial systems

Future-proof Trusted Platform Module expanding trust from personal computing to connected devices

ST33KTPM is the latest addition to the STSAFE-TPM family, a widely used and standardized Trusted Platform Module that serves as a cornerstone of security for PCs and servers. TPMs are required by Microsoft Windows and natively supported by Linux operating systems.

ST33KTPM offers improved performance, enhanced security, and increased memory capacity to effectively address current and future security challenges.

The independent security certifications by Common Criteria, TCG and FIPS provide a high level of confidence and can be leveraged to meet regulatory requirements.

The ST33KTPM family offers three products with different interfaces and lifetimes to support all ecosystem requirements.

KEY FEATURES AND BENEFITS

- Proven and standardized security solution
- High assurance based on Common Criteria, TCG, and FIPS 140 certifications
- Easy integration with Windows, Linux OS, and TCG TPM software stack
- Cryptographic services with improved performance
- Firmware upgradable to new standardized features and cryptography

KEY APPLICATIONS

- PCs, workstations and servers
- Network equipment
- Home and building automation
- Point of sales
- EV charging station

KEY USES CASES

- Platform trusted identity
- Device health attestation
- Anti-couterfeiting
- Protection of keys and critical data
- Cryptographic toolbox
- Secure channel communication (TLS)

Key features

- TCG TPM 2.0 latest specifications compliant (Rev. 1.59)
- Extended cryptography support (up to RSA 4096, ECC NIST P256 & P384, EC BN256, SHA1, SHA2-256 & 384, SHA3-256 & 384, AES 128-192-256)
- TCG compliant SPI or I²C interface selectable dynamically
- Non-volatile memory (200 kB)
- TPM firmware upgrade through fault tolerant loading process
- TPM firmware & critical data self-recovery (NIST SP800-193)
- Consumer and Industrial JESD-47 qualifications
- Available in thin UFQFPN32 standard package and small footprint package WLCSP24
- Extended operating temperature range (-40°C to 105°C)

Ecosystem

- Expansion board for Raspberry PI® and STM32MPx MPU for both SPI and I²C interfaces
- Software package with use cases and utilities (firmware upgrade)
- Windows HLK certification and major Linux distributions support

Certifications

ST33KTPM products received the following certifications:

- Common Criteria EAL4+ conformant to TCG Protection Profile augmented with resistance to high-potential attacks (AVA_VAN.5)
- TCG certificate and is compliant with FIPS 140-3 certificate with physical security level 3

To check the certification status, please refer to the list of certified products on the relevant websites.

Upgradability

ST33KTPM products are designed to support the following evolutions through firmware upgrades

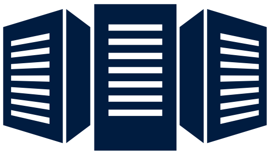
- Cryptographic services for EV charging standard ISO15118-20
- Future TCG standard versions
- Post-Quantum Cryptography (SP800-108, FIPS 203 and 204) and
- Security improvements to thwart new security attacks

Security

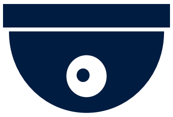
ST33KTPM products benefit from advanced hardware and software security protections against state of the art logical and physical attacks.

TPM application examples

COMPUTER



SERVER



CAMERA

EV CHARGER

Product summary

Product name	Application segment	TPM version	Interfaces	Packages	Certification	Temperature range [°C]	Lifetime
ST33KTPM2XSPI	Consumer	2.0 Rev 1.59	SPI	UFQFPN32	CC EAL4+ FIPS 140-3 (Physical Security Level 3)	-40 to +105	10 years
ST33KTPM2X	Consumer		SPI or I²C				
ST33KTPM2I	Industrial (JESD-47 qualified)			UFQFPN32 WF WLCSP24			20 years

Order code: FL2312ST33KTPM

For more information on ST products and solutions, visit www.st.com