STSAFE™-TPM
Standardized solution for trusted devices

Expanding trust from personal computing to connected devices

The security of computing platforms and the protection of users' assets have become a tremendous challenge not only for OEMs who design connected devices but also for end users increasingly concerned about their privacy and the protection of their data.
The growing deployment of connected consumer devices and industrial IoT equipment makes this challenge even more critical.
STSAFE-TPM relies on ST's secure microcontroller hardware to offer the most comprehensive and cost-effective system-on-chip solution for trusted computing.

KEY FEATURES

- TPM 1.2 & TPM 2.0 libraries
- TPM 1.2 & TPM 2.0 switch capability
- Secure Field Upgrade mode for TPM firmware
- Common criteria (CC) EAL4+, TCG and FIPS 140-2 certified
- Windows 10 Redstone (RS) approved
- Compatible with Linux TPM drivers
- -40°C/+105°C extended temperature range

KEY BENEFITS

- Built upon high-end secure microcontroller
- Certified hardware-based root of trust
- Large secure user non-volatile memory
- TPM credentials root signed by independent certification authority (CA)
- Seamless integration (ISO/IEC 11889 compliant)

KEY APPLICATIONS

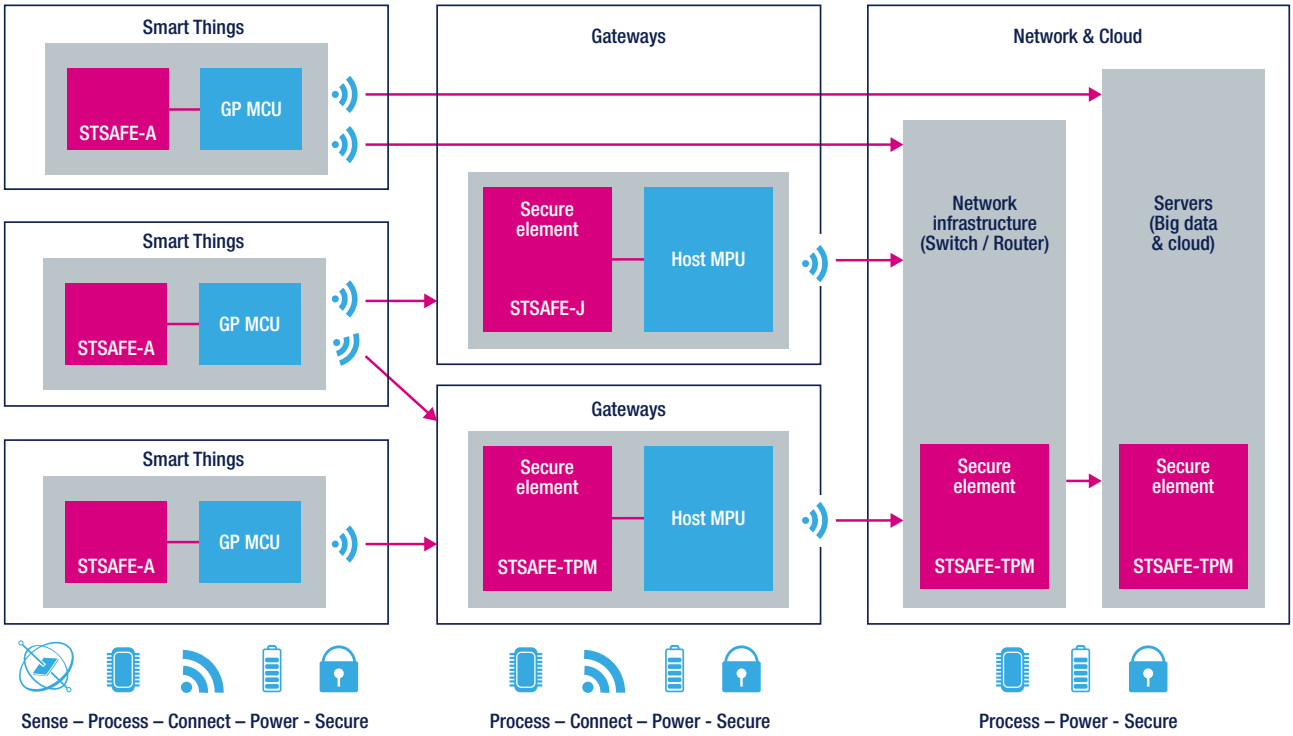
- Personal computing
- PC, servers, and tablets
- Peripherals
- Industrial computing
  - Single-board computers
  - Programmable logic controllers
- Network equipment
  - Routers and switches
  - Base stations and access points
- Home & building automation
  - Gateways
- Medical devices
- Automotive solutions

STSAFE-TPM

The standardized and certified solution for trusted computing

Computing is no longer about traditional personal computers.
Today, it has expanded to include new types of devices that systematically integrate connectivity.
As a result, the sense of ubiquity that these technologies brings to users also emphasizes new security concerns.
The Trusted Computing Group (TCG), an international standardization body formed by more than 100 industry leaders, provides open standards and specifications addressing security challenges such as device integrity, health checks, strong user authentication, secure network access and the protection of data and assets.
Fully compliant with TCG's Trusted Platform Module (TPM) specifications, STSAFE-TPM products are also Common Criteria EAL4+ as well as FIPS 140-2 certified.
Available in different packages and interfaces, this cost-effective system-on-chip provides a flexible solution for a wide range of connected devices. STSAFE-TPM products are qualified to operate under an extended industrial temperature range making them the most suitable and comprehensive TPM offering on the market.

TYPICAL STSAFE-TPM "TRUST ANCHOR" IMPLEMENTATION



PRODUCT PORTFOLIO

Product name *	TPM support	TCG interface	Package	Operating temperature range	NVM Storage
ST33TPHF2ESPI	TPM 1.2 / TPM 2.0	TCG SPI	TSSOP28, VFQFPN 32	–40 to +105 °C	34 Kbytes
ST33TPHF20SPI	TPM 2.0	TCG SPI	TSSOP28, VFQFPN 32	–40 to +105 °C	110 Kbytes
ST33TPHF2EI2C	TPM 1.2 / TPM 2.0	TCG I2C	TSSOP28, VFQFPN 32	–40 to +105 °C	34 Kbytes
ST33TPHF20I2C	TPM 2.0	TCG I2C	TSSOP28, VFQFPN 32	–40 to +105 °C	110 Kbytes

* Note: The Product Name listed above is not the orderable part number;
for the orderable part number, please refer to the product datasheet or contact your nearest sales representative