STSAFE-V100-TPM

Discrete TPM for automotive applications

A standardized TPM solution for a wide range of automotive use cases

Add security to new use cases with a cryptographic toolbox. An easy-to-integrate discrete TPM solution reduces development time with a standardized API and integrated cryptographic keys.

The automotive-grade STSAFE-V100-TPM is based on ST33KTPM, the latest generation of STSAFE-TPM products. Independently certified Common Criteria, TCG and FIPS, ST33KTPM system-on-chips meet regulatory requirements and provide a high level of security.

STSAFE-V100-TPM supports security functions required for authentication, secure boot, secure storage, software update, platform integrity, and other use cases that require secure services.

KEY FEATURES & BENEFITS

- Standardized TPM solution
- Hardware AEC-Q100 Grade 2 qualified
- Hardware CC EAL6+ certified
- Discrete TPM compliant with TCG standard
- Easy integration with standardized API
- Build secure systems with root of trust
- Future-proof solution with firmware updates

KEY APPLICATIONS

- EV charging
- Vehicle telematics
- Secure gateway
- ADAS

Product features

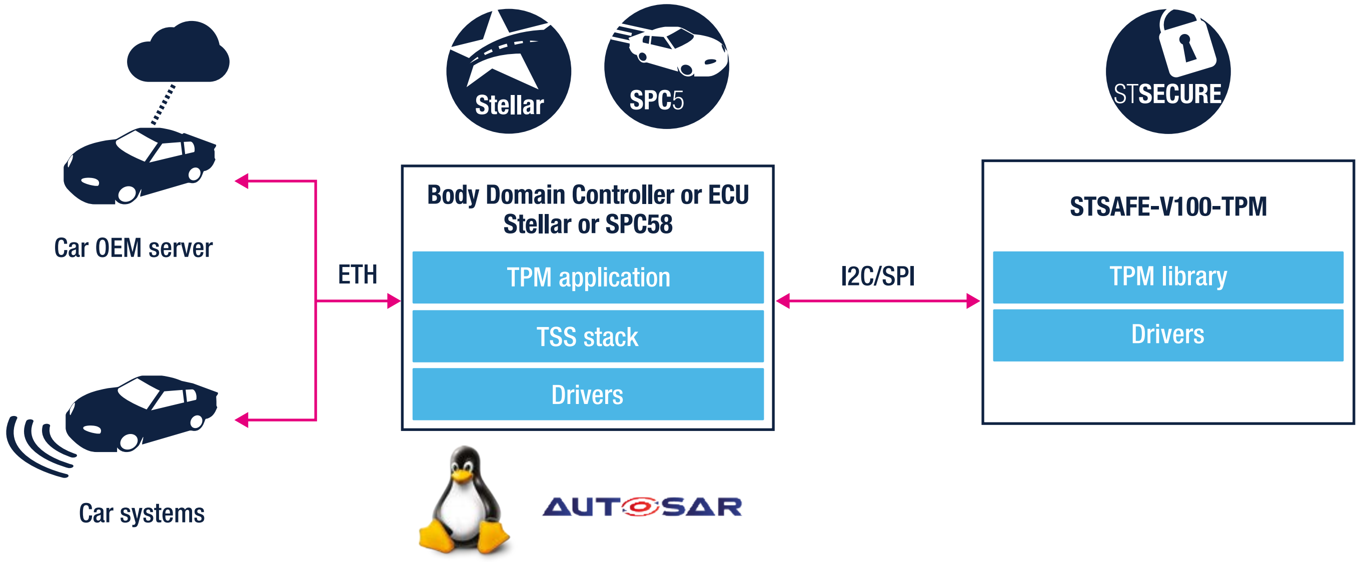
TPM features

- Compliant with the latest TCG TPM specification (2.0 Rev. 1.59)
- Extended cryptography support
- Non-volatile memory (200 kbyte)
- TPM firmware, critical data protection & firmware recovery (NIST SP800-193)
- TPM firmware upgrade through fault tolerant loading process (self-recovery)

Hardware features

- Highly reliable flash memory with error correction code
- AEC-Q100 qualified with extended temperature range (-40°C to +105°C)
- Electrostatic discharge (ESD) protection up to 4 kV (HBM)
- Available in thin UFQFPN32 WF package
- TCG compliant SPI or I²C interface selectable dynamically

Block diagram



Product portfolio

Order code	TPM version	Interface	Certification	Package	Operating Temperature Range
STSAFE-V100-TPM	TCG TPM 2.0 Rev. 1.59	I²C or SPI	HW CC EAL6+ & AEC-Q100 grade 2	UFQFPN32 WF or TSSOP20	-40°C to +105°C