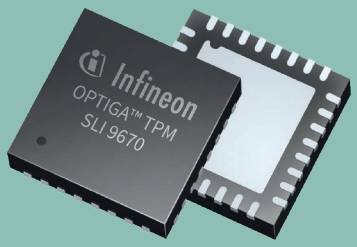

Product brief

OPTIGA™ TPM SLI 9670 for automotive security

The OPTIGA™ TPM SLI 9670 is a quality hardened Trusted Platform Module (TPM) for special use in automotive applications and based on a tamper resistant secured micro-controller using advanced hardware security technology.

As turn-key solution it is flashed with a securely coded firmware according to latest TCG family 2.0 specifications offering a rich feature set of security functions, like key management, authentication, signature functions (signing/verifying), encryption/decryption, secured logging and secured time.

The SLI 9670 is qualified according to the automotive AEC-Q100 standard making it an ideal solution for automotive applications in telematics, gateway, multi media head units and other ECUs with strong security requirements. This TPM is also security certified according to Common Criteria EAL4+.

Customer values

- Tamper resistant hardware architecture with performant core and peripheral set (e.g. crypto coprocessors, TRNG) based on market leading security expertise
- Reduced risk based on proven technology (standardized and market approved security solution preprogrammed with rich security functions (TCG standard TPM 2.0))
- Flexibility thanks to a wide range of integrated security functions (e.g. dedicated key management)
- Secured key store and management: secured personalization (key injection in secured environment), additional keys generated on-chip
- Updatability of TPM firmware offers longterm crypto agility and sustainability
- Plug-and-play security solution
  - Easy and cost efficient system integration through available open source drivers (e.g. for LINUX) and fast time to market

www.infineon.com/Auto-TPM
www.infineon.com/car-security

Key features

- Standardized and market approved turn-key security solution (TCG standard TPM 2.0)
- High-end tamper resistant security controller with advanced cryptographic algorithms implemented in hardware (RSA-2048, ECC-256, SHA-256)
- Highly reliable NVM technology
- SPI interface
- Extended temperature range (-40°C to 105°C)
- Automotive qualification according to AEC-Q100
- Security certification according Common Criteria EAL4+
- Available in a VQFN-32 package

Applications

- Telematics control units
- Connected gateways
- Multi media head units
- ECUs requiring strong security protection

OPTIGA™ TPM SLI 9670

A rich set of security functions ready to support demanding automotive security use cases

The OPTIGA™ TPM SLI 9670 becomes a companion chip to automotive ECUs providing a hardware root of trust, ciphering and deciphering in a tamper-resistant and certified environment to secure OTA software updates or store secret keys and credentials.

Providing a secured implementation of the more than 90 commands according to TCG specification the OPTIGA™ TPM SLI 9670 offers ready-to-use security to complex automotive systems and supports automotive security use cases like

- Secured key store and management
- Remote attestation
- Privacy protection
- Authentication
- Diagnostic access

to enable and secure a wide range of innovative automotive applications such as car sharing, remote car access, over the air updates, mobile phone integration in infotainment, fleet management. The SLI 9670 can be used in various host platforms and host operating systems.

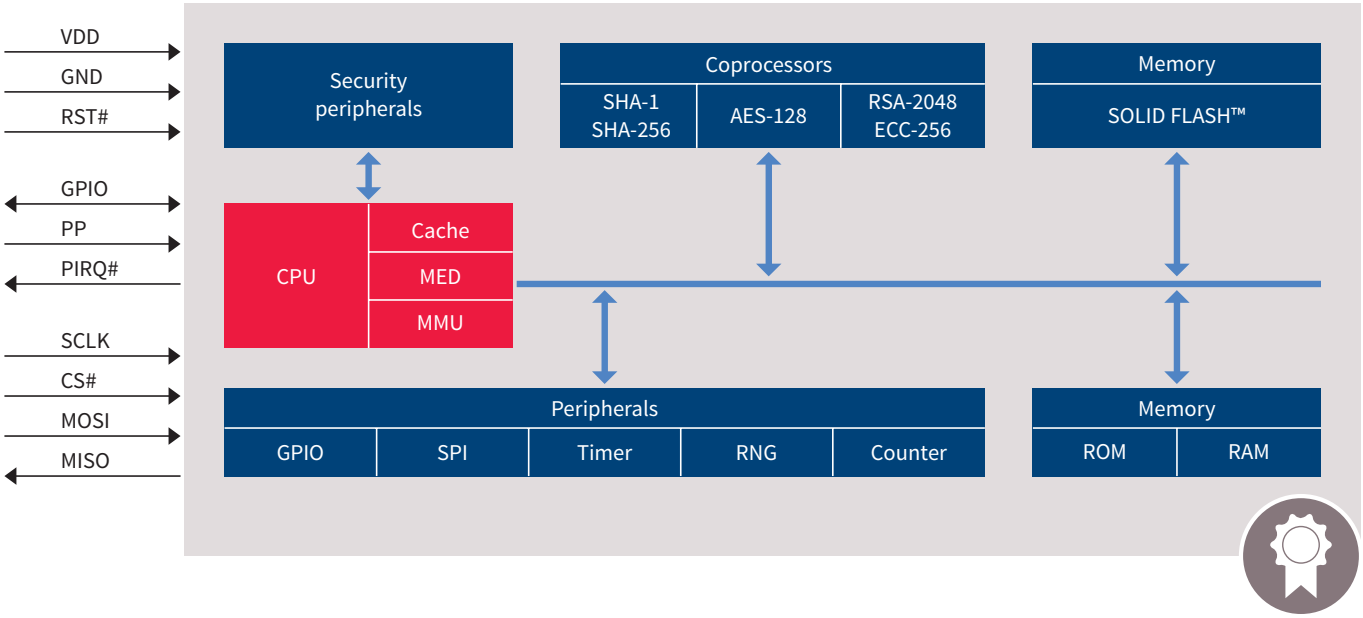

Figure 1 The hardware of the OPTIGA™ TPM SLI 9670 consisting of a tamper-resistant secured MCU along with sophisticated cryptographic hardware modules and further peripherals, such as a random number generator. Advanced hardware security technology, which includes internal memory and bus encryption as well as shielding and sensors provides protection against physical and logical attacks.

Published by
Infineon Technologies AG
81726 Munich, Germany

Order Number: B189-I0683-V1-7600-EU-EC-P
Date: 10 / 2018