Product brief

OPTIGA™ TPM SLM 9670

Standardized and certified TPM 2.0 security solution for industrial & other demanding applications

OPTIGA™ TPM SLM 9670 – Designed for demanding applications
The OPTIGA™ TPM SLM 9670 is a member of the OPTIGA™ TPM family. It addresses the requirements of industrial and other demanding applications where an extended temperature range, an extended lifetime and industrial-grade quality are key.

Pushing beyond the qualifications processes performed for standard TPMs, the OPTIGA™ TPM SLM 9670 is qualified according to the industrial JEDEC JESD47 standard to enable the requisite performance under demanding environmental conditions.

Rich feature and function set to secure industrial use cases
OPTIGA™ TPM SLM 9670 offers high levels of flexibility to support innovative smart factory and Industry 4.0 use cases that call for robust security based on:

- Strong digital device IDs and device authentication
- Secured communication for data confidentiality and IP protection
- Integrity protection of devices and software. Software updates included

A ready-to-use security building block, SLM 9670 is equipped with a variety of functions to secure industrial devices and systems. These include:

- Key storage and management
- Identification and authentication
- Signature generation and verification
- Software and firmware integrity attestation
- Secured logging and secured time

A tamper-resistant MCU stores and protects secrets such as cryptographic keys and other security-critical data like integrity measurements or counters. In addition, SLM 9670 hosts essential cryptographic operations including the generation and verification of keys and signatures using sophisticated cryptographic hardware coprocessors.

Standardized and certified
OPTIGA™ TPM SLM 9670 is fully compliant with the Trusted Platform Module (TPM) standards issued by the Trusted Computing Group (TCG). It is listed within the TCG Certified Products List based on functional and security evaluations performed by an independent third party according to Common Criteria EAL4+. In addition, it is compliant with FIPS 140-2 Level 2 (Physical Security Level 3).

Key benefits

- Standardized security chip compliant with TCG TPM 2.0 standard
- Secured storage for critical data and secrets
- Advanced protection mechanisms against physical and logical attacks
- Support for cryptographic algorithms RSA-1028, RSA-2048, ECC NIST P256, ECC BN256, SHA-1, SHA-256
- Ext. temp. range: -40 to 105 °C
- Ext. lifetime: 20 years
- JEDEC JESD47 industrial qualification
- Security evaluated and certified independently

Target applications

- Industrial PCs, servers, Programmable Logic Controllers (PLC)
- Network infrastructure devices & equipment like gateways, routers, wireless access points, and switches

OPTIGA™ TPM SLM 9670

Standardized and certified TPM 2.0 security solution bringing the security of your system to the next level

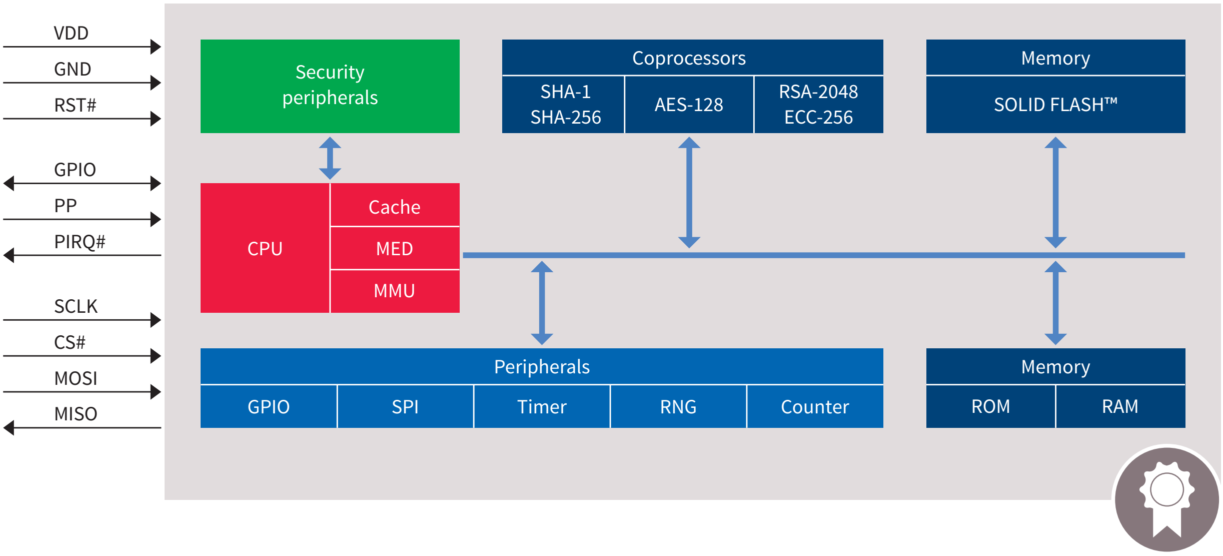

Figure 1: The OPTIGA™ TPM SLM 9670 hardware is based on a tamper-resistant secured microcontroller (MCU). It leverages advanced hardware security technology, including sophisticated hardware coprocessors and security peripherals, to deliver strong protection against logical and physical attacks.

Supported by a complete ecosystem

Based on the open, vendor-neutral global TPM standard created by TCG, the OPTIGA™ TPM family is a widely used and proven solution supported by a far-reaching ecosystem. Major rich operating systems support OPTIGA™ TPM, offering plug-and-play usability. Additionally, a wide selection of software offerings, including libraries and applications, is available from open source projects and leading commercial vendors – also through the Infineon Security Partner Network (ISPN).

The **OPTIGA™ TPM** product family includes various products supporting the Trusted Computing Group (TCG), Trusted Platform Module (TPM) standards, targeted at meeting the requirements of different end applications.

Product name	TPM specification	Interface	Certifications	Package	Operating temperature range	Qualification	Targeted end application
SLB 9670	TPM 1.2/TPM 2.0	SPI	CC EAL 4+ FIPS140-2 Level 2 (Physical Security Level 3)	VQFN-32	-20 to 85 °C	–	Standard
SLM 9670	TPM 2.0				-40 to 105 °C	JEDEC JESD 47	Industrial
SLI 9670	TMP 2.0				-40 to 105 °C	AEC-Q100 qualification grade 2	In-car

Published by
Infineon Technologies AG
81726 Munich, Germany

Order Number: B189-I0761-V1-7600-EU-EC-P
Date: 03 / 2019

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices, please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question, please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.