PRODUCT BRIEF

OPTIGA™ TPM SLB 9673

Ready-to-use TPM with I²C interface and PQC-protected firmware-update mechanism

The OPTIGA™ TPM SLB 9673 is the latest member of the OPTIGA™ TPM family. This standardized and certified[1)] ready-to-use security solution comes with an I²C interface. It serves as a robust foundation to identify and authenticate network infrastructure devices and equipment as well as industrial machines such as factory robots and Programmable Logic Controllers (PLC).

Feature-rich turnkey security to meet security challenges
The OPTIGA™ TPM SLB 9673 is designed to be future-proof – it comes with stronger algorithms with longer key lengths and is offering a PQC-protected firmware update mechanism. Moreover, to support the NIST SP 800-193 Platform Firmware Resiliency Guidelines, it integrates resiliency features of platform firmware and data against potentially destructive attacks. Thus, it brings the security of your system to the next level.

The OPTIGA™ TPM SLB 9673 offers an extended memory for new features and is accompanied by various tools to support design activities (host software, demo boards, etc.) and allow for easy integration.

Natively supported by Microsoft Windows and the major Linux distributions and derivatives, the OPTIGA™ TPM SLB 9673 is a ready-to-use security building block, available in a wide range of modules with different temperature ranges and features to fit individual needs and use cases.

It is ideal to support computing platforms and embedded systems use cases that call for robust security:

- Protection of keys and secrets
- Anti-counterfeiting
- Device health attestation to verify the device integrity
- Secured firmware update
- Secured cloud onboarding
- Secure channel for encrypted, protected communication with Transport Layer Security (TLS)

Infineon is committed to the long-term availability of OPTIGA™ TPM SLB 9673 and offers tailored support and maintenance through the Infineon Security Partner Network (ISPN). The ISPN helps to implement and deploy secured solutions, based on Infineon's hardware-based security solutions like the OPTIGA™ TPM.

Key features

- High-end security controller with a higher strength of security
- Support for latest specifications of TCG TPM 2.0 standard revision 1.59
- TCG, CC and FIPS certifications
- Support for various cryptographic algorithms: up to RSA-4096, AES-128, AES-256, ECC NIST P256, ECC BN256, ECC NIST P384, SHA-1, SHA2-256, SHA2-384
- Extended non-volatile memory (51 kB)
- Firmware upgrade capability with PQC-protected firmware update mechanism
- I²C interface
- Thin UQFN-32 package

Key benefits

- Proven and standardized turnkey security solution
- High confidence level based on Common Criteria and FIPS certification
- Faster cryptographic operations (2-4 times faster, depending on the functions)
- Easy integration with Windows and Linux OS platforms

www.infineon.com/OPTIGA-TPM-SLB9673

TRUSTED® COMPUTING GROUP

Fully certified and state-of-the-art security

OPTIGA™ TPM SLB 9673 is based on Infineon's advanced hardware security technology with a strong focus on resisting logical and physical attacks.

It is fully compliant with the Trusted Platform Module (TPM) specification issued by the Trusted Computing Group (TCG). Independently evaluated, the OPTIGA™ TPM SLB 9673 has received Common Criteria EAL4+ security certification[1]. In addition, it is compliant with FIPS 140-2[2] Level 2 (Physical Security Level 3).

The OPTIGA™ TPM SLB 9673 takes these strong security capabilities to a new level based upon a future-proof hardware with a PQC-protected Firmware Update Mechanism for today's and tomorrow` s security challenges.

OPTIGA™ TPM product family

Infineon's OPTIGA™ TPM product family consists of standardized security controllers which provide a wide range of security functions for computing platforms ranging from PCs and laptops to servers, industrial control systems and automotive applications. They are security-evaluated from development to manufacturing by independent third-party labs and certified in line with TCG, Common Criteria and FIPS requirements and specifications.

As one of the historical promoters of security solutions, Infineon offers a broad portfolio of certified items on the official TCG product list. With a strong presence and chairs in various working groups, we strive to innovate and further advance future security based on open standards.

Our customers are strongly benefiting from the advantages of such a standardized and fully interoperable security component.

Product summary OPTIGA™ TPM SLB 9673

Sales code	TPM version	Interface	Package	Temp. range [°C]	Security certifications	Key features
SLB 9673XU2.0 FW26.13	2.0 rev. 1.59	I^{2}C	PG-UQFN-32	-40 … +85	CC EAL4+[1] FIPS 140-2[2] Level 2 (Physical Security Level 3)	RSA, ECC, AES, SHA, NIST RNG SP800-90A/B, 3GPIO and firmware update capability with PQC protection. Management of **configurable commands** and support of **bulk encryption** via the command **TPM2_EncryptDecrypt2**. Full personalization with **4** endorsement keys (EK) and **4** EK certificates (RSA 2048, **RSA 3072**, ECC NIST P256, ECC NIST P384).
SLB 9673AU2.0 FW26.13				-40 … +105		

OPTIGA™ product family: a standardized solution

The OPTIGA™ family of embedded security solutions includes OPTIGA™ Authenticate, OPTIGA™ Connect, OPTIGA™ Trust, and OPTIGA™ TPM. They are designed for easy integration into embedded systems to protect the confidentiality, integrity and authenticity of information and devices. These hardware-based security solutions scale from basic authentication chips to sophisticated implementations.

[1] TCG certified product list: https://trustedcomputinggroup.org/membership/certification/tpm-certified-products

[2] FIPS 140-2 certification pending: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

Public

Date: 10 / 2023

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.

Scan QR code and explore offering
www.infineon.com