PRODUCT BRIEF

OPTIGA™ TPM SLB 9672

Ready-to-use computing security solution with PQC-protected firmware update mechanism

OPTIGA™ TPM SLB 9672 is the latest member of the OPTIGA™ TPM family. This standardized and certified[1)] security solution serves as a robust foundation to identify and authenticate PCs, servers, and connected devices, and to protect data integrity and confidentiality.

Feature-rich, ready for current and future security challenges
OPTIGA™ TPM SLB 9672 is future-proof – it comes with extended memory and stronger cryptographic algorithms, and is the first TPM in the market that offers a PQC-protected firmware update mechanism using XMSS signatures. Integrated resiliency features allow the TPM firmware to be recovered in compliance with the NIST SP 800-193 Platform Firmware Resiliency Guidelines. This, combined with improved computational performance, takes system security to the next level.

In addition, OPTIGA™ TPM SLB 9672 offers various tools to support design activities (host software, demo boards, etc.) and simplify integration.

Natively supported by Microsoft Windows and the major Linux distributions and derivatives, OPTIGA™ TPM SLB 9672 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, such as:

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

Infineon is committed to the long-term availability of OPTIGA™ TPM SLB9672, offering 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.

www.infineon.com/OPTIGA-TPM-SLB9672

TRUSTED® COMPUTING GROUP

Key features

- High-end standardized security controller
- PQC-protected firmware update mechanism using XMSS signatures
- Support for latest specifications of TCG TPM 2.0 standard (revision 1.59)
- TCG, CC and FIPS certifications
- Windows HLK certification
- 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)
- SPI interface
- Thin UQFN-32 package

Customer benefits

- Proven, 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

Applications

- Servers and PCs such as notebooks, desktops, tablets, and workstations
- Programmable Logic Controllers (PLC)
- Network infrastructure devices and equipment such as gateways, routers, wireless access points, network interface cards, and switches

Fully certified and future-proof

OPTIGA™ TPM SLB 9672 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 9672 has received Common Criteria EAL4+ security certification[1]. In addition, it is compliant with FIPS 140-2[2] Level 2 (Physical Security Level 3) as well as the latest Microsoft Windows HLK certification requirements.

OPTIGA™ TPM SLB 9672 takes the strong security capabilities of OPTIGA™ TPM to a new level as this future-proof hardware comes with a PQC-protected firmware update mechanism, based on XMSS signatures, making it fit 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 comput- ing platforms ranging from PCs and laptops to servers, industrial control systems, and automotive applications. The security capabilities are evalu- ated 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 longest-standing, proven 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, the com- pany strives to innovate and further advance future security based on open standards. Infineon customers are already reaping the many standardization and interoperability benefits of OPTIGA™ TPM security components.

Product summary OPTIGA™ TPM SLB 9672

Sales code	TPM version	Interface	Package	Temp. range [°C]	Security certifications	Key features
SLB 9672VU2.0 FW15.23	2.0 rev. 1.59	SPI	PG-UQFN-32	-20 … +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. Full personalization with 3 endorsement keys (EK) and 3 EK certificates (RSA-2048, ECC NIST P256, ECC NIST P384).
SLB 9672XU2.0 FW15.23				-40 … +85		
SLB 9672XU2.0 FW16.13				-40 … +85		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 9672AU2.0 FW16.13				-40 … +105		

OPTIGA™ embedded security solutions: Robust, flexible and easy to integrate

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

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

© 2023 Infineon Technologies AG.
All rights reserved.

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