

Product Brief

OPTIGA™ TPM

Certified security solutions for Trusted Computing in PC and embedded applications

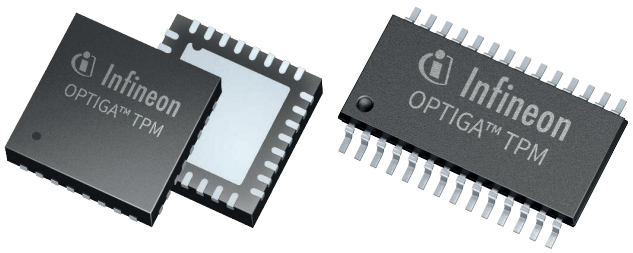
The Infineon OPTIGA™ TPM (Trusted Platform Module) family is a standardized security controller family which provides a wide range of security functions for embedded platforms. As the leader of Trusted Computing solutions Infineon offers a broad range of products meeting your specific requirements.

Security and functionality
All OPTIGA™ TPM products are based on Infineon's advanced hardware security technology. The products are designed according to the Trusted Computing Group (TCG) specifications and are certified Common Criteria[1)] CC EAL4+. The security functions include system and data integrity, authentication, secured communication, secured data storage and secured updates.

Performance and power
Implemented on a 16-bit state-of-the-art security controller from Infineon, the products meet the latest Microsoft Windows boot time and performance criteria. Furthermore the products are supported in Linux OS and derivates.
A sleep current of down to 110 µA allows smooth integration into a broad range of devices requiring power efficient battery operated designs.

Extended temperature range and packages
The OPTIGA™ TPM family supports an improved commercial temperature range as standard (-20 °C to +85 °C) as well as an extended temperature range (-40 °C to +85 °C) for industrial applications. The OPTIGA™ TPM is available in TSSOP-28 package or the small VQFN-32 package (5 x 5 mm²), which saves precious board space on your mobile platforms.

Migrate to TCG TPM 2.0 today
Leading the way into the future Infineon is the first provider offering a TPM 2.0 product according to the latest specification. With this early expertise we support your smooth transition to the new standard.



www.infineon.com/tpm

Key features[2)]

- Standardized security controller
- TCG certified products
- Products with TPM 1.2 and 2.0
- Standard & extended temperature range (-40 °C to +85 °C)
- Firmware upgrade capability
- SPI, I²C & LPC interface
- VQFN-32 & TSSOP-28 package
- CC and FIPS certification

Customer values

- Innovative security solutions provided by the market leader
- High confidence level based on Common Criteria certification
- Easy integration based on standardization

Applications

- Notebooks/PCs/tablets/servers
- Networking components
- Industrial automation
- Single board devices
- Home automation
- Automotive

1) The Trusted Computing Group (TCG) specifications for the standardized TPM v1.2 only consider LPC and SPI interfaces. The I²C interface is not part of the TCG defined specification. The SLB 9645 is built on the TCG compliant, EAL4+ certified TPM hardware and firmware, with the addition of I²C support.
2) Not all features apply to all product configurations – please refer to product data book for further details.

OPTIGA™ TPM

Certified security solutions for Trusted Computing in PC and embedded applications

Fully certified & state-of-the-art security

For new products of the Infineon OPTIGA™ TPM family the Common Criteria certification is a key focus. As the first and still leading the list, Infineon had its TPMs listed on the official TCG product list showing that the TCG TPM standard is fulfilled.

Infineon is a driver in the Trusted Computing Group (TCG), the standardization organization formed to develop open, vendor-neutral, global industry standards for hardware security. With an Infineon representative serving as the TCG president and a strong presence and chairs in various working groups, Infineon is working on future security standards and driving innovation.

Product summary[2)]

Sales code	TPM version	Interface	Temperature range	Package	Common Criteria certified	Typical / recommended use
SLB 9645						
SLB 9645TT1.2	1.2 rev. 116	I²C	-20 … +85	TSSOP-28		Notebook, desktops, tablets, mobile computing on non x86
SLB 9645XQ1.2	1.2 rev. 116	I²C	-40 … +85	VQFN-32		Industrial embedded computing on non x86
SLB 9645XT1.2	1.2 rev. 116	I²C	-40 … +85	TSSOP-28		Industrial embedded computing on non x86
SLB 9660						
SLB 9660TT1.2	1.2 rev. 116	LPC	-20 … +85	TSSOP-28	✓	Notebook, desktops, tablets on x86 & embedded computing
SLB 9660VQ1.2	1.2 rev. 116	LPC	-20 … +85	VQFN-32	✓	Notebook, desktops, tablets on x86 & embedded computing
SLB 9660XT1.2	1.2 rev. 116	LPC	-40 … +85	TSSOP-28	✓	Industrial embedded computing on x86
SLB 9660XQ1.2	1.2 rev. 116	LPC	-40 … +85	VQFN-32	✓	Industrial embedded computing on x86
SLB 9665						
SLB 9665TT2.0	2.0 rev. 1.16	LPC	-20 … +85	TSSOP-28	✓	Notebook, desktops, tablets on x86/x64 & embedded computing
SLB 9665VQ2.0	2.0 rev. 1.16	LPC	-20 … +85	VQFN-32	✓	Notebook, desktops, tablets on x86/x64 & embedded computing
SLB 9665XT2.0	2.0 rev. 1.16	LPC	-40 … +85	TSSOP-28	✓	Industrial embedded computing on x86/x64
SLB 9665XQ2.0	2.0 rev. 1.16	LPC	-40 … +85	VQFN-32	✓	Industrial embedded computing on x86/x64
SLB 9670						
SLB 9670VQ1.2	1.2 rev. 116	SPI	-20 … +85	VQFN-32	✓	All architectures
SLB 9670XQ1.2	1.2 rev. 116	SPI	-40 … +85	VQFN-32	✓	All architectures
SLB 9670VQ2.0	2.0 rev. 1.16	SPI	-20 … +85	VQFN-32	✓[3)]	All architectures
SLB 9670XQ2.0	2.0 rev. 1.16	SPI	-40 … +85	VQFN-32	✓[3)]	All architectures

2) Not all features apply to all product configurations – please refer to product data book for further details.
3) Certification ongoing

OPTIGA™ product family

Infineon's OPTIGA™ family consists of products and solutions for securing embedded systems. All products are based on secured hardware and software. In addition to the OPTIGA™ TPM products, the overall product family also includes the OPTIGA™ Trust line of products with products and solutions for device authentication.

Published by
Infineon Technologies AG
85579 Neubiberg, Germany

© 2015 Infineon Technologies AG.
All Rights Reserved.

Order Number: B189-I0166-V2-7600-EU-EC-P
Date: 10 / 2015

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.

Общество с ограниченной ответственностью «МосЧип» ИНН 7719860671 / КПП 771901001
Адрес: 105318, г.Москва, ул.Щербаковская д.3, офис 1107

Данный компонент на территории Российской Федерации

Вы можете приобрести в компании MosChip.

Для оперативного оформления запроса Вам необходимо перейти по данной ссылке:

http://moschip.ru/get-element

Вы можете разместить у нас заказ для любого Вашего проекта, будь то серийное производство или разработка единичного прибора.

В нашем ассортименте представлены ведущие мировые производители активных и пассивных электронных компонентов.

Нашей специализацией является поставка электронной компонентной базы двойного назначения, продукции таких производителей как XILINX, Intel (ex.ALTERA), Vicor, Microchip, Texas Instruments, Analog Devices, Mini-Circuits, Amphenol, Glenair.

Сотрудничество с глобальными дистрибьюторами электронных компонентов, предоставляет возможность заказывать и получать с международных складов практически любой перечень компонентов в оптимальные для Вас сроки.

На всех этапах разработки и производства наши партнеры могут получить квалифицированную поддержку опытных инженеров.

Система менеджмента качества компании отвечает требованиям в соответствии с ГОСТ Р ИСО 9001, ГОСТ РВ 0015-002 и ЭС РД 009

Офис по работе с юридическими лицами:

105318, г.Москва, ул.Щербаковская д.3, офис 1107, 1118, ДЦ «Щербаковский»

Телефон: +7 495 668-12-70 (многоканальный)

Факс: +7 495 668-12-70 (доб.304)

E-mail: info@moschip.ru

Skype отдела продаж:
moschip.ru
moschip.ru_4
moschip.ru_6
moschip.ru_9