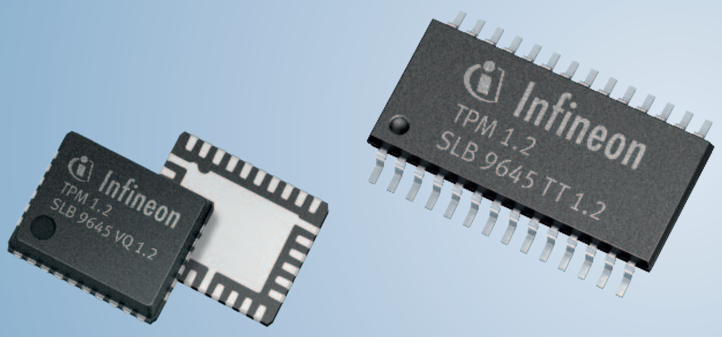

Product Brief

OPTIGA™ TPM SLB 9645/60/65

TPM v1.2 and 2.0 for Highest Level of Certified Platform Protection

Infineon is a leading force in the Trusted Computing Group and provider of micro-controllers for platform security applications since the introduction of the first Trusted Platform Modules (TPM) in 2003. Infineon TPMs were the first to be certified according to the rigorous Common Criteria (EAL4+) evaluation.

The new SLB 9645/60/65 products of the OPTIGA™ TPM family are leading the way into the next generation of trusted computing: supporting more and different operating systems and CPU architectures and the migration from TPM 1.2 to 2.0.

Based on newest security and chip technology, a variety of products with different interfaces, packages and temperature ranges allows system designers to make the best choice for their needs.

Security and Functionality

All OPTIGA™ TPM products are based on the same advanced hardware security technology. The TPM 1.2 implementation has already achieved CC EAL4+ certification and serves as a basis for all TPM 1.2 products and firmware upgrades.[1] The TPM 2.0 implementation is based on the TCG's current 2.0 specification.

Performance and Power

Implemented on a state-of-the-art 16-bit security controller from Infineon, the products meet Microsoft Windows 8 boot time and performance criteria. A sleep current of 150µA (typ.) allows for power efficient battery operated designs.

Extended Temperature Range and Packages

With support for standard or extended temperature range the products of the OPTIGA™ TPM family meet the requirements for industrial and embedded applications which previously could not be equipped with a TPM security processor.
A smaller VQFN package (5 x 5mm^2) saves precious board space on mobile platforms.

Migrate to TCG TPM 2.0

Depending on the operating system and applications the migration to TPM 2.0 can present challenges: Firmware-update the OPTIGA™ TPM SLB 9660 from 1.2 to 2.0 or the SLB 9665 from 2.0 to 1.2 and have the flexibility you need.

www.infineon.com

Main Features

All Products
- HW ready for TPM 1.2 and 2.0
- Standard (-20 … +80°C) and wide temperature range (-40 … +85°C)
- TSSOP-28 and VQFN-32 package
- Optimized for battery operated devices: low standby power consumption (typ.150µA)
- Meeting Intel, Microsoft and Google certification criteria for successful platform qualification

SLB 9645 – 1.2
- Compliant to TPM 1.2 Rev. 116
- I^{2}C interface up to 400kbps
- Based on Common Criteria
- EAL4+ certified TPM 1.2 hardware and firmware [1]

SLB 9660 – 1.2
- Compliant to TPM 1.2 Rev. 116
- LPC interface 24/33MHz
- FW upgrade to TPM 2.0
- TCG and Common Criteria EAL4+ (certification pending)
- FIPS 140-2 certified mode (certification pending)
- TIS 1.3
- Pin-compatible to SLB 9665

SLB 9665 – 2.0
- Compliant to TPM 2.0 Rev. 0.9x
- LPC interface 24/33MHz
- FW upgrade to TPM 1.2
- TIS 1.3
- Pin compatible to SLB 9660

OPTIGA™ TPM

TPM v1.2 and 2.0 for Highest Level of Certified Platform Protection

Product Summary

Sales Code (SLB…)	TPM Version	Interface	Temp. Range [°C]	Package	Typical/recommended use
SLB 9645					
9645 TT1.2 FW133.32	1.2 Rev. 116	I^{2}C	-20 … +80	TSSOP-28	Notebook, Desktops, Tablets, mobile computing on Windows 8 RT, Linux
9645 XQ1.2 FW133.32	1.2 Rev. 116	I^{2}C	-40 … +85	VQFN	Industrial embedded computing
9645 XT1.2 FW133.32	1.2 Rev. 116	I^{2}C	-40 … +85	TSSOP-28	Industrial embedded computing
9645 TT1.2 FW133.32GOOG	1.2 Rev. 116	I^{2}C	-20 … +80	TSSOP-28	Google Chromebook on ARM
9645 VQ1.2 FW133.32GOOG	1.2 Rev. 116	I^{2}C	-20 … +80	VQFN	Google Chromebook on ARM
SLB 9660					
9660 TT1.2 FW4.40	1.2 Rev. 116	LPC	-20 … +80	TSSOP-28	Notebook, Desktops, Tablets on x86
9660 VQ1.2 FW4.40	1.2 Rev. 116	LPC	-20 … +80	VQFN	Notebook, Desktops, Tablets on x86
9660 XT1.2 FW4.40	1.2 Rev. 116	LPC	-40 … +85	TSSOP-28	Industrial embedded computing on x86
9660 XQ1.2 FW4.40	1.2 Rev. 116	LPC	-40 … +85	VQFN	Industrial embedded computing on x86
9660 TT1.2 FW4.40GOOG	1.2 Rev. 116	LPC	-20 … +80	TSSOP-28	Google Chromebook on x86
9660 VQ1.2 FW4.40GOOG	1.2 Rev. 116	LPC	-20 … +80	VQFN	Google Chromebook on x86
SLB 9665					
9665 TT1.2 FW5.00	2.0 Rev. 0.96	LPC	-20 … +80	TSSOP-28	Windows 8 on x86
9665 VQ1.2 FW5.00	2.0 Rev. 0.96	LPC	-20 … +80	VQFN	Windows 8 on x86

Note

1) The Trusted Computing Group (TCG) protection profile for the standardized TPM v1.2 only considers an LPC interface.
The I^{2}C interface is not part of the TCG defined specification and cannot be certified formally.
The SLB 9645 is built on the TCG compliant, EAL4+ certified TPM hardware and firmware, with the addition of I^{2}C support.

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

3) TPM 2.0 upgradeability statement is based on TCG library and PC Client specification 2.0 Rev. 0.96.

Published by
Infineon Technologies AG
85579 Neubiberg, Germany

Visit us:
www.infineon.com

Order Number: B189-H9831-X-X-7600
Date: 09 / 2013

Attention please!
The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie"). With respect to any examples or hints given herein, any typical values stated herein and/or any information regarding the application of the device, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

Information
For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office (www.infineon.com).

Warnings
Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office. Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.