

Information note

N° 079/24

confidential

Dear customer,

With this Infineon Technologies AG information note, we would like to inform you about the following

Introduction of a firmware security update for OPTIGA™ TPM SLB 9665 and SLB/SLM/SLI 9670 families

Infineon Technologies AG

Postal address D-81726 München Internet www.infineon.com Headquarters Am Campeon 1-15, D-85579 Neubiberg Phone +49 (0)89 234-0

Chairman of the Supervisory Board Dr. Herbert Diess

Management Board Jochen Hanebeck (CEO), Elke Reichart, Dr. Sven Schneider, Andreas Urschitz, Dr. Rutger Wijburg

Registered office Neubiberg Commercial register Amtsgericht München HRB 126492

Information note

N° 079/24

confidential

► Products affected

- The affected product list is attached to this Info Note

► Detailed change information

Subject Infineon has been contacted by the TCG-VRT (Trusted Computing Group – Vulnerability Response Team) about a vulnerability in their official TCG reference implementation of the TPM 2.0 specification (case identifier “VRT0009”).

We are planning to offer an update for the affected products to address this vulnerability from the TCG reference implementation. Our policy is to reflect state-of-the-art in our security solutions. Therefore, the following update will also be included:

- TPM crypto library in the latest version

Reason For security reasons, Infineon strongly recommends updating the affected products with the latest firmware.

As per TCG decision, the details on VRT0009 are under public disclosure embargo and further details will be available at a later point in time.

Description

<u>Old</u>	<u>New</u>
■ TPM with TCG reference code implementation subject to TCG VRT0009 vulnerability.	■ Customers updating TPM firmware to fully utilize the advantages of TPM with state-of-the-art protection
■ --	■ Improved Asymmetric Crypto Library
■ SLB9665 (TPM2.0): FW5.00 through FW5.63	■ SLB9665 (TPM2.0): FW5.66
■ SLB9670 (TPM2.0): FW7.00 through FW7.63	■ SLB9670 (TPM2.0): FW7.66
■ SLB9670 (TPM2.0): FW7.85	■ SLB9670 (TPM2.0): FW7.86
■ SLM9670: FW13.11 ■ SLI9670: FW 13.11	■ SLM9670: FW13.16 ■ SLI9670: FW13.16

Information note

N° 079/24

confidential

► Product identification

The traceability is achieved by new SP-numbers (order numbers) for each new FW-Version

► Impact of change

New products:

Infineon will deliver new products of the SLB/SLM/SLI9670 including a firmware with the updated functionality. For all new firmware versions, new SP numbers (order numbers) have been created.

Older firmware versions will still be available but are not recommended for existing and new designs.

In existing designs new TPM versions can be replaced easily. New production lots from system suppliers should be converted to the new version as well.

Existing products (in market)

- Existing products can be updated through firmware updates during the device assembly process or on the device in the field.
To learn more about the detailed preconditions and FW-update options, customers are asked to check the confidential library myICP which provides access to relevant files and instructions.
For further questions, contact Infineon technical support.

► Attachments

Detailed change information can be found: MyICP in the library Trusted Computing in each product folder (e.g. "TPM SLB xxx Documents and Tools folder" includes the update for the SLB xxx.)

► Intended start of delivery

Timeline for parts delivery:

- SLB9670 (TPM2.0): FW7.66 – 05/2025
- SLB9670 (TPM2.0): FW7.86 – 05/2025
- SLM9670: FW13.16 – 05/2025
- SLI9670: FW13.16 – 05/2025

Timeline for FW update availability:

- SLB9665 (TPM2.0): FW5.66 – 02/2025
- SLB9670 (TPM2.0): FW7.66 – 02/2025
- SLB9670 (TPM2.0): FW7.86 – 02/2025
- SLM9670: FW13.16 – 02/2025
- SLI9670: FW13.16 – 02/2025

Information note

N° 079/24

confidential

If you have any questions, please do not hesitate to contact your local sales office.