INFORMATION NOTE

N° 133/17

Dear Customer,

With this INFINEON Technologies Information Note we would like to inform you about the following

Introduction of TPM firmware security update regarding RSA key generation of SLB 96xx family (see products affected)

Infineon Technologies AG
Postal Address Headquarters: Am Campeon 1-12, D-85579 Neubiberg, Phone +49 (0)89 234-0
Chairman of the Supervisory Board: Wolfgang Mayrhuber
Management Board: Dr. Reinhard Ploss (CEO), Dominik Asam, Dr. Helmut Gassel, Jochen Hanebeck
Registered Office: Neubiberg Commercial Register
Amtsgericht München HRB 126492

INFORMATION NOTE

N° 133/17

Introduction of TPM firmware security update for RSA key generation of SLB 96xx family (see products affected)

▶ Products affected:

Detailed affected product list:

- SLB9645 (TPM1.2): FW133.32, FW149.32
- SLB9655 (TPM 1.2): FW4.23, FW4.31, FW4.32, FW4.33
- SLB 9656 (TPM1.2): FW4.23, FW4.31, FW4.32, FW4.33
- SLB9660 (TPM1.2): FW4.40, FW4.42
- SLB9670 (TPM1.2): FW6.10, FW6.40, FW6.41, FW6.42
- SLB9665 (TPM2.0): FW5.00, FW5.40, FW5.50, FW5.51, FW5.60, FW5.61
- SLB9670 (TPM2.0): FW7.10, FW7.40, FW7.60, FW7.61

▶ Detailed Change Information:

Subject: TPM firmware update (exact firmware version numbers see above) is recommended only for customers using RSA key generation functionality.

Reason: For security reasons, the affected products require a firmware update. The update has been made available; and it is advised that all relevant customers access this update.

Description:

Old	New
■ Customers using the RSA key generation functionality within the impacted TPM products listed.	Customers updating TPM firmware to utilize full advantages of TPM hardware security for RSA key generation that meets the latest state-of-the-art protection
■ Products with old firmware in market: • SLB9645 (TPM1.2): FW133.32, FW149.32 • SLB9655/9656 (TPM1.2): FW4.23, FW4.31, FW4.32, FW4.33 • SLB9660 (TPM1.2): FW4.40, FW4.42 • SLB9670 (TPM1.2): FW6.10, FW6.40, FW6.41, FW6.42 • SLB9665 (TPM2.0): FW5.00, FW5.40, FW5.50, FW5.51, FW5.60, FW5.61 • SLB9670 (TPM2.0): FW7.10, FW7.40, FW7.60, FW7.61	■ The following products and firmware include the updated functionality and are starting to be shipped: • SLB 9645 (TPM1.2): FW133.33 • SLB 9655/9656 (TPM1.2): FW4.34 • SLB 9660 (TPM1.2): FW4.43 • SLB 9670 (TPM1.2): FW6.43 • SLB 9665 (TPM2.0): FW5.62 • SLB 9670 (TPM2.0): FW7.62

INFORMATION NOTE

N° 133/17

▸ Product Identification:

New firmware versions for all affected TPMs of SLB 96xx family from October 2017 onwards

- SLB 9645 (TPM1.2): FW133.33
- SLB 9655/9656 (TPM1.2): FW4.34
- SLB 9660 (TPM1.2): FW4.43
- SLB 9670 (TPM1.2): FW6.43
- SLB 9665 (TPM2.0): FW5.62
- SLB 9670 (TPM2.0): FW7.62

▸ Impact of Change:

New products:
As stated previously, Infineon will deliver new products 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 both in the factory and in the field

To learn more about the detailed preconditions and update options, customers are asked to check the confidential library myICP. Here you can access the relevant files and instructions.

▸ Attachments:

Detailed change information can be found:

- My ICP in the library Trusted Computing in each product folder (e.g. “TPM SLB 9655 Documents and Tools folder” includes the update for the SLB 9665 as well as the Q&A.

Access for myICP:

Either refer to:

https://www.infineon.com/cms/en/profile/#/myDashboard

“Login and registration (for externals)”

Or follow this detailed description

To get access to myICP please register under myInfineon (go to https://www.infineon.com/cms/en/ and click on the upper right corner (myInfineon login). Please register and confirm your registration via the confirmation email. In the next step please contact your Distribution partner (for partner please contact Infineon)in order to get access to the confidential part of Myinfineon called MyICP. You will then be promoted as a user of this confidential part and will need to confirm this via a second confirmation email. Afterwards you will have access to myICP where confidential documents are stored.
Once you are logged in and your access is confirmed, please go to Mydashboard

(upper right corner) and to my projects and documents. You will then land on the myICP space. Under Sites I have access to you will find Trusted Computing Documents. Please click on this and open the respective product folders.

Please note: Access to myICP is only available to customers with a current NDA.

If no existing NDA is in place, please contact your Distribution partner to generate an NDA with Infineon.

▶ Intended start of delivery:

- SLB 9645 (TPM1.2) FW133.33 – 01/2018
- SLB 9655 (TPM 1.2) FW4.34 – 02/2018
- SLB 9656 (TPM1.2) FW4.34 – 02/2018
- SLB 9660 (TPM1.2) FW4.43 – 11/2017
- SLB 9670 (TPM1.2) FW6.43 – 12/2017
- SLB 9665 (TPM2.0) FW5.62 – 10/2017
- SLB 9670 (TPM2.0) FW7.62 – 10/2017

If you have any further questions, please do not hesitate to contact your Distribution representative or Sales office.