



## Assurance Continuity Maintenance Report

**BSI-DSZ-CC-0958-2015-MA-02**

**Infineon Technologies AG Trusted Platform Module  
SLB9670\_1.2, v6.40.0190.00, v6.41.0197.00,  
v6.41.0198.00, v6.42.0204.00 and v6.42.0205.00**

from

**Infineon Technologies AG**



SOGIS  
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements*, version 2.1, June 2012 and the developers Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0958-2015.

The change to the certified product is at the level of implementation and guidance documentation. The change has no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0958-2015 dated 16 April 2015 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0958-2015.



Common Criteria  
Recognition Arrangement  
for components up to  
EAL 4

Bonn, 23 February 2017

The Federal Office for Information Security



## Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the Infineon Technologies AG Trusted Platform Module SLB9670\_1.2, v6.40.0190.00, v6.41.0197.00, v6.41.0198.00, v6.42.0204.00 and v6.42.0205.00, Infineon Technologies AG, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The Infineon Technologies AG Trusted Platform Module SLB9670\_1.2, v6.40.0190.00, v6.41.0197.00, v6.41.0198.00, v6.42.0204.00 and v6.42.0205.00 was changed due to the following TPM software fixes, which are described in more detail in [2]:

- The implementations of the TPM\_NV\_ReadValue and TPM\_NV\_WriteValue commands were improved by additional checks.
- The implementation of the TPM\_FieldUpgrade command was corrected, fixing an issue where sporadically an error code had been returned incorrectly under specific circumstances.

Configuration Management procedures required a change in the product identifier. Therefore, the version number changed from v6.41.0197.00 and v6.41.0198.00 to v6.42.0204.00 and v6.42.0205.00. As in the preceding maintenance process BSI-DSZ-CC-0958-2015-MA-01 which (for logistical reasons related to the firmware update process) introduced two technically identical new versions, the newly introduced versions v6.42.0204.00 and v6.42.0205.00 are technically identical, and are assigned separate version numbers only for the same logistical reasons.

The changes are also related to an update of the user guidance [6] and [8]. The changes in the user guidance provide some additional or updated information but do not affect the assurance.

## Conclusion

The change to the TOE is at the level of implementation and guidance documentation. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5].

The Security Target was editorially updated [7].

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0958-2015 dated 16 April 2015 is of relevance and has to be considered when using the product.

#### **Additional obligations and notes for the usage of the product:**

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG<sup>1</sup> Section 9, Para. 4, Clause 2).

This report is an addendum to the Certification Report [3].

---

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

## References

- [1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012
- [2] Impact Analysis SLB9670\_1.2, Infineon Technologies AG, Version 1.4, 23 December 2016 (confidential document)
- [3] Certification Report BSI-DSZ-CC-0958-2015 for SLB9670\_1.2 v6.40.0190.00, Bundesamt für Sicherheit in der Informationstechnik, 16 April 2015
- [4] Security Target: BSI-DSZ-CC-0958-2015, Version 1.0, Security Target Trusted Platform Module SLB9670\_1.2, Infineon Technologies AG, 25 March 2015
- [5] Configuration List: Evaluation Documentation - Configuration Management SLB9670\_1.2, Infineon Technologies AG, V0.6, 23 December 2016 (confidential document)
- [6] OPTIGA™ TPM SLB 9670 TPM 1.2 Trusted Platform Module, Databook Rev. 1.8, Infineon Technologies AG, 03 November 2016
- [7] Security Target Trusted Platform Module SLB9670\_1.2, Infineon Technologies AG, Version 1.2, 23 December 2016
- [8] OPTIGA™ TPM SLB 9670 TPM 1.2 Trusted Platform Module, Errata and Updates, Rev. 1.7, Infineon Technologies AG, 16 November 2016