Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0958-2015-MA-01

Infineon Technologies AG Trusted Platform Module SLB9670_1.2, v6.40.0190.00 and v6.41.0197.00 and v6.41.0198.00

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 2015-04-16 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, 3 May 2016

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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 and v6.41.0197.00 and v6.41.0198.00, 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 and v6.41.0197.00 and v6.41.0198.00 was changed to implement a minor bug fix. The version v6.40.0190.00 had an error with the effect that after a specific combination of different attacks, the TPM entered an unresponsive state, i.e. became inaccessible to any user or attacker. By means of a small change in the ordering of initialization code in the firmware, the problem could be fixed, without affecting the TOE security functionality in any other manner.

Configuration Management procedures required a change in the product identifier. Therefore the version number changed from v6.40.0190.00 to v6.41.0197.00 and v6.41.0198.00. The new versions v6.41.0198.00 and v6.41.0198.00 include the identical source code except the different version number. Having these two version numbers with identical content is necessary for logistic reasons of the field upgrade process, to prevent the installation of TPM firmware versions with a lower version number as the actual version.

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 2015-04-16 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.

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

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis for Common Criteria with Assurance Level EAL4 augmented (EAL4+), SLB9670_1.2, Version 1.3, 2016-04-01 (confidential document)

[3] Certification Report BSI-DSZ-CC-0958-2015 for SLB9670_1.2 v6.40.0190.00, Bundesamt für Sicherheit in der Informationstechnik, 2015-04-16

[4] Security Target: BSI-DSZ-CC-0958-2015, Version 1.0, 2015-03-25, Security Target Trusted Platform Module SLB9670_1.2, Infineon Technologies AG

[5] Configuration List: Evaluation Documentation - Configuration Management SLB9670_1.2, Infineon Technologies AG, V0.5, 2016-03-07 (confidential document)

[6] TPM Trusted Platform Module Version 1.2 Errata and Updates, Infineon Technologies AG, Rev.1.6, 2016-03-08

[7] Security Target: BSI-DSZ-CC-0958-2015, Version 1.1, 2016-03-08, Security Target Trusted Platform Module SLB9670_1.2, Infineon Technologies AG

[8] TPM Trusted Platform Module SLB9670 TCG Rev. 116, Databook, Infineon Technologies AG, Ref. 1.6, 2016-02-12