Assurance Continuity Maintenance Report

BSI-DSZ-CC-1020-2016-MA-01

Infineon Technologies AG Trusted Platform Module SLB9665_2.0, v5.60.2677.00, v5.61.2785.00, v5.61.2789.00

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-1020-2016.

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.

Common Criteria

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-1020-2016 dated 27 October 2016 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-1020-2016.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 16 December 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 SLB9665_2.0, v5.60.2677.00, v5.61.2785.00, v5.61.2789.00, 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 SLB9665_2.0, v5.60.2677.00, v5.61.2785.00, v5.61.2789.00 was changed due to an improved abort handling of the deterministic random bit generator and memory management with the objective of improving the reliability of the TOE. Also the AES self-test is switched to a known answer test in CFB mode. Additionally the firmware was hardened by calling the change of the register masking periodically. Configuration Management procedures required a change in the product identifier. Therefore, the version number changed from v5.60.2677.00 to v5.61.2785.00, v5.61.2789.00 (two new version numbers with identical functionality are introduced for logistical reasons related to the firmware update process).

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 <u>not</u> been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1020-2016 dated 27 October 2016 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[1] 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] Evaluation Documentation SLB9665_2.0 Impact Analysis, Infineon Technologies AG, Version 1.7, 4 November 2016 (confidential document)

[3] Certification Report BSI-DSZ-CC-1020-2016 for Infineon Technologies AG Trusted Platform Module SLB9665_2.0 v5.60.2677.00, Bundesamt für Sicherheit in der Informationstechnik, 27 October 2016

[4] Security Target BSI-DSZ-CC-1020, Version 1.2, Security Target, Trusted Platform Module SLB9665_2.0, Infineon Technologies AG, 25 August 2016

[5] Evaluation Documentation SLB9665_2.0 Configuration Management Version 0.5, 07 November 2016 (confidential document)

[6] OPTIGA™TPM SLB 9665 TPM2.0 Trusted Platform Module Databook, Infineon Technologies AG, Revision 2.7, 18 November 2016 (confidential document)

[7] Security Target, Trusted Platform Module SLB9665_2.0, Infineon Technologies AG, Version 1.3, 2 December 2016

[8] OPTIGA™TPM SLB 9665 TPM2.0 Trusted Platform Module Errata and Updates, Infineon Technologies AG, Revision 1.8, 18 November 2016 (confidential document)