Assurance Continuity Maintenance Report

BSI-DSZ-CC-0915-2016-MA-03

BCM_SPS02 Secure Processing System with Firmware version 002.030

from

NXP

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-0915-2016.

The change to the certified product is at the level of bug fixing. 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-0915-2016 dated 25 February 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-0915-2016.

Bonn, 2 December 2016

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 BCM_SPS02 Secure Processing System with Firmware version 002.030, NXP, 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 BCM_SPS02 Secure Processing System with Firmware version 002.030, was changed due to bug fixes. Configuration Management procedures required a change in the product identifier. Therefore the version number changed from Firmware version 002.020 to Firmware version 002.030.

Conclusion

The change to the TOE is at the level of implementation. 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 [6].

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-0915-2016 dated 25 February 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.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [7].

According to the scheme rules, evaluation results outlined in the document ETR for composite evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR for composite evaluation is not older than eighteen months and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

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 BCM_SPS02 with FW v002.030, Revision 0.5, 28.09.2016, NXP Semiconductors (confidential document)

[3]   Certification Report BSI-DSZ-CC-0915-2016 for BCM_SPS02 Secure Processing System with IC Dedicated Software Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, 25 February 2016

[4]   Security Target BSI-DSZ-CC-0915-2016, Version 3.3, 2016-01-21, Security Target for the BCM_SPS02, Broadcom Corporation (confidential document)

[5]   Configuration list, Rev. 2.3, 15. September 2016, NXP Semiconductors (confidential document)

[6]   Security Target BSI-DSZ-CC-0915-2016, Version 3.5, 2016-09-28, Security Target for the BCM_SPS02, Broadcom Corporation (confidential document)

      Security Target BSI-DSZ-CC-0915-2016, Version 1.2, 2016-11-28, Security Target Lite for the BCM_SPS02, Broadcom Corporation (sanitised public document)

[7]   EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP) for the BCM_SPS02, Version 2, 2016-05-13, TÜV Informationstechnik GmbH (confidential document)

[8]   EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY) for the BCM_SPS02, Version 2, 2016-05-13, TÜV Informationstechnik GmbH (confidential document)