



## Assurance Continuity Maintenance Report

**BSI-DSZ-CC-0915-2016-MA-02**

**BCM\_SPS02 Secure Processing System with  
Firmware version 002.010 or 002.020**

from

**Broadcom Corporation**



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-0915-2016.

The certified product itself did not change. The changes are related to including an additional production site already evaluated into the scope of the certificate.

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.



Common Criteria  
Recognition Arrangement  
for components up to  
EAL 4

Bonn, 27 July 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 [5] and the Evaluation Technical Report [8] (updated due to a partial ALC re-evaluation).

The vendor for the BCM\_SPS02 Secure Processing System with Firmware version 002.010 or 002.020, Broadcom Corporation, 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 certified product itself did not change.

The changes are related to including an additional production site already evaluated into the scope of the certificate. The Common Criteria assurance requirements:

ALC – Life cycle support (i.e. ALC\_CMC.4, ALC\_CMS.5, ALC\_DEL.1, ALC\_DVS.2, ALC\_LCD.1, ALC\_TAT.2)

are fulfilled for the following site used for Assembly (WLBGA):

Amkor - Taoyuan  
AMKOR T1  
No. 1, Kao-Ping Sec, Chung-Feng Rd, Lungtan Township,  
Taoyuan County,  
Taiwan,  
R.O.C.

## Conclusion

The change to the TOE is at the level of an additional production site which is already evaluated. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [6].

The Security Target [5] is still valid for the TOE.

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-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 [8].

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 Report for the BCM\_SPS02 ALC Maintenance, Version 0.3, 2016-03-30, Broadcom Corporation (confidential document)
- [3] Certification Report BSI-DSZ-CC-0915-2016 for BCM\_SPS02 Secure Processing System with IC Dedicated Software, Version 1.0 from Broadcom Corporation, Bundesamt für Sicherheit in der Informationstechnik, 25 February 2016
- [4] Assurance Continuity Maintenance Report BSI-DSZ-CC-0915-2016-MA-01 for BCM\_SPS02 Secure Processing System with Firmware version 002.010 or 002.020 from Broadcom Corporation, Bundesamt für Sicherheit in der Informationstechnik, 1 June 2016
- [5] SECURITY TARGET LITE for the BCM\_SPS02, Version 1.1, 2016-05-24, Broadcom Corporation (public version)
- [6] Configuration list for the BCM\_SPS Version 2.2, 2016-06-24, Broadcom Corporation (confidential 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)