



## Assurance Continuity Maintenance Report

**BSI-DSZ-CC-0837-V3-2016-MA-02**

**NXP Secure Smart Card Controller  
P60x080/052/040yVC(Y/Z/A)/yVG with IC Dedicated  
Software**

from

**NXP Semiconductors Germany GmbH**



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-0837-V3-2016 updated by BSI-DSZ-CC-0837-V3-2016-MA-01.

The change to the certified product is at the level of development/production sites. The change has no effect on assurance. The certified product itself did not change. The changes are related to including an additional production site that is already certified 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-0837-V3-2016 dated August 5, 2016 updated by BSI-DSZ-CC-0837-V3-2016-MA-01 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-0837-V3-2016 dated August 5, 2016 updated by BSI-DSZ-CC-0837-V3-2016-MA-01.

Bonn, 7 June 2017

The Federal Office for Information Security



Common Criteria  
Recognition Arrangement  
for components up to  
EAL 4



## 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 NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG with IC Dedicated Software, NXP Semiconductors Germany GmbH, 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 that is already certified into the scope of the certificate. The Common Criteria assurance requirements:

ALC – Life cycle support (i.e. ALC\_CMC.5, ALC\_CMS.5, ALC\_DEL.1, ALC\_DVS.2, ALC\_FLR.1, ALC\_LCD.1, ALC\_TAT.3)

are fulfilled for the following added sites:

SPIL, Siliconware Precision Industries Co., Ltd., Chung Shan Facility and Da Fong Facility Chung Shan Facility: No. 153, Sec. 3, Chung Shan Rd., Tantz, Taichung, Taiwan, R.O.C.

(Test centre, wafer treatment, module assembly)

The procedure lead to an updated version of the Evaluation Technical Report (ETR) [7] as well as an editorial update to the ETRfc [6].

## Conclusion

The change to the TOE is at the level of production sites. The change has no effect on assurance. As a result of the changes the evaluation reference list for the TOE has been updated [5].

The Security Target [4] 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-0837-V3-2016 dated August 5, 2016 updated by BSI-DSZ-CC-0837-V3-2016-MA-01 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 [6].

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.

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 Report, NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG Impact Analysis Report Rev. 1.0, 15 March 2017
- [3] Certification Report BSI-DSZ-CC-0837-V3-2016 for NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG with IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, August 5, 2016 and Maintenance Addendum BSI-DSZ-CC-0837-V3-2016-MA-01, June 07, 2017
- [4] Security Target Lite BSI-DSZ-CC-0837-V3-2016, Version 2.3, 2016-02-05, NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG Security Target, NXP
- [5] Evaluation Reference List, NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG, NXP Semiconductors, Business Unit Identification, Rev. 1.51 26 January 2017
- [6] Evaluation Technical Report for Composite Evaluation (ETR COMP) for the P60x080/052/040yVC(Y/Z/A)/VG, version 3, 2016-07-04, TÜV Informationstechnik GmbH
- [7] Evaluation Technical Report Summary (ETR SUMMARY) for the P60x080/052/040yVC(Y/Z/A)/VG, version 3, 2017-04-24, TÜV Informationstechnik GmbH