Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0897-V2-2014-MA-01

NXP Secure Smart Card Controller P60D080/052/040yVC(Z/A)/yVG including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1

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-0897-V2-2014.

The certified product itself did not change. The changes are related to an update of the documentation and including an additional production site already evaluated and certified into the scope of the certificate BSI-DSZ-CC-0939-2015.

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-0897-V2-2014 dated 24 October 2014 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-0897-V2-2014.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 15 June 2015

The Federal Office for Information Security

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

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 P60D080/052/040yVC(Z/A)/yVG including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1, 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 already evaluated and certified into the scope of the certificate BSI-DSZ-CC-0939-2015. 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 and ALC_TAT.2)

are fulfilled for the following site used for Wafer Processing:

Ardentec Corporation, Test Centre Kaiyuan Site (K Site)
No. 24, Wen-Huan Rd.
Hsin-Chu Industrial Park,
Hu-Kou
Hsin-Chu Hsien
Taiwan 30351,R.O.C.

Note that the Wafer Test Service of the site is not used, only the Wafer Level Chip Scale Packaging (WLCSP) service is used.

Beside the introduction of the Ardentec Corporation, Test Centre Kaiyuan Site (K Site) only some minor editorial changes in the documentation have been done.

Conclusion

The change to the TOE is at the level of production sites and documentation. The change has no effect on assurance. As a result of the changes the Evaluation Reference List for the TOE has been updated [6].

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-0897-V2-2014 dated 24 October 2014 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 NXP Secure Smart Card Controller P60D080/052/040yVC(Z/A)/yVG, Rev. 1.1, 26 March 2015 (confidential document)

[3] Certification Report BSI-DSZ-CC-0897-V2-2014 for NXP Secure Smart Card Controller P60D080/052/040yVC(Z/A)/yVG including IC Dedicated Software MIFARE Plus MF1PLUSx0 or MIFARE Plus MF1PLUSx0 and MIFARE DESFire EV1, Bundesamt für Sicherheit in der Informationstechnik, 24 October 2014

[4] Security Target Lite BSI-DSZ-CC-0897-V2-2014, Version 2.0, 21 August 2014, NXP Secure Smart Card Controller P60D080/052/040yVC(Z/A)/yVG Security Target Lite, NXP Semiconductors (sanitised public document)

[5] NXP Secure Smart Card Controller P60x080/052/040yVC(Z/A)/yVG, Configuration List, Version 01.50, 23 July 2014, NXP Semiconductors, Business Unit Identification (confidential document)

[6] Evaluation Reference List, NXP Secure Smart Card Controller P60D080/052/040PVC(Y/Z/A)/PVG and NXP Secure Smart Card Controller P60D080/052/040yVC(Z/A)/yVG, NXP Semiconductors, Business Unit Identification, Rev. 1.44, 26 March 2015 (confidential document)

[7] Product data sheet addendum: SmartMX2 family P60x040/052/080 VC/VG Wafer and delivery specification, NXP Semiconductors, Revision 3.4, Document Number 237234, 18 July 2014 (confidential document)

[8] ETR for composite evaluation according to AIS 36, Version 3, 17 October 2014, TÜV Informationstechnik GmbH (confidential document)