Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0845-V2-2013-MA-02

NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y/B) with IC Dedicated Software FW5.0

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-0845-V2-2013.

The change to the certified product is at the level of new sites and configuration options. The change has no effect on assurance. The identification of the maintained product is indicated by an extension of the product name.

The certified product itself did not change.

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-0845-V2-2013 dated 19 December 2013 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-0845-V2-2013.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 16 October 2014

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 NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y/B) with IC Dedicated Software FW5.0, 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 NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y/B) with IC Dedicated Software FW5.0 was changed due to the need for extended production capacity and second source capabilities. Configuration Management procedures required a change in the product identifier. Therefore another product name was introduced, P60x144/080PVA(B).

The certified product hardware itself did not change.

The changes are related to including a additional sites already evaluated/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 sites added:

Ardentec Corporation
No. 3, Gungye 3rd Rd.
Hsin-Chu Industrial Park,
Hu-Kou,
Hsin-Chu Hsien
Taiwan 30351, R.O.C.

NedCard Shanghai Microelectronics Co. Ltd.
Standardized Plant Building #8, No. 789
Puxing Road, Caohejing
Hi-Tech Park, EPZ, 201114 Shanghai
People's Republic of China

NXP Semiconductors Netherlands B.V.
Campus buildings BX, FB, FD and BF
Gerstweg 2
6534AE Nijmegen
The Netherlands

The following two sites were certified by Netherlands Scheme for Certification in the area of IT Security (NSCIB). In those two particular cases the certificates are recognised by BSI.

NXP High Tech Campus Building 60 Secure Room 131
Building 60, High Tech Campus
5656AG, Eindhoven
The Netherlands

Atos Bydgoszcz
Building BETA Secure Room B20S1
Biznes Park
ul. Kraszewskiego 1
85-240 Bydgoszcz
Poland

For formal reasons it was neccessary to provide an updated version of the ETR for comopsition [8]. No new tests were done, therefore the validity of the previous ETR for composition [7] is not extended.

Conclusion

The change to the TOE is at the level of development/production sites and configuration options. 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 not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0845-V2-2013 dated 19 December 2013 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] Impayt Analysis Report, NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y/B), Rev. 2.1, 02 September 2014, NXP Semiconductors, Business Unit Identification, (confidential document)

[3] Certification Report BSI-DSZ-CC-0845-V2-2013 for NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y) with IC Dedicated Software FW5.0, Bundesamt für Sicherheit in der Informationstechnik, 19 December 2013

[4] NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y) Security Target Lite, BSI-DSZ-CC-0845-V2-2013, NXP Semiconductors, Business Unit Identification, Rev. 2.11, 24 October 2013 (sanitised public document)

[5] Configuration List NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y/B), Revision 2.20, NXP Semiconductors, Business Unit Identification, 08 August 2014 (confidential document) and
Firmware Configuration List NXP Secure Smart Card Controller P60x144/080PVA/PVA(B)/PVE, Revision 1.7, NXP Semiconductors, 09 July 2014 (confidential document) and
Appendix of the Configuration List for composite evaluation NXP Secure Smart Card Controller P60x144/080eVA/eVA(Y/B), NXP Semiconductors, Revision 2.30, 08 August 2014 (confidential document) and
Customer specific Appendix of the Configuration List NXP Secure Smart Card Controller P60x144/080eVA/eVA(Y/B), NXP Semiconductors, Revision 2.30, 08 August 2014 (confidential document) and
Evaluation Reference List NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y/B) and NXP Secure Smart Card Controller P60x144/080yVA/yVA(B), Rev. 1.10, NXP Semiconductors, Business Unit Identification, 02 September 2014 (confidential document)

[6] Security Target lite NXP Secure Smart Card Controller P60x144/080PVA(Y/B), Revision 2.20, NXP Semiconductors, Business Unit Identification, 08 August 2014 (sanitised public document)

[7] ETR for composition according to AIS36, NXP P60x144/080PVA/PVA(Y), T-Systems GEI GmbH, Version 1.7, 5 December 2013 (confidential document)

[8] ETR for composition according to AIS36, NXP P60x144/080PVA/PVA(Y/B), T-Systems GEI GmbH, Version 1.8, 02 October 2014 (confidential document)

[9] Evaluation Technical Report, NXP P60x144/080PVA/PVA(Y/B), T-Systems GEI GmbH, Version 2.0, 02 October 2014 (confidential document)