Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0837-2013-MA-01

NXP Smart Card Controller P60D080/052/040PVC(y) and P60C080/052/040PVC(y) with IC dedicated Software

from

NXP Semiconductors Germany GmbH

Common Criteria Recognition Arrangement
for components up to EAL4

Common Criteria

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-0837-2013.

The changes to the certified product are at the level of chip configuration and of specific identification numbers, changes that have no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product.

The nature of the changes was considered by the ITSEF TÜV Informationstechnik GmbH, approved by BSI. The conclusion was that they are classified as minor changes with no impact on security 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-0837-2013 dated 24 June 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-0837-2013.

Bonn, 4 February 2014

SOGIS IT SECURITY CERTIFIED

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 Smart Card Controller P60D080/052/040PVC and P60C080/052/040PVC 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 NXP Smart Card Controller P60D080/052/040PVC and P60C080/052/040PVC with IC dedicated Software, was changed due to yield improvement. The updated product configuration was examined by the ITSEF. As concluded by the ITSEF only minor changes are implemented, thus allowing for a maintenance process.

Configuration Management procedures required a change in the product identifier. Therefore the name of the IC hardware was modified to NXP Secure Smart Card Controller P60x080/052/040PVC(Y). A version number within the security chip is altered for unambiguous identification. An update of the guidance documentation is not needed.

Conclusion

The change to the TOE is at the level of chip configuration. The change has no effect on assurance. As a result of the changes the configuration lists for the TOE have been updated [5], [6], [7].

The documents Security Target [8], Security Target Lite [9] and configuration lists ([5], [6], [7]) were editorially updated to reflect the changes made.

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-0837-2013 dated 24 June 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 correctly 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 [10].

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[1] 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] NXP Secure Smart Card Controller P60x080/052/040PVC Impact Analysis Report, Rev. 1.1, 18 December 2013, BSI-DSZ-CC-0837 (confidential document)

[3] Certification Report BSI-DSZ-CC-0837-2013 for NXP Smart Card Controller P60D080PVC and its major configurations P60D052PVC, P60D040PVC, P60C080PVC, P60C052PVC and P60C040PVC, Bundesamt für Sicherheit in der Informationstechnik, 24 June 2013

[4] Security Target Lite BSI-DSZ-CC-0837-2013, Version 1.0, 13 December 2012, NXP Secure Smart Card Controller P60x080/052/040PVC, NXP Semiconductors (sanitised public document)

[5] Configuration List, NXP Secure Smart Card Controller P60x080/052/040PVC/PVC(Y) Configuration List, Version 1.2, 18 December 2013, NXP Semiconductors (confidential document)

[6] Customer specific Appendix of the Configuration List, NXP Secure Smart Card Controller P60x080/052/040PVC, Version 1.2, 18 December 2013, NXP Semiconductors (confidential document)

[7] Appendix of the Configuration List for composite evaluation, NXP Secure Smart Card Controller P60x080/052/040PVC, Version 1.2, 18 December 2013, NXP Semiconductors (confidential document)

[8] Security Target, NXP Secure Smart Card Controller P60x080/052/040PVC/PVC(Y), Version 1.2, 18 December 2013, NXP Semiconductors (confidential document)

[9] Security Target Lite, NXP Secure Smart Card Controller P60x080/052/040PVC/PVC(Y), Version 1.2, 18 December 2013, NXP Semiconductors (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the product NXP Secure Smart Card Controller P60x080/052/040PVC, Version 5, 23 April 2013, BSI-DSZ-CC-0837, TÜV Informationstechnik GmbH (confidential document)