Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0555-2009-MA-01

NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD051V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software

from

NXP Semiconductors Germany GmbH

Common Criteria Recognition Arrangement
for components up to EAL4

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 1.0, February 2004 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-0555-2009.

The changes to the certified product are at the level of chip configuration, identification of different delivery forms and of other 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.

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, the assurance as outlined in the Certification Report BSI-DSZ-CC-0555-2009 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0555-2009.

Bonn, 30 December 2010

Common Criteria

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 P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD051V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each 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 TOE was changed due to

- Adding the major configuration P5CD051V1A. P5CD051V1A supports all minor configuration options presented in the Security Target [4] resp. [5]. Its major differences to other configurations are as follows: The EEPROM space available to the Security IC Embedded Software is reduced to 52 kBytes minus 256 Bytes, which are reserved for security rows (128 Bytes) and configuration data (128 Bytes). The contactless interface is enabled and configured for contactless communication according to ISO/IEC 14443 A. The hardware itself has not been changed;
- Changing the 4 Byte identifier related to the Mifare Mode;
- Generalizing the wafer delivery form and the module delivery form as outlined in the Security Target [4] resp. [5] chapter 1.4.1.3.

The changes are not significant from the standpoint of security, however Configuration Management procedures require a change in the identification number or name of the TOE including the new configurations. The extended new name of the TOE is: NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD051V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software.

Conclusion

The changes to the TOE are at the level of chip configuration, identification of different delivery forms and of other specific identification numbers, changes that have no effect on assurance. Examination of the evidence indicates that the changes performed are limited to configuration data for the TOE and related documentation.

The documents Security Target, Security Target Lite, Data Sheet and the Guidance Delivery and Operation Manual were editorially updated to reflect the changes made

(see [4], [5], [6], [7]). As a result of the changes the configuration list for the TOE [8] and specific list to support composite evaluations ([9], [10]) have been updated, too.

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.

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. 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 [11].

According to the scheme rules, evaluation results outlined in the document ETR for composition as listed above can usually be used for composite evaluations building on top, as long as the ETR for composition document is not older than one year and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

The document ETR for composition [11] has been updated recently as the result of a successful re-assessment of the TOE assurance. It outlines observations and recommendations to be followed by the Embedded Software developer and the evaluator of the composite product.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG Section 9, Para. 4, Clause 2).

This report is an addendum to the Certification Report [3].

References

[1] Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] P5CD016/021/041/051V1A and P5Cx081V1A Impact Analysis Report Rev. 1.0, December 16th, 2010, BSI-DSZ-CC-0555 (confidential document)

[3] Certification Report BSI-DSZ-CC-0555-2009 for NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification, Version 1.0, BSI, November 10th, 2009

[4] NXP Secure Smart Card Controllers P5CD016/021/041/051V1A and P5Cx081V1A Security Target, Version 1.4, October 25th, 2010 (confidential document)

[5] NXP Secure Smart Card Controllers P5CD016/021/041/051V1A and P5Cx081V1A Security Target Lite, Version 1.4, October 25th, 2010 (sanitised public document)

[6] Guidance, Delivery and Operation Manual NXP Secure Smartcard Controllers P5CD016/021/041/051 and P5Cx081, NXP Semiconductors, Business Unit Identification, Revision 1.4, 15 December 2010

[7] Data Sheet P5CD016/021/041/051 and P5Cx081 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Revision 3.3, 25 October 2010

[8] Configuration List for the NXP P5CD016/021/041/051 and P5Cx081 Secure Smart Card Controllers family, BSI-DSZ-CC-0555, NXP Semiconductors, Business Unit Identification, Version 1.1, 25 October 2010 (Confidential document)

[9] Configuration List for composite evaluation NXP P5CD016/021/041/051V1A and P5Cx081V1A, BSI-DSZ-CC-0555, NXP Semiconductors, Business Unit Identification, Version 1.2, 25 October 2010 (Confidential document)

[10] Customer specific appendix of the Configuration List NXP P5CD016/021/041/ 051V1A and P5Cx081V1A, BSI-DSZ-CC-0555, NXP Semiconductors, Business Unit Identification, Version 1.2, 25 October 2010 (Confidential document)

[11] ETR for composition according to AIS 36 for the Product NXP P5CD081V1A Secure Smart Card Controller, Version 1.2, 17 December 2010, BSI-DSZ-CC-0555, T-Systems GEI GmbH (confidential document)