Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0404-2007-MA-08

NXP Smart Card Controller P5CD040V0B, P5CD020V0B, P5CD012V0B, P5CC040V0B, P5CC021V0B

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 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-0404-2007 updated by a re-assessment on November 18th, 2011.

The change to the certified product is at the level of TOE documentation. The changes have no effect on assurance.

The certified product itself did not change. The changes are related to an update of the user guidance [6], the configuration list [5] and the data sheet [8].

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-0404-2007 dated July 5th, 2007, updated by a re-assessment on November 18th, 2011 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-0404-2007.

Bonn, 16 December 2011

SOGIS
INFORMATION TECHNOLOGY SECURITY
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

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 P5CD040V0B, P5CD020V0B, P5CD012V0B, P5CC040V0B, P5CC021V0B, 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. Due to recent lab measurements further requirements during the operation of the NXP Smart Card Controller P5CD040V0B, P5CD020V0B, P5CD012V0B, P5CC040V0B, P5CC021V0B have to be fulfilled for proper SPA and DPA resistance. The user guidance [6] was updated in this context. Only guidelines on proper software programming and examples have been updated/ added. The Configuration List [5] and the Data Sheet [8] were updated to reflect the changes. The version of the product remains unchanged. The changes are not significant from the standpoint of security.

Conclusion

The change to the TOE is at the level of documentation. The change has no effect on assurance. As a result of the changes the configuration list [5] as well as the data sheet [8] for the TOE have been updated. The Security Target [4] was editorially updated [7].

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-0404-2007 dated July 5th, 2007, updated by a re-assessment on November 18th, 2011 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [9] and [10] are the current versions of the ETR for composite evaluation and the ETR itself.

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 [9].

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 one year 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 Section 9, Para. 4, Clause 2).

In addition to the baseline certificate BSI notes that cryptographic functionalities with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for this functionality it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The Cryptographic Functionality 2-key Triple DES (2TDES) provided by the TOE achieves a security level of maximum 80 Bits (in general context).

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] Impact Analysis report P5CD040/ P5CC040/ P5CD020/ P5CC021/ P5CD012 V0B, Rev. 1.1, November 15th, 2011 (confidential document)

[3] Certification Report BSI-DSZ-CC-0404-2007 for “NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software”, Bundesamt für Sicherheit in der Informationstechnik, July 5th, 2007

[4] Security Target Lite, Evaluation of the P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.0, March 21st, 2007 (sanitized public document)

[5] Configuration List, Evaluation of the NXP P5Cx012/02x/040/073/080/144 family of Secure Smart Card Controllers, NXP Semiconductors, Business Unit Identification, Version 2.4, Nov 14th 2011(Confidential document)

[6] Guidance, Delivery and Operation Manual for the P5Cx012/02x/040/073/080/144V0B family of Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Rev. 1.9, May 31st, 2011

[7] Security Target Lite, Evaluation of the NXP P5CD040V0B Secure Smart Card Controller, NXP Semiconductors, Business Unit Identification, Version 1.91, November 14th, 2011

[8] Product Data Sheet, P5Cx012/02x/040/073/080/144 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Revision 3.9, Document Number: 126539, September 16th, 2011

[9] ETR for composition, NXP P5CD040V0B Secure Smart Card Controller, BSIDSZ- CC-0404, T-Systems GEI GmbH, Version 1.53,November 14th, 2011 (confidential document)

[10] Evaluation Technical Report, NXP P5CD040V0B Secure Smart Card Controller, BSI-DSZ-CC-404, T-Systems GEI GmbH, Version 1.53, November 16th, 2011 (confidential document)