Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0555-2009-MA-02

NXP Secure Smart Card Controllers P5CD016/021/041/051V1A and P5Cx081V1A

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-0555-2009 updated by a re-assessment on 3 November 2011.

The changes to the certified product are at the level of implementation, guidance and life cycle. The changes have no effect on assurance.

The nature of the changes was considered by the ITSEF T-Systems GEI 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-0555-2009 dated 10 November 2009 updated by a re-assessment on 3 November 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-0555-2009.

Bonn, 4 June 2012

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 Secure Smart Card Controllers P5CD016/021/041/051V1A and P5Cx081V1A, 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 Controllers P5CD016/021/041/051V1A and P5Cx081V1A has undergone changes in the implementation and life cycle to improve yield and logistic.

Configuration Management procedures required a change in the product identifier. The product name as given in the security target did not change. The customer can identify the version of the chip by checking the Device Coding Byte. The procedure is described in the Data Sheet.

The changes also include an update of the user guidance manual.

Conclusion

The changes to the TOE are at the level of implementation, guidance and life cycle. The changes have no effect on assurance. 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 [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-0555-2009 dated 10 November 2009 updated by a re-assessment on 3 November 2011 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [8] and [9] 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 [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 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[1] 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].

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 CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] Impact Analysis Report, P5CD016/021/041/051V1A and P5Cx081V1A, BSI-DSZ-CC-0555, Rev. 1.2, 23 February 2012 (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”, Bundesamt für Sicherheit in der Informationstechnik, 10 November 2009

[4] Security Target Lite BSI-DSZ-0555-2009, Version 1.3, 21 September 2009, P5CD016/021/041V1A and P5Cx081V1A NXP Smart Card Controllers, NXP Semiconductors (sanitised public document)

[5] 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 1.2 (Confidential document); in combination with: Configuration List for composite evaluation NXP P5CD016/021/041/051V1A and P5Cx081V1A, BSI-DSZ-CC-0555, NXP Semiconductors, Business Unit Identification, Version 1.3; in combination with: Customer specific appendix of the Configuration List NXP P5CD016/021/041/051V1A and P5Cx081V1A, BSI-DSZ-CC-0555, NXP Semiconductors, Business Unit Identification, Version 1.3 (confidential document)

[6] Guidance, Delivery and Operation Manual NXP Secure Smartcard Controllers P5CD016/021/041/051 and P5Cx081, NXP Semiconductors, Business Unit Identification, Revision 1.5, Document Number 171615 ,14 January 2011 (confidential document)

[7] Security Target Lite NXP Secure Smart Card Controllers P5CD016/021/041/051V1A and P5Cx081V1A, NXP Semiconductors, Revision 1.5, 19 September 2011

[8] ETR for composition, NXP P5CD081V1A Secure Smart Card Controller, BSI-DSZCC-0555, T-Systems GEI GmbH, Version 1.35, 28 October 2011 (confidential document)

[9] Evaluation Technical Report, NXP P5CD081V1A Secure Smart Card Controller, BSI-DSZCC-0555, T-Systems GEI GmbH, Version 1.4, 28 October 2011 (confidential document)