Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0645-2010-MA-01

NXP Secure Smart Card Controllers P5Cx128V0A/P5Cx145V0A, MSO

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-0645-2010.

The change to the certified product is at the level of TOE configuration and documentation. The changes have no effect on assurance. The identification of the maintained product is indicated by an additional version number compared to the certified product.

The certified product itself did not change. The changes are related to an additional configuration option of the TOE, to a change of the UID convention, to an update of the user guidance, and to an update of the Security Target.

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-0645-2010 dated 23 July 2010 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-0645-2010.

Bonn, 11 April 2011

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

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 P5Cx128V0A/P5Cx145V0A, MSO, 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 P5Cx128V0A/P5Cx145V0A, MSO were changed due to an additional configuration option of the TOE, to a change of the UID convention, to an update of the user guidance [6], and to an update of the Security Target [4]. The configuration list [5] and the data sheet [10] were updated to reflect the changes. Configuration Management procedures required an additional version number in the product identifier. Therefore the product name was extended by the additional major configuration P5CN145V0A.

Conclusion

The change to the TOE is at the level of TOE configuration and TOE documentation. 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], the user guidance [6], the data sheet [10], and the configuration list [5] were updated.

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-0645-2010 dated 23 July 2010 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 [8] 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 P5Cx128V0A/P5Cx145V0A, MSO, BSI-DSZ-CC-0645, Rev. 1.0, 31.01.2011, NXP Semiconductoers (confidential document)

[3] Certification Report BSI-DSZ-CC-0645-2010 for “NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software”, Bundesamt für Sicherheit in der Informationstechnik, 23.07.2010

[4] NXP Secure Smart Card controllers P5Cx128V0A/P5Cx145V0A, MSO Security Target, NXP Semiconductors, Business Unit Identification, Rev. 1.7, 16.12.2010 (confidential document)

[5] NXP Secure Smart Card controllers P5Cx128V0A/P5Cx145V0A, MSO Configuration List, NXP Semiconductors, Business Unit Identification, BSI-DSZ-CC-0645, Rev. 1.3, 25.01.2011; in combination with: External Configuration List for the NXP P5Cx128V0A/P5Cx145V0A family Secure Smart Card controllers, BSI-DSZ-CC-0645, NXP Semiconductors, Business Unit Identification, BSI-DSZ-CC-0645, Rev. 1.2, 25.01.2011; in combination with: Customer specific appendix of the Configuration List for the NXP P5Cx128V0A/P5Cx145V0A family Secure Smart Card controllers, BSI-DSZ-CC-0645, NXP Semiconductors, Business Unit Identification, BSI-DSZ-CC-0645, Rev. 1.1, 25.01.2011 (Confidential documents)

[6] NXP Secure Smart Card controllers P5Cx128V0A/P5Cx145V0A, MSO Guidance, Delivery and Operation Manual, NXP Semiconductors, Business Unit Identification, Rev. 1.4, 25.01.2011, Document number 185114

[7] NXP Secure Smart Card controllers P5Cx128V0A/P5Cx145V0A, MSO Security Target Lite, NXP Semiconductors, Business Unit Identification, Rev. 1.7, 16.12.2010

[8] ETR for composition according to AIS 36 for the Product NXP P5Cx128V0A/P5Cx145V0A, MSO Secure Smart Card Controller, Version 1.1, 15th July 2010, BSI-DSZ-CC-0645, T-Systems GEI GmbH (confidential document)

[9] Evaluation Technical Report, V. 1.1, 15th July 2010, BSI-DSZ-CC-0645, NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO; P5CC128V0A, MSO, each including IC Dedicated Software (confidential document)

[10] Data Sheet P5Cx128/P5Cx145 Family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Rev. 3.2, 25 January 2011, Document Number 177932