Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0645-2010-MA-02

NXP Secure PKI Smart Card Controllers P5CD145V0v; P5CC145V0v; P5CD128V0v, P5CC128V0v and P5CN145V0v, each including 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 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 updated by a re-assessment on 30 September 2011.

The changes to the certified product are at the level of implementation and life cycle. The changes have no effect on assurance. The identification of the maintained product is indicated by a modification of the product name.

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-0645-2010 dated 23 July 2010 updated by a re-assessment on 30 September 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-0645-2010.

Bonn, 27 February 2012

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY 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 Secure PKI Smart Card Controllers P5CD145V0v; P5CC145V0v; P5CD128V0v, P5CC128V0v and P5CN145V0v, each including 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 Secure PKI Smart Card Controllers P5CD145V0v; P5CC145V0v; P5CD128V0v, P5CC128V0v and P5CN145V0v, each including IC Dedicated Software has undergone changes in the implementation and life cycle to improve yield and logistic.

Configuration Management procedures required a change in the product identifier. Therefore the product type version was was changed from V0A to V0B.

The changes are related to including an additional development/production site already evaluated/certified into the scope of the certificate. The Common Criteria assurance requirements

ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

are fulfilled for the following site used for inlay production:

Smartrac Technology Germany GmbH
Gewerbeparkstraße 10
51580 Reichshof
Nordrhein-Westfalen
Bundesrepublik Deutschland

Conclusion

The changes to the certified product are at the level of implementation and life cycle. The changes have no effect on assurance. As a result of the changes the configuration list [5] and the data sheet [10] for the TOE have been updated. The Security Target [4] has been editorially updated [7].

Following the vote of the ITSEF T-Systems GEI GmbH the nature of the changes are classified as minor changes. Therefore certificate maintenance is the correct path to continuity of assurance.

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 updated by a re-assessment on 30 September 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 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).

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 cryptographic 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).

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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] Referenz IAR P5Cx128V0A/ P5Cx145V0A, MSO Impact Analysis Report, Rev. 1.3 Dec 13th, 2011(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] Security Target Lite BSI-DSZ-0645, Version 1.6, 07 June 2010, P5Cx128V0A/P5Cx145V0A, MSO NXP Smart Card Controllers, NXP Semiconductors (sanitised public document)

[5] NXP Secure Smart Card Controllers P5Cx128V0v/P5Cx145V0v Configuration List, NXP Semiconductors, Business Unit Identification, BSI-DSZ-CC-0645, Rev. 1.5, 22 September 2011; in combination with: External Configuration List for the NXP P5Cx128V0v/P5Cx145V0v family Secure Smart Card Controllers, BSI-DSZ-CC-0645, NXP Semiconductors, Business Unit Identification, Version 1.5, 18 August 2011; in combination with: Customer specific appendix of the Configuration List for the NXP P5Cx128V0v/P5Cx145V0v family Secure Smart Card Controllers, BSI-DSZ-CC-0645, NXP Semiconductors, Business Unit Identification, Version 1.5, 18 August 2011 (confidential documents)

[6] NXP Secure Smartcard Controllers P5Cx128/P5Cx145V0v, Guidance, Delivery and Operation Manual, NXP Semiconductors, Business Unit Identification, Rev. 1.5, 18 Aug 2011, Document number. 185115

[7] NXP Secure Smart Card Controllers P5Cx128V0v/P5Cx145V0v, MSO Security Target Lite, NXP Semiconductors, Business Unit Identification, Rev. 2.0, 18 August 2011 (sanitised public document)

[8] ETR for composition according to AIS36, BSI-DSZ-CC-0645, NXP P5Cx128V0A/P5Cx145V0A, MSO Secure Smart Card Controller, V1.33, September 29th, 2011 (confidential document)

[9] Evaluation Technical Report, BSI-DSZ-CC-0645, NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CN145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO; P5CC128V0A, MSO, each including IC Dedicated Software, V1.21, September 29th, 2011 (confidential document)

[10] Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Rev. 3.4, 16 September 2011, Document Number 177934