Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0465-2008-MA-02

NXP Smart Card Controller P5CC037V0A with specific 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-0465-2008 updated by a re-assessment on 31 July 2012.

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

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-0465-2008 dated 20 June 2008 updated by a re-assessment on 31 July 2012 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-0465-2008.

Bonn, 31 July 2012

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 P5CC037V0A with specific 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 changes of the NXP Smart Card Controller P5CC037V0A with specific IC Dedicated Software are at the level of guidance documentation and life cycle to improve logistic. The changes have no effect on assurance.

Due to the last reassessment process further requirements for the user guidance [6] have to be fulfilled. The Data Sheet [10] was updated to correct errors and align the content with other Data Sheets and do not affect security functions of the product.

An additional production site already evaluated into the scope of the certificate BSI-DSZ-CC-0666 was also included. The new site is used with identical interfaces and conditions as assessed in the above referenced certificate. The Common Criteria assurance requirements

ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.3),
ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.2, ALC_TAT.2)

are fulfilled for the following site used as Test Center and for Module Assembly :

NXP Semiconductors Taiwan Ltd
Assembly Plant Kaohsiung (APK)
10, Jing 5th Road
Nantze Export Processing Zone
81170 Kaohsiung
Taiwan (TW)

Conclusion

The change to the TOE is at the level of guidance documentation and life cycle. 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-0465-2008 dated 20 June 2008 updated by a re-assessment on 31 July 2012 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 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).

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

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, NXP P5CC037V0A Secure Smart Card Controller, NXP Semiconductors, Version 1.1, July 09th, 2012 (confidential document)

[3] Certification Report BSI-DSZ-CC-0465-2008 for NXP Smart Card Controller P5CC037V0A with specific IC Dedicated Software of NXP Semiconductors Germany GmbH, Bundesamt für Sicherheit in der Informationstechnik, 20 June 2008

[4] Security Target Lite, Evaluation of the P5CC037V0A Secure Smart Card Controller, NXP Semiconductors, Business Line Identification, Version 1.6, July 16th, 2009

[5] Configuration List for the NXP P5xC012/02x/037/052V0A, P5CC052V0B family of Secure Smart Card Controllers, BSI-DSZ-CC-0466/0465/0464, Version 1.6, NXP Semiconductors, Business Unit Identification, February 24, 2012 (Confidential document)

[6] Guidance, Delivery and Operation Manual for the P5xC012/02x/037/052V0A family of Secure Smart Card Controllers, NXP Semiconductors, BUID, Revision 1.8, Doc. No. 139918, 12. April 2012

[7] Security Target Lite, Evaluation of the P5CC037V0A Secure Smart Card Controller, NXP Semiconductors, Business Line Identification, Version 1.7, 22 February 2012

[8] ETR for composition for the NXP P5CC037V0A Secure Smart Card Controller, BSI-DSZ-CC-0465, T-Systems GEI GmbH, Version 1.7, 25.07.2012

[9] ETR for the NXP P5CC037V0A Secure Smart Card Controller, BSI-DSZ-CC-0465, T-Systems GEI GmbH, Version 1.5, 25.07.2012 (Confidential document)

[10] Data Sheet, P5xC012/02x/037/052 family Secure contact PKI smart card controller, NXP Semiconductors, Revision 3.9, Document Number: 129039, 30 June 2011

[11] Configuration List for composite evaluation of the P5xC012/02x/037/052V0A family,NXP Semiconductors, Rev. 1.5, February 24th, 2012