Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0465-2008-MA-04

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 2.1, June 2012 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 change to the certified product comprises the inclusion of an additional production site already certified into the scope of the certificate. The change has no effect on assurance.

The certified product itself did not change.

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, 19 December 2013

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 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 NXP Smart Card Controller P5CC037V0A with specific IC Dedicated Software was changed to extend production capacity and second source capabilities.

The certified product itself did not change.

The changes are related to including an additional production site already certified into the scope of the 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 NedCard Shanghai Microelectronics Co. Ltd used for Testing and Module Assembly:

NedCard Shanghai Microelectronics Co. Ltd.
Standardized Plant Building #8, No. 789
Puxing Road, Caohejing
Hi-Tech Park, EPZ, 201114 Shanghai
People’s Republic of China

Conclusion

The change to the TOE is at the level of production sites. 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] is still valid for the TOE.

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 [6] and [7] 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 [6].

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).

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 “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report, P5CC037V0A, Rev. 1.0, October 30, 2013 (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, June 20, 2008

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

[5] Configuration List for the NXP P5xC012/02x/037/052V0A, P5CC037/052V0B family of Secure Smart Card Controllers, BSI-DSZ-CC-0466/0465/0464, Version 1.8, NXP Semiconductors, Business Unit Identification, October 30, 2013 (Confidential document)

[6] ETR for composition for the NXP P5CC037V0A Secure Smart Card Controller, BSI-DSZ-CC-0465, T-Systems GEI GmbH, Version 1.7, July 25, 2012

[7] ETR for the NXP P5CC037V0A Secure Smart Card Controller, BSI-DSZ-CC-0465, T-Systems GEI GmbH, Version 1.5, July 25, 2012 (Confidential document)