Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0349-2006-MA-02

NXP Secure Smart Card Controller P5CT072V0Q, P5CD072V0Q, P5CD036V0Q, including specific Inlay Packages OM95xx, each 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-0349-2006 updated by a re-assessment on 18 January 2011.

The changes to the certified product are at the level of the restrictions in the Guidance Documentation. The changes have no effect on assurance. The certified product itself did not change. The changes are related to an update of the user guidance [6].

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-0349-2006 updated by a re-assessment on 18 January 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-0349-2006.

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

Bonn, 26 January 2011

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], the Security Target [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the NXP Secure Smart Card Controller P5CT072V0Q, P5CD072V0Q, P5CD036V0Q, including specific Inlay Packages OM95xx, each 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 Secure Smart Card Controller P5CT072V0Q, P5CD072V0Q, P5CD036V0Q, including specific Inlay Packages OM95xx, each with specific IC Dedicated Software did not change. There are following product related changes:

1. **Voltage Class A & B restrictions:** This change is intended to improve the product security during execution of DES operations in voltage range class A and B. This is described in the updated Guidance, Delivery and Operation Manual [6].
2. **Change to 4 Byte ID**: Up to now MIFARE ICs and Emulation implementations as here in this P5CT072 and its configurations are featuring a unique identifier (UID) with the length of 4Byte. The 4 byte unique ID is superseded by a 4 Byte ID. This 4 Byte Identifier is related to the Mifare Mode only and has no dependency to security features described in the Security Target.

The changes are only related to requirements for the embedded software for the composite evaluations. The intended restrictions outlined in the Guidance Documentation [6] improve product security. This mentioned Guidance Documentation has been evaluated in an other certification procedure in the BSI. Therefore, the changes are not significant from the standpoint of security.

Conclusion

The changes to the certified product are at the level of the restrictions in the Guidance Documentation. The changes have no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5]. Specific lists supporting composite evaluations [6], [8] have been updated, too.

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-0349-2006 updated by a re-assessment on 18 January 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 composition as listed above can usually be used for composite evaluations building on top, as long as the ETR for composition document 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 this evaluation (see BSIG Section 9, Para. 4, Clause 2). In addition to the baseline certificate BSI notes that cryptographic functions 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 these functions 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, BSI-DSZ-CC-349, P5CT072V0Q, P5CD072V0Q, P5CD036V0Q, Rev.1.0, 25 May 2010 (confidential document)

[3] Certification Report BSI-DSZ-CC-0349-2006 for Phillips Secure Smart Card Controller P5CT072V0Q, P5CD072V0Q, P5CD036V0Q, including specific Inlay Packages OM95xx, each with specific IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, 28 March 2006

[4] Security Target BSI-DSZ-0349, Version 1.2, 24 September 2008, Evaluation of the P5CT072/P5CD072/P5CD036 V0Q Secure Smart Card Controller, NXP Semiconductors, Business Line Identification (confidential document)

[5] Configuration List, Evaluation of the Philips P5CT072V0S/Q, Secure Smart Card Controller, Philips Semiconductors, Business Line Identification, Version 1.7, 20 May 2010 (confidential document)

[6] Guidance, Delivery and Operation Manual for the NXP P5CT072V0S / V0Q, Secure Triple Interface Smart Card Controller, NXP Semiconductors, Business Line Identification, Version 1.4, 19 May 2010 (confidential document)

[7] Security Target Lite BSI-DSZ-0349, Version 1.3, 24 September 2008, Evaluation of the P5CT072/P5CD072/P5CD036 V0Q Secure Smart Card Controller, NXP Semiconductors, Business Line Identification (sanitised public document)

[8] ETR for composition for the NXP P5CT072V0Q Secure 8-bit Smart Card Controller, BSI-DSZ-CC-0349, T-Systems GEI GmbH, Version 1.4, 05.10.2010 (confidential document)

[9] ETR (Evaluation Technical Report) for the Product NXP P5CT072V0Q Secure Smart Card Controller, BSI-DSZ-CC-0349, T-Systems GEI GmbH, Version 1.3, 07.10.2010 (confidential document)