Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0410-2007-MA-07

NXP Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B, P5CC073V0B each with IC Dedicated Software

from

NXP Semiconductors Germany GmbH

Common Criteria Recognition Arrangement
for components up to EAL4

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-0410-2007.

The change to the certified product is at the level of a the module delivery form, which is a change that has no effect on assurance. The TOE version 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.

Therefore, the assurance as outlined in the Certification Report BSI-DSZ-CC-0410-2007 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0410-2007.

Bonn, 6. November 2009

Common Criteria

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], the Security Target [6] and the Evaluation Technical Report as outlined in [7].

The vendor for the NXP Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B, P5CC073V0B each with 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 P5CD080V0B, P5CN080V0B, P5CC080V0B, P5CC073V0B each with IC Dedicated Software was changed due to new module delivery form. To reduce the effort for further new module type implementations it is intended to replace the subtype by the placeholder “n”. This leads to the naming extension “Xn” replacing all discrete named module types in the certification documentation, where “Xn” indicates module package form. The change is not significant from the standpoint of security, the TOE version does not change. For further new module type implementations it is intended to replace the subtype by the placeholder “n”. The change is not significant from the standpoint of security.

Conclusion

The change to the TOE is at the level new module delivery form, a change that has no effect on assurance. Examination of the evidence indicates that the changes are limited to the introduction of the generalization of the module delivery form. The Security Target Lite was editorially updated [4]. 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. 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 4, Para. 3, 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' (www.bsi.bund.de). 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 P5CD080/ P5CN080/ P5CC080/P5CC073 V0B Secure Smart Card Controller, NXP Semiconductors, Rev. 1.0, Sep. 29th (confidential document)

[3] Certification Report BSI-DSZ-CC-0410-2007 for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B each with specific IC Dedicated Software, Bundesamt für Sicherheit in der Informationstechnik, 5. July 2007

[4] Security Target Lite, Evaluation of the NXP P5CD080/ P5CN080/ P5CC080/ P5CC073 V0B Secure Smart Card Controller, NXP Semiconductors, Business Line Identification, Rev.1.7, September 28th, 2009, BSI-DSZ-CC-0410-2007

[5] Configuration List of the NXP P5Cx012/02x/040/073/080/144 family of Secure Smart Card Controllers, Version 1.8, 12 March 2009, NXP Semiconductors, Business Line Identification (Confidential document)

[6] Security Target, Evaluation of the NXP P5CD080/ P5CN080/ P5CC080/ P5CC073 V0B Secure Smart Card Controller, NXP Semiconductors, Business Line Identification, Rev.1.7, September 28th, 2009, BSI-DSZ-CC-0410-2007

[7] ETR, NXP P5CD080V0B Secure Smart Card Controller, BSI-DSZ-CC-0410, Version 1.2, 25 June, 2009