Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0466-2008-MA-01

NXP Smart Card Controller P5CC052V0A with specific 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-0466-2008. A reassessment proofing the resistance against high attack potential (AVA_VLA.4) has been performed at 2009-08-21 of T-Systems assessment report and was approved at 2009-09-08.

The change to the certified product is at the level of new module delivery form 'silver module' for the evaluated products, a change that has no effect on assurance. No changes of hardware or IC dedicated software are applied, the TOE version does 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-0466-2008 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-0466-2008.

Bonn, 8. September 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 [4], the Evaluation Technical Report [7] and ETR for composition as outlined in [8].

The vendor for the NXP Smart Card Controller P5CC052V0A with specific IC Dedicated Software, 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 P5CC052V0A with specific IC Dedicated Software were changed due to new module delivery form XD for the evaluated products. The difference between the evaluated package X0 and the new package XD (PCM1.1-Pd) is that the golden contact area of the PCM1.1 is covered by an additional thin palladium layer due to market requirements. 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”. This leads to the naming extension “Xn” replacing all discrete named module types in the certification documentation, where “Xn” indicates module package form. Since the used package has no impact on the overall security of the TOE.

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 performed are limited to the new 'silver module'. The Security Target Lite was editorially updated [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.

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 for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001

[2] Impact Analysis Report, NXP P5CC052V0A Secure Smart Card Controller, NXP Semiconductors, Version 1.1, July 09th, 2009 (confidential document)

[3] Certification Report BSI-DSZ-CC-0466-2008 BSI-DSZ-CC-0464-2008 for NXP Smart Card Controller P5CC052V0A with specific IC Dedicated Software of NXP Semiconductors Germany GmbH from 24 June 2008

[4] Security Target, Evaluation of the NXP P5CC052V0A Secure Smart Card Controller, NXP Semiconductors, Business Line Identification, Version 1.5, July 09th, 2009 (Confidential document)

[5] Configuration List for the NXP P5xC012/02x/037/052 family of Secure Smart Card Controllers, BSI-DSZ-CC-0466, Version 1.2, NXP Semiconductors, April 16th, 2008 (Confidential document)

[6] Security Target lite, Evaluation of the NXP P5CC052V0A Secure Smart Card Controller, NXP Semiconductors, Business Line Identification, Version 1.5, July 09th, 2009

[7] ETR for the NXP P5CC052V0A Secure Smart Card Controller, BSI-DSZ-CC-0466, T-Systems GEI GmbH, Version 1.1, 21.08.2009 (Confidential document)

[8] ETR for composition for the NXP P5CC052V0A Secure Smart Card Controller, BSI-DSZ-CC-0466, T-Systems GEI GmbH, Version 1.2, 21.08.2009 (Confidential document)