Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0411-2007-MA-02

NXP Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B with additional delivery form MOB6

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-0411-2007.

The change to the certified product is at the level of generation of specific new TOE configurations before TOE delivery. A new version of the data sheets is considered. The changes have no effect on assurance. The identification of the new configurations of the product is indicated by the product name NXP Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B with additional delivery form MOB6.

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-0411-2007 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-0411-2007.

Bonn, 18 July 2008

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 [5] and the Evaluation Technical Report as outlined in [6].

The vendor for the NXP Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B with additional delivery form MOB6, 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 wafer thickness changed to 75 µm is a standard delivery type for the TOE P5CD144V0B, P5CN144V0B and P5CC144V0B certified under reference BSI-DSZ-CC-0411-2007 [3] and BSI-DSZ-CC-0411-2007-MA-01 [7]. Furthermore, it can be concluded that this thickness can be regarded as already covered and now additionally used for this new module MOB6. This means that the security relevant investigations have been performed already in that context. This change is therefore not security relevant. The ISO14443A contact-less interface and the S^2C interface are enabled and the ISO7816 contact interface is enabled. For the identification of a specific NXP P5CD144V0B chip, the Device Coding Bytes stored in the EEPROM can be used: The value 2B hex for P5CD144V0B, 2A hex for P5CN144V0B and 29 hex for P5CC144V0B in Device Coding Byte DC2 identifies the chip configuration. As the TOE functionality did not change, it is indicated by the chip identifier T034B (see [3]). The Configuration List was updated [6].

Conclusion

The change to the TOE is at the level of generation of specific new TOE configurations before TOE delivery, a change that has no effect on assurance. The changes have no effect on assurance or the information taken over was already evaluated. Examination of the evidence indicates that the changes required are limited to the identification of configuration information. The Security Target [5], the Security Target Lite [4] and the Configuration List [6] were editorially updated. 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. 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-0411-2007, Rev. 1.0, 27 June 2007, P5CD144/P5CC144/P5CN144, NXP Semiconductors Germany GmbH (confidential document)

[3] Certification Report BSI-DSZ-CC-0411-2007 for NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific Dedicated software, BSI

[4] Security Target Lite BSI-DSZ-0411-2007, Version 1.3, 4 February 2008, P5CD144V0B, NXP Semiconductors Germany GmbH (sanitised public document)

[5] Security Target BSI-DSZ-CC-0411-2007, Evaluation of the NXP P5CD144V0B Secure Smart Card Controller, Version 1.3, NXP Semiconductors Germany GmbH, 4 February 2008 (confidential document)

[6] Configuration List, BSI-DSZ-CC-0404/0410/0411, Version 1.4, 21 April 2008, NXP P5Cx012/02x/040/073/080/144V0B family of Secure Smart Card Controller, NXP Semiconductors Germany GmbH, Business Line Identification (confidential document)

[7] Assurance Continuity Maintenance Report BSI-DSZ-CC-0411-2007-MA-01, 30 April 2007, NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software, BSI