Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0439-2008-MA-01

NXP Smart Card Controller P5CD012V0B with IC dedicated software: Secured Crypto Library Release 2.0

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-0439-2008.

The change to the certified product is at the level of the generation of a specific new TOE configuration by blocking the memory size in the final step of the production test process, a change that has no effect on assurance. A new version of the data sheets is considered. The changes have no effect on assurance. The identification of the new configuration of the product is indicated by the product name NXP Smart Card Controller P5CD012V0B with IC dedicated software: Secured Crypto Library Relaese 2.0.

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-0439-2008 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-0439-2008.

Common Criteria

Bonn, 7 July 2008

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 P5CD012V0B with IC dedicated software: Secured Crypto Library Release 2.0, 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 new configuration P5CD012V0B is configured at the end of the production process and was already assessed within the Assurance Continuity Maintenance Report BSI-DSZ-CC-0404-2007-MA-01 having the same hardware platform like the NXP chip P5CD040V0B, indicated by the nameplate T036B with the only difference that the available EEPROM size is 12 kByte instead of 40 kByte.

For the identification of a specific NXP P5CD012V0B chip, the Device Coding Bytes stored in the EEPROM can be used: The value 20 hex in Device Coding Byte DC2 identifies the chip configuration P5CD012V0B. The chip identifier is T036B (see [3]). An updated configuration list [6] was provided.

The Crypto Library has already been evaluated on the P5CD040V0B under certification number BSI-DSZ-CC-0439-2008 [3]. Since the Crypto Library do not depend on EEPROM memory size, this change does not have any impact on security.

Conclusion

The change to the TOE is at the level of the generation of a specific new TOE configuration by blocking the EEPROM memory size from 40 kByte to 12 kByte in the final step of the production test process, a change that has no effect on assurance. Examination of the evidence indicates that the changes peformed are limited to the identification of configuration information of the TOE. The Security Target [5], the Security Target Lite [4] and the User Guidance [8] 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-0439-2008, Rev. 1.0, 7 December 2007, Secured Crypto Library on the P5CD012V0B (confidential document)

[3] Certification Report BSI-DSZ-CC-0439-2008 for NXP Secure Smart Card Controller P5CD040V0B with IC dedicated software: Secured Crypto Library Release 2.0, 26.06.2008, BSI

[4] Security Target Lite BSI-DSZ-0439-2008, Version 1.2, 06 December 2007, Secured Crypto Library on the P5CD040V0B, NXP Semiconductors Germany GmbH (sanitised public document)

[5] Security Target BSI-DSZ-0439-2008, Version 1.2, 07 December 2007, Secured Crypto Library on the P5CD040V0B, NXP Semiconductors Germany GmbH (confidential document)

[6] Evaluation Technical Report, 4.0, 16 May 2007, Secured Crypto Library on the P5CD040V0B, Brightsight BV (confidential document)

[7] Configuration List, Evaluation of the NXP P5CX02x/040/073/080/144 family of Secure Smart Card Controller, Version 1.4, 21 April 2007, NXP Semiconductors Germany GmbH, Business Line Identification (confidential document)

[8] User Guidance, Revision 3.2, December 07 2007, Secured Crypto Library on the P5Cx012/02x/040/080/144 Family, NXP Semiconductors Germany GmbH