Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0439-2008-MA-02

NXP Smart Card Controller P5CD040V0B with IC dedicated software: Secured Crypto Library Release 2.1

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 changes to the certified product are at the level of sourcecode adding a secondary version of the RSA Key Generation, documentation and adapted functional tests, a change that has no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the certified product.

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.

Bonn, 30 September 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 [4] and the Evaluation Technical Report as outlined in [6].

The vendor for the NXP Smart Card Controller P5CD040V0B with IC dedicated software: Secured Crypto Library Release 2.1, 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.

Four changes are added to the baseline report [3] of NXP Smart Card Controller P5CD040V0B with IC dedicated software: Secured Crypto Library Release 2.1:

- For performance reasons, an insecure RSA key generation mode is added and shall be executed in a secure environment only, as it can be given during Smart Card personalization. Code changes had been performed to the RSA Key Generation subsystem of the Crypto Library. The functional tests have been adapted. The evaluation facility gave a comissioned statement. The Security Target [4], the Security Target Lite [5], the User Guidance Manuals [8]–[10], the Configuration List [7] and the Implementation Description [14] had been adapted. The producer has performed additional tests [2].
- The Hardware User Guidance document [11] already lists limitations for the usage of the DES coprocessor voltage. The Crypto Library User Guidance [8] adapts these restrictions to be taken into account when using the library.
- Due to export restrictions of the Chiasmus encryption software to countries outside the E.U. the delivery procedure has to be changed. The delivery procedure stays the same, but the Chiasmus encryption is removed and requirements on the quality of the PGP keys to be used have been added to the Delivery and Operation manual [12].
- Due to latest findings in cryptographic research the hash algorithm SHA-1 does not fulfill the requirements for Strength of Function: High any more. Therefore this claim is removed from the Security Target [4], the Security Target Lite [5] and the Strenght of Function documentation [13].

The changes effecting sourcecode, functional testing and documentation of the Crypto Library reflect a minor change from the standpoint of security. The insecure RSA key generation mode is not secured against side-channel attacks. During its execution the environment has to avoid side-channel attacks.

Configuration Management procedures required a change in the version number from Secured Crypto Library Release 2.0 to Release 2.1.

Conclusion

The change to the TOE is at the level of sourcecode, adding an insecure version of the RSA Key Generation for usage in a secure environment only, documentation considering the four listed changes and adapted functional tests, changes that has no effect on assurance. Examination of the evidence indicates that the code changes performed are limited to the RSA Key Generation subsystem of the Crypto Library.

The Security Target [4], the Security Target Lite [5], the User Guidance Manuals [8]–[10], the Configuration List [7], the Implementation Description [14], the Strenght of Function documentation [13] and the Delivery and Operation manual [11] were editorially updated.

Consideration of the change leads to the conclusion that the overall impact of the identified changes on the assurance of the TOE 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-MA-02, Secured Crypto Library, Revision 1.1, NXP Semiconductors Germany GmbH, 14. August 2008 (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, Bundesamt für Sicherheit in der Informationstechnik, 26 June 2008

[4] Security Target BSI-DSZ-CC-0439-2008, Version 1.4, 11 August 2008, Secured Crypto Library on the P5CD040V0B, NXP Semiconductors Germany GmbH (confidential document)

[5] Security Target Lite BSI-DSZ-CC-0439-2008, Version 1.4, 11 August 2008, Secured Crypto Library on the P5CD040V0B, NXP Semiconductors Germany GmbH (sanitised public document)

[6] Evaluation Technical Report, Version 4.0, 16 May 2008, Secured Crypto Library on the P5CD040V0B, Brightsight BV (confidential document)

[7] Configuration list for the TOE, 1.7, 11 August 2008, NXP Semiconductors Germany GmbH (confidential document)

[8] User Guidance: Secured Crypto Library on the P5Cx02x/040/080/144 family, Revision 3.4, 11 August 2008, NXP Semiconductors Germany GmbH

[9] User Guidance: Secured Crypto Library on the SmartMX – Secured RSA Key Generation Library, Revision 4.1, 10 March 2008, NXP Semiconductors Germany GmbH

[10] User Guidance: Secured Crypto Library on the SmartMX – SHA Library, Revision 4.1, 12 June 2008, NXP Semiconductors Germany GmbH

[11] Guidance, Delivery and Operation Manual for the P5Cx012/02x/040/073/ 080/144V0B Family of Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.7, 25. Ferbruary 2008

[12] Secured Crypto Library on the SmartMX – Delivery and Operation, Rev. 0.3, 20 May 2008, NXP Semiconductors Germany GmbH (confidential document)

[13] NXP Semiconductors Evaluation Documentation: Secured Crypto Library on the SmartMX - AVA_SOF.1, Revision 0.3, June 24th, 2008

[14] Evaluation Documentation: Crypto Library on SmartMX – Implementation of RSA Key Generation Subsystem, Revision 1.5, 09 June 2008, NXP Semiconductors Germany GmbH