Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0439-2008-MA-03

Crypto Library V2.1 on P5CD040V0B, P5CC040V0B, P5CD020V0B, P5CC021V0B, P5CD012V0B

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's last maintenance is at the level of the documentation, a change that has no effect on assurance. The identification of the maintained product is indicated by the same version number compared to the last maintained 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, 21 June 2010

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 [3].

The vendor for the Crypto Library V2.1 on P5CD040V0B, P5CC040V0B, P5CD020V0B, P5CC021V0B, P5CD012V0B, 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 Crypto Library V2.1 on P5CD040V0B, P5CC040V0B, P5CD020V0B, P5CC021V0B, P5CD012V0B was not changed. The User Guidance [6] has been changed. The new guidance document was taken from Crypto Library Version 2.2 evaluated within the certification procedure BSI-DSZ-CC-0609. NXP has merged the guidance information for Crypto Library version 2.1 and for version 2.2 into one document [6]. In addition the Security Target and the Security Target Lite were editorially updated ([4] and [7]).

The change is not significant from the standpoint of security.

Note on additional Update: Shortly before this maintenance activity was started a Re-Assessment of AVA aspects had been performed by the ITSEC Brightsight resulting in a new version of the ETR and ETR for composite evaluation documents. Due to editorial changes these documents have been updated by 15 June 2010 (see [9] and [10]).

Conclusion

The change with respect to the last maintenance of the TOE is at the level of the documentation, a change that has no effect on assurance.

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 obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [10].

According to the scheme rules, evaluation results outlined in the document ETR for composition as listed above can usually be used for composite evaluations building on top, as long as the ETR for composition document is not older than one year and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG Section 9, Para. 4, 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' (https://www.bsi.bund.de).

This report is an addendum to the Certification Report [3] and the maintenance report [8].

References

[1] Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements”, version 1.0, February 2004

[2] IAR Crypto Library on SmartMX v2.1, Rev. 1.0, 2010-06-10 (confidential document)

[3] Certification Report BSI-DSZ-CC-0439-2008, NXP Smart Card Controller P5CD080V0B with IC dedicated software:Secured Crypto Library Release 2.0, 2008-06-13

[4] Security Target: Crypto Library v2.1 on P5CD040V0B/ P5CC040V0B/ P5CD020V0B/ P5CC021V0B, P5CD012V0B Security Target, Rev. 1.4.2, 2010-05-10 (confidential document)

[5] List of Configuration Items, Version 1.7.2, 2010-05-10 (Confidential document)

[6] User Guidance: Secured Crypto Library on the P5Cx02x/040/080/144 Family, Rev. 3.9, 2010-05-06

[7] Security Target Lite: Crypto Library v2.1 on P5CD040V0B/ P5CC040V0B/ P5CD020V0B/ P5CC021V0B, P5CD012V0B Security Target, Rev. 1.4.2, 2010-05-10 (public document)

[8] 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, 2008-09-30

[9] Evaluation Technical Report Crypto Library V2.1 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B EAL5+, 2010-06-15, version 3.0 (confidential document)

[10] ETR for composition, NXP Crypto Library v2.1 on the P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B according to AIS36, June 15, 2010, Version 2.0 (confidential document)