Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0633-2010-MA-01

Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s)

from

NXP Semiconductors Germany GmbH

Common Criteria Recognition Arrangement
for components up to EAL4

Common Criteria

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-0633-2010 updated by a re-assessment on 29 February 2012.

The changes to the product are caused by an addition to the user guidance manual of the underlying hardware platform. The hardware platform has also undergone a procedure to include an additional production site which led to identical, but differently named hardware. The identification of the maintained product is indicated by an extension of the product name.

The nature of the changes was considered by the ITSEF Brightsight BV, approved by BSI. The conclusion was that they are classified as minor changes with no impact on assurance and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0633-2010 dated 19 November 2010 updated by a re-assessment on 29 February 2012 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0633-2010.

Bonn, 4 July 2013

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

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], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s), 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 V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s) was changed due to an addition to the user guidance manual of the underlying hardware platform. It is a locally confined change at the level of implementation. Also the hardware platform has undergone a procedure to include a new production site. This caused a change to the name of the otherwise identical hardware. Configuration Management procedures required a change in the product identifier. Therefore the product name changed from “Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A” to “Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s)”.

The changes are related to an update of the user guidance [5].

Conclusion

The change to the TOE is at the level of implementation and guidance documentation. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [4].

The Security Target 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.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-0633-2010 dated 19 November 2010 updated by a re-assessment on 29 February 2012 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [7] and [8] are the current versions of the ETR for composite evaluation and the ETR itself.

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 [7].

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

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[1] Section 9, Para. 4, Clause 2).

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

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

References

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

[2] IAR, Crypto Library V2.7/V2.9 on SmartMX Impact Analysis Report, Rev. 0.6, 25 June 2013, NXP Semiconductors, Business Unit Identification (confidential document)

[3] Certification Report BSI-DSZ-CC-0633-2010 for Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A, Bundesamt für Sicherheit in der Informationstechnik, 19 November 2010

[4] List of Configuration Items for Crypto Library v2.7 on P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s), 14 May 2013 (confidential document)
List of Configuration Items for Crypto Library v2.9 on P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s), 14 May 2013 (confidential document)

[5] Secured Crypto Library on SmartMX on the P5CD016/021/041/081 and P5CC081 – User guidance manual, Revision 1.6, 3 June 2013 (confidential document)

[6] Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s). Security Target Lite, Revision 1.5, 8 May 2013 (sanitised public document)

[7] ETR for composition “Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A according to AIS36”, Brightsight, Revision 5.0, 27 February 2012 (confidential document)

[8] Evaluation Technical Report, Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A, Brightsight, Revision 7.0, 27 February 2012 (confidential document)