Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0750-2011-MA-01

Crypto Library V2.7 on P5CD145V0v / P5CC145V0v / P5CD128V0v / P5CC128V0v

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-0750-2011 updated by a re-assessment in 2012.

The change to the certified product is at the level of including a maintenance process of the underlying hardware platform. The change has no effect on assurance. The identification of the maintained product is indicated by an adaptation of the product name.

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.

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-0750-2011 dated July 11th 2011 updated by a re-assessment in 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-0750-2011.

Bonn, 10 August 2012

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 on P5CD145V0v / P5CC145V0v / P5CD128V0v / P5CC128V0v, 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 on P5CD145V0v / P5CC145V0v / P5CD128V0v / P5CC128V0v was maintained due to a maintenance process of the underlying hardware platform which resulted in a changed product identifier (V0v where v is either A or B). There is no change in the Crypto Library software.

The Crypto Library V2.7 provided functions run identical to the P5CD145/ CC145/ CD128/ CC128 V0A platform on the derived P5CD145/ CC145/ CD128/ CC128 V0B hardware which is functionally identical.

Configuration Management procedures required a change in the product identifier. Therefore the product name was changed to indicate the additional platform derivative. As a result the configuration list for the TOE has been updated [4].

Conclusion

The change to the TOE is at the level of including a maintenance process of the underlying hardware platform. 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 [5].

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-0750-2011 dated July 11th 2011 updated by a re-assessment in 2012 is of relevance and has to be considered when using the product. As a result of this re-assessment, the documents [6] and [7] 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 [6].

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 one year 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).

In addition to the baseline certificate BSI notes that cryptographic functionalities 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 this functionality 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).

The Cryptographic Functionalities 2-key Triple DES (2TDES), RSA 1024, ECC 160, SHA1 used as collision-resistant hash function, provided by the TOE achieves a security level of maximum 80 Bits (in general context).

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 on SmartMX P5Cx128V0v/P5Cx145V0v”, NXP Semiconductors, Business Unit Identification, Revision 1.10, May 04th, 2012 (confidential document)

[3] Certification Report BSI-DSZ-CC-0750-2011 for Crypto Library V2.7 on P5CD145V0A, MSO/ P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO, Bundesamt für Sicherheit in der Informationstechnik, 11.04.2011

[4] NXP Semiconductors Evaluation Documentation: Secured Crypto Library on the SmartMX – Life Cycle, Revision 0.5, April 20th, 2012 (Confidential document)

[5] Security Target - Crypto Library V2.7 on SmartMX P5CD145V0v / P5CC145V0v / P5CD128V0v / P5CC128V0v, NXP Semiconductors, Business Unit Identification, Revision 1.2, March 29th , 2012

[6] ETR for composition “Crypto Library V2.7 on P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO”, Brightsight, Revision 8.0, August 2nd, 2012

[7] Evaluation Technical Report, “Crypto Library V2.7 on P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO”, Brightsight, Revision V7.0, August 6th, 2012