Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0845-V2-2013-MA-01

NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y) with IC Dedicated Software FW5.0

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 2.1, June 2012 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-0845-V2-2013.

The certified product itself did not change. The changes are related to additional production sites.

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-0845-V2-2013 dated 19 December 2013 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-0845-V2-2013.

Bonn, 1 April 2014

SOGIS 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 NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y) with IC Dedicated Software FW5.0, 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 certified product itself did not change. The changes are related to additional production sites.

According to [1] the evaluation facility T-Systems GEI GmbH conducted a subset evaluation for the assurance class ALC. T-Systems GEI GmbH is an evaluation facility recognised by the certification body of BSI.

The result of the subset evaluation was that the Common Criteria assurance requirements

ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_FLR.1 ,ALC_LCD.1, ALC_TAT.3)

are fulfilled for the following sites used for Inlay Production:

SMARTRAC Technology Wehnrath GmbH
Gewerbeparkstraße 10
51580 Reichshof
Germany

SMARTRAC Technology Ltd.
142 Moo 1 Hi-Tech Industrial Estate,
Tambon ban Laean, Amphor Bang-Pa-In,
Phra Nakorn Si Ayutthaya 13160,
Thailand

Conclusion

The certified product itself did not change. The changes are related to including two additional production sites. The change has no effect on assurance. As a result of the changes the configuration list for the TOE has been updated [5]. The Security Target [4] is still valid for the TOE.

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-0845-V2-2013 dated 19 December 2013 is of relevance and has to be considered when using the product.

As a result of this maintenance procedure, the Evaluation Technical Report [6] was partially updated concerning the ALC aspects.

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.

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

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] Impact Analysis Report NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y), Rev. 1.1, 18 March 2014 (confidential document)

[3] Certification Report BSI-DSZ-CC-0845-V2-2013 for NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y) with IC Dedicated Software FW5.0, Bundesamt für Sicherheit in der Informationstechnik, 19 December 2013

[4] Security Target NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y), NXP Semiconductors, Rev. 2.11, 24 October 2013

[5] Configuration List NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y), NXP Semiconductors, Rev.2.12, 17 March 2014

[6] Evaluation Technical Report BSI-DSZ-CC-0845-V2, Version 1.9, 19 March 2014, T-Systems GEI GmbH (confidential document)

[7] ETR for composition according to AIS36, NXP P60x144/080PVA, T-Systems GEI GmbH, Version 1.7, 05 December 2013