Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0858-V2-2015-MA-02

NXP Secure PKI Smart Card Controllers P5CD128V0v/V0B(s), P5CC128V0v/V0B(s), P5CD145V0v/V0B(s), P5CC145V0v/V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software

from

NXP Semiconductors Germany GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 2.1, June 2012 and the developer's 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-0858-V2-2015 updated by a partial re-evaluation of Assurance Class ALC as outlined in the ETR dated 20 December 2016.

The certified product remains unchanged, however its development environment has received improvements in the overall security concept as detailed in the Impact Analysis Report (IAR). The change has no effect on assurance of the certified TOE. The certified product itself did not change. The changes are related to the site NXP Hamburg which was re-evaluated for this Assurance Continuity Maintenance Report.

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-0858-V2-2015 dated 27 April 2015 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-0858-V2-2015.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 29 December 2016

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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 PKI Smart Card Controllers P5CD128V0v/V0B(s), P5CC128V0v/V0B(s), P5CD145V0v/V0B(s), P5CC145V0v/V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software, 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 and to the site, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The product as certified under NXP Secure PKI Smart Card Controllers P5CD128V0v/V0B(s), P5CC128V0v/V0B(s), P5CD145V0v/V0B(s), P5CC145V0v/V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software, itself did not change.

The results of the maintenance process affirm the successful implementation of measures to uphold and strengthen the security of the development environment at NXP Hamburg site. The ALC re-evaluation has been performed by the ITSEF T-Systems GEI GmbH. This assessment comprehends various site visits as detailed in the Site Visit Report [8]. The Common Criteria assurance requirements:

ALC – Life cycle support (ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_FLR.1, ALC_LCD.1, ALC_TAT.2)

are fulfilled for the following site:

NXP Semiconductors Germany GmbH
Business Unit Security and Connectivity
Stresemannallee 101
D-22529 Hamburg
Germany

used for development, customer support, test center, Master IT Provisioning and delivery.

Conclusion

The change to the TOE is at the level of improvements of the overall security concept as indicated in the IAR [2]. As a result of the changes the configuration list [7] for the TOE has been updated. Only the environment documentation was changed, specifically site security documents according to IAR chapter 2.1.2.

The Security Target [4] is still valid for the unchanged 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.

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-0858-V2-2015 [3] dated 27 April 2015 is of relevance and has to be considered when using 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 [5].

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 PKI Smart Card Controllers P5CD128V0v/V0B(s), P5CC128V0v/V0B(s), P5CD145V0v/V0B(s), P5CC145V0v/V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software, Revision 0.1, 19 September 2016, NXP Semiconductors Germany GmbH (confidential document)

[3] Certification Report BSI-DSZ-CC-0858-V2-2015 for NXP Secure PKI Smart Card Controllers P5CD128V0v/V0B(s), P5CC128V0v/V0B(s), P5CD145V0v/V0B(s), P5CC145V0v/V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software, 27 April 2015, Bundesamt für Sicherheit in der Informationstechnik (public document)

[4] Security Target BSI-DSZ-CC-0858-V2-2015, Version 2.1, 16 November 2012, NXP Secure Smart Card Controllers P5Cx128/P5Cx145 V0v/V0B(s) Security Target, NXP Semiconductors, Business Unit Identification (confidential document)

Security Target Lite BSI-DSZ-CC-0858-V2-2015, Version 2.1, 16 November 2012, NXP Secure Smart Card Controllers P5Cx128V0v/P5Cx145V0v(s) Security Target Lite, NXP Semiconductors, Business Unit Identification (sanitised public document)

[5] ETR for composite evaluation according to AIS 36, Version 1.3, 27 January 2015, ETR for composition, T-Systems GEI GmbH (confidential document)

[6] Evaluation Technical Report BSI-DSZ-CC-0858-V2, Version 2.4, 20 December 2016, T-Systems GEI GmbH (confidential document)

[7] NXP Secure Smart Card Controllers P5Cx128V0v/P5Cx145V0v(s) Configuration List, Revision 2.1, 19 September 2016, NXP Semiconductors Germany GmbH (confidential document)

[8] Site Visit Report NXP BU S&C Hamburg, Version 3.4, 20 December 2016, T-Systems GEI GmbH (confidential document)