



Assurance Continuity Maintenance Report

BSI-DSZ-CC-0858-V2-2015-MA-01

**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 Security Documentation. 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 21 July 2016.

The certified product remains unchanged, however its development environment has received improvements of the overall security concept as detailed in the ALC Documentation. 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.

Bonn, 27 July 2016

The Federal Office for Information Security



Common Criteria
Recognition Arrangement
for components up to
EAL 4



Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the developer's Security Documentation [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [4], its Security Target and the Evaluation Technical Report as outlined in [7].

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 updated Security Documentation [2] to the BSI for approval. The Security Documentation is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the Security Documentation 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 changes are related to improvements in the security of the development environment at NXP Hamburg site as outlined in updated Security Documentation. The ALC re-evaluation has been performed by the ITSEF T-Systems GEI GmbH. 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

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

Additional site:

NXP Semiconductors India Private Limited
Manyata Tech Park
Nagawara Village, Kasaba Hobli,
Bangalore 560 045
India

The evaluation deliverables are provided by:

NXP Semiconductors Germany GmbH
Business Unit Security and Connectivity

Stresemannallee 101
D-22529 Hamburg

or

NXP Semiconductors (Thailand)
Assembly Plant Bangkok, Thailand (APB)
303 Moo 3 Chaengwattana Rd.
Laksi, Bangkok 10210 Thailand

for the hardware platform and

NXP Semiconductors GmbH
Business Unit Security and Connectivity
Document Control Office
Mikron-Weg 1
A-8101 Gratkorn

for the documentation of the TOE.

Following sites are involved for the production of the TOE wafer fab and associated mask shops:

Semiconductor Factory (chipfinishing and wafer production):
Systems on Silicon Manufacturing Co. Pte. Ltd. (SSMC)
70 Pasir Ris Drive 1
Singapore 519527
Singapore

Mask Shop for SSMC:
Toppan Photomasks Korea Ltd.
345-1, Sooha-Ri ShinDoon-Myon
467-840 Ichon
South Korea

Semiconductor Factory (chipfinishing):
GLOBALFOUNDRIES Singapore Pte Ltd.
60 Woodlands Industrial Park D, Street 2
Singapore, 738406

Semiconductor Factory (wafer production):
GLOBALFOUNDRIES Singapore (Tampines) Pte Ltd.
1 Tampines Industrial Avenue 5
Singapore 528830

Mask Shop for Globalfoundries:
Photronics Singapore Pte. Ltd.
6 Loyang Industrial Park
Singapore 507099

Mask Shop for Globalfoundries:
Photronics Semiconductors Mask Corp. (PSMC)
1F, No.2, Li-Hsin Rd.
Science-Based Industrial Park

Hsin-Chu City
Taiwan R.O.C.

In addition, the following sites are involved for the bumping, testing, module assembly and inlay assembly of the TOE:

Wafer Bumping:
Chipbond Technology Corporation
No. 3, Li-Hsin Rd. V
Science Based Industrial Park
Hsin-Chu City
Taiwan R.O.C.

Test Centre:
NXP Semiconductors GmbH
IC Manufacturing Operations - Test Center Hamburg (IMO TeCH)
Stresemannallee 101
D-22529 Hamburg

Test Centre:
Assembly Plant Kaohsiung
NXP Semiconductors Taiwan Ltd.
#10, Jing 5th Road, N.E.P.Z, Kaohsiung 81170
Taiwan, R.O.C

Test Center and Module Assembly:
NXP Semiconductors (Thailand)
Assembly Plant Bangkok, Thailand (APB)
303 Moo 3 Chaengwattana Rd.
Laksi, 10210 Bangkok
Thailand

Module Assembly:
NedCard B.V.
Bijsterhuizen 25-29
6604 LM Wijchen
The Netherlands

Inlay assembly:
HID Global Galway
Paic Tionscail na Tulaigh
Balle na hAbhann
Co. Galway
Ireland

Inlay assembly:
Smartrac Technology Ltd.
142 Moo, Hi-Tech Industrial Estate
Tambon Ban Laean, Amphor Bang-Pa-In
13160 Ayutthaya
Thailand

Conclusion

The change to the TOE is at the level of improvements of the overall security concept as outlined in the ETR [7]. As a result of the changes the ETR comprises an updated ALC and Site Visit Report [2] whereas the configuration list for the TOE did not change.

The Security Target [5] 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 [4] 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 [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 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 [4].

References

- [1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012
- [2] Site Visit Report NXP BU S&C Hamburg, Chapter 5.1 to 5.7, Version 3.0, 21 July 2016, T-Systems GEI GmbH (confidential document)
- [3] Site Visit Report – Addendum NXP BUID Hamburg, Version 1.0, 21 July 2016, T-Systems GEI GmbH (confidential document)
- [4] 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)
- [5] 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)
- [6] ETR for composite evaluation according to AIS 36, Version 1.3, 27 January 2015, ETR for composition, T-Systems GEI GmbH (confidential document)
- [7] Evaluation Technical Report BSI-DSZ-CC-0858-V2, Version 2.21, 21. July 2016, T-Systems GEI GmbH (confidential document)