Bundesamt
für Sicherheit in der
Informationstechnik

Assurance Continuity Maintenance Report

BSI-DSZ-CC-0978-V2-2017-MA-01

NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with 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-0978-V2-2017

The certified product itself did not change. The changes are related to changes in the sites used to build the TOE. The life cycle security has continuously been assured by site certifications for each site used.

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-0978-V2-2017 dated 27 September 2017 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-0978-V2-2017.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 17 August 2018

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 Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with 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, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The certified product NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC Dedicated Software itself did not change.

The changes are related to an update of life cycle security aspects. The ALC re-evaluation was performed by the ITSEF TÜV Informationstechnik GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [6]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4].

The sites and related certificates listed in Annex B of Certification Report BSI-DSZ-CC-0978-V2-2017 are replaced by the following development and production sites:

Site	Task within the evaluation
NXP Semiconductors Hamburg Business Unit Identification Troplowitzstrasse 20 22569 Hamburg Germany	Development, Delivery and customer support
NXP Semiconductors Development Center Eindhoven Building 46, High Tech Campus 5656AE, Eindhoven The Netherlands	Development center
NXP Semiconductors RQC & NPIT & MM Nijmegen NXP Semiconductors Netherlands B.V. Gerstweg 2 6534AE Nijmegen The Netherlands	Development and Manufacturing, Regional Quality Center - Europe
NXP Semiconductors Austria GmbH Styria Gratkorn	Document control

Site	Task within the evaluation
Business Unit Identification Mikron-Weg 1 8101 Gratkorn Austria	
NXP Semiconductors High Tech Campus Eindhoven Building 60, High Tech Campus Secure Room 131 5656AE, Eindhoven The Netherlands	IT Engineering and Generic Support
Development Center NXP Bangalore NXP Semiconductors India Private Limited Manyata Technology Park Nagawara Village, Kasaba Hobli, Bangalore 560045 India	TOE database
Colt Hamburg Obenhauptstrasse, 22335 Hamburg - Germany	TOE database
Akquinet Hamburg Ulzburger Strasse 201, 22850 Norderstedt - Germany	TOE database
TSMC-FAB Tainan (14A) and Hsinchu (2/5&8) Taiwan Fab 14A: 1-1, Nan-Ke North Rd., Tainan Science Park, Tainan 741-44, Taiwan, R.O.C., Fab 2 and 5: 121, Park Ave. 3, Hsinchu Science Park, Hsinchu 300-77, Taiwan, R.O.C., Fab 8 25, Li-Hsin Rd., Hsinchu Science Park, Hsinchu, 300-78, Taiwan, R.O.C.	Mask data preparation, Mask and wafer production
Chipbond Technology Corporation Taiwan No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C.	Bumping
NXP Semiconductors Test Center Europe - Hamburg (TCE-H) Troplowitzstrasse 20	Test Center, configuration of the Fabkey and delivery

Site	Task within the evaluation
22569 Hamburg Germany	
Assembly & Test Bangkok (ATBK) (former APB) Thailand 303 Moo 3 Chaengwattana Rd. Laksi, Bangkok 10210 Thailand	Test centre, wafer treatment, module assembly and delivery
Assembly & Test Kaohsiung (ATKH) (former APK) Taiwan #10, Jing 5th Road, N.E.P.Z, Kaohsiung 81170 Taiwan, R.O.C	Test centre, wafer treatment, module assembly and delivery
HID Global Ireland Paic Tionscail na Tulaigh Balle na hAbhann Co. Galway, Ireland	Inlay assembly
Smartrac Technology Ltd. (Linxens) Thailand Street: 142 Moo, Hi-Tech Industrial Estate Tambon Ban Laean, Amphor Bang-Pa-In 13160 Ayutthaya, Thailand	Inlay assembly
HID Global Malaysia HID Global Malaysia Sdn Bhd No 2, Jalan I-Park 1/1, Kawazan Perindustrian i-Park, Bandar Indahpura, Kulai, 81000 Johor, Malaysia	Inlay assembly

Table 1: Relevant development/production sites for the respective TOE configurations

The following site was evaluated within the course of the evaluation, but is not part of the life-cycle of the TOE:

Site	Address	Function
Amkor T1 Taiwan	Amkor T1, Taoyuan, Taiwan (short reference: Amkor_Tao): AMKOR T1, No. 1, Kao-Ping Sec, Chung-Feng Rd, Lungtan Township, Taoyuan County, Taiwan	Bumping

Table 2: Sites audited in the course of the evaluation, but not part of the life-cycle

Conclusion

The maintained change is at the level of an update of life cycle security aspects covered by newer audits and/or site certificates for each site of the life cycle considered herein. The change has no effect on product assurance.

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-0978-V2-2017 dated 27 September 2017 is of relevance and has to be considered when using the product.

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.

The evaluation of the composite product or system must also consider the evaluation results as outlined in the documents ETR for composite evaluation [6] and ETR for composite evaluation Addendum [7]. The sections contained in the ETR for composite evaluation Addendum [7] replace the respective sections of the ETR for composite evaluation [6]. All sections not mentioned in the addendum have not been updated, because those are not affected by the changes in scope of the partial ALC re-evaluation for maintenance BSI-DSZ-CC-0978-V2-2017-MA-01.

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).

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] chapter 9.2.

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 “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012

[2] NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG Impact Analysis Report, Version 0.1, 2018-06-04, NXP Semiconductors (confidential document)

[3] Certification Report BSI-DSZ-CC-0978-V2-2017 for NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC Dedicated Software, 27 September 2017, Bundesamt für Sicherheit in der Informationstechnik

[4] NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE Security Target Lite, Version 2.61, 2015-10-14, NXP Semiconductors

[5] NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE Evaluation Reference List, Version 1.45, 2018-06-11, NXP Semiconductors (Confidential document)

[6] Evaluation Technical for Composite Evaluation (ETR COMP) for the P60x144/080yVA/VA(Y/B/X)/VE, version 2, 2017-09-14, TÜV Informationstechnik GmbH.

[7] Evaluation Technical for Composite Evaluation Addendum (ETR COMP) for the P60x144/080yVA/VA(Y/B/X)/VE, version 1, 2018-07-25, TÜV Informationstechnik GmbH.