Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1136-V3-2022-MA-01

NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4)

from

NXP Semiconductors Germany GmbH

SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] 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-1136-V3-2022.

The certified product itself did not change. The changes are related to an update of life cycle security aspects.

Considering 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-1136-V3-2022 dated 7 September 2022 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-1136-V3-2022.

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

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

Bonn, 17 May 2023

The Federal Office for Information Security

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 procedures on Assurance Continuity [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 Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), NXP Semiconductors Germany GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements according to the procedures on Assurance Continuity [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 an update of life cycle security aspects. The ALC re-evaluation was performed by the ITSEF TUV Informationstechnik GmbH. The procedure led to an updated version of the Evaluation Technical Report (ETR) [5]. The ETR for Composition [6] was not renewed.

The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4]. The Security Target did not change.

The development and production sites as listed in Annex B of the certification report [3] were updated by this partial ALC re-evaluation as listed below:

Name of Site	Company Name / Address	Function
NXP Hamburg	NXP Semiconductors Germany GmbH Troplowitzstr. 20 22529 Hamburg Germany	Project management, central design database, HW/FW/SW development and verification, security architecture and evaluation, flaw remediation, trust provisioning, and customer support, IT support.
NXP Gratkorn	NXP Semiconductors Austria GmbH Mikronweg 1 8101 Gratkorn Austria	Project management, HW/FW/SW development and verification, security architecture and evaluation, trust provisioning, and document control system (DocStore).
NXP Eindhoven	NXP Semiconductors Eindhoven HTC-46.3-west (Development Center) Building 46, High Tech Campus 5656AE, Eindhoven The Netherlands	HW/FW/SW development, security architecture. IT engineering and generic support.

NXP Nijmegen	NXP Semiconductors Nijmegen B.V. Gerstweg 2 6534AE Nijmegen The Netherlands	Verification of design data and mask data, sample preparation.
NXP Glasgow	NXP Glasgow EK Pegasus House, Scottish Enterprise Technology Park, Bramah Ave East Kilbride, Glasgow G75 0RD Scotland, UK	Hardware development, security architecture and reviews.
NXP Leuven	NXP Semiconductors Interleuvenlaan 80 B-3001 Leuven Belgium	Hardware development, security reviews.
GlobalLogic Wroclaw	GlobalLogic Ul. Strzegomska 48A 53-611 Wroclaw Poland	SW development and verification.
Sii Gdansk	SII Olivia Prime Building, 10th floor, Grunwaldzka 472E 80-309 Gdansk Poland	SW development and verification.
NXP IT Eindhoven	See NXP Eindhoven.	See NXP Eindhoven.
Akquinet Datacenter Hamburg	Akquinet Datacenter Hamburg Ulzburger Strasse 201 22850 Norderstedt Germany	Data center.
Colt Hamburg	AtlasEdge Hamburg Data Centre[1] Obenhauptstrasse 1C 22335 Hamburg Germany	Data center.
Digital Realty Phoenix	Digital Realty Data Center 120 E Van Buren St, Phoenix AZ 85004 U.S.A.	Data center.
Equinix Singapore	EQUINIX 20 Ayer Rajah Crescent, IBX SG1, Level 5 Unit 5, Ayer Rajah Industrial Park 139964 Singapore	Data center.
NXP Bangalore	NXP India Private Limited Manyata Technology Park, Nagawara Village, Kasaba Hobli, Bangalore 560 045 India	Data center.
NXP Bucharest	NXP Semiconductors Romania Campus 6, Bulevardul Iuliu Maniu 6L, 061103 Bucureşti Romania	IT engineering and support.
NXP Guadalajara	NXP Guadalajara Periferico Sur #8110 Col. El Mante JALISCO, 45609 Tlaquepaque Mexico	IT engineering and support.
NXP Master IT	NXP Semiconductors HTC Building 60	Virtual IT Network and Administration site.

1 The Colt Data Center Hamburg, Obenhauptstrasse, was aquired by AtlasEdge Data Centres end of 2021. The certificate and related documentation still refers to the old name.

	High Tech Campus 5656 Eindhoven Netherlands	
Global Foundries Singapore (Fab 7)	GLOBALFOUNDRIES Singapore Pte Ltd 60 Woodlands Industrial Park D, Street 2 Singapore, 738406	Mask and wafer production.
Global Foundries Dresden (Fab 1)	GlobalFoundries Fab 1 Dresden, Wilschdorfer Landstrasse 101, 01109 Dresden, Germany	Mask and wafer production.
AMTC Dresden	Advanced Mask Technology Center GmbH & Co KG (AMTC) Rähnitzer Allee 9 01109 Dresden Germany	Wafer mask production.
	Toppan Photomasks Inc. 400 Texas Avenue Round Rock, TX 78664 USA	IT administration for AMTC Dresden.
Chipbond Hsinchu	Chipbond Technology Corporation No. 3, Li-Hsin Rd. V Science Based Industrial Park Hsin-Chu City Taiwan, R.O.C.	Bumping.
NXP Hamburg TCE-H	See NXP Hamburg.	See NXP Hamburg.
NXP ATBK	NXP Semiconductors Thailand (ATBK) 303 Moo 3 Chaengwattana Rd., Laksi Bangkok 10210 Thailand	Test centre, wafer treatment, module assembly, (pre-) personalization, delivery, and test program engineering (TPE).
NXP ATKH	NXP Semiconductors Taiwan Ltd (ATKH) #10, Chin 5th Road, N.E.P.Z Kaohsiung 81170 Taiwan, R.O.C.	Test centre, wafer treatment, module assembly, (pre-) personalization, and delivery.
Linxens Thailand	Linxens Co., Ltd. 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang Pa-In 13160 Ayutthaya Thailand	Inlay production.
HID Malaysia	HID Global Sdn. Bhd. No. 2, Jalan i-Park 1/1 Kawasan Perindustrian i-Park Bandar Indahpura 81000 Kulai, Johor Malaysia	Inlay production.
ASE Kaohsiung	Advanced Semiconductor Engineering Inc., No 26, Jing 3rd Rd., Nanzih Dist., Kaohsiung, Taiwan	Wafer Testing, Wafer Treatment.
SIPI Chicago	Sipi Metals & Materials 1720 N. Elston Avenue Chicago, Illinois 60642-1579 United States	Secure Scapping.

Table 1: Development and production sites

As a result of the partial ALC re-evaluation, the following sites are integrated per their

site certificates:

- ASE Kaohsiung, Site Certification BSI-DSZ-CC-S-0196-2022.
- SIPI Chicago, Site Certification NSCIB-SS-0200410-CR2.

Conclusion

The maintained change is at the level of life cycle security aspects. The change has no effect on product assurance.

Considering 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-1136-V3-2022 dated 7 September 2022 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.

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[2] and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

2 In this case the eighteen month time frame is related to the date of the initial version [6] of the Evaluation Technical Report for Composite Evaluation as the updates made afterwards are not related to updates of AVA evaluation tasks.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[3] 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].

3 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 2.2, 30 September 2021

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.0, November 2019

[2] Impact Analysis Report, Version 0.1, 2023-01-10, NXP Semiconductors

[3] Certification Report BSI-DSZ-CC-1136-V3-2022 for NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), 2022-09-07, Bundesamt für Sicherheit in der Informationstechnik

[4] Security Target Lite BSI-DSZ-CC-1136-V3-2022, Version 2.6, 2022-06-13, NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, NXP Semiconductors

[5] Evaluation Technical Report NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) B1, BSI-DSZ-CC-1136-V3-MA01, Version 2, 2023-05-16, Evaluation Technical Report Summary, TÜV Informationstechnik GmbH (confidential document)

[6] ETR for composite evaluation according to AIS 36 for the Product 7121, BSI-DSZ-CC-1136-V3-2022, Version 2, 2022-08-25, Evaluation Technical Report For Composite Evaluation (ETR Comp), TÜV Informationstechnik GmbH (confidential document)