Site Security Certification Report

Semiconductor Manufacturing North China (Beijing) Corporation

Sponsor:	***NXP Semiconductors Germany GmbH*** **Troplowitzstrasse 20** **22529 Hamburg** **Germany**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-SS-0276578-CR**
Report version:	**1**
Project number:	**0276578**
Author(s):	**Hans-Gerd Albertsen**
Date:	**14 June 2021**
Number of pages:	**9**
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Currently the Common Criteria Recognition Arrangement (CCRA) and SOG-IS Mutual Recognition Agreement (SOGIS-MRA) do not cover the recognition of Site Certificates. However, the evaluation process followed all the rules of these agreements and used the agreed supporting document for Site certification *[CCDB]*. Therefore, the results of this evaluation and certification procedure can be re-used by any scheme in a subsequent product evaluation and certification procedure that makes use of the certified site.

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate would indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations. As Site Certificates are not covered, these logos are not present.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the site Semiconductor Manufacturing North China (Beijing) Corporation. The operator of the site is SMNC (Beijing) located in Beijing, P.R.C. NXP Semiconductors Germany GmbH located in Hamburg, Germany acts as the sponsor of the evaluation and certification.

The evaluated site is: Semiconductor Manufacturing North China (Beijing) Corporation.

The site is used by NXP Semiconductors Germany GmbH to participate in the production of Security ICs (Wafer Fab).

The site activities could be related to Phase 3 of the seven Phases of the Lifecycle Model as defined in *[PP]*.

The site has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 11.06.2021 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the Site Security Target *[SST]*, which identifies assumptions made during the evaluation and the level of confidence (evaluation assurance level) the site is intended to satisfy for product evaluations. Users of this site certification are advised to verify that their own use of, and interaction with, the site is consistent with the Site Security Target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] and *[STAR]*[2] for this site provide sufficient evidence that it meets the EAL6 assurance components ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 at AVA_VAN.5 level, and ALC_LCD.1.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* and the Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, version 1.0, Revision 1 *[CCDB]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions of the Common Criteria and that the site will be listed on the NSCIB Certificates list. It should be noted that the certification results only apply to the specific site, used in the manner defined in the *[SST]*.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

2 Certification Results

2.1 Identification of Site

The Target of Evaluation (TOE) for this evaluation is the Semiconductor Manufacturing North China (Beijing) Corporation located in Beijing, P.R.C.

2.2 Scope: Physical

The site address is NO.18 Wenchang Road, Beijing Development Area, Beijing, People Republic of China. It comprises multiple buildings within the campus. The areas in scope are FAB2-P1 and FAB2-P2. The external boundary of the campus is guarded by an electronic fence with six main entrances.

The areas where the relevant activities take place are as follows.

Security areas of Fab2-P1:

- The Design Rule Check Room (Room 6085) is on the 6th floor of BO1 building.
- The FA lab (Room 6129) and RE Lab #1 (Room 6128) are on the 1st floor of P1C building
- The Mask Shop is on the 3rd floor of P1C building.
- The Mask Bank is on the 3rd floor of P1C building.
- The IT office (Room 1M28) is on the 1M floor of BO1 building.
- The Security Control Center (Room 1014) is on the 1st floor of BO1 building.

Security areas of Fab2-P2:

- The clean room is on the 2nd and 3rd floor of P2A and P2B building.
- The RE Lab #2 (Room 1062) is on the 1st floor of P2B building.
- The FGWH #1 (Room 1001) is on the 1st floor of P2A building.
- The FGWH #2 (Room 1038) is on the 1st floor of P2B building.
- The IT office (Room 2020) is on the 2nd floor of BO2 building.
- The IT server room (Room 2007) is on the 2nd floor of BO2 building.
- The Security Control Center (Room 1051) is on the 1st floor of BO2 building.

2.3 Scope: Logical

This site is used as wafer fab for Security ICs.
The site provides the services and/or processes covered in the scope of the site evaluation process as follows.

- Mask inspection
- Security mask management
- Security wafer manufacturing (incl. WAT (Wafer Acceptance Test), OQA (Outgoing Quality assurance), fault analysis, and wafer reliability test)
- Security wafer management
- Mask/wafer scrap management/destruction
- Secure wafer shipment
- Return mask back to SMIC (Shanghai) mask operation for repair/remount
- Receive wafers from clients

For Security ICs (e.g. smartcard products), these activities could be related to Phase 3 of the seven Phases of the Lifecycle Model in *[PP]*.

Within those phases, the site is involved in

- ALC_DVS to control access to the assets (at AVA_VAN.5 level).
- ALC_CMC/CMS to handle the site internal documentation and TOE development related configuration items.

- ALC_LCD as part of TOE development.

2.4 Evaluation approach

The evaluation is a first evaluation, based on developer documentation.

In the evaluation all evaluator actions have been performed including a site visit. For assessment of the ALC_DVS aspects, the Minimum Site Security Requirements *[MSSR]* have been used.

2.5 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[3] which references other evaluator documents. To support re-use of the site evaluation activities a derived document *[STAR]*[2] was provided and approved. This document provides details of the site evaluation that have to be considered when this site is used in a product evaluation.

The evaluation lab concluded that the site meets the assurance requirements listed in the *[SST]* as assessed in accordance with *[CC], [CEM]* and *[CCDB]*.

2.6 Comments/Recommendations

The Site Security Target (*[SST]*) contains necessary information about the usage of the site. During a product evaluation, the evidence for the fulfillment of the Assumptions listed in the *[SST]* shall be examined by the evaluator of the product when re-using the results of this site evaluation.

[3] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator and is not releasable for public review.

3 Site Security Target

The Site Security Target of Semiconductor Manufacturing North China (Beijing) Corporation, NQR-QUSM-99-3005, Version 2.0, 12 April 2021 *[SST]* is included here by reference.

Please note that for the need of publication a public version *[SST-Lite]* has been created and verified according to *[ST-SAN]*

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MSSR	Minimum Site Security Requirements
NSCIB	Netherlands scheme for certification in the area of IT security

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.
[CCDB]	Supporting Document Guidance: CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
[ETR]	Evaluation Technical Report NXP SMNC (Beijing), 21-RPT-223, Version 2.0, 31 May 2021.
[MSSR]	Joint Interpretation Library, Minimum Site Security Requirements, Version 3.0, February 2020.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[PP]	Security IC Platform Protection Profile with Augmentation Packages, Rev 1.0, 13 January 2014, registered under the reference BSI-CC-PP-0084-2014.
[SST]	Site Security Target of Semiconductor Manufacturing North China (Beijing) Corporation, NQR-QUSM-99-3005, Version 2.0, 12 April 2021.
[SST-Lite]	Security Target Lite of Semiconductor Manufacturing North China (Beijing) Corporation, NQR-QUSM-99-3007, Version 2.0,12 April 2021
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.
[STAR]	Site Technical Audit Report NXP SMNC (Beijing), 21-RPT-225, Version 2.0, 31 May 2021.

(This is the end of this report).