Site Security Certification Report

Semiconductor Manufacturing North China (Beijing) Corporation

Sponsor:	***NXP Semiconductor Germany GmbH*** **Beiersdorfstraße 12** **22529 Hamburg** **Germany**
Site Operator:	***Semiconductor Manufacturing North China (Beijing) Corporation*** **No. 18, Wen Chang Road, Beijing Development Area** **Beijing, 100176** **P.R. China**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-SS-2300067-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300067-01**
Author(s):	**Brian Smithson**
Date:	**28 August 2023**
Number of pages:	**9**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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, TrustCB 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 TrustCB 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 TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence 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, TrustCB 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, 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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

At the time of publication, the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) do not cover the recognition of Site Certificates. The site-security evaluation process, however, 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 reused by any scheme in subsequent product evaluations and certification procedures that make use of the certified site.

Presence of the CCRA and SOG-IS logos on this certificate would indicate that the certificate is issued in accordance with the provisions of the CCRA and the SOG-IS MRA and is recognised by the participating nations. The CCRA and the SOG-IS MRA do not cover site certification, however, so these logos are not present on this certificate.

1 Executive Summary

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

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

The site is used by NXP Semiconductor Germany GmbH to participate in the production and testing of hardware for secure IC hardware products. To perform its activities, the site uses the Semiconductor Manufacturing North China (Beijing) Corporation provided remote IT-infrastructure and local IT equipment (workstations, router, VPN) and works according to the Semiconductor Manufacturing North China (Beijing) Corporation defined processes.

The site is used for wafer manufacturing, and its scope includes related security areas.

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 SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 28 August 2023 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 this site 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]*.

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions of the Common Criteria and that the site certificate will be included on the NSCIB Certificates list. Note that the certification results apply only to the specific site, used in the manner defined in the *[SST-Lite].*

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available 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 Site Identification

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

2.2 Scope: Physical

This site certification considers a campus location occupied only by Semiconductor Manufacturing North China (Beijing) Corporation.

The site is primarily for wafer manufacturing. There are two general areas, Fab2-P1 with seven main buildings, and Fab2-P2 with six main buildings. The area where the relevant activities take place is limited to:

- Fab2-P1 includes the Design Rule Check room, the Labs, the Mask shop, the Mask bank, IT office, and Security Control Center for Fab2-P1:
  - The related security areas are located as below floors/ rooms of buildings:
  - 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.
- Fab2-P2 includes the Clean Room, a Lab, Finished Goods Warehouses, IT office, and Security Control Center for 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 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

The site provides the following services and/or processes:

- Mask inspection
- Receipt of wafers from clients
- Security mask management
- Security wafer manufacturing
- Security wafer management
- Mask/wafer scrap management/destruction
- Return masks to mask operation for repair/remount
- Security wafer shipment

For smartcard products, these activities could be related to Phase 3 of the seven phases of the Lifecycle Model in *[PP]*.

Within that phase, 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 and testing

The activities of Fab2-P2 include wafer manufacturing, WAT (Wafer Acceptance Test), OQA (Outgoing Quality Assurance), wafer warehousing, wafer dispatch and scrapping. The scrap wafer and mask will be destroyed on the site. The activities of Fab2-P1 include mask inspection, mask management and DRC.

The site performs the secure shipment to the client. It only refers to the internal shipments and/or shipments between sites and not to shipment to customer or end user. Therefore, ALC_DEL is not scope of the site. This site does not have a direct role in ALC_TAT and therefore those activities in an associated TOE evaluation are not impacted by the operations of this site.

2.4 Evaluation Approach

The evaluation is a new evaluation of a previous-evaluated site (NSCIB-SS-21-0276578). In the evaluation all evaluator actions, including an in-person site visit, have been performed. For assessment of the ALC_DVS aspects, the Minimum Site Security Requirements *[MSSR]* have been used.

2.5 Evaluation Results

The evaluation lab documented its evaluation results in the *[ETR]*[3], which references other evaluator documents. To support reuse of the site evaluation activities a derived document *[STAR]*[4] was provided and approved. This document provides details of the site evaluation that must 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 fulfilment of the Assumptions listed in the *[SST]* shall be examined by the evaluator of the product when reusing the results of this site evaluation.

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

[4] 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.

3 Site Security Target

The Site Security Target of Semiconductor Manufacturing North China (Beijing) Corporation for Tulips, QR-ISMG-SC-3012, v4, 25 June 2023 *[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 definitions 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
TOE	Target of Evaluation

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 Site Audit “SMNC Beijing”, 23-RPT-590, v2.0, 23 August 2023

[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 2.6, 02 August 2022

[PP] Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Revision 1.0, 13 January 2014

[SST] Site Security Target of Semiconductor Manufacturing North China (Beijing) Corporation for Tulips, QR-ISMG-SC-3012, v4, 25 June 2023

[SST-lite] Site Security Target Lite of Semiconductor Manufacturing North China (Beijing) Corporation for Tulips, QR-ISMG-SC-3016, v4, 18 July 2023

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

[STAR] Site Technical Audit Report - NXP SMNC Beijing, 23-RPT-591, v2.0, 23 August 2023

(This is the end of this report.)