Site Security Certification Report

NXP Shanghai Puxi site

Sponsor:	***NXP Semiconductors Germany GmbH*** **Troplowitzstrasse 20** **22529 Hamburg** **Germany**
Site Operator:	***NXP (China) Management Ltd.*** **BM InterContinental Business Centre** **100 Yu Tong Road** **Shanghai 200070** **P.R.C.**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-SS-222678-CR3**
Report version:	**1**
Project number:	**222678_3**
Author(s):	**Brian Smithson**
Date:	**18 July 2022**
Number of pages:	**9**
Number of appendices:	**0**

Head Office:
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 Netherlands Chamber of Commerce (KVK), 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 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, 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, 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

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 NXP Shanghai Puxi site. The operator of the site is NXP (China) Management Ltd. located in Shanghai, P.R.C. NXP Semiconductors Germany GmbH located in Hamburg, Germany is the sponsor of the evaluation and certification.

The evaluated site is: NXP Shanghai Puxi site.

The site is used by NXP Business Line Connectivity & Security to participate in the development and testing of hardware/software for secure IC hardware products. To perform its activities, the site uses the NXP Semiconductors Germany GmbH-provided remote IT-infrastructure and local IT equipment (workstations, router, VPN) and works according to the NXP Competence Center Crypto & Security-defined processes.

The site provides services such as: generation of the source code of embedded and IC dedicated software and the creation of development related documents; generation of the analog and digital hardware designs, embedded and IC dedicated software, and the creation of development related documents; and, verification and validation process with or without the use of simulation tools. These activities could be related to Phase 1 and Phase 2 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 18 July 2022 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]*.

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 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]*.

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 NXP Shanghai Puxi site located in Shanghai, China.

2.2 Scope: Physical

The site comprises of three floors, named 19F to 21F. This physical scope of the site certification is only the development area located on floor 19F and the data center on floor 20F. The development area is identified as the area containing the rooms 1909 to 1924 (covering cubicles WS19001-WS19053), and the data center is identified as room 2021.

2.3 Scope: Logical

The site is used for IC Embedded Software Development, Test Program Development, Verification and Validation (Phase 1 of the Lifecycle defined in *[PP]*) and/or IC Development, IC Dedicated Software Development, Verification and Validation (Phase 2), providing services such as:

- The generation of the source code of embedded and IC dedicated software and the creation of development related documents.
- The generation of the analog and digital hardware designs, embedded and IC dedicated software and the creation of development related documents
- Verification and validation process with or without the use of simulation tools.

To support the above services the site uses an appropriate secure IT environment with a local secure data center.

Within those lifecycle 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 and testing.

2.4 Evaluation Approach

The evaluation is a re-evaluation, based on developer documentation of a minor site change.

In the evaluation all evaluator actions, including a site visit, have been performed. Due to COVID-19 lockdown in Shanghai, the site audit was carried out virtually on 16 June 2022. 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]*.

[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.

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 Site Security Target

The Site Security Target NXP Shanghai Puxi, NXPOMS-1719007347-3870, version 1.4, 15 June 2022 *[SST]* is included here by reference.

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 NXP Shanghai Puxi site, 22-RPT-311, v1.0, 20 June 2022
[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, BSI-CC-PP-0084-2014, Revision 1.0, 13 January 2014
[SST]	Site Security Target NXP Shanghai Puxi, NXPOMS-1719007347-3870, version 1.4, 15 June 2022
[STAR]	Site Technical Audit Report NXP Shanghai Puxi site, 22-RPT-312, v1.0, 06 July 2022

(This is the end of this report.)