TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Version 2018-1

Site Security Certification Report

NXP (China) Management Ltd.

Sponsor and developer:	***NXP (China) Management Ltd.*** **BM InterContinental Business Center** **100 Yu Tong Road** **Shanghai 200070** **P.R.C**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-SS-222678- CR**
Report version:	**1.0**
Project number:	**222678**
Author(s):	**Hans-Gerd Albertsen**
Date:	**14 March 2019**
Number of pages:	**10**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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

Certificate

Standard
Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)

Certificate number
SS-19-222678

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

NXP (China) Management Ltd.
BM InterContinental Business Center
100 Yu Tong Road
Shanghai 200070
R.P.C.

Site and assurance level

NXP (China) Management Ltd.

EAL6 Assurance Components:

- ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 (at AVA_VAN.5 level), and ALC_LCD.1.

Project number
222678

Evaluation facility
Brightsight BV located in Delft, the Netherlands

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045) and the Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, version 1.0, Revision 1

The site identified in this certificate has been evaluated by an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 and the Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, version 1.0, Revision 1 for conformance to the Common Criteria for IT Security Evaluation version 3.1. This certificate applies only to the specific site as indicated and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the site by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the site by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity
Date of issue : **20-03-2019**
Certificate expiry : **20-03-2021**

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Currently the Common Criteria Recognition Arrangement (CCRA) and SOGIS-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 NXP (China) Management Ltd.. The operator of the site is NXP (*China) Management Ltd.* located in Shanghai, R.P.C. and they also act as the sponsor of the evaluation and certification.

The evaluated site is: NXP (China) Management Ltd..

The site is used by NXP (China) Management Ltd**.** to participate in the IC Embedded Software Development, Test Program Development, Verification and Validation and/or IC Development, IC Dedicated Software Development, Verification and Validation.

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 Semiconductors Germany GmbH defined processes.

The site activities could be related to Phase 1 and 2 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 11.03.2019 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-Lite]*, 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 site does not contribute to nor detract from ALC_TAT.3 since the used tools and techniques will be defined upfront by the client (see A.Project-Setup) they are TOE specific and cannot be seen as product type specific. All tools must be provided by the client.

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-Lite]*.

[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 NXP (China) Management Ltd. located in Shanghai 200070, P.R.C.

2.2 Scope: Physical

This site certification considers 2 floors of the BM InterContinental Business Center, 100 Yu Tong Road occupied only by NXP (China) Management Ltd.

The area where the relevant activities take place is limited to floor 19 (rooms 1909 to 1924) & floor 20 (room 2021).

2.3 Scope: Logical

This site is used for IC Embedded Software Development, Test Program Development, Verification and Validation and/or IC Development, IC Dedicated Software Development, Verification and Validation.

The tools for the development and testing activities are provided by the client (see A.Project-Setup).

For Security ICs (e.g. smartcard products), these activities could be related to Phase 1 and/or Phase 2 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 and Test Program 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]* 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-Lite]* as assessed in accordance with *[CC], [CEM]* and *[CCDB]*.

2.6 Comments/Recommendations

The Site Security Target (*[SST-Lite]*) and the Site Technical Audit Report *[STAR]* contain necessary information about the usage of the site. During a product evaluation, the evidence for the fulfillment of the Assumptions listed in the *[SST-Lite]* and mandatory Checking for Re-use in the *[STAR]* 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 NXP Shanghai, [SST] Site Security Target - NXP Shanghai v0.8.pdf, 26.02.2019 as well as the Security Target Lite, *[SST-Lite]* Site Security Target Lite - NXP Shanghai v0.8.pdf, 12.03.2019 are included here by reference.

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 (China) Management Ltd., 19-RPT-011 v2.0 ETR NXP Shanghai.pdf, v2.0., 08.03.2019.

[MSSR] Joint Interpretation Library, Minimum Site Security Requirements, Version 2.1, December 2017.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 1 September 2017.

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

[SST] Site Security Target NXP Shanghai, [SST] Site Security Target - NXP Shanghai v0.8.pdf, 26.02.2019.

[SST-Lite] Site Security Target Lite NXP Shanghai, Site Security Target lite – NXP Shanghai v0.8.pdf, 12.03.2018.

[STAR] Site Technical Audit Report NXP (China) Management Ltd., 19-RPT-012 v2.0 STAR NXP Shanghai.pdf, v2.0 08.03.2019.

[NPI-Hand] NPI 3.0 Handbook - BU S&C, 02 October 2017.

[CI-list] NXP Shanghai – Development Center - Configuration List, 30 November 2018.

[ALC-CM] BU S&C ALC-CM - Common Criteria Documentation, 21 November 2017.

[ALC-CMPro] BU S&C Configuration and Data Management Procedure, 19 December 2016

[ALC-CMPlan] BU S&C Configuration Management Plan, 14 August 2018.

[ALC-DesEnv] BU S&C Design Environment Maintenance, 13 February 2017

[SSM] Site Security Manual - NXP Shanghai Development Center v0.6, 27 February 2019.

[MSSR-DOC] Check List MSSR V2.1_SHAv1.0.xlsx, 30 November 2018.

[SMM] BU S&C Security Management Manual, 02 July 2018.

[SRO] BU S&C Security Requirements Overview, 28 April 2017.

[Tal-Acq] A Guide to NXP Talent Acquisition, 05 October 2017.

[Id-Man-Pol] Identity Management Policy, 15 January 2017.

[O-Board] Off Boarding, 31 August 2017.

[CoC-Train] S&C Security Code of Conduct Training Guideline, 12 November 2018.

[Vis-Pro] Visitor Procedure, 30 April 2018.

[Pack-Del] BU S&C - Packing and Delivery Requirements for Security Products, 22 June 2017.

[Sec-Obj] BU S&C Security Objects, 11 June 2017.

[Sec-Dev-Env] S&C China Secure Development Environment, 27 February 2019.

[HLD-Arch] HLD Architecture 0.991.

[HLD-Conn] HLD Connectivity 1.7.

(This is the end of this report).