Site Security Certification Report

NXP Sophia Antipolis

Sponsor:	***NXP Semiconductors Germany GmbH*** **Beiersdorfstraße 12** **22529 Hamburg** **Germany**
Site Operator:	***NXP Sophia Antipolis*** **80 route des Lucioles** **Sophia Antipolis** **06560 Valbonne** **France**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-SS-2400036-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400036-01**
Author(s):	**Haico Haak**
Date:	**26 July 2024**
Number of pages:	**9**
Number of appendices:	**0**

CONTENTS

Foreword 3

Recognition of the Certificate 4

1 Executive Summary 5

2 Certification Results 6

2.1 Site Identification 6
2.2 Scope: Physical 6
2.3 Scope: Logical 6
2.4 Evaluation Approach 6
2.5 Evaluation Results 6
2.6 Comments/Recommendations 7

3 Site Security Target 8

4 Definitions 8

5 Bibliography 9

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.

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 Sophia Antipolis. The sponsor of the evaluation and certification is NXP Semiconductors Germany GmbH located in Hamburg, Germany and the operator of the site is NXP Sophia Antipolis.

The evaluated site is: NXP Sophia Antipolis.

The site is used by NXP Semiconductors Germany GmbH to participate in the development and testing of software (Embedded & IC Dedicated Software) and the development of hardware for secure

IC hardware products. To perform its activities, the site uses the corporate provided remote IT-infrastructure and local IT equipment (workstations, router, VPN) and works according to the NXP Semiconductors Germany GmbH defined CCC&S processes.

The site activities are 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 26-07-2024 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), 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]*.

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 site NXP Sophia Antipolis located in Sophia Antipolis, France.

2.2 Scope: Physical

This site certification considers a single building location occupied only by NXP Sophia Antipolis.

The entire building identified in the [SST] §2.1 is in the scope of the certification. The surroundings of this building are not in scope. Therefore, the walls of this building form the physical boundary of the site. All areas in scope are classified as YELLOW and RED areas. The terms YELLOW area and RED area are defined in the NXP internal document [SRO]. Those locations contain security areas with restricted access under control of NXP where only authorized persons can enter.

2.3 Scope: Logical

This site is used for development and testing of Embedded Software and IC Dedicated Software and development of hardware for secure integrated circuits. To perform its activities, the site uses the corporate IT infrastructure and services remotely and works according to NXP CCC&S processes.

The corporate IT infrastructure has been covered by a separate site certification. The applicable aspects of the IT infrastructure consumed at this site were verified during this site certification.

For security ICs, 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 testing

2.4 Evaluation Approach

In the evaluation all evaluator actions, including a site visit, have been performed. The site audit was carried out in-person. 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 NXP Sophia Antipolis Site Security Target, Rev. 1.1, 28 March 2024 *[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
CCC&S	Competence Center Crypto & 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 Site Audit NXP Sophia Antipolis, Version 3.0, 3 July 2024
[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]	NXP Sophia Antipolis Site Security Target, Rev. 1.1, 28 March 2024
[STAR]	Site Technical Audit Report - NXP Sophia Antipolis, Version 2.0, 3 July 2024

(This is the end of this report.)