TRUSTCB
TRUST AND VERIFY

Site Security Certification Report

NXP Caen

Sponsor:	***NXP Semiconductors Germany GmbH*** **Beiersdorfstraße 12** **22529 Hamburg** **Germany**
Site Operator:	***NXP Semiconductors France*** **2 Esplanade Anton Phillips – Colombelles** **14600 Caen** **France**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-SS-2400141-01-CR**
Report version:	**2.0**
Project number:	NSCIB-**2400141-01**
Author(s):	**Alireza Rohani**
Date:	**20 March 2025**
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 Caen. The sponsor of the evaluation and certification is NXP Semiconductors Germany GmbH located in Hamburg, Germany and the operator of the site is NXP Semiconductors France.

The evaluated site is: NXP Caen.

The site is used by NXP Semiconductors Germany GmbH to participate in the development, testing and production of hardware/software for secure IC hardware products.

The site 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 20 March 2025 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, CEM:2022 *[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, CC:2022 *[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]*.

This document was re-issued on 20 March 2025 as version 2.0 to reference an updated [ETR] and updated [STAR]. These reports were updated as a result of a correction to the audit date of the site.

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 Caen located in Caen, France.

2.2 Scope: Physical

The buildings A & B are in the scope of the SST. The surroundings of this building are not in the scope of the SST. Therefore the walls of this building form the physical boundary of the site.

2.3 Scope: Logical

The following services and/or processes provided by the site are in the scope of the site evaluation process:

- Development
- Internal Shipment
- IT Support

NXP Caen Site Services related to life cycle phases:

- Security IC Embedded Software Development (Phase I)
- IC Embedded Software Development and testing (Phase I)
- IC Design (Phase II)
- IC Dedicated Software Development and testing (Phase II)

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

This site does not have a direct role in ALC_TAT and ALC_DEL, 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 first evaluation.

In the evaluation all evaluator actions, including a 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.

[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.

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 Site Security Target

The NXP Semiconductors Caen, Site Security Target, rev 3.3, date: 23 January 2025 *[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 1 to 5, CC:2022 Revision 1, November 2022
[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, CEM:2022 Revision 1, Novembre 2022
[ETR]	Evaluation Technical Report Site Audit NXP Semiconductors Caen, 25-RPT-1369, version 3.0, date: 19 March 2025
[MSSR]	Joint Interpretation Library, Minimum Site Security Requirements, Version 3.1, December 2023
[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 Semiconductors Caen, Site Security Target, rev 3.3, date: 23 January 2025
[STAR]	Site Technical Audit Report – NXP Caen, 25-RPT-174, version 3.0, date: 19 March 2025

(This is the end of this report.)