



TRUST AND VERIFY

TrustCB Site Certification Scheme

Site Security Certification Report

NXP Semiconductors Glasgow

Sponsor: ***NXP Semiconductors Netherlands***
Elektronicaweg 40
2628 XG Delft
The Netherlands

Site Operator: ***NXP Semiconductors Glasgow***
Pegasus House, 3 Bramah Avenue,
Scottish Enterprise Technology Park
East Kilbride, Glasgow, G75 0RD
United Kingdom

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2,
2612 CT Delft,
The Netherlands

Report number: **SiteCC-2600074-01-CR**

Report version: **1**

Author(s): **Brian Smithson, site_cc@trustcb.com**

Date: **10 July 2026**

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	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

TrustCB is a fully independent commercial Certification Body specialising in the provision of high-assurance, security certifications for ICT products and associated sites, processes and services.

TrustCB is widely recognised for its schemes and certification work referencing the Common Criteria (CC) and Common methodology (CEM) for Information Technology Security Evaluation. CC and CEM are published by ISO/IEC as ISO/IEC 15408, Evaluation criteria for IT security and ISO/IEC 18045 Methodology for IT security evaluation (CC).

Common Criteria based Site Certifications have long been recognised in demonstrating security in a product lifecycle. TrustCB has significant experience in the certification of sites referencing the SOG-IS recognised Netherlands Scheme for Certification in the Area of IT Security (NSCIB) scheme.

Since “site certification” is not explicitly defined in the EUCC Regulation, (EU) 2024/482, TrustCB has developed the TrustCB **Site Certification Scheme**. The scheme is in full alignment with EUCC requirements and State of the Art documents, and ready for recognition across cooperating schemes.

Importantly, the scheme is built on the NSCIB site-audit framework. Its principles are aligned with those adopted under the SOG-IS agreement and used by the SOG-IS based national schemes, now all superseded by EUCC. As such, the TrustCB Site Certification scheme ensures continuity with the recognised best practices used for STAR acceptance under SOGIS, as the ecosystem is now firmly transitioned to EUCC.

By awarding a TrustCB Site Certification Scheme certificate, TrustCB B.V. certifies that a site complies with the security requirements specified in the associated Site Security Target, in compliance the Common Criteria standards.

The consumer of this certification should review the Site Security Target (SST) in addition to this Certification Report, to gain an understanding of any assumptions made during the evaluation, and the level of confidence that the 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) does 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 are available for use in any scheme in subsequent product evaluations and certification procedures that make use of the certified site.

The reuse of this certification with a third-party Certification Body should always be checked with the intended consuming Certification Body ahead of being reused.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the NXP Semiconductors Glasgow. The sponsor of the evaluation and certification is NXP Semiconductors Netherlands located in Hamburg, Germany and the operator of the site is NXP Semiconductors Glasgow.

The evaluated site is: NXP Semiconductors Glasgow.

The site is used by NXP Semiconductors Netherlands to participate in the development and testing of software for secure IC hardware products. To perform its development activities the site uses the NXP CCC&S provided and managed remote IT-infrastructure. Locally available IT equipment like workstations or VPN router is also provided and managed by NXP CCC&S directly. CCC&S is the abbreviation for “Competence Center Crypto & Security”.

The site performs IC Embedded Software Development and testing and/or IC Dedicated Software Development and testing and therefore 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 2026-07-10 with the approval of the ETR. The site audit was performed 2026-03-19.

The certification procedure has been conducted in accordance with the provisions of the TrustCB Site Certification Scheme [TrustCB-SP]

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 Certification Body for this site certification activity, declares that the evaluation meets all the conditions of the Common Criteria and that the site certificate will be included on the TrustCB webpage of certified sites.

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 Semiconductors Glasgow located in East Kilbride Glasgow, Scotland.

2.2 Scope: Physical

This site certification considers a single two-story building occupied only by NXP Semiconductors Glasgow.

The area where the relevant activities take place is limited to:

Ground floor

- Left Wing: Development and Testing of non-secure products (yellow zone)
- Left Wing: Standalone Access badge system and CCTV recordings (red zone)
- Rest: Visitor area (green zone), access to building and elevator (yellow zone)

First floor

- Left Wing and corridor: Server room (red zone), Development and Testing of non-secure products (yellow zone)
- Right Wing: High secure development area (red zone), High secure IT room (red zone; inside the high secure development area)

2.3 Scope: Logical

The NXP Glasgow site contributes to the IC Embedded Software Development and IC Development. For 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 testing

This site does not have a direct role in ALC_DEL and 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 re-evaluation, based on developer documentation of minor site changes.

In the evaluation all evaluator actions, including a site visit, have been performed. The site audit was carried out in-person with one evaluator for one day. 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

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.

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 Site Security Target

The NXP Semiconductors Glasgow Site Security Target, NXPOMS-1719007347-4756, v2.2, May 2026 [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
SST	Site Security Target
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, November 2022
[ETR]	Evaluation Technical Report Site Audit NXP Semiconductors Glasgow, 26-RPT_828, v2.0, July 2026
[MSSR]	EUCC Scheme State-of-The-Art Document - Minimum Site Security Requirements, Version 2.0, February 2025
[PP]	Security IC Platform Protection Profile including Functional Packages, Version 2.0, BSI-CC-PP-0084-V2-2026, February 25, 2026
[TrustCB-SP]	TrustCB Scheme procedure - Site Certification v1.1
[SST]	NXP Semiconductors Glasgow Site Security Target, NXPOMS-1719007347-4756, v2.2, May 2026
[STAR]	Site Technical Audit Report – NXP Semiconductors Glasgow, 26-RPT-827, v1.0, July 2026

(This is the end of this report.)