

Site Security Certification Report

Huawei Xi'an V10-5 Development Site

Sponsor & Site Operator: ***Huawei Technologies Co., Ltd.***
Administration Building, Headquarters of Huawei
Technologies Co., Ltd., Bantian, Longgang District,
Shenzhen, 518129,
P.R.C

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

Report number: **NSCIB-SS-2300148-01-CR**

Report version: **1**

Project number: **NSCIB-2300148-01**

Author(s): **Kjartan Jæger Kvassnes**

Date: **23 October 2024**

Number of pages: **8**

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	6
3 Site Security Target	7
4 Definitions	7
5 Bibliography	8

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.

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) 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 Huawei Xi'an V10-5 Development Site. The operator of the site is Huawei Technologies Co., Ltd. located in Xi'an, P.R.C and they also act as the sponsor of the evaluation and certification.

The evaluated site is:

Huawei Xi'an V10-5 Development Site.
No. 127 Jinye Road, Yenta District, Xi'an City, Shanxi Province,
P.R.China

The Huawei Xi'an V10-5 Development Site is located in the Room C31, 5th floor of Building V10 on the campus, which is classified as the red zone area within Huawei. This area consists of an entry region, an open development area, a testing room, a meeting room and an IT server room.

The site is a secure area with restricted access where only authorized persons can enter. Within the development area, only members of the development team are entitled to access sensitive information like source code, design material and confidential development documentation. To enforce such access restriction, a combination of physical, procedural, personnel and logical measurements have been installed.

The site has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 23 October 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 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].

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 Huawei Xi'an V10-5 Development Site located in Xi'an, P.R.C.

2.2 Scope: Physical

This site certification considers a single building location occupied only by Huawei Technologies Co., Ltd.

The area where the relevant activities take place is limited to Room C31, 5th floor of Building V10.

2.3 Scope: Logical

The site performs activities are Security IC Embedded Software Development (Phase 1), IC Embedded Software Testing (Phase 1), IC Design and testing (Phase 2) as defined in 'Security IC Platform Protection Profile with Augmentation Packages'(PP-0084).

To perform its activities the site uses the Huawei provided and managed remote IT infrastructure. Locally available IT equipment like workstations or VPN router is also provided and managed by Huawei IT authorized support directly or remotely.

The site performs secure shipment to the client, which only refers to internal shipments and/or shipments between sites and not to shipment to customer or end user. Therefore ALC_DEL is not scope.

2.4 Evaluation Approach

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.

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 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.

3 Site Security Target

The Site Security Target Huawei Xi'an V10-5 Development Site, Version 1.1, Dated 17 October 2023 [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:

HSDL	High Security Development Lab
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 Site Audit Huawei Xi'an V10-5 Development Site, 23-RPT-1311, Version 3.0, Dated 19 April 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
- [SST] Site Security Target Huawei Xi'an V10-5 Development Site, Version 1.1, Dated 17 October 2023
- [STAR] Site Technical Audit Report - Huawei Xi'an V10-5 Development Site, 23-RPT-1312, version 3.0, Dated 19 April 2024

(This is the end of this report.)