

Site Security Certification Report

Fraunhofer Institute for Applied and Integrated Security AISEC

Sponsor & Site Operator: ***Fraunhofer Institute for Applied and Integrated Security AISEC***
Lichtenbergstraße 11,
85748 Garching,
Germany

Evaluation facility: ***TÜV Informationstechnik GmbH***
Am TÜV 1
45307 Essen, Germany

Report number: **NSCIB-SS-2300171-CR**

Report version: **1**

Project number: **NSCIB-2300171-01**

Author(s): **Alireza Rohani/ Kjartan Jæger Kvassnes**

Date: **22 February 2024**

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	7
2.5 Evaluation Results	7
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.

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 Fraunhofer AISEC. The operator of the site is Fraunhofer Institute for Applied and Integrated Security AISEC located in Garching, Germany and they also act as the sponsor of the evaluation and certification.

The evaluated site is: Fraunhofer Institute for Applied and Integrated Security AISEC.

The site is used by Fraunhofer Institute for Applied and Integrated Security AISEC to participate in the testing of hardware/software for secure IC hardware products. To perform its activities, the site uses the Fraunhofer Institute for Applied and Integrated Security AISEC provided remote IT-infrastructure and local IT equipment (workstations, router, VPN) and works according to the Fraunhofer Institute for Applied and Integrated Security AISEC defined processes.

The site activities could be related to Phase 2 and Phase 3 and above of the seven phases of the Lifecycle Model as defined in [PP].

The site has been evaluated by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 22 February 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 EAL7 assurance components ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 (at AVA_VAN.5 level).

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 Fraunhofer Institute for Applied and Integrated Security AISEC located in Garching, Germany.

2.2 Scope: Physical

This site certification considers a single building solely occupied by Fraunhofer Institute for Applied and Integrated Security AISEC

The area where the relevant activities take place is:

- Second upper floor (for US readers: third floor):
 - Hardware Security Laboratory (secure area for storage and testing of secure products),
- Ground Floor (for US readers: first floor):
 - Reception desk (CCTV and alarm system operation),
 - Facility management office (access control management).
- Basement:
 - Security systems room (secure area hosting CCTV/access control/alarm systems).

2.3 Scope: Logical

The site performs testing of security integrated circuits. The following life-cycle phases as defined in the Protection Profiles (PP) [3] and [4] are subject of this SST:

- Phase 2: IC Development (i.e., testing of engineering samples)
- Phase 3: IC Manufacturing and all phases after that (i.e., testing of final products).

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

- Testing of security integrated circuits,
- receiving of test samples from client,
- receiving of test plans from client,
- providing of test procedures and test result data to client,
- storing of test plans and test results data on secure servers,
- storing of test samples before sending back to the client,
- secure reception and preparation for sending of secure tangible items,
- secure reception and provision of data (non-tangible items).

For smartcard products, these activities could be related to Phase 1 and/or Phase 2 and above 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

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

In the evaluation all evaluator actions, including an 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 Fraunhofer AISEC, Version 1.3, 31 January 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
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 Fraunhofer Institute for Applied and Integrated Security AISEC, Version 1.0, 14 February 2024
- [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] Site Security Target Fraunhofer AISEC, Version 1.3, 31 January 2024
- [STAR] Site Technical Audit Report Fraunhofer Institute for Applied and Integrated Security AISEC, Version 1.0, 14 February 2024

(This is the end of this report.)