

Site Security Certification Report

INESA Shanghai

Sponsor and site owner: **Shanghai INESA Intelligent Electronics CO., Ltd.**
No. 818, Jin Yu Road, Jin Qiao Export Processing,
Zone Pudong, Shanghai
China

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

Report number: **NSCIB-SS-210064-CR2**

Report version: **1**

Project number: **210064_2**

Author(s): **Hans-Gerd Albertsen**

Date: **18 August 2021**

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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, TÜV Rheinland Nederland 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 INESA Shanghai. The operator of the site is Shanghai INESA Intelligent Electronics CO., Ltd. located in Shanghai, China and they also act as the sponsor of the evaluation and certification.

The evaluated site is: INESA Shanghai.

The site is used by Shanghai INESA Intelligent Electronics CO., Ltd. to participate in (i) wafer testing, sawing and backgrinding, (ii) module packaging and testing (including pre-personalisation), (iii) warehousing, and (iv) secure shipment to the client of secure IC hardware products (Security ICs). To perform its activities, the site uses its own equipment and IT-infrastructure but works according to the production specification provided by the client. This comprises test programs and assembly instructions.

The site activities are related to Phase 3 (only for IC testing and pre-personalisation) and Phase 4 of the seven phases of the Lifecycle Model as defined in [PP].

The site has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 16 August 2021 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, 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].

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates 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 (STAR) 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 INESA Shanghai located in Shanghai, China.

2.2 Scope: Physical

This site certification considers a two-building location occupied only by Shanghai INESA Intelligent Electronics CO., Ltd.

The area where the relevant activities take place is limited to (i) the 1st and 2nd floor of the wafer manufacturing part of the Office/Wafer Manufacturing Building, (ii) the 2nd and 3rd floor of the office part of the Office/Wafer Manufacturing building and (iii) the 1st and 2nd floor (only changing room) of the Module Manufacturing building.

2.3 Scope: Logical

This site is used for (i) wafer testing, sawing, and backgrinding (ii) module packaging and testing (including pre-personalisation), (iii) warehousing, and (iv) secure shipment to the client. The site uses its own equipment and IT-infrastructure but works according to the production specification provided by the client. This comprises test programs and assembly instructions.

For smartcard products, these activities are related to Phase 3 (only for IC testing and pre-personalisation) and Phase 4 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 testing and assembly.

2.4 Evaluation Approach

The evaluation is a re-evaluation, based on developer documentation of a major site change (now covering also wafer grinding and pre-personalisation).

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], which references other evaluator documents. To support reuse of the site evaluation activities a derived document [STAR] 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 Site Security Target

The Site Security Target INESA Shanghai, YDZNCC-ZD-001, Version 1.5, 08 June 2021 [SST] is included here by reference.

Please note that for the need of publication a public version [SST-lite] has been created and verified according to [ST-SAN].

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 Site INESA Shanghai, 21-RPT-642, Version 2.0, 13 August 2021
- [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 2.5, 28 March 2019
- [PP] Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Revision 1.0, 13 January 2014
- [SST] Site Security Target INESA Shanghai, YDZNCC-ZD-001, Version 1.5, 08 June 2021
- [SST-lite] Site Security Target Lite INESA Shanghai, YDZNCC-ZD-lite v1.5, 29 July 2021
- [ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
- [STAR] Site Technical Audit Report – INESA Shanghai, 21-RPT-641, Version 2.0, 13 August 2021

(This is the end of this report.)