Site Security Certification Report

Inesa Shanghai

Sponsor and developer:	***Shanghai INESA Intelligent Electronics Co., Ltd.*** **No, 818, Jin Yu Road, Free Trading Zone** **Shanghai, China P.R., 201206**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-SS-210064-CR**
Report version:	**1**
Project number:	**210064**
Author(s):	**NLNCSA/Hans-Gerd Albertsen**
Date:	**03 September 2019**
Number of pages:	**12**
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**SS-19-210064**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Shanghai INESA Intelligent Electronics Co., Ltd.** **No. 818, Jin Yu Road, Free Trading Zone** **Shanghai, China P.R., 201206**
Site and assurance level	**Inesa Shanghai** EAL6 Assurance Components: ▪ ALC_CMC.5, ALC_CMS.5, ALC_DVS.2 (at AVA_VAN.5 level), and ALC_LCD.1
Project number	**210064**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045) and the Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, version 1.0, Revision 1

The site identified in this certificate has been evaluated by an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 and the Supporting Document Guidance CCDB-2007-11-001 Site Certification, October 2007, version 1.0, Revision 1 for conformance to the Common Criteria for IT Security Evaluation version 3.1. This certificate applies only to the specific site as indicated and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the site by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the site by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of 1st issue	: **06-09-2019**
	Certificate expiry	: **06-09-2021**

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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 license 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, in order 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

Currently the Common Criteria Recognition Arrangement (CCRA) and SOGIS-Mutual Recognition Agreement (SOGIS-MRA) do not cover the recognition of Site Certificates. However, the evaluation process 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 re-used by any scheme in a subsequent product evaluation and certification procedure that makes use of the certified site.

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate would indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations. As Site Certificates are not covered, these logos are not present.

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 and sawing, (ii) module packaging and testing, (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 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 initialization) 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 14-08-2019 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* and *[SST-Lite]*, 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 it 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 of the Common Criteria and that the site will be listed on the NSCIB Certificates list. It should be noted that the certification results only apply to the specific site, used in the manner defined in the *[SST]* and *[SST-Lite]*.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator and is not releasable 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 Identification of Site

The Target of Evaluation (TOE) for this evaluation is the Inesa Shanghai located in Shanghai 201206, 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) the1st 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 and sawing, (ii) module packaging and testing, (iii) warehousing, and (iv) secure shipment to the client. The site uses its own equipment and IT-infrastructure but works according the production specification provided by the client. This comprises test programs and assembly instructions.

For smartcard products (Security ICs), these activities are related to Phase 3 (only for IC testing and Initialization) and Phase 4 of the seven Phases of the Lifecycle Model in *[PP]*.

Within this phase, 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 related configuration items.
- ALC_LCD as part of TOE testing and assembly.

2.4 Evaluation approach

The evaluation is a first evaluation, based on developer documentation.

In the evaluation all evaluator actions have been performed including a site visit. For assessment of the ALC_DVS aspects, the Minimum Site Security Requirements *[MSSR]* have been used.

2.5 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[3] which references other evaluator documents. To support re-use of the site evaluation activities according to *[ALCreuse]* a derived document *[STAR]* was provided and approved. This document provides details of the site evaluation that have to 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]*), the Site Security Target Lite (*[SST-Lite]*) and the Site Technical Audit Report *[STAR]* contain necessary information about the usage of the site. During a product evaluation, the evidence for the fulfillment of the Assumptions listed in the *[SST]* and *[SST-Lite]* shall be examined by the evaluator of the product when re-using the results of this site evaluation.

[3] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator and is not releasable for public review.

3 Site Security Target

The Site Security Target INESA Shanghai, YDZNCC-ZD-001 Site Security Target INESA Shanghai v1.4.pdf, Rev.1.4, 02.08.2019 *[SST]* as well as the Site Security Target Lite Inesa Shanghai, YDZNCC-ZD-lite Site Security Target Lite INESA Shanghai v1.4.pdf, Rev. 1.4, 02.08.2019 *[SST-Lite]* are included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms 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

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[ALCreuse]	ISCI-WG1, ALC Site Audit Reuse Exchange Procedure, Version 1.0 draft, September 2017.
[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 Inesa Shanghai, 19-RPT-583 ETR INESA V2.0.pdf, Rev. 2.0, 02.08.2019.
[MSSR]	Joint Interpretation Library, Minimum Site Security Requirements, Version 1.1, July 2013
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.3, 1 April 2017.
[PP]	Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, Rev 1.0, 13 January 2014.
[SST]	Site Security Target INESA Shanghai, YDZNCC-ZD-001 Site Security Target INESA Shanghai v1.4.pdf, Rev.1.4, 02.08.2019.
[SST-Lite]	Site Security Target Lite INESA Shanghai, YDZNCC-ZD-lite Site Security Target Lite INESA Shanghai v1.4.pdf, Rev. 1.4, 02.08.2019.
[STAR]	Site Technical Audit Report Inesa Shanghai, 19-RPT-582 STAR INESA V2.0.pdf, Rev. 2.0, 02.08.2019.

[FPC]	风险与评估处理表/ Threats and risk processing	V0.1
[FJCC]	风险与机遇控制程序/ Threats and risk controlling	C/0 2017-07-10
[TYGC]	体系有效性测量管理规定 / System effectiveness assessment regulation	2013-07-01
[WCK]	文件程序控制 / File management regulation	Version B / 2015-05-17
[GPKC]	管理评审控制程序 / Management review processing	C/7 2017-07-10
[AQZRS]	安全责任书 / Security responsibility	2018-01
[JYKC]	纠正和预防措施控制程序 / Corrective and preventive control processing	Version 新 2013-07-01
[WXKC]	文件化信息控制程序 / Documented information management	C/14 2017-07-10

[BCGGC]	保密品仓库管理工作程序 / Confidential warehouse work procedures	Version C / 2019-03-15
[XZAGG]	信息资产安全管理规定 / Information assets security management regulation	Version C 2019-07-15
[FDCL]	废兰膜、带芯片条带处置流程 / Scarp management	Version E 2013-08-01
[YGSC]	员工手册 / Employee handbook	Version 2016
[AXPK]	安全信息的培训与考核 / Information security training and assessment	Version 新2018-10-18
[MXGZ]	门禁系统管理制度 / Physical access management	Version B 2019-05-10
[FKGG]	访问控制管理规定 / Access control management	Version A 2015-08-04
[LRCAGG]	来访人员出入安全管理规定 / Visitor security management	Version A 2013-08-01
[JZBGG]	技术状态变更管理规范 / Technical specification update management	Version I 2018-02-05
[WXAGG]	网络和系统安全管理规定 / Network and system security management	Version 新 2013-06-26
[XAG]	信息安全规定 / Information security requirement	A/0 2010-04-06
[XASGG]	信息安全事件管理规定 / Information security accident management	Version 新 2013-07-01
[KPI]	2018年度员工岗位职责及KP目标确认书/ 2018 KPI clarification	N/A
[NBSJ]	内部审计管理制度 / Internal audit management	HR-201808
[SCX]	生产线控制计划 / Production line control	Version AH 2018-11-09
[GBAZ]	各部门安全职责 / Security responsibilities of each department	Version 新 2013-08-23
[SASZYY]	生产安全事故综合应急预案 / Production emergency plan	Version A 2017-03-09
[DSFBX]	第三方保密协议 / Third party confidential contract	2018-11-20
[SGD]	施工单 / Construction unit	2016-10-14
[YXAGS]	员工信息安全管理手册 / Employee information	2017-12

	security management handbook	
[BCCSGG]	保密品测试程序及数据管理规定/ Confidential test program and data management regulation	Version 新/ 2018-07-08
[PVGTCP]	人员、车辆、物品进出控制流程 / People、Vehicle& Goods Turnover Control Process	Version T / 2019-04-26
[SGPR]	保安巡视制度 / Security guard patrol regulation	Version 新 / 2019-04-26
[CDOG]	受控文件作业指导书 / Controlled document operational guidance	Version B / 2013-8-1
[SKJ]	生产线控制计划/ Production line control plan	Version B / 2015-05-17
[CI-list]	CI list	2019-05-13
[NDAST]	防撕标签保密协议/ NDA for ordering the seal tape	2019-05-30
[WHBY]	NST1625L维护及保养/ NST1625L Maintenance	2019-07-11
[SML]	服务器系统维护记录 / Server Maintenance Log	2019-07-15

(This is the end of this report).