Reference: 2023-35-INF-4423-v1
Target: Limitada al expediente
Date: 10.12.2024

Created by: I007
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2023-35**
TOE	**LINXENS TIANJIN SITE**
Applicant	**91120116MA06KM9N7T - Linxens Tianjin Co.,Ltd.**
References	

[EXT-8803] Certification Request

[EXT-9279] Evaluation Technical Report

Certification report of the site LINXENS TIANJIN SITE, as requested in [EXT-8803] dated 08/10/2023, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9279] received on 11/10/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site LINXENS TIANJIN SITE.

Developer/manufacturer: Linxens Tianjin Co.,Ltd.

Sponsor: Linxens Tianjin Co.,Ltd..

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R5

To re-use ALC certified security assurance components in evaluations up to EAL6.

Security Assurance Components: AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1, AST_SSS.1, ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_LCD.1 and ALC_FLR.1.

Resistance to Attack Potential: High.

Evaluation end date: 26/07/2024.

Re-use expiration date: 03/01/2027[1].

All the assurance components required by the evaluation have been assigned a “PASS” verdict are resistant to attackers with a High attack potential. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied, as defined by the Common Criteria v3.1 R5, the supporting document guidance CCDB-2007-11-001 Site Certification [SCER] and the JIWG supporting document Minimum site security requirements [MSSR].

The assurance components are chosen in order to re-use ALC certified security assurance components in evaluations up to EAL6. It has been assumed that the security measures are resistant to attacks performed by attackers with a *High* attack potential.

Considering the obtained evidences during the instruction of the certification request of the site LINXENS TIANJIN SITE, a positive resolution is proposed.

[1] This audit was performed as an on-site audit and therefore the re-use of evaluation activities is limited at most to 30 months since the site audit date (03/07/2024) as this site has been previously audited on site by this CB.

SITE SUMMARY

The site name is LINXENS TIANJIN SITE (hereinafter referred to as "LXT"), which is located at:

NO 68, Zhenxiang Road,

Binhai Maritime Hi-tech Area

300459 Tianjin China

This location is a campus, which belongs to Linxens Tianjin Co, Ltd.

This campus consists of several buildings and not all of them are within the physical scope of the site. Physical areas within the evaluation scope are listed below:

- Guardhouse room 1 (1st floor of guardhouse 1 building)
- Guardhouse room 2 (1st floor of guardhouse 2 building)
- Reception/Dispatching area (1st floor of plant building)
- Warehouse (1st floor of plant building)
- Wafer room (1st floor of plant building)
- Finished good room (1st floor of plant building)
- Packing area (1st floor of plant building)
- Module workshop (1st floor of plant building)
- IT server room (2nd floor of plant building)
- DCC room (2nd floor of plant building)
- Card making room (1st floor of plant building)
- Production office (1st floor of plant building)
- Laboratory (1st floor of plant building)

SITE DESCRIPTION

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

- Reception of secured product
- Registration of secured product for identification
- Storage of secured products including sawn wafer, unfinished module, finished module

- Assembly into Modules (Production includes following steps: Die Bonding, Wire Bonding, Encapsulation)
- Functional testing of finished modules (physical electrical testing)
- Quality control testing for incoming raw materials and production process
- Visual inspection of finished modules
- Warehousing and dispatch of finished modules
- Storage of wafer scrap and die chips rejected.
- Product security flaw collection, verification, correction and corrective action delivery

The complete flow of the security IC modules for smart card products at the site is covered by the SST. In addition, the management of the security IC modules for IC embedding processes and the site security are covered by the SST. The production flow of the security IC modules on the site starts with the receiving of parts of the product (raw materials) up to the packaging and shipment of the finished security IC modules or smart cards.

TYPICAL LIFE CYCLE OF SUPPORTED TOEs

It is assumed that product certifications which refer to this certificate are related to a TOE that follows a TOE life-cycle according to [PP84], chap. 1.2.3. The LINXENS TIANJIN SITE covers the Phase 4 (IC Packaging) according to [PP84].

SECURITY ASSURANCE REQUIREMENTS

The site was evaluated with all the evidence required to fulfil the evaluation activities resistant to attackers with a **High** attack potential, according to Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5.

The assurance components are chosen in order to re-use ALC certified security assurance components in evaluations up to EAL6. Therefore, it has been assumed that the security measures are resistant to attackers with a High attack potential.

Assurance Class	Assurance Components
AST: Site Security Target Evaluation	AST_INT.1 SST introduction
	AST_CCL.1 Conformance claims
	AST_SPD.1 Security problem definition
	AST_OBJ.1 Security objectives

	AST_ECD.1 Extended components definition
	AST_REQ.1 Security assurance requirements
	AST_SSS.1 Site summary specification
ALC: Life-cycle support	ALC_CMC.5 Advanced support
	ALC_CMS.5 Development tools CM coverage
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.1 Basic flaw remediation

Please note that:

- The evaluation does not cover ALC_DEL family because the site does not perform external deliveries (to the end-user) and ALC_DEL.1 is therefore not applicable (it has been excluded from the SST). Deliveries from this site are internal and have been evaluated as part of the ALC_DVS.2 family.
- The evaluation does not cover ALC_TAT family because no development activities are carried out in this site.

IDENTIFICATION

Site Name	LINXENS TIANJIN SITE
Site Location	NO 68, Zhenxiang Road, Binhai Maritime Hi-tech Area 300459 Tianjin China
Areas in the scope of the certificate as declared in the	Refer to chapter 2.1 “Identification of the Site” in [SST].

SST	
Activities in the product development	Life cycle phases: • Phase 4 (IC Packaging)
Site Security Target	Site Security Target LINXENS TIANJIN SITE, revision 0.19, 18/07/2024
Evaluation Level	Common Criteria v3.1 R5 To re-use ALC certified security assurance components in evaluations up to EAL6.
Security Assurance Components	ALC_CMC.5,ALC_CMS.5,ALC_DVS.2,ALC_LCD.1,ALC_FLR.1,AST_INT.1,AST_CCL.1,AST_SPD.1,AST_OBJ.1,AST_ECD.1,AST_REQ.1,AST_SSS.1.
Attack Potential	High

SECURITY POLICIES

LINXENS TIANJIN SITE shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Site Security Target [SST], chapter 4.3 “Organizational Security Policies”.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

Each site operating in a production flow must rely on preconditions provided by the previous site. Each site has to rely on the information received by the previous site/client. This is reflected by the assumptions that must be defined for the interface.

The detail of the assumptions considered to be applicable is documented in the Site Security Target [SST], chapter 4.4 “Assumptions”.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the site LINXENS TIANJIN SITE, although the agents implementing attacks have a High attack potential for the Security Assurance Requirements ALC_CMC.5,ALC_CMS.5,ALC_DVS.2,ALC_LCD.1,ALC_FLR.1,AST_INT.1,AST_CCL.1,AST_SPD.1,AST_OBJ.1,AST_ECD.1,AST_REQ.1,AST_SSS.1, and always fulfilling the assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the site security properties and the associated certificate, do not guarantee any resistance.

The detail of these threats is documented in the Site Security Target [SST], chapter 4.2 “Threats”.

DOCUMENTS

The site evaluation has been based on the evidences listed in the chapter 5 “List of evaluation evidence” of the Evaluation Technical Report of LINXENS TIANJIN SITE [EXT-9279].

These evidences describe the global procedures and security measures in the site. For each specific TOE, some accessory documents including specific characteristics of the TOE should be provided in addition to the above evidences.

The above evidences should be made available to ITSEFs in order to re-use the results of this certificate.

EVALUATION RESULTS

The site LINXENS TIANJIN SITE has been evaluated against the Security Target [SST].

All the assurance components required by the evaluation have been assigned a “PASS” verdict are resistant to attackers with a High attack potential. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied, as defined by the Common Criteria v3.1 R5, the supporting document guidance CCDB-2007-11-001 Site Certification [SCER] and the JIWG supporting document Minimum site security requirements [MSSR].

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the site are provided. These have been collected along the evaluation process and are detailed to be considered.

- There is not any recommendation from the evaluation team.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site LINXENS TIANJIN SITE, a positive resolution is proposed.

This Certification Report only applies to the site and its evaluated scope as indicated. The confirmed assurance components are only valid on the condition that all assumptions and preconditions required by the site, as given in this report and in the Site Security Target, are observed.

The owner of the certificate is obliged:

1. when advertising the Site Certificate or the fact of the Site Certification, to refer to the Site Certification Report as well as to provide the Site Certification Report and the Site Security Target and documentation mentioned herein to any client for the application and proper usage of the certified site,
2. to inform this Certification Body immediately about vulnerabilities of the site that have been identified by the sponsor or applicant or any third party after issuance of the certificate,
3. to inform this Certification Body immediately about security relevant changes in the scope of the evaluated site, e.g. changes related to the logical and physical development and production environment, to processes, and to services of the site.

In case of changes to the certified site, the validity can be extended to the changed site, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified site, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

RE-USE OF THE SITE CERTIFICATE

The re-use of this Site Certificate is limited to the extent defined in the Spanish Certification Body (CCN) Technical Interpretation “IT-003 Instrucción técnica: reutilización de resultados mediante la certificación de centros de desarrollo” [IT003], the Supporting Document Guidance Site Certification [SCER] and the SOG-IS Smartcard and similar devices supporting documents, such as the Minimum site security requirements [MSSR].

The results from a site certification can be re-used for product certifications. For each specific TOE, accessory documents including specific TOE characteristics should be evaluated in addition to the above specified documents. These evidences shall rely and shall be consistent with the evidences used in the site certificate evaluation and in the Site Security Target.

Currently the Recognition Agreements in place do not cover the recognition of Site Certificates. However, the evaluation process performed was outlined according to the rules of the agreements

and by using the agreed supporting document on Site Certification [SCER] and [MSSR]. Therefore, the results of this evaluation and certification procedure can be re-used by the issuing scheme in a subsequent product evaluation and certification procedure.

When re-using the results of the activities that uphold this site certificate in a product evaluation, the scheme responsible for certifying the product may decide to fully recognize the results or contact this scheme to query about specific assurance activities carried out in the scope of this site certification.

SITE CERTIFICATE VALIDITY REVIEW

In this case, and according to arrangements in SOG-IS Smart Card and similar devices technical domain, to re-use the evaluation activities that uphold this Site Certificate in a product specific evaluation, a reassessment of the assurance activities validity should be done at most 30 months after the site audit date as this site has been previously certified by means of an on-site audit by this Certification Body. Therefore, a reassessment of the assurance activities validity should be done before 03/01/2027.

SHARED TECHNICAL AUDIT REPORT (STAR)

The evaluation activities carried out in this site certification dossier have been summarized in a Shared Technical Audit Report (STAR). This STAR has been validated by this Certification Body according to [START]. The reference of the STAR is:

- **Report name**: SITE TECHNICAL AUDIT REPORT (STAR). LINXENS TIANJIN SITE.
- **Report ID**: CCELXT001R2-STAR-M1.
- **Version**: M1.
- **Issue Date**: 11/10/2024.
- **Issuing ITSEF**: Applus Laboratories.
- **Site audit dates**: 2nd and 3rd July 2024.

The STAR report constitutes an evaluation evidence, therefore according to article 25 of Presidential Order PRE/2740/2007 which regulates the CCN Certification Body, written authorization must be requested by Applus Laboratories to the Certification Body to share any information of this certification dossier (including the STAR report) with third parties.

It is expected that if the applicant Linxens Tianjin Co.,Ltd. is willing to share the STAR report with any third party, they may contact Applus Laboratories to perform an authorization request to the CCN Certification Body to distribute this report.

SITE SECURITY TARGET

Along with this certification report, the complete site security target (SST) of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- Site Security Target LINXENS TIANJIN SITE, version 0.19, 18/07/2024.

The public version of this document constitutes the SST Lite. The SST Lite has also been reviewed for the needs of publication according to sanitation [SANT], and it is published along with this certification report in the Certification Body. The SST Lite identifier is:

- Site Security Target Lite LINXENS TIANJIN SITE, version 0.8, 18/07/2024.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
JIWG	Joint Interpretation Working Group of SOG-IS
OC	Organismo de Certificación
SOG-IS	Senior Officials Group Information Systems Security
SST	Site Security Target
TOE	Target of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[IT-003] Instrucción técnica: reutilización de resultados mediante la certificación de centros de desarrollo. Versión 3. Date 07-11-2019.

[MSSR] Joint Interpretation Library. Minimum Site Security Requirements. Version 3.1. Date December 2023.

[PP84] EUROSMART's Protection Profile "Security IC Platform Protection Profile with Augmentation packages". Version 1.0, 2014.

[SANT] Common Criteria Recognition Arrangement. ST sanitising for publication. Document number CCDB-2006-04-004. Date April, 2006.

[SCER] Common Criteria. Supporting Document Guidance. Site Certification. Document number CCDB-2007-11-001. Version 1.0, Revision 1, Date October, 2007.

[SST] Site Security Target LINXENS TIANJIN SITE, version 0.19, 18/07/2024.

[START] Joint Interpretation Library. Site Technical Audit Report Template. Version 1.0. February 2018.