Reference: 2025-19-INF-4714-v1
Target: Limitada al expediente
Date: 05.02.2026

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

# CERTIFICATION REPORT

| | |
|---|---|
| Dossier # | **2025-19** |
| TOE | **LINXENS SINGAPORE CHANGI SITE** |
| Applicant | **UN200312306H - LINXENS SINGAPORE PTE LTD** |
| References | |

[EXT-9473] Certification Request

[EXT-9894] Evaluation Technical Report

Certification report of the site LINXENS SINGAPORE CHANGI SITE, as requested in [EXT-9473] dated 21/02/2025, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9894] received on 24/10/2025.

**CONTENTS**

# EXECUTIVE SUMMARY

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

The following services and/or processes provided by Linxens Singapore Pte. Ltd. (LXS) are considered under the scope of this evaluation.

- Secure reception, identification, registration and storage of Smart Card wafers
- Assembly into Modules (Production includes the following steps: Die Bonding, Wire Bonding, Encapsulation, Inspection and Electrical Testing which does the functional testing of module to ensure is passed in Electrical testing)
- Secure delivery (internal shipment) of Smart Card wafers/modules.
- Cryptographic Key management (The key management is only performed in order to open a secure channel with the IC to load the initialization data.)
- Secure reception, storage, loading of the initialization data (COS and Applet) for Smart Card Products

Secured storage of scraps and secured handling of offsite destruction.

**Developer/manufacturer**: LINXENS SINGAPORE PTE LTD.

**Sponsor**: LINXENS SINGAPORE PTE 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:** ALC_CMC.5,ALC_CMS.5,ALC_DVS.2,ALC_LCD.1,AST_INT.1,AST_CCL.1,AST_SPD.1,AST_OBJ.1,AST_ECD.1,AST_REQ.1,AST_SSS.1.

**Resistance to Attack Potential**: High.

**Evaluation end date**: 23/10/2025.

**Re-use expiration date:** 04/12/2027[1].

[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 (04/06/2025) as this site has been previously audited on site by this CB.

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 SINGAPORE CHANGI SITE, a positive resolution is proposed.

## *SITE SUMMARY*

The LINXENS SINGAPORE CHANGI SITE is located at

BLK 22, CHANGI NORTHWAY,

SINGAPORE

498810

SINGAPORE

The Linxens Changi Singapore site (LXS) is located on a fenced and guarded campus that is owned by Linxens Singapore Pte. Ltd. and is not shared with other companies, which contains several buildings. CCTV controls the perimeter of the building in the scope of the evaluation and the access control to the building is by means of an employee badge (one-factor authentication). Tailgating is prevented by means of a turnstile on the building entrance. Several detections and stop mechanisms are implemented, such as physical access control mechanisms, CCTV (on the perimeter, entrance and corridors within the building) and alarms to guarantee the security of the LXS premises.

Relevant secure areas in the scope of the evaluation (concerning the production activities or guaranteeing the security of such activities), which are located on several mentioned buildings, are the following:

- Blk 24 building:
    - Workshop: Production, electrical testing, OS and Applet loading Area (level 1)

  - Wafer Storage Room (level 2)
  - Secure HSM Room (cryptographic key management area) (level 1)
  - Security IT Rooms (level 2).
  - Security systems (Access control + CCTV) room (level 2).
  - Packing room
  - R&D Cal lab
- Blk 22 building:
  - Security IT room for Firewall server (level 2)
- Security Guard house (located on the campus entrance)

Additional security mechanisms are implemented for the secure areas such as two-factor access control (by means of an employee badge and PIN) or two employee badges and PIN to enforce four-eyes principle, dedicated CCTV monitoring the activities conducted inside the secure areas and intrusion alarms. Only authorized employees can access the secure areas on a need-to-know principal basis.

### *SITE DESCRIPTION*

The following services and/or processes provided by Linxens Singapore Pte. Ltd. (LXS) are considered under the scope of this evaluation.

- Secure reception, identification, registration and storage of Smart Card wafers
- Assembly into Modules (Production includes the following steps: Die Bonding, Wire Bonding, Encapsulation, Inspection and Electrical Testing which does the functional testing of module to ensure is passed in Electrical testing)
- Secure delivery (internal shipment) of Smart Card wafers/modules.
- Cryptographic Key management (The key management is only performed in order to open a secure channel with the IC to load the initialization data.)
- Secure reception, storage, loading of the initialization data (COS and Applet) for Smart Card Products
- Secured storage of scraps and secured handling of offsite destruction.

All these services are performed in LXS site considering the proper level of physical and logical security measures to guarantee the confidentiality and integrity of the data generated and the manufactured physical assets.

To perform these activities, the site uses the Linxens Mantes provided and managed the IT-infrastructure. Locally available IT equipment like workstations or VPN routers may be also provided and managed by Linxens Mantes.

It is assumed that product certifications, which will refer to the [SST], will be related to a target of evaluation that follows a TOE life-cycle. The LXS site covers:

- Phase 4: Security IC packaging, testing and pre-personalization.
- Phase 5: Composite Product Integration.

### *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 SINGAPORE CHANGI SITE covers the Phase 4 (IC Packaging) and Phase 5 (Composite Product Integration) 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 attacks performed by 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 |

Please note that ALC_DEL.1 has been excluded from the SST since this site does not perform external deliveries and ALC_DEL.1 is therefore not applicable.

The site does not provide services that are covered by ALC_TAT as no development activities are carried out in this site.

## IDENTIFICATION

| | |
|---|---|
| **Site Name** | LINXENS SINGAPORE CHANGI SITE |
| **Site Location** | BLK 22, CHANGI NORTHWAY,<br>SINGAPORE<br>498810<br>SINGAPORE |
| **Areas in the scope of the certificate as declared in the SST** | Refer to section 2.2 of [SST] |
| **Activities in the product development** | Life cycle phases:<br>• Phase 4 (IC Packaging)<br>• Phase 5 (Composite Product Integration) |
| **Site Security Target** | *Site Security Target 9308, Version 0.24, 17/10/2025* |
| **Evaluati** | Common Criteria v3.1 R5. |

| | |
|---|---|
| **on Level** | 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,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 SINGAPORE CHANGI 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], section 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], section 4.4 (Assumptions).

### *CLARIFICATIONS ON NON-COVERED THREATS*

The following threats do not suppose a risk for the site LINXENS SINGAPORE CHANGI 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,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], section 4.2 (Threats).

## DOCUMENTS

The site evaluation has been based on the evidences listed in the chapter 5 (Evaluation evidence) of the Evaluation Technical Report of LINXENS SINGAPORE CHANGI SITE [EXT-9894].

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 SINGAPORE CHANGI 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.

- The evaluation team did not consider it necessary to provide any additional recommendations.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site LINXENS SINGAPORE CHANGI 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 04/12/2027.

## 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 SINGAPORE CHANGI SITE.
- **Report ID**: CCELXS001R3-STAR-M0.
- **Version**: M0.
- **Issue Date**: 23/10/2025.
- **SHA256**: D269F232E6F8B24DEBEF1EACDF2B06D53ACB6CB28743670F19BDFB1D894FDBC3
- **Issuing ITSEF**: Applus Laboratories.
- **Site audit dates**: 03/06/2025 - 04/06/2025.

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 SINGAPORE PTE 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 9308, Version 0.24, 17/10/2025*.

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 9308, Version 0.7, 24/10/2025*.

## 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, 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 9308, Version 0.24, 17/10/2025.

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