Reference: 2024-22-INF-4488-v1
Target: Limitada al expediente
Date: 08.04.2025

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

CERTIFICATION REPORT

Dossier #	**2024-22**
TOE	**Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN)**
Applicant	**91360100MAC6MB1K4A - Giesecke+Devrient (Jiangxi) Technology Co., Ltd.**
References	

[EXT-9047] Certification Request

[EXT-9308] Evaluation Technical Report

Certification report of the site Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN), as requested in [EXT-9047] dated 06/05/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9308] received on 31/10/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN).

Developer/manufacturer: Giesecke+Devrient (Jiangxi) Technology Co., Ltd.

Sponsor: Giesecke+Devrient (Jiangxi) Technology 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_DEL.1, ALC_DVS.2 and ALC_LCD.1.

Resistance to Attack Potential: High.

Evaluation end date: 22/10/2024.

Re-use expiration date: 07/02/2027[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 Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN), 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 (07/08/2024) as this site has been previously audited on site by this CB.

SITE SUMMARY

The Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN) is located at

399 Huoju Avenue, High-New Tech Development Zone,

Nanchang City, Jiangxi Province, 330096 P.R.China.

The production area of GDCNMS NAN is located in a fenced and guarded site that is leased by Giesecke+Devrient (Jiangxi) Technology Co., Ltd. under a lease agreement and is not shared with other companies. There is a three floors office building and a one floor production building. There are cameras monitoring the whole fences with electronic walls on the physical fences.

The areas belonging to the assets include loading bay, vault, main embedded devices production room, both clean rooms, embedded devices workshop (packaging station included), security control centre, product storage area and server room are located in the production building.

Data gen room is in the second floor of office building. Mantraps control access to data gen room and production areas. Cameras and alarm control system monitor the activities in the production building and Data gen room.

Giesecke+Devrient (Jiangxi) Technology Co., Ltd. provides services for initialisation and pre-personalisation of dies as well as initialisation, pre-personalisation and personalization of embedded devices and is abbreviated by 'GDCNMS NAN'.

When not in initialisation or pre-personalisation, dies on wafer are securely stored in the vault. Same happens for embedded devices, including personalisation. The vault is in the warehouse inside of the high security area at the first floor of the building.

The server infrastructure is located in a dedicated server room. Physical Security Management, IT and the local IT administrators are located at GDCNMS NAN.

The supporting IT services are provided by GDM (Giesecke+Devrient München) located at a secure area with restricted access which has been audited.

SITE DESCRIPTION

The following services and/or processes provided by Giesecke+Devrient (Jiangxi) Technology Co., Ltd. are in the scope of the site evaluation process:

- Secure reception, storage and transportation of dies on wafer (the term 'wafer' is used throughout the rest of this document describing either single dies or dies on wafer) and embedded devices' modules and devices. Delivery includes transportation for secure destruction.
- Secure reception and storage of initialisation, pre-personalisation data for wafer and initialisation, pre-personalisation and personalisation data for embedded devices production.

- Secure reception and storage of cryptographic keys, derivation of wafer specific pre-personalisation keys and embedded devices pre-personalisation and personalisation keys.
- Wafer initialisation and pre-personalisation.
- Embedded devices production comprising initialisation, pre-personalisation and personalisation.
- Secure destruction of defective/broken embedded devices.

The site evaluation covers only the handling and production of wafer and embedded devices with Sm@rtSIM CX and Sm@rtSIM NextGen.

The term 'handling' in this regard comprises secure reception, storage and shipment of wafers and embedded devices as well as secure reception and storage of data for wafer initialisation and pre-personalisation or for embedded devices initialisation, pre-personalisation and personalisation.

The reception of wafer and embedded modules comprises a verification of the correctness of the shipped items with respect to the transportation documents and - if applicable - the verification of integrity of seals used for secure transportation of items.

The storage of wafer and embedded devices is done in a specially secured vault at GDCNMS NAN with restricted access. The number of items is tracked from reception of the items until the shipment of the items.

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 Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN) covers the phase 3 'IC Manufacturer', phase 4 'IC Packaging', phase 5 'Smartcard Product Manufacturer' and phase 6 'Personalize' 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_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model

Please note that the evaluation does not cover ALC_TAT family because no development activities are carried out in this site.

IDENTIFICATION

Site Name	Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN)
Site Location	399 Huoju Avenue, High-New Tech Development Zone, Nanchang City, Jiangxi Province, 330096 P.R.China.
Areas in the scope of the certificate as declared in the SST	Refer to chapter 2.1 in [SST]
Activities in the product development	Life cycle phases: • Phase 3 'IC Manufacturer' • Phase 4 'IC Packaging' • Phase 5 'Smartcard Product Manufacturer' • Phase 6 'Personalize'
Site Security Target	Site Security Target for Giesecke+Devrient (Jiangxi) Technology Co.,

	Ltd., version 3.4, 25/09/2024
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_DEL.1, ALC_DVS.2 and ALC_LCD.1.
Attack Potential	High

SECURITY POLICIES

Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN) 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 (Organisational 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 Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN), although the agents implementing attacks have a High attack potential for the Security Assurance Requirements 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_DEL.1, ALC_DVS.2 and ALC_LCD.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 (Evaluation evidence) of the Evaluation Technical Report of Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN) [EXT-9308].

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 Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN) 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 destruction of scrap is limited to TOEs bigger than 4mm each edge.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN), a positive resolution is proposed.

This Certification Report only applies to the site and its evaluated scope as indicated. The confirmed assurance components is 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.

Additionally, this Certification Body wants to remark the following:

- This site consumes services that are managed from Giesecke+Devrient Development Center Germany and therefore the current certificate validity is conditioned by the certificate BSI-DSZ-CC-S-0261, valid by the time of the issuing of this certificate. A revocation of the certificate of Giesecke+Devrient Development Center Germany may imply the revocation of the current certificate. As far as a new certificate covers Giesecke+Devrient Development Center Germany services provided to Giesecke+Devrient (Jiangxi) Technology Co., Ltd. (GDCNMS NAN), the current certificate will be valid.

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 07/02/2027.

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). Giesecke+Devrient (Jiangxi) Technology Co., Ltd.
- **Report ID**: CCEGAD009R2-STAR-M0.
- **Version**: M0.
- **Issue Date**: 22/10/2024.
- **SHA256:** 1b6819f482ec431604f988f62166daf563b26fcdd66a4ea10a88b155e578857d
- **Issuing ITSEF**: Applus Laboratories.
- **Site audit dates**: 06/08/2024 – 07/08/2024.

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 Giesecke+Devrient (Jiangxi) Technology 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 for Giesecke+Devrient (Jiangxi) Technology Co., Ltd., version 3.4, 25/09/2024.

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 for Giesecke+Devrient (Jiangxi) Technology Co., Ltd., version 3.4, 25/09/2024.

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 for Giesecke+Devrient (Jiangxi) Technology Co., Ltd., Version 3.4, 25/09/2024.

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