Reference: 2021-49-INF-3843-v1
Target: Limitada al expediente
Date: 13.06.2022

Created by: I006
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2021-49**
TOE	**Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch**
Applicant	**914202003098530 79Y - Giesecke+Devrient (China) Technologies Co.Ltd. Huangshi Branch**
References	
	[EXT-7410] Certification Request
	[EXT-7766] Evaluation Technical Report

Certification report of the site Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch, as requested in [EXT-7410] dated 26/10/2021, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7766] received on 17/05/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch.

The site is used for Smart Card Production (including inlay manufacturing).

Developer/manufacturer: Giesecke+Devrient (China) Technologies Co.Ltd. Huangshi Branch

Sponsor: Giesecke+Devrient (China) Technologies Co.Ltd. Huangshi Branch.

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R5

To re-use certified ALC components in evaluations up to EAL5 + ALC_DVS.2 + AVA_VAN.5

Security Assurance Components: ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, AST_CCL.1, AST_ECD.1, AST_INT.1, AST_OBJ.1, AST_REQ.1, AST_SPD.1 and AST_SSS.1.

Resistance to Attack Potential: High.

Evaluation end date: 25/05/2022.

Re-use expiration date: 15/08/2023[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 certified ALC components in evaluations up to EAL5 + ALC_DVS.2 + AVA_VAN.5. It has been assumed that the security measures are resistant to attacks performed by attackers with a *High* attack potential.

[1] This audit was performed as a virtual site audit according to [IT-013] and [JIL-COVID] policies, and therefore the re-use of evaluation activities is limited at most to 18 months since the site audit date (14-15/02/2022) as this site has been previously certified by means of a virtual site audit only.

Considering the obtained evidences during the instruction of the certification request of the site Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch, a positive resolution is proposed.

SITE SUMMARY

The Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch is located at:

151 Hangzhou West Road,

Huangshi City Hubei Province, 435000

PRC (People´s Republic of China)

The production area of GDCHINA HS is located on a fenced and guarded area that is owned by Giesecke+Devrient (China) Technologies Co.,Ltd. Huangshi Branch and is not shared with other companies.

SITE DESCRIPTION

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

- Secure reception, storage and delivery of Smart Card modules and Smart Cards (these different types of Smart Card related products are referred to as 'Smart Cards' throughout the rest of this document). Delivery includes delivery for secure destruction.
- Secure reception and storage of initialisation data for Smart Card Production
- Secure reception and storage of cryptographic keys, derivation of card specific personalisation keys.
- Smart Card Production comprising flash loading, completion (i.e. finishing the Smart Card OS), and initialisation of contact (incl. dual interface) cards and contactless cards or modules
- Secure inlay manufacturing
- Secure destruction of Smart Card modules and Smart Cards

The site evaluation covers only the handling and production (i.e. the services/processes listed above) of STARCOS products (i.e. passports, ID cards, signature cards, German Health cards eGK, etc. based on G+D's STARCOS operating system) and Smart Cafe Expert products (i.e. passports, ID cards, signature cards, etc. based on G+D's Smart Café Expert operating system).

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 (China) Technologies Co. Ltd., Huangshi Branch covers the covers Phase 4 (IC Packaging) by providing inlay

manufacturing and Phase 5 (Composite Product Integration) by providing the services of inlay assembly, configuration, completion and initialisation 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 the results in evaluations up to EAL5 + ALC_DVS.2 + AVA_VAN.5. 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.4 Production support, acceptance procedures and automation
	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

IDENTIFICATION

Site Name	Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch
Site Location	151 Hangzhou West Road, Huangshi City Hubei Province, 435000

	PRC (People´s Republic of China)
Areas in the scope of the certificate as declared in the SST	The production area of GDCHINA HS is located on a fenced and guarded area that is owned by Giesecke+Devrient (China) Technologies Co.,Ltd. Huangshi Branch and is not shared with other companies.
Activities in the product development	Life cycle phases: • Phase 4 (IC Packaging) by providing inlay manufacturing and • Phase 5 (Composite Product Integration) by providing the services of inlay assembly, configuration, completion and initialisation
Site Security Target	Site Security Target for Giesecke+Devrient Mobile Security China Huangshi Branch Version 1.6/09.05.2022
Evaluation Level	Common Criteria v3.1 R5 To re-use certified ALC components in evaluations up to EAL5 + ALC_DVS.2 + AVA_VAN.5
Security Assurance Components	ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, AST_CCL.1, AST_ECD.1, AST_INT.1, AST_OBJ.1, AST_REQ.1, AST_SPD.1 and AST_SSS.1.
Attack Potential	High

SECURITY POLICIES

Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch 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 threats documented in the Site Security Target [SST], chapter 4.2 (Threats) do not suppose a risk for the site Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch, although the agents implementing attacks have a High attack potential for the Security Assurance Requirements ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, AST_CCL.1, AST_ECD.1, AST_INT.1, AST_OBJ.1, AST_REQ.1, AST_SPD.1 and 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.

DOCUMENTS

The site evaluation has been based on the evidences listed in the chapter 4 (Evaluation evidence) of the Evaluation Technical Report of Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch [EXT-7766].

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 (China) Technologies Co. Ltd., Huangshi Branch 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

The laboratory has not additional comments on the evaluation.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site Giesecke+Devrient (China) Technologies Co. Ltd., Huangshi Branch, 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.

Additionally, this Certification Body wants to remark the following:

1. This site consumes services that are managed from Giesecke+Devrient München and therefore the current certificate validity is conditioned by the certificate BSI-DSZ-CC-S-0185-2021 valid by the time of the audit. A revocation of the certificate of Giesecke+Devrient München may imply the revocation of this certificate. As far as a new certificate covers Giesecke+Devrient München services provided to Giesecke+Devrient Development Center China, the current certificate will be valid.
2. Reuse of evaluation of activities for multisite development projects are bound to those certified sites which are listed in section 2.2.2 of the [SST]. In case of revocation of some of the certificates in this list, reuse of evaluation activities cannot be applied.
3. This site certificate support integration by reusing ALC certified components into product evaluations up to the evaluation assurance level EAL5 augmented with ALC_DVS.2 and AVA_VAN.5.

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 18 months after the site audit date as virtual site audit procedure of [IT-013] and [JIL-COVID] policies has been applied and 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 15/08/2023.

According to [JIL-COVID], despite from the 18 months mentioned, a "virtual audit" should be replaced by a regular on-site audit as soon as the restrictions of the pandemic situation and scheduling of the parties involved allows for.

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 [ASAREP]. The reference of the STAR is:

- **Report name**: SITE TECHNICAL AUDIT REPORT (STAR). Giesecke+Devrient (China) Technologies Co.,Ltd. Huangshi Branch.
- **Report ID**: CCEGAD008R1-STAR-M1.
- **Version**: M1.
- **Issue Date**: 11/05/2022.
- **Issuing ITSEF**: Applus Laboratories.
- **Site audit dates**: 14/02/2022 & 15/02/2022

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 (China) Technologies Co.Ltd. Huangshi Branch 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 Mobile Security China Huangshi Branch Version 1.6/09.05.2022.

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 Mobile Security China Huangshi Branch Version 1.6/09.05.2022.

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:

[ASAREP] ISCI WG1 - ALC Site Audit Reuse Exchange Procedure, draft version 1.1. March 2018.

[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.

[IT-013] Instrucción técnica temporal para la realización de actividades de evaluación con motivo del coronavirus COVID-19, versión 6.

[JIL-COVID] JIL Temporary Covid19 pandemic operational SOGIS evaluation and certification policy and rules, Version 1.4, February 2022.

[MSSR] Joint Interpretation Library. Minimum site security requirements. Version 3.0 Date February 2020.

[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 Mobile Security China Huangshi Branch Version 1.6/09.05.2022