Reference: 2024-20-INF-4526-v1
Target: Limitada al expediente
Date: 15.07.2025

Created by: CERT13
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-20**
TOE	**Giesecke and Devrient Development Center India (DCI)**
Applicant	**27AAGCG3270K1ZF - Giesecke+Devrient MS India Pvt Ltd**
References	

[EXT-9045] Certification Request

[EXT-9424] Evaluation Technical Report

Certification report of the site Giesecke and Devrient Development Center India (DCI), as requested in EXT-9045 dated 07/04/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report EXT-9424 dated 21/11/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site Giesecke and Devrient Development Center India (DCI) .

Developer/manufacturer: Giesecke+Devrient MS India Pvt Ltd

Sponsor: Giesecke+Devrient MS India Pvt 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 EAL5 + ALC_DVS.2 + AVA_VAN.5

Security Assurance Components: ALC_CMC.4 ,ALC_CMS.5, 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: 16/07/2025

Re-use expiration date: 28/02/2027[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 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.

Considering the obtained evidences during the instruction of the certification request of the site Giesecke and Devrient Development Center India (DCI), a positive resolution is proposed.

[1] This audit was performed as an on site audit according to [IT-013], and therefore the re-use of evaluation activities is limited at most to 30 months since the site audit date 28/02/2027.

SITE SUMMARY

The Giesecke and Devrient Development Center India (DCI) is located at

Erandwane, Padale Prime, Plot No 9/1A

411004 Pune

India

The site DCI covers only one building. The site is used for development of Smart Card software and testing. Development and testing activities are restricted to the designated development area. The server infrastructure including the CM system is located in a dedicated server room. Administrative services, physical security management and central IT-services are also located in this building. For multisite development, services provided by the administration may also be fully or partly be provided to other development sites. The services provided by this site to other sites of Giesecke+Devrient are listed in the document 'Services provided to other G+D sites by Giesecke+Devrient Development Center India'.

The Smart Card Software Development area (also denoted as ‘secure development area’ in this document) is a security area with restricted access. Only authorised persons are allowed to enter this area. The building is secured by mantraps which can only be entered after successful authentication by card (company badge, visitor badge). The security area consists of single floors which are secured by doors which can only be opened after successful authentication by card (company badge, visitor badge). The secure development area covers the following areas:

- 1st floor,
- 2nd floor,
- 3rd floor

Access rights on access cards are granted and revoked by the person responsible for physical site security.

For the development of the Smart Card Software a configuration management system is used. Access to the software development storage servers is restricted to authorised persons. Successful authentication by login name and password or access card and password is required for access to the software development storage servers.

SITE DESCRIPTION

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

> Smart Card Software Development (Smart Card OS Development, Smart Card Applet and Application Development, Testing, Release of developed components).

The site evaluation covers the development of products based on the following operating systems:

- Sm@rtSIM
- Sm@rtSIM CX
- Sm@rtSIM NextGen
- Convego JOIN
- Sm@rtCafé® Expert
- JCOP

Supporting services at DCI:

- Management of physical security and IT-Security
- IT-Services (storage, backup, etc.)
- Administrative Services (e.g. Human Resources related services)

Supporting services are provided by G+D Headquarters and covered with the valid certificate [BSI-DSZ-CC-S-0260-2023] by the time of the audit. As far as the certificate is valid, services can be used by DCI.

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 and Devrient Development Center India (DCI) covers the Phase 1 (IC Embedded Software Development) 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 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_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model

IDENTIFICATION

Site Name	Giesecke and Devrient Development Center India (DCI)
Site Location	Erandwane, Padale Prime, Plot No 9/1A 411004 Pune India
Areas in the scope of the certificate as declared in the SST	Refer to section 2.1 Identification of the Site in [SST]
Activities in the product development	Life cycle phases: • Phase 1
Site Security Target	Site Security Target Giesecke + Devrient Development Center India (DCI) Version/Date: Version 3.6/08.11.2024
Evaluation Level	Common Criteria v3.1 R5

	To re-use ALC certified security assurance components in evaluations up to EAL5 + ALC_DVS.2 + AVA_VAN.5
Security Assurance Components	ALC_CMC.4 ,ALC_CMS.5, 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 and Devrient Development Center India (DCI) 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 Giesecke and Devrient Development Center India (DCI), although the agents implementing attacks have a High attack potential for the Security Assurance Requirements ALC_CMC.4 ,ALC_CMS.5, 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.

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 Giesecke and Devrient Development Center India (DCI) [EXT-9424].

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 and Devrient Development Center India (DCI) 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 verdict of this certificate depends on the certificate of G+D Headquarters and covered with the valid certificate [BSI-DSZ-CC-S-0260-2023] by the time of the audit. As far as the certificate is valid, services can be used by DCI. A revocation or expiration of [BSI-DSZ-CC-S-0260-2023] would imply the revocation of the certificate of DCI site.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site Giesecke and Devrient Development Center India (DCI), 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 G+D Headquarters and therefore, the current certificate validity is conditioned by the certificate BSI-DSZ-CC-S-0260-2023 valid by the time of the audit. A revocation of the certificate of G+D Headquarters may imply the revocation of this certificate. As far as a new certificate covers G+D Headquarters services provided to Giesecke+Devrient Development Center India (DCI), 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 there has been an on-site audit. Therefore, a reassessment of the assurance activities validity should be done before 28/02/2027.

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 Development Center India (DCI)
- **Report ID**: CCEGAD002R5-STAR-M1.
- **Version**: M1.
- **Issue Date**: 11/11/2024
- **Issuing ITSEF**: Applus Laboratories
- **Site audit dates**: 27-28/08/2024.

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 MS India Pvt 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 Giesecke + Devrient Development Center India (DCI), version 3.6.

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 Giesecke + Devrient Development Center India (DCI), version 3.6.

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

[MSSR] Joint Interpretation Library. Minimum site security requirements. Version 3.1

[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 Giesecke + Devrient Development Center India (DCI), version 3.6.

[SST_Lite] Site Security Target Lite Giesecke + Devrient Development Center India (DCI), version 3.6.

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