

Reference: 2024-24-INF-4575-v1  
Target: Limitada al expediente  
Date: 29.07.2025

Created by: CERT15  
Revised by: CALIDAD  
Approved by: TECNICO

## CERTIFICATION REPORT

---

|            |                                                                      |
|------------|----------------------------------------------------------------------|
| Dossier #  | <b>2024-24</b>                                                       |
| TOE        | <b>Giesecke+Devrient Development Center Spain (DCS)</b>              |
| Applicant  | <b>B10742195 - Giesecke+Devrient Mobile Security TCD Iberia S.L.</b> |
| References |                                                                      |
|            | [EXT-9121] 2024-05-10_2024-24_solicitud_certificacion                |
|            | [EXT-9579] 2025-04-10_2024-24_ETR_vM1                                |

---

Certification report of the site Giesecke+Devrient Development Center Spain (DCS) , as requested in [EXT-9121] dated 10/05/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9579] received on 10/04/2025.

## CONTENTS

|                                                           |    |
|-----------------------------------------------------------|----|
| EXECUTIVE SUMMARY .....                                   | 3  |
| SITE SUMMARY.....                                         | 4  |
| SITE DESCRIPTION .....                                    | 5  |
| TYPICAL LIFE CYCLE OF SUPPORTED TOEs.....                 | 5  |
| SECURITY ASSURANCE REQUIREMENTS .....                     | 6  |
| IDENTIFICATION .....                                      | 6  |
| SECURITY POLICIES.....                                    | 7  |
| ASSUMPTIONS AND OPERATIONAL ENVIRONMENT .....             | 7  |
| CLARIFICATIONS ON NON-COVERED THREATS .....               | 7  |
| DOCUMENTS .....                                           | 8  |
| EVALUATION RESULTS .....                                  | 8  |
| COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM ..... | 8  |
| CERTIFIER RECOMMENDATIONS .....                           | 9  |
| RE-USE OF THE SITE CERTIFICATE .....                      | 9  |
| SITE CERTIFICATE VALIDITY REVIEW .....                    | 10 |
| SHARED TECHNICAL AUDIT REPORT (STAR) .....                | 10 |
| SITE SECURITY TARGET.....                                 | 11 |
| GLOSSARY.....                                             | 11 |
| BIBLIOGRAPHY .....                                        | 11 |

## EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site Giesecke+Devrient Development Center Spain (DCS) .

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

Embedded Software Development (Embedded OS Development, Embedded 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 CX
- Sm@rtSIM Next Generation
- SmartCafe Expert
- Convego JOIN
- STARCOS

In addition, product lines which require EMVCo related type approvals are developed in the same environment following the same procedures as the products named above.

Supporting services at DCS from other sites:

- IT-Services (storage, backup, etc.)

Supporting Services are provided from the building BCN4. The supporting services comprise documentation generation for other G+D sites.

**Developer/manufacturer:** Giesecke+Devrient Mobile Security TCD Iberia S.L.

**Sponsor:** Giesecke+Devrient Mobile Security TCD Iberia S.L..

**Certification Body:** Centro Criptológico Nacional (CCN).

**ITSEF:** Applus Laboratories

**Protection Profile:** No.

**Evaluation Level:** Common Criteria v3.1

To re-use ALC certified security assurance components in evaluations up to EAL5

**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.4, ALC\_CMS.5, ALC\_DVS.2 and ALC\_LCD.1

**Resistance to Attack Potential:** High.

**Evaluation end date:** 08/05/2025

**Re-use expiration date:** 09/06/2027<sup>1</sup>.

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. 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 Development Center Spain (DCS) , a positive resolution is proposed.

## ***SITE SUMMARY***

The Giesecke+Devrient Development Center Spain (DCS) is located at

Avinguda Baix Llobregat, 3-5, 5<sup>th</sup> floor

Sant Joan Despí, 08970

Barcelona, Spain

which will be abbreviated by 'DCS' (Development Center Spain) throughout the rest of the document.

In addition, the security centre housing the primary systems for CCTV monitoring, alarm control and access control as well as its related tools server are located in:

Giesecke+Devrient ePayments Iberia S.A.

Carrer del Número 114, nº 27 , Polígon Pratenc

El Prat de Llobregat, 08820

Barcelona, Spain

which will be abbreviated by 'GDIEP' (G+D Iberia ePayments) throughout the rest of the document.

The site covers one site where CC relevant development is performed: BCN4. DCS is located in 3 rented floors within building BCN4. Building BCN4 is shared with other companies, but the 5th, 6th and 7th floors are used by G+D exclusively. The site is used for development of embedded software and testing (including Smart Cards). Development and testing activities are restricted to the designated development area (5th floor). The server infrastructure is located in a dedicated server room within the 5<sup>th</sup> floor, while the back-up system is located in the robots room within a dedicated rack.

On the other hand, the security centre housing the primary systems for CCTV monitoring, alarm control and access control and the production servers used for internal deliveries are located in the security control room of GDIEP.

For multisite development, the services provided by GDM may also be fully or partly the same as for this site. The services provided by this site to other sites of G+D are listed in the document 'Services provided to other G+D sites by Giesecke+Devrient Development Center Spain'. The services provided by other sites of G+D used by the site defined in chap. 2.1 are listed in the document 'Services provided by other G+D sites used by Giesecke+Devrient Development Center Spain'. No services are provided to clients or 3rd parties within the scope of evaluation.

## **SITE DESCRIPTION**

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

Embedded Software Development (Embedded OS Development, Embedded 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 CX
- Sm@rtSIM Next Generation
- SmartCafe Expert
- Convego JOIN
- STARCOS

In addition, the security centre housing the primary systems for CCTV monitoring, alarm control and access control as well as its related tools server are located in:

Supporting services at DCS from other sites:

- IT-Services (storage, backup, etc.) “

Supporting Services are provided from the building BCN4. The supporting services comprise documentation generation for other G+D sites.

## 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 Development Center Spain (DCS) 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. 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                                               |
|---------------------------------------------|--------------------------------------------------------------------|
| <b>AST: Site Security Target Evaluation</b> | 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                               |
| <b>ALC: Life-cycle support</b>              | 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                       |

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.

## IDENTIFICATION

|                                                                     |                                                                                                                            |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Site Name</b>                                                    | Giesecke+Devrient Development Center Spain (DCS)                                                                           |
| <b>Site Location</b>                                                | Avinguda Baix Llobregat, 3-5, 5 <sup>th</sup> floor<br>Sant Joan Despí, 08970<br>Barcelona, Spain                          |
| <b>Areas in the scope of the certificate as declared in the SST</b> | See chapter 2.1 of [SST3.4]                                                                                                |
| <b>Activities in the product development</b>                        | Life cycle phases: <ul style="list-style-type: none"> <li>Phase 1 'IC Embedded Software Development'</li> </ul>            |
| <b>Site Security Target</b>                                         | Site Security Target Giesecke+Devrient Development Center Spain (DCS), version 3.4, 27/02/2025                             |
| <b>Evaluation Level</b>                                             | Common Criteria v3.1 R5<br>To re-use ALC certified security assurance components in evaluations up to EAL5                 |
| <b>Security Assurance Components</b>                                | AST_INT.1, AST_CCL.1, AST_SPD.1, AST_OBJ.1, AST_ECD.1, AST_REQ.1, AST_SSS.1, ALC_CMC.4, ALC_CMS.5, ALC_DVS.2 and ALC_LCD.1 |
| <b>Attack Potential</b>                                             | High                                                                                                                       |

## SECURITY POLICIES

Giesecke+Devrient Development Center Spain (DCS) 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 [SST3.4], 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 [SST3.4], 4.4 Assumptions.

## CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the site Giesecke+Devrient Development Center Spain (DCS), 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.4, ALC\_CMS.5, 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 [SST3.4], 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 Development Center Spain (DCS) [EXT-9579].

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 Development Center Spain (DCS) has been evaluated against the Security Target [SST3.4].

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.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site Giesecke+Devrient Development Center Spain (DCS) , 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.

## 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. Therefore, a reassessment of the assurance activities validity should be done before 09/06/2027.

## 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 Spain (DCS)
- **Report ID:** CCEGAD010.
- **Version:** M1
- **Issue Date:** 10/04/2025.
- **Issuing ITSEF:** Applus Laboratories.
- **Site audit dates:** 09/12/2024-11/12/2024.

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 Mobile Security TCD Iberia S.L. 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 Spain (DCS), version 3.4, 27/02/2025

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 Giesecke+Devrient Development Center Spain (DCS), version 3.4, 27/02/2025

## 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 3.0 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.

[SST3.4] Site Security Target Giesecke+Devrient Development Center Spain (DCS), version 3.4, 27/02/2025

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