Reference: 2024-8-INF-4392-v1
Target: Limitada al expediente
Date: 06.09.2024

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

# CERTIFICATION REPORT

| | |
|---|---|
| Dossier # | **2024-8** |
| TOE | **Giesecke + Devrient ePayments Iberia** |
| Applicant | **A58357021 - Giesecke + Devrient ePayments Iberia S.A.** |
| References | |

[EXT-8996] Certification Request

[EXT-9174] Evaluation Technical Report

Certification report of the site Giesecke + Devrient ePayments Iberia, as requested in [EXT-8996)] dated 07/03/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9174] received on 03/07/2024.

**CONTENTS**

# EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the site Giesecke + Devrient ePayments Iberia.

**Developer/manufacturer**: Giesecke + Devrient ePayments Iberia S.A.

**Sponsor**: Giesecke + Devrient ePayments Iberia S.A.

**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

**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,AST_SSS.1

**Resistance to Attack Potential**: High.

**Evaluation end date**: 08/08/2024.

**Re-use expiration date:** 24/11/2026[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. 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 ePayments Iberia, a positive resolution is proposed.

[1] This audit was performed as a on site audit and therefore the re-use of evaluation activities is limited at most to 30 months since the site audit date (23-24/05/2024).

## *SITE SUMMARY*

The Giesecke + Devrient ePayments Iberia is located at

Giesecke + Devrient ePayments Iberia S.A.

Carrer del Número 114, no. 27 / Poligon Pratenc

08820 El Prat de Llobregat (Barcelona)

Spain

The production area of Giesecke + Devrient ePayments Iberia, abbreviated 'GDIMS', is located on a fenced and guarded area that is owned by Giesecke + Devrient ePayments Iberia and is not shared with other companies.

Giesecke + Devrient ePayments Iberia provides services for Smart Card Production and is abbreviated by 'GDIMS'.

When not in production Smart Cards and Smart Card Modules are securely stored in the vault. The main vault is located in the warehouse inside of the high security area at the ground 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 GDIMS.

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 ePayments Iberia are in the scope of the site evaluation process:

- Secure reception, storage, delivery and destruction 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).
- 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 completion (i.e. loading the Smart Card OS), and initialisation (i.e. loading necessary keys and initialisation data) of contact (incl. dual interface) cards and contactless cards or modules
- Secure inlay manufacturing

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), Sm@rtCafé Expert products (i.e. passports, ID cards, signature cards, etc. based on G+D's Smart Café Expert operating system), Convego Join, Sm@rtSIM CX and Sm@rtSIM NextGen products (eUICC and iUICC). In addition, products which require EMVCo related type approvals are produced and handled in the same environment following the same procedures as the products named above.

The term 'handling' in this regard comprises secure reception, storage, destruction and delivery of Smart Card ICs, Smart Card modules and Smart Cards as well as secure reception and storage of data for Smart Card Production.

The reception of Smart Card ICs, Smart Card modules and Smart Cards comprises a verification of the correctness of the delivered items with respect to the delivery documents and - if applicable - the verification of integrity of seals used for secure transportation of items.

The storage of Smart Card related items is done in a specially secured vault at GDIMS with restricted access. The number of items is tracked from reception of the items until the delivery of the items.

The services of secure reception, storage, destruction and delivery of Smart Card products and related items not only covers G+D's own products but also third party products, because the same processes apply for these products as for G+D's products. Therefore the site evaluation also covers these third party products.

## *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 ePayments Iberia covers the Phase 4 (IC Packaging) 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. 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 |

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

Please note that ALC_TAT.3 has been excluded from the SST since the development tools and its versions are TOE specific and therefore it is more efficient to cover it together at the product evaluation time.

## IDENTIFICATION

| | |
|---|---|
| **Site Name** | Giesecke + Devrient ePayments Iberia |
| **Site Location** | Carrer del Número 114, no. 27 / Poligon Pratenc<br>08820 El Prat de Llobregat (Barcelona)<br>Spain |
| **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:<br>• Phase 4 (IC Packaging) |
| **Site Security Target** | Site Security Target Giesecke + Devrient ePayments Iberia<br>Version/Date: Version 2.2/06.05.2024 |

| | |
|---|---|
| **Evaluation Level** | Common Criteria v3.1 R5<br>To re-use ALC certified security assurance components in evaluations up to EAL5 + ALC_DVS.2 |
| **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,AST_SSS.1. |
| **Attack Potential** | High |

## SECURITY POLICIES

Giesecke + Devrient ePayments Iberia 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 + Devrient ePayments Iberia, 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, 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 (Evaluation evidence) of the Evaluation Technical Report of Giesecke + Devrient ePayments Iberia [EXT-9174].

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 ePayments Iberia 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.

This verdict depends on the certificate of G+D Headquarters (whose sites evaluated under the CC methodology are identified as DCG and GDM) validated by the BSI [STAR_0260_v4.2]. Ensure that the mentioned certificate is valid when reusing these results. Finally, a revocation or expiration of [STAR_0260_v4.2] would imply the revocation of the certificate of the site under evaluation.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the site Giesecke + Devrient ePayments Iberia, 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 verdict depends on the certificate of G+D Headquarters (whose sites evaluated under the CC methodology are identified as DCG and GDM) validated by the BSI [STAR_0260_v4.2]. Ensure that the mentioned certificate is valid when reusing these results. Finally, a revocation or expiration of [STAR_0260_v4.2] would imply the revocation of the certificate of the site under evaluation.

## 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 24/11/2026.

## 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 ePayments Iberia
- **Report ID**: CCEGAD007R3-STAR-M0.
- **Version**: M0.
- **Issue Date**: 27/06/2024.
- **Issuing ITSEF**: Applus Laboratories.
- **Site audit dates**: 23-24/05/2024.

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 ePayments Iberia S.A. 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 ePayments Iberia, version 2.2.

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 ePayments Iberia, version 2.2.

## 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 Giesecke + Devrient ePayments Iberia, version 2.2.

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