TRUST AND VERIFY

TrustCB Site Certification Scheme

Site Security Certification Report

AUSTRIA CARD Vienna

Sponsor & Site Operator:	***AUSTRIA CARD – Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Vienna*** **Lamezanstrasse 4-8** **1230 Vienna** **Austria**
Evaluation facility:	***TÜV Informationstechnik GmbH*** **Am TÜV 1, 45307 Essen, Germany**
Report number:	**SiteCC-2600080-01-CR**
Report version:	**1**
Author(s):	**Alireza Rohani, site_cc@trustcb.com**
Date:	**19 October 2026**
Number of pages:	**10**
Number of appendices	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety

CONTENTS

Foreword 3

Recognition of the Certificate 4

1 Executive Summary 5

2 Certification Results 7

2.1 Site Identification 7
2.2 Scope: Physical 7
2.3 Scope: Logical 7
2.4 Evaluation Approach 7
2.5 Evaluation Results 7
2.6 Comments/Recommendations 8

3 Site Security Target 9

4 Definitions 9

5 Bibliography 10

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Foreword

TrustCB is a fully independent commercial Certification Body specialising in the provision of high-assurance, security certifications for ICT products and associated sites, processes and services.

TrustCB is widely recognised for its schemes and certification work referencing the Common Criteria (CC) and Common methodology (CEM) for Information Technology Security Evaluation. CC and CEM are published by ISO/IEC as ISO/IEC 15408, Evaluation criteria for IT security and ISO/IEC 18045 Methodology for IT security evaluation.

Common Criteria based Site Certifications have long been recognised in demonstrating security in a product lifecycle. TrustCB has significant experience in the certification of sites referencing the SOG-IS recognised Netherlands Scheme for Certification in the Area of IT Security (NSCIB) scheme.

Since “site certification” is not explicitly defined in the EUCC Regulation, (EU) 2024/482, TrustCB has developed the TrustCB **Site Certification Scheme**. The scheme is in full alignment with EUCC requirements and State of the Art documents, and ready for recognition across cooperating schemes.

Importantly, the scheme is built on the NSCIB site-audit framework. Its principles are aligned with those adopted under the SOG-IS agreement and used by the SOG-IS based national schemes, now all superseded by EUCC. As such, the TrustCB Site Certification scheme ensures continuity with the recognised best practices used for STAR acceptance under SOGIS, as the ecosystem is now firmly transitioned to EUCC.

By awarding a TrustCB Site Certification Scheme certificate, TrustCB B.V. certifies that a site complies with the security requirements specified in the associated Site Security Target, in compliance the Common Criteria standards.

The consumer of this certification should review the Site Security Target (SST) in addition to this Certification Report, to gain an understanding of any assumptions made during the evaluation, and the level of confidence that the site satisfies the security requirements stated in the Site Security Target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

At the time of publication, the Common Criteria Recognition Arrangement (CCRA) does not cover the recognition of Site Certificates. The site-security evaluation process, however, followed all the rules of these agreements and used the agreed supporting document for site certification *[CCDB]*. Therefore, the results of this evaluation and certification procedure are available for use in any scheme in subsequent product evaluations and certification procedures that make use of the certified site.

The reuse of this certification with a third-party Certification Body should always be checked with the intended consuming Certification Body ahead of being reused.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the site AUSTRIA CARD Vienna. The operator of the site is AUSTRIA CARD – Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Vienna located in Vienna, Austria and they also act as the sponsor of the evaluation and certification.

The evaluated site is: AUSTRIA CARD Vienna.

The site is used by AUSTRIA CARD – Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Vienna to participate in the development and testing and of software for secure IC products. To perform its activities, the site uses the AUSTRIA CARD – Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Vienna provided remote IT-infrastructure and local IT equipment (workstations, router, VPN) and works according to the AUSTRIA CARD – Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Vienna defined processes.

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

- Secure software development,
- Testing (debugging, functional verification),
- Documentation relating to the developed software (e.g. functional and security specifications, software architecture, design, implementation and interface documentation, test specifications, test data and test reports, application notes, configuration management documentation, vulnerability handling and flaw remediation documentation, security advisories and corrective-action guidance, and SBOMs or component lists)
- Secure management and handling of transport, authentication and key protection keys for smartcards and similar devices,
- Secure delivery and reception of code, tools, documentation, keys and other data.

The site activities could be related to Phase 1 of the seven phases of the Lifecycle Model as defined in different Protection Profiles. For the details of the PPs, please refer to the [SST] references [2] to [12].

The site has been evaluated by TÜV Informationstechnik GmbH located in Essen, Germany. The evaluation was completed on 19 October 2026 with the approval of the ETR. The site audit was performed on 25 and 26 August 2026.

The certification procedure has been conducted in accordance with the provisions of the TrustCB Site Certification Scheme *[TrustCB-SP]*

The scope of the evaluation is defined by the Site Security Target *[SST]*, which identifies assumptions made during the evaluation and the level of confidence (evaluation assurance level) the site is intended to satisfy for product evaluations. Users of this site certification are advised to verify that their own use of, and interaction with, the site is consistent with the Site Security Target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report *[ETR]*[1] and *[STAR]*[2] for this site provide sufficient evidence that this site meets the assurance components ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2 (at AVA_VAN.5 level), ALC_FLR.3, ALC_LCD.1, ALC_TAT.2[3], ALC_FLR.4 (extended), ALC_SBM.1 (extended) and ALC_PSR.1 (extended). The extended components are taken from [EUCC-CRA] and [prEN 18330].

---

1 The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 The site does not contribute to the aspect ALC_TAT. The aspect has been claimed in order to ensure the assessment of related items during the evaluation process and to support the reuse of the evaluation results in a product evaluation accordingly.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM:2022 *[CEM]* and the Supporting Document Guidance: CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1 *[CCDB]*, for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 *[CC]*.

TrustCB B.V., as Certification Body for this site certification activity, declares that the evaluation meets all the conditions of the Common Criteria and that the site certificate will be included on the TrustCB webpage of certified sites.

Note that the certification results apply only to the specific site, used in the manner defined in the *[SST]*.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

2 Certification Results

2.1 Site Identification

The site that is covered by this evaluation is the AUSTRIA CARD Vienna located in Vienna, Austria.

2.2 Scope: Physical

This site certification considers a single building location occupied only by AUSTRIA CARD – Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Vienna.

The area where the relevant activities take place is limited to:

- Reception,
- Security Office,
- Development Environment,
- Server Rooms hosting the CM system, Backups, Firewall, CCTV, Alarm- and Access Control,
- Shipment and Reception areas for physical goods

2.3 Scope: Logical

The following life cycle phase as defined in the Protection Profiles (refer to the [SST] for exact PPs) which is subject of the certification:

- Phase 1: IC Embedded Software Development.

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

- Secure software development,
- Testing (debugging, functional verification),
- Documentation relating to the developed software (e.g. functional and security specifications, software architecture, design, implementation and interface documentation, test specifications, test data and test reports, application notes, configuration management documentation, vulnerability handling and flaw remediation documentation, security advisories and corrective-action guidance, and SBOMs or component lists)
- Secure management and handling of transport, authentication and key protection keys for smartcards and similar devices,
- Secure delivery and reception of code, tools, documentation, keys and other data.

2.4 Evaluation Approach

The evaluation is a re-evaluation, based on developer documentation of a site change.

In the evaluation all evaluator actions, including a site visit, have been performed. There was an in-person audit performed at the site. For assessment of the ALC_DVS aspects, the Minimum Site Security Requirements *[MSSR]* have been used.

2.5 Evaluation Results

The evaluation lab documented its evaluation results in the *[ETR]*[4], which references other evaluator documents. To support reuse of the site evaluation activities a derived document *[STAR]*[5] was

[4] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

provided and approved. This document provides details of the site evaluation that must be considered when this site is used in a product evaluation.

The evaluation lab concluded that the site meets the assurance requirements listed in the *[SST]* as assessed in accordance with *[CC], [CEM]* and *[CCDB]*.

2.6 Comments/Recommendations

The Site Security Target *[SST]* contains necessary information about the usage of the site. During a product evaluation, the evidence for fulfilment of the Assumptions listed in the *[SST]* shall be examined by the evaluator of the product when reusing the results of this site evaluation.

[5] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

3 Site Security Target

The Site Security Target, Austria Card Vienna, version 4.0, date: 2026-09-21 *[SST]* is included here by reference.

Please note that for the need of publication a public version *[SST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MSSR	Minimum Site Security Requirements
SST	Site Security Target
TOE	Target of Evaluation

Reproduction of this report is authorised only if the report is reproduced in its entirety.

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts 1 to 5, CC:2022 Revision 1, November 2022
[CCDB]	Supporting Document Guidance: CCDB-2007-11-001 Site Certification, October 2007, Version 1.0, Revision 1
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[ETR]	ETR FOR SITE CERTIFICATION (ETR SUMMARY), version 1.0, date: 2026-10-07
[MSSR]	EUCC Scheme State-of-The-Art Document - Minimum Site Security Requirements, Version 2.0, February 2025
[TrustCB-SP]	TrustCB Scheme procedure - Site Certification v1.1
[SST]	Site Security Target, Austria Card Vienna, version 4.0, date: 2026-09-21
[SST-lite]	Site Security Target – Lite, Austria Card Vienna, Version 4.0-Lite, Date: 2026-09-21
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR]	SITE TECHNICAL AUDIT REPORT (STAR) AUSTRIA CARD - AUSTRIA CARD – Plastikkarten und Ausweissysteme Gesellschaft m.b.H., Version 1.0, Date: 2026-10-07
[EUCC-CRA]	ENISA Analysis Report: “Cyber Resilience Act implementation via EUCC and its applicable technical elements, Annexes”, Final Version 27/01/2025
[prEN 18330]	Draft prEN 18330, Cybersecurity requirements for smartcards or similar devices, including secure elements - Application layer, January 2026

(This is the end of this report.)

Reproduction of this report is authorised only if the report is reproduced in its entirety.