CERTIFICATION REPORT

ITSEF: DEKRA Testing and Certification **Applicant:** Miguel Fadrique Bañón Puente
TOE: SGOC - Certification Body Management System **Representative:** Miguel Bañón
Scope: Common Criteria for Information Technology Security Evaluation, v3.1, r5 at EAL1

References

CC Common Criteria v3.1 Revision 5
CEM CEM v3.1 Revision 5
ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security
ISO/IEC 17025 General requirements for competence of calibration and testing laboratories.
ISO/IEC 17065 Conformity assessment - Requirements for bodies certifying products, processes and services
CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.
SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
NASK-PC1 NASK IT Security Evaluation and Certification Scheme
NASK-PT10 NASK Certification Body Quality Manual
NASK-P33 NASK Certification Body Product certification procedure

List of related documents

1. [DOC-CAP-V1.0] SGOC Certification Application, issue date 28.01.2021
2. [ETR-FIN-V1.1] Evaluation Technical Report, v. 1.1, issue date 10.05.2021

Introduction

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been tested at an approved Laboratory (IT security evaluation facility) – on the basis of the IT Security Evaluation and Certification Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. This certification report, and its associated certificate, applies only to the identified version and release of the product in its tested and evaluated configuration. The evaluation has been conducted in accordance with the provisions of the NASK-PC1 Scheme, and the conclusions of the Laboratory in the technical evaluation report are consistent with the evidence. This report, and its associated certificate, are not an endorsement of the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the NASK National Research Institute, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration.

Certification overview

The NASK's "IT Security Evaluation and Certification Scheme" provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a approved Laboratory under the oversight of the Certification Body, which is managed by the NASK National Research Institute. Laboratory is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2018- The General Requirements for the Competence of Testing and Calibration Laboratories. By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated Security Target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the Laboratory. The Certification Report, Product Certificate and Security Target are posted to the Certified Products List for the IT Security Evaluation and Certification Scheme published by NASK National Research Institute.

TABLE OF CONTENT

Executive Summary

This document constitutes the Certification Report for the certification file of the product:
SGOC – Certification Body Management System
TOE Version: 21.814

Developer:	Miguel Bañón
Sponsor:	Miguel Bañón
Security target:	Certification Body Management System Security Target v. 21.814
Protection Profile:	None
Laboratory/ITSEF:	DEKRA Testing and Certification S.A.U.
Evaluation Level:	Common Criteria version 3.1 release 5, Evaluation Assurance Level EAL1
Evaluation end date:	10/05/2021
Expiration Date:	10/06/2025 (tbc)

All the assurance components required by the evaluation level EAL1 of Common Criteria standard have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigned the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL1, as defined by the Common Criteria v3.1 Revision 5 and the CEM v3.1 Revision 5. Considering the obtained evidences during the process of the certification of the product SGOC - Certification Body Management System v. 21.814, a positive resolution by Certification Body is proposed.

TOE Summary

SGOC is an information and document management system for cybersecurity Conformity Assessment Body (CAB). It allows managing Information for licensing and product certification processes, in a coordinated manner to the internal CAB operating procedures.
Information related to such processes are handled as “dossiers”, and SGOC allows recording and managing the dossier information and documentation.
SGOC is a client-server software TOE intended to be used concurrently by the staff of the CAB.
The major security features of the TOE are the following:

- Identification and authentication of SGOC users;
- Security management of user accounts, their roles, assignment of users to dossiers, assignment of document distribution levels, application access tokens and user passwords;
- Access control policy and function to regulate the access of users to the SGOC client components: applications, modules and screens;
- Information flow control policy and function to regulate the access of SGOC users to dossier information and documents;
- Generation and review of audit information related to the activity of the SGOC users;
- Trusted channels between the SGOC client and server components. SGOC initiates such channels when interacting with the documentation server, and relies in the operational environment configuration for the setting up of secure communications with the dossier database server, Oracle Database XE.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil the evaluation level EAL1, according to Common Criteria v3.1 Revision 5.

Assurance Class	**Assurance Component**
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements

	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Security Functional Requirements

Functional requirement	Description
FIA: Identification and authentication	FIA_UID.2 User identification before any action
	FIA_UAU.2 User authentication before any action
FMT: Security management	FMT_SMR.1 Security roles
	FMT_MSA.3 Static attribute initialisation
	FMT_MSA.1 Management of security attributes
	FMT_SMF.1 Specification of Management Functions
FDP: User Data Protection	FDP_ACC.2 Complete access control
	FDP_ACF.1 Security attribute based access control
	FDP_IFC.2 Complete information flow control
	FDP_IFF.1 Simple security attributes
FAU: Security audit	FAU_GEN.1 Audit data generation
	FAU_SAR.1 Audit review
	FAU_SAR.3 Selectable audit review
	FAU_STG.1 Protected audit trail storage
FTP: Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel

Identification

Product: SGOC - Certification Body Management System, release 21.814

Security Target: Certification Body Management System Security Target, v. 21.814, issue date 8th May 2021

Security Policy

There are no Organizational Security Policies defined in the Security Target.

Assumptions and Clarification of Scope

Usage Assumptions

The Security Target [EVD-ST-V21.814] does not contain any assumptions related to the user.

Environmental Assumptions

The assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.
The complete list of assumptions can be found in the Security Target [EVD-ST-V21.814], section 3.

Clarification of Scope

The Security Target [EVD-ST-V21.814] does not contain any threats.

Architectural Information

Physical scope

The TOE is delivered in a single file, SGOC_installation.21.814.zip. This file is distributed directly by the developer to the CAB using secure methods agreed in advance to the distribution, for example, by upload to a secure cloud service.
The distribution file includes all TOE components and files, including guidance and the required evidence for the evaluation of the TOE, such as this document.
For convenience, the SGOC client components also distribute non-TOE libraries, Oracle Instant Client, and for Windows the Microsoft Visual Studio 2017 Redistributable as well.

SGOC requires as operational environment a centralized server to store and serve both dossier information and documents, and then the operational environment for the SGOC clients. At the time of issuing this document, the supported server configuration, and non-TOE software, is the following:

- Oracle Linux R7-U9
- Apache Web Server, as included in the Oracle Linux distribution.
- Oracle Database XE 18c-1.0-1

At the client side, SGOC requires the following non-TOE libraries to interact with Oracle Database XE:

- For Oracle Linux, Oracle Instant Client v19.10.0.0.0
- For Windows 10 64bit, Oracle Instant Client v19.9.0.0.0
- For macOs Big Sur, Oracle Instant Client v19.8.0.0.0

The following non-TOE operating systems are supported for the client part of SGOC, all at their latest versions and patches as available at the date of issuing this document:

- Oracle Linux R7-U9
- Windows 10 64bit
- macOs Big Sur

Users of SGOC may use the word processor of their choice to edit the dossier documentation. However, if users choose to use Microsoft Word when operating on the Windows 10 64bit platform, SGOC provides a data merge capability that allows documents to obtain information from dossiers and be included in the document text automatically.
SGOC does not have any dependency on any particular hardware, so any non-TOE hardware platform can be used as long as it is supported by the previously defined set of required non-TOE software components.

Logical scope

SGOC identifies and authenticate users prior to any action. Once the user is successfully identified and authenticated, it is assigned a functional role within SGOC.
The user is then provided with a menu of available applications. Applications are composed of modules, and these are a set of screens. The "Security manager" can configure, for each user role, access or denial rules to applications, modules or individual screens. This "Security manager" is also in charge of configuring the SGOC user roles and users.
Every access of a SGOC user to a screen is logged, and this audit trail can be reviewed by the "Security Manager". In the event of a SGOC client being unable to register such accesses, the user is informed and the application is closed.
User roles within SGOC are given a numerical code and a description, with the lowest number being the role with lowest privileges.
Any SGOC user can create a product certification or an ITSEF licensing dossier, introducing into the system the information and documentation received during the initial phase of the certification or licensing services. Each CAB may have different definition of these services and phases.
Staff of the CAB shall be assigned to manage dossiers. Such an assignment can only be done by a user with a numeric role with a minimum value of 30, normally reserved to CAB management personnel.
Once members of the staff are assigned to a dossier, only they will be able to access the dossier information. Users with a adequate assigned role , normally reserved to CAB personnel like Technical or Quality managers, have access to every dossier in SGOC.
Documents can be related to a dossier, for example an Evaluation Technical Report in the case of a product certification dossier. Documents related to a dossier are only accessible to those with access to the dossier. Documents not related to a dossier are considered to be of the interest of the full CAB, and then accessible to all users of SGOC.
SGOC includes an application to manage non-conformities of the CAB. Every action performed over the information of a non-conformity, in terms of updates or modifications, is logged by SGOC, and such audit trail can be reviewed by all SGOC users.
The same logging capabilities are provided by SGOC over the information and documentation of a dossier, in terms of updates or modifications. Such audit trails can also be reviewed by all SGOC users.
Documents managed by SGOC are stored in a non-TOE Apache Web Server. Communications with this server are secured by TLS, with the secure channel being initiated by SGOC.

Product Documentation

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version:

1. [EVD-ST-V21.814] Security Target, v. 21.814, issue date 8.05.2021
2. [EVD-UM-V21.814] User Manual, v. 21.814, issue date 8.05.2021
3. [EVD-AM-V21.814] Administration Manual, v. 21.814, issue date 8.05.2021
4. [EVD-SDS-V21.814] System Specification, Design and Source Code, v. 21.814, issue date 8.05.2021
5. [EVD-RAD-V21.1111] System Specification, Design and Source Code, v. 21.1111, issue date 8.05.2021
6. [EVD-PI-V21.814] Programmatic Interfaces, v. 21.814, issue date 8.05.2021

Security Target

Along with this certification report, the complete Security Target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

Certification Body Management System Security Target v. 21.814, issue date 8th May 2021

The public version of this document is the same as complete Security Target described above and it is published along with this certification report on the Certification Body website.

IT security evaluation

The Evaluation Assurance Level EAL1 requires the independent testing provided by evaluator.
The evaluator has performed an installation and configuration of the TOEs and their operational environment following the steps included in the installation and operation manual. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to Security Target.
The main objective of the tests performed by the evaluator was to check that the security functional requirements are implemented as expected and that the TSFIs definitions are consistent with the TOE. The evaluator's independent test plan was SFR oriented, and the functionality of each SFR included at the Security Target has been considered. The independent tests plan covered the whole TOE functionality: all the SFRs have been tested through their TSFIs.

All the 21 test cases have obtained a PASS verdict.

Penetration testing

The attack potential used for this evaluation is consistent with AVA_VAN.1: BASIC attack potential.
The developed test plan is based on vulnerability survey of information available in the public domain is performed by the evaluator to ascertain potential vulnerabilities that may be easily found by an attacker. TOE configuration used to execute the penetration test plan was consistent with the evaluated configuration according to the Security Target.

After providing all planned tests the evaluator concluded that there were not exploitable vulnerabilities in the TOE operational environment according to the scope of this evaluation.

Evaluated Configuration

The TOE Security Target defines supported configurations in sections 1.3 TOE Overview and 1.4 TOE Description. For the evaluation purposes the TOE has been installed following the Installation Guide [EVD-AM-V21.814].
The environment used by the evaluator was based on VMWare 15 for running the machines. One server and tree client machines have been set up for the testing environment:

- The server installed in an updated Oracle Linux version (R7-U9-Server)
- The linux client running Oracle Linux R7-U9 and has IP address xx.yy.zz.19.

- The macOS client running Big Sur version 11.3 Beta and has IP address xx.yy.zz.77.
- The Windows client running Windows 10 Pro build 19042 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target for an attack potential Basic.
The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class	Assurance Component	Laboratory Verdict	Certification Body Evaluation
ADV: Development	ADV_FSP.1 Basic functional specification	PASS	CONFORMANT
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS	CONFORMANT
	AGD_PRE.1 Preparative procedures	PASS	CONFORMANT
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	PASS	CONFORMANT
	ALC_CMS.1 TOE CM coverage	PASS	CONFORMANT
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	PASS	CONFORMANT
	ASE_ECD.1 Extended components definition	PASS	CONFORMANT
	ASE_INT.1 ST introduction	PASS	CONFORMANT
	ASE_OBJ.1 Security objectives for the operational environment	PASS	CONFORMANT
	ASE_REQ.1 Stated security requirements	PASS	CONFORMANT
	ASE_TSS.1 TOE summary specification	PASS	CONFORMANT
ATE: Tests	ATE_IND.1 Independent testing - conformance	PASS	CONFORMANT
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey	PASS	CONFORMANT

Evaluator Comments/Recommendations

Recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and shall to be considered when using the product.

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

Certifier Recommendations

Considering the obtained and validated evidences during the certification process of the product SGOC - Certification Body Management System v. 21.814 evaluation, **a positive resolution is proposed**.

Glossary

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ITSEF	Information Technology Security Evaluation Facility
CB	Certification Body
TOE	Target Of Evaluation

Bibliography

The following standards and documents have been used for the evaluation of the product:

[CC31p1]	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1, Revision 5
[CC31p2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components, Version 3.1, Revision 5
[CC31p3]	Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, Version 3.1, Revision 5
[CEM31]	Common Criteria for Information Technology Security Evaluation. Evaluation Methodology, Version 3.1 Revision 5

Created by: Paweł Kripiec
Reviewed by: Paweł Kostkiewicz
Approved by: Paweł Kripiec