Certification Body Management System

Security Target

May 8, 2021

Preface

This document describes security properties of the “Certification Body Management System” (**SGOC**).

Audience

This document is intended for end-users of the “Certification Body Management System”, that may need to install and operate the product in a secure manner. It is also useful to cybersecurity evaluators and certifiers that may be involved in the evaluation and certification of security properties of the “Certification Body Management System”.

Contents

Acronyms

SGOC Certification Body Management System

CAB Conformity Assessment Body

ITSEF Information Technology Security Evaluation Facility

References

[1] ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security

[2] Common Criteria for Information Technology Security Evaluation. April 2017. Version 3.1 Revision 5.

[3] Certification Body Management System Management System. System Specification, Design and Source Code. Version 21.814.

[4] RADsec, the access control application. System Specification, Design and Source Code. Version 21.1111.

[5] Certification Body Management System. User manual. Version 21.814.

[6] Certification Body Management System. Administration manual. Version 21.814.

[7] Certification Body Management System. Programmatic Interfaces. Version 21.814.

[8] SGOC_Configuration_List.21.814.txt

1 ST Introduction

1.1 ST Reference

- Document title: “Certification Body Management System Security Target”
- Document version: 21.814

1.2 TOE Reference

- TOE name : “Certification Body Management System” (**SGOC**)
- TOE version: 21.814

1.3 TOE Overview

SGOC is an information and document management system for cybersecurity Conformity Assessment Bodies Conformity Assessment Body (CAB). It allows to manage Information Technology Security Evaluation Facility (ITSEF) 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 to record and manage the dossier information and documentation.

A very relevant aspect of a dossier is the handling of the many associated documents that the execution of the related process will create. Documents will be received from external parties, like an ITSEF submitting evaluation reports for validation, and will be created internally by the CAB, sometimes in response to those received documents. Documents created by the CAB need to comply with internal restrictions on their review and approval authorities. **SGOC** includes features to model this documentation workflow.

SGOC is a client-server software TOE intended to be used concurrently by the staff of the CAB. Users of **SGOC** are grouped by functional roles.

Access to the information of a dossier and to its associated documentation is restricted by **SGOC** to the staff assigned to the management of such dossiers. Users belonging to certain roles have access to all existing dossiers and associated documents.
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.
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**.

1.4 TOE Description

1.4.1 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. They are to found at the following paths:

- For **Windows**, in **<installation path>/sgoc/runtime/Windows/lib**;
- for **Linux**, in **<installation path>/sgoc/runtime/Linux/lib**;
- and for **macOs**, in **<installation path>/sgoc/runtime/Darwin/lib**.

1.4.2 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 numeric role with a minimum value of 20, 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 accesible 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**.

2 CC Conformance Claims

This Security Target is conformant to “ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security” [1] and to “Common Criteria for Information Technology Security Evaluation. April 2017. Version 3.1 Revision 5.” [2]. This Security Target is also conformant to Part 2 and to Part 3 of the cited standards, at EAL1.

3 Security Objectives for the Operational Environment

OE-INST The server operational environment shall be configured following the TOE installation guidance.

OE-OPER The operational environment shall be kept secure and operated in a trusted manner.

OE-TIME The operational environment shall provide reliable time stamps.

4 Security Requirements

4.1 Security Functional Requirements

4.1.1 FIA: Identification and authentication

4.1.1.1 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

4.1.1.2 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

4.1.2 FMT: Security management

4.1.2.1 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [

- **Numerical code 50, “Security manager”**
- **Numerical code 30, “Certification unit manager”**
- **Numerical code 22, “Technical manager”**
- **Numerical code 21, “Quality manager”**
- **Numerical code 20, “Record manager”**
- **Numerical code 10, “Certifier”**
- **Numerical code 9, “External certifier”**

].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

4.1.2.2 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [**"RADsec SFP"**, **"Dossier SFP"**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**"Security manager"**] to specify alternative initial values to override the default values when an object or information is created.

4.1.2.3 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**"RADsec SFP"**, **"Dossier SFP"**] to restrict the ability to [**change_default, modify, delete**] the security attributes [**user role**] to [**"Security manager"**]

4.1.2.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- **Assign and de-assign a user to a dossier ("Dossier SFP"), by SGOC users with a role with a numeric value greater or equal than 30.**
- **Assign the distribution level to a document ("Dossier SFP"), by any SGOC user.**
- **Assign and revoke access and denial tokens ("RADsec SFP"), by users with the role of "Security manager".**
- **Change the password of a user.**

].

4.1.3 RADsec Security Functional Policy ("RADsec SFP")

4.1.3.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [**"RADsec SFP"**] on [

- **List of subjects: SGOC users;**
- **List of objects: SGOC applications, modules and screens.**

] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

4.1.3.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [**"RADsec SFP"**] to objects based on the following: [

- **List of subjects: SGOC users;**
- **List of objects: SGOC applications, modules and screens. These are hierarchical, i.e., an application is composed of modules, and these are composed of screens.**
- **List of attributes: the user group of the SGOC user.**

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**A SGOC user belonging to a given user role can access a particular application, module or screen if and only if**

- **An access token has been given to the user role to access the object, and no deny token has been given to that user role to a parent object, or**
- **An access token has been given to a parent object for the role, and no deny access token has been given to that role for the specific object.**

].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

4.1.4 Dossier Security Functional Policy ("Dossier SFP")

4.1.4.1 FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the [**"Dossier SFP"**] on [

- **List of subjects: SGOC users;**
- **List of objects: dossier information and documentation.**

] and all operations that cause that information to flow to and from subjects covered by the SFP.
Note: "Dossier information" means the information stored in the following database tables:

- "Applicants of a dossier"
- "Assigned evaluators"
- "Assigned external experts"
- "Certificate closure"
- "Certification scope"
- "Decisions/resolutions"

- “Dossier duration”
- “Dossier reviews”
- “Dossiers”
- “Licensing security level”
- “Nonconformities”
- “Scope: protection profiles”
- “Scope: standards”

Note: “Documentation” means the information stored in the following database tables, as well as the associated document file stored at the server:

- “Document input registry”
- “Document versions”
- “Documents”
- “Last operation on a document”
- “Output registry”
- “References to input documents.”
- “References to output documents.”

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

4.1.4.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [**“Dossier SFP”**] based on the following types of subject and information security attributes: [

- **List of subjects: SGOC users;**
- **List of objects: dossier information and documentation;**
- **List of attributes: the SGOC user role, the assignment of a user to a dossier, and the document distribution level.**

]
Note: Assignment of a SGOC user to a dossier can be done in the following ways:

- As certifier;
- As informed staff;
- As user belonging to an informed user role or category;

Note: The distribution level of a document can be one of the following:

- “D”, “Limited to the dossier”

- “I”, “Internal to the Certification Body”
- “S”, “Internal to the Scheme”
- “P”, “Public”

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- **Access to “dossier information”:**
  - **Any SGOC user can have access to the “dossier information” of a specific dossier, if such dossier has not yet been assigned to any SGOC user.**
  - **Once the dossier is assigned to any SGOC user, a SGOC user can have access to the “dossier information” if the user has been assigned to such dossier.**
- **Access to “documentation” depends on the distribution level of such documents:**
  - **“Internal to the Scheme” and “Public” documents can be accessed by all SGOC users.**
  - **“Internal to the Certification Body” documents can be accessed by all SGOC users with a role with a numeric value greater or equal than 10 (i.e., all users except external certifiers).**
  - **“Limited to the dossier” documents can be accessed:**
    1. **If the dossier has not been assigned to any SGOC user, or if the document has not yet been assigned to a dossier, by all SGOC users.**
    2. **If the document has been assigned to a dossier, and that dossier has been assigned to any SGOC user, by that user.**

]

FDP_IFF.1.3 The TSF shall enforce the [**none**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**Regardless of the previous rules, a user can access the information of any dossier, and all documents, if the associated user role numerical code is equal or greater than 20.**]

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**none**].

4.1.5 FAU: Security audit

4.1.5.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

1. Start-up and shutdown of the audit functions **of the SGOC client application**;
2. All auditable events for the [**not specified**] level of audit; and
3. **All access to SGOC screens.**

4. **Every insertion, deletion or update of information related to non-conformities.**
5. **Every insertion, deletion or update of information related to dossiers.**
6. **Every insertion, deletion or update of information related to documents.**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

1. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and [1]
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**]

4.1.5.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**all SGOC users**]] with the capability to read [

- **All users can read audit records related to non-conformities and to access to the SGOC screens.**
- **Users can read audit records related to dossiers and documents, provided they have access to such dossiers and documents.**

] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

4.1.5.3 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**sorting by any field**] of audit data based on [**the following logical operators:**

- **"equal to"**
- **"less than"**
- **"greater than"**
- **"not equal to"**
- **"like"**
- **"between"**
- **"null"**
- **"not null"**
- **"max"**
- **"min"**
- **"count"**

].

[1] Reliable time-stamps are provided by the environment, and the TOE relies in such information when producing audit records. Hence, FPT_STM.1 is not implemented by the TOE.

4.1.5.4 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [**prevent**] unauthorised modifications to the stored audit records in the audit trail.

4.1.6 FTP: Trusted path/channels

4.1.6.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [**the TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**uploading and downloading files between the SGOC client and the server**].

4.2 Security Assurance Requirements

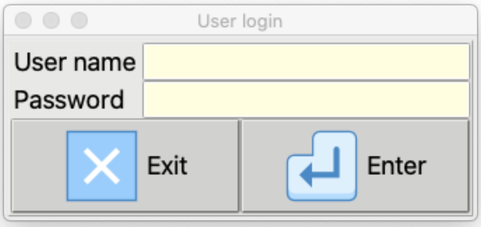
As indicated in section 2, this Security Target provides a basic level of assurance by complying to the Evaluation Assurance Level 1, that includes, amongst others, the following security assurance requirements:

Requirement	**Related evidence**
ADV_FSP.1	"Certification Body Management System Management System. System Specification, Design and Source Code." [3] "RADsec, the access control application. System Specification, Design and Source Code." [4] "Certification Body Management System. Programmatic Interfaces." [7]
AGD_OPE.1	"Certification Body Management System. User manual."[5]
AGD_PRE.1	"Certification Body Management System. Administration manual." [6]
ALC_CMC.1	Refer to sections 1.1 and 1.2 of this document.
ALC_CMS.1	Refer to the configuration list provided in file "SGOC_Configuration_List.21.814.txt" [8].
ASE_CCL.1	Refer to section 2 of this document.
ASE_INT.1	Refer to section 1 of this document.
ASE_OBJ.1	Refer to section 3 of this document.
ASE_REQ.1	Refer to section 4 of this document.
ASE_TSS.1	Refer to section 5 of this document.

5 TOE Summary Specification

5.1 FIA: Identification and authentication

The following login dialog will appear on launching the **SGOC** client application.



User login

User name

Password

Figure 5.1: Initial login

Once a valid user name and password are provided, the login dialog turns into the main **SGOC** window. The number of applications that will appear depend on the access rights of the associated user role.

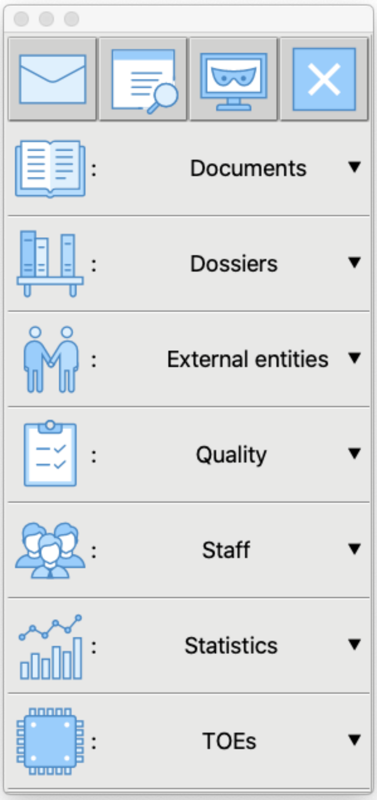


Figure 5.2: Main window and menu

SGOC relies on the non-TOE element of the environment, **Oracle Database XE**, to provide user identification and authentication services.

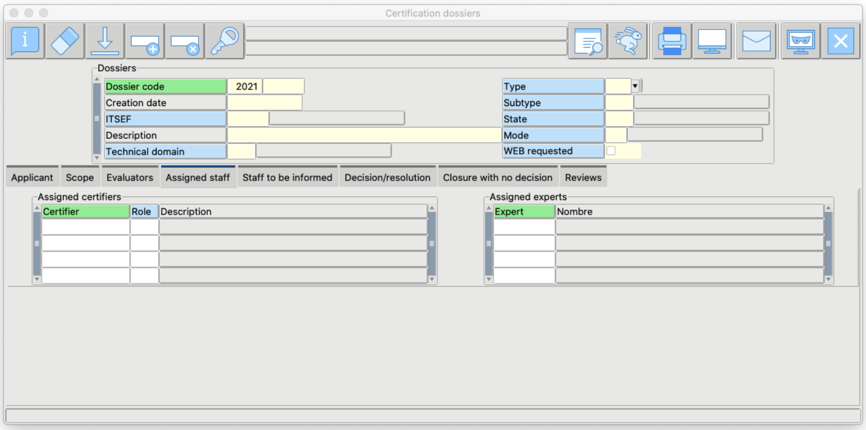
“FIA_UID.2 User identification before any action” (4.1.1.1)
“FIA_UAU.2 User authentication before any action” (4.1.1.2)

5.2 FMT: Security management

The “Security manager” can access a specific **SGOC** application (“RADsec”) that allows to manage users, their roles, and the access rights of user roles.

“FMT_SMR.1 Security roles” (4.1.2.1)
“FMT_MSA.3 Static attribute initialisation” (4.1.2.2)
“FMT_MSA.1 Management of security attributes” (4.1.2.3)
“FMT_SMF.1 Specification of Management Functions” (4.1.2.4)

The “Certification unit manager” can assign users to dossiers in the dossier editing windows. There is one of such window for each type of dossier, i.e., certification, licensing and review dossiers.


Certification dossiers

Dossiers

Dossier code	2021	Type	
Creation date		Subtype	
ITSEF		State	
Description		Mode	
Technical domain		WEB requested	□

Applicant | Scope | Evaluators | Assigned staff | Staff to be informed | Decision/resolution | Closure with no decision | Reviews

Assigned certifiers

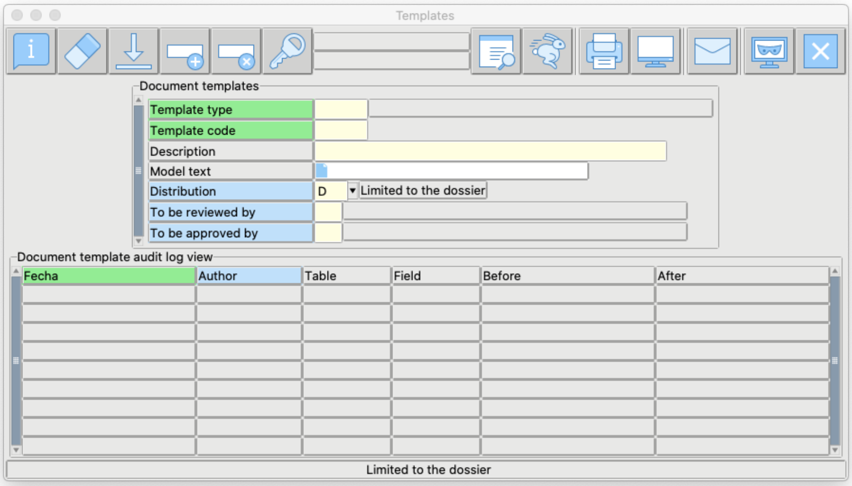
Certifier	Role	Description

Assigned experts

Expert	Nombre

Figure 5.3: Dossier and user assignment

SGOC users can create document templates. These templates define, amongst other things, the default distribution level for documents created from them.


Templates

Document templates

Template type		
Template code		
Description		
Model text		
Distribution	D	Limited to the dossier
To be reviewed by		
To be approved by		

Document template audit log view

Fecha	Author	Table	Field	Before	After

Limited to the dossier

Figure 5.4: Document templates

When a document is created by an **SGOC** user, the default distribution level is inherited from the associated template, if any. This can be changed by the user. When a particular document is assigned to a dossier, the distribution level is reset to ’D’.

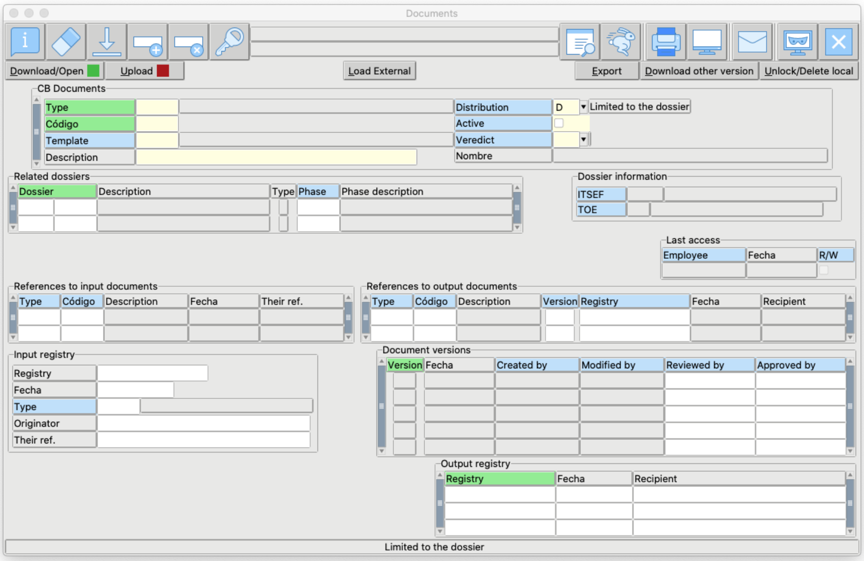


Figure 5.5: Editing documents

SGOC users can change their password using the following dialog, which can be accessed from the main menu or from any of the editing windows:

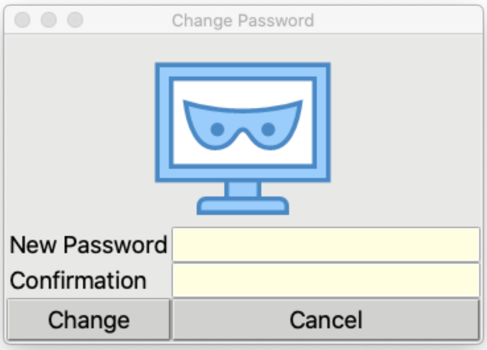


Figure 5.6: "Change Password" dialog

"FMT_SMF.1 Specification of Management Functions" (4.1.2.4)

5.3 RADsec Security Functional Policy ("RADsec SFP")

This security policy requires no action or intervention from **SGOC** users. Any attempt to access a **SGOC** application, module or application will be mediated by the access control function. The result of the access control function will remove from the user interface those elements to which the user role has no access rights.

“FDP_ACC.2 Complete access control” (4.1.3.1)
“FDP_ACF.1 Security attribute based access control” (4.1.3.2)

5.4 Dossier Security Functional Policy (“Dossier SFP”)

Equally silent to the end user, the implementation of this security policy removes from the accessible information those dossiers and documents that the user should not have access to.

“FDP_IFC.2 Complete information flow control” (4.1.4.1)
“FDP_IFF.1 Simple security attributes” (4.1.4.2)

5.5 FAU: Security audit

Generation of the audit data is automatic and never notified to the user triggering the audited event.
To review the audit trail, the **SGOC** client application provides several screens with access to dossier, document and non-conformity events. These screens will only show the audit logs of those dossiers and documents that the user has access to.
To review the audit trail of screen access, the “Security manager” also has available a similar screen.
All the screens in the **SGOC** client application have a general search function that allows to query and sort the related information, including the audit records.

“FAU_GEN.1 Audit data generation” (4.1.5.1)
“FAU_SAR.1 Audit review” (4.1.5.2)
“FAU_SAR.3 Selectable audit review” (4.1.5.3)
“FAU_STG.1 Protected audit trail storage” (4.1.5.4)

5.6 FTP: Trusted path/channels

Every file transfer between the **SGOC** client application and the **Apache Web Server** is initiated by the **SGOC** client side, and in this initialization, requested to be done with TLS. The protocol version and cryptographic algorithms are left to negotiation, depending on the configuration of the **Apache Web Server**.

“FTP_ITC.1 Inter-TSF trusted channel” (4.1.6.1)

6 Release notes

6.0.1 Version 21.814

Common Criteria evaluated version.

Index