Soffid IAM
Security Target

Version 10

05/03/2025

Prepared for:

Prepared By:

Content

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

Although this ST does not claim conformance to any Protection Profile, its security requirements are based on the following PP:

- Standard Protection Profile for Enterprise Security Management Identity and Credential Management v2.1.

The Security Problem Definition, Security Objectives and Security Functional Requirements for the TOE and the operational environment (Chapters 3, 4, 5 and 6.1) have been copied verbatim from the mentioned PP.

1.1 ST Reference

ST Title: Soffid IAM

ST Version: 10

ST Author: L. Miranda (Clover), G. Campoy (Clover), J.M. Sierra (Clover), I. Rojas (Clover), P. García (Soffid)

ST Publication Date: 5/3/2025

1.2 TOE Reference

The TOE, developed by Soffid, has the following components: PAM-Launcher v.1.4.36, PAM-Store v.1.4.36, IAM-Sync v.3.5.22, IAM-Console 3.5.57, soffid-pasr-jdbc 1.4.12, soffid-pasr-rdp 1.4.12, and soffid-pasr-ssh 1.4.12.

1.3 TOE Overview

Soffid IAM is a converged Identity Governance and Administration (IGA) and Privileged Account Management (PAM) solution designed to help enterprises to improve the

security and efficiency of managing their users' identities and access. The solution enables enterprises to centralize identity and access management, allowing them a more efficiently managed access to systems and applications, improve the security of their information, and comply with regulatory requirements.

The importance of Soffid IAM for enterprises lies in its ability to help protect critical enterprise data from internal and external threats, enabling more secure and effective management of access to the organization's resources. In addition, Soffid IAM can also help improve business efficiency and productivity by reducing the time and resources required to manage user identities and access, which can lead to significant cost savings. In summary, Soffid IAM is an important solution for enterprises looking to improve security, efficiency, and compliance.

Soffid IAM needs a Linux server to run with at least 16GB RAM, 250GB disk space, a MariaDB database engine and Docker.

1.3.1 Features and Functionalities

Soffid IAM has one of the most extensive feature sets in the market, including attribute management, identity governance, access control and privileged account management.

- Centralized identity and access management: enables enterprises to centrally manage user identities and access, which allows administrators to grant, revoke and modify access permissions in real time.
- Password and authentication management: Soffid IAM offers a secure password management solution that allows users to set strong passwords and protect them with additional security measures.
- Report and audit: Soffid IAM provides detailed reporting and auditing of user activity and access permissions, allowing enterprises to have a complete and detailed view of user activity.
- Catalog and audit of privileged accounts: Soffid IAM is capable of inventorying, cataloging, and logging the usage of privileged accounts.

- Integration with other solutions: Soffid IAM can integrate with other enterprise solutions, such as Active Directory.

1.3.2 Tools and Concepts

Console

Soffid IAM is always accessed through the management console, a web-based tool designed in accordance with the OWASP best practices guide. In addition, it has reinforced mechanisms to respond to brute force attacks. Soffid IAM has a self-service web portal usable from any device, including Android or iOS devices, in portrait or landscape format and fully configurable.

Users can select the language in which they want to use the console, from Catalan, Spanish or English.

Security

Soffid IAM users can be identified by three specific roles inside of the system. These roles are created to guarantee a secure distribution of responsibilities. The roles are created during the installation of the TOE and can be identified as:

- Administrator User: This role gives the user the ability to manage and modify all the functionalities and security attributes of the system.
- Basic User: This role is assigned to users without any privileged permissions. It allows users to access their own information and linked accounts in the console, as well as modify their password.
- PAM Access: This role can be assigned to Basic Users, enabling them to access specific remote systems through the PAM process.

Role management

Role management is an important feature of Soffid IAM, allowing companies to simplify and improve identity and access management, ensuring that users have the right permissions to perform their tasks and limiting access to unnecessary resources.

Workflow engine

Workflow engine is key to Soffid IAM because enables enterprises to automate business and identity and access management processes, improve efficiency and accuracy, meet audit and compliance requirements, and ensures transparency and collaboration throughout processes.

User Provisioning

An essential piece of Soffid IAM that enables enterprises to automate the creation, update and deletion of user accounts, access resources across multiple systems and applications, improve efficiency and accuracy, reduce errors and costs associated with manual user account management, and improve security and operational efficiency.

Privileged Accounts

They are a critical aspect of information security in organizations and Soffid IAM solution includes secure and robust privileged account management. The solution enables centralized management of privileged accounts across multiple systems and applications, implementation of specific security policies and monitoring of privileged account usage.

1.4 TOE Description

This section describes the evaluated TOE components, the configurations and the environment needed for the tests. This includes the logical and physical boundaries of the TOE.

1.4.1 Evaluated Components of the TOE

The TOE is a software application which is made of different components that interact among them to bring application functionalities together. These components, with the versions used in the evaluation, are:

Component	Version
IAM-console	3.5.57
Sync-server	3.5.22
PAM-launcher	1.4.36
PAM-store	1.4.36
soffid-pasr-ssh	1.4.12
soffid-pasr-rdp	1.4.12
soffid-pasr-jdbc	1.4.12

Table 1: Toe components and versions

These components are configured following the guidance documentation [PES-SOFFID].

1.4.2 Physical Boundary

The physical boundary of the TOE does not include the application server software Apache TomEE, the Operating System (OS), or any other third-party software which is required for the TOE to run. Even though these components are not under the scope of the TOE, the TOE requires the following components, and their corresponding versions, to be installed:

Component	Solution
Server OS	CentOS Stream 9
Container software	Docker Engine: V:23.0.1
Application Server	Apache Tomcat V:8.5.41
Soffid Repository	MariaDB V:11.1.2
Firefox Browser	Firefox V:131.0.2

Table 2: Third-party software and versions used on evaluation

The following systems and versions have been used as external agents:

- Linux server: Ubuntu 23.04
- Active Directory: Windows server 2019 standard
- Windows server: Windows 10 PRO 10.0.19045
- Database administrador client: DBeaver 22.3.0
- MySQL server: MariabDB 10.11.2
- Linux SSH connection: Remmina 1.4.25
- Windows remote desktop: Xfreerdp 2.6.1
- Browser: Firefox V:131.0.2

1.4.2.1 Hardware Specifications

The hardware layer (outside of the TOE) that has been used for the evaluation of the TOE has the following specifications:

Hardware Component	Specification
CPU	2 CPUs
RAM	16 GB
Data storage	250 Gb

Table 3: Hardware specifications used on evaluation

1.4.3 Logical Boundaries

The logical TOE boundary is composed by the following TOE Security Functions:

- Enterprise Security Management
- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF

- TOE Access
- Trusted Path/Channels

1.4.3.1 Enterprise Security Management

The TOE provides the ability to authenticate and identify users using their own internal authentication mechanism. The TOE also has the ability to securely import already existing user´s authentication information, together with their attributes and configuration, from an Active Directory into the Soffid Repository. The TOE has the ability to securely manage user's attributes and functions within the system.

The TOE provides the functionality of defining a password policy that complies with the security requirements of the TSF.

1.4.3.2 Security Audit

The TOE generates logs of every action performed by the users within the application. These logs record every configuration or changes that are made. The TOE also generates logs of all the remote connections sessions. These logs are stored according to the action that is being documented. On the one hand, configurations and events related to the docker containers and sessions from PAM Access record screen capture and keystrokes are stored inside the corresponding docker volume. On the other hand, rest of actions are stored inside the local database, which in the TOE architecture is represented by the Soffid Repository component.

1.4.3.3 Cryptographic Support

The TOE ensures secure communications in support of TLS and HTTPS communications. The TOE ensures the communication between the components is secure and complies with the minimum standards established in [CCN-STIC-807]. Trust needed to enforce secure and private communications stems from Certification Authority (CA) acting as a trusted third party.

1.4.3.4 Identification and Authentication

The TOE guarantees the association of each user with the role associated to the corresponding account. When a user authenticates to the TOE, this user is given the corresponding abilities depending on their account's role. The three roles defined in the TOE are: Administrative Users, Basic Users and PAM Access. The Administrator User role grants the user full authority to manage and modify all functionalities and security attributes of the system. The Basic User role, on the other hand, is assigned to users without any privileged permissions, allowing them to access their own information and linked accounts in the console, as well as modify their password. Additionally, PAM Access can be granted to Basic Users, providing them with the capability to access a specific remote system through the PAM process; however, this access is optional and may not be given to all Basic Users.

The TOE provides mechanisms to prevent the possibility of unauthorized access to an account. The credentials associated with an account are stored locally and properly hashed. The TOE also provides the ability to configure the maximum number of authentication attempts and secure policies for the establishment of the password quality.

1.4.3.5 Security Management

The TOE is managed by authorized administrator through a web GUI, which in the TOE architecture is represented by Console component. The TOE uses a role-based access control policy, where the actions a user can do are defined after the user is authenticated in the system and the role for this user is determined. Administrative users have the ability to make all the security management decisions within the TOE.

1.4.3.6 Protection of the TSF

The TOE hashes all passwords and user's credentials before they are stored inside the Soffid Repository. The TOE does not offer any mechanism to disclose the plain text stored credential. The Soffid Repository is created in an individual container.

1.4.3.7 TOE Access

The user can terminate their own session at any moment by login out of the user account.

The TOE can be configured to display an informative banner, this banner will be displayed before allowing any user to authenticate into the TOE.

1.4.3.8 Trusted Path/Channels

The TOE provides a secure communication among the containers where each of the components are hosted using HTTPS and TLS.

When a communication is established between the TOE and an external agent located out of the TOE´s evaluation scope, that connection needs to be secured, following the necessary procedures to protect it. There are four different types of remote access connections with external agents: 1) Connection with a Windows system is done through the RDP windows protocol, 2) connection with a Linux system is done using SSH, 3) connection with a database is done using JDBC and 4) communication with Active Directory is done using LDAPS. External agents need to be configured according to their respective security requirements, so when the TOE connect with them, that communication is properly protected.

1.5 TOE Architecture

Figure 1 displayed below, is an illustrated representation of the TOE architecture. The figure shows that the TOE is composed of several internal components that interact among themselves to ensure that TOE´s expected functionalities can be performed accordingly.

On the one hand, there are five internal components interacting among themselves using secure channels:

- Console: A simple and fully intuitive web interface that provides the Administrator User with complete access to all system functions remotely, across all platforms, without requiring any programming knowledge. Meanwhile, it enables the Basic User to access and manage their information and tasks relevant to their role.

- Sync server: Contains all the management logic of the external systems, synchronizing the information in the Soffid Repository with the information in the Active Directory and the user information in the external Windows and Linux agents.
- Soffid Repository: Represents a local database where the information related to identities, user accounts, passwords and configuration is stored. For the evaluated configuration it is used MariaDB as Relational DataBase Management System but, as indicated previously, it is not under the scope of the TOE.
- PAM Store: Contains the auditing information from sessions performed through the PAM Jump Server. The sessions logs include video recording and keystrokes. All information is stored protected by encryption.
- PAM Jump server: Allows user access to critical systems. On the one hand, it provides a HTTPS interface to the VNC server in the Temporary Containers, and on the other hand, it records video and keyboard.
- Temporary containers: Is a template container featuring a server that the PAM Jump Server connects to. This temporary container then connects to the remote systems securely. There is one variant of temporary container for each remote system type: rdp, ssh and jdbc.

All these previous components are built on their individual docker containers and they are connected within the same network using HTTPS and JDBC (TLS).

On the other hand, there are five external systems, not under the scope of the TOE, connected to different components of the TOE through secure connections. Every connection with a component of the TOE represents a functionality is in the scope of the TOE. There are four types of connections between the internal components and external systems:

- The LDAPS management connection: This connection is done to import users and accounts from the Active Directory into the TOE.

- The SSH connection: This connection is used to establish a secure remote session with an external Linux server through PAM using SSH. This connection is done using Remmina client.
- The RDP connection: This connection is used to establish a secure remote session with an external Windows server through PAM using RDP with TLS. This connection is done using XFreeRDP client.
- The JDBC connection: There are two connections. The first connection is used to establish a secure remote session with an external MySQL server through PAM using JDBC with TLS. This connection is done using a DBeaver client which acts as a database administrator. The second connection is used to connect the internal components with the Soffid Repository. It also uses JDBC with TLS and is developed within the internal components.

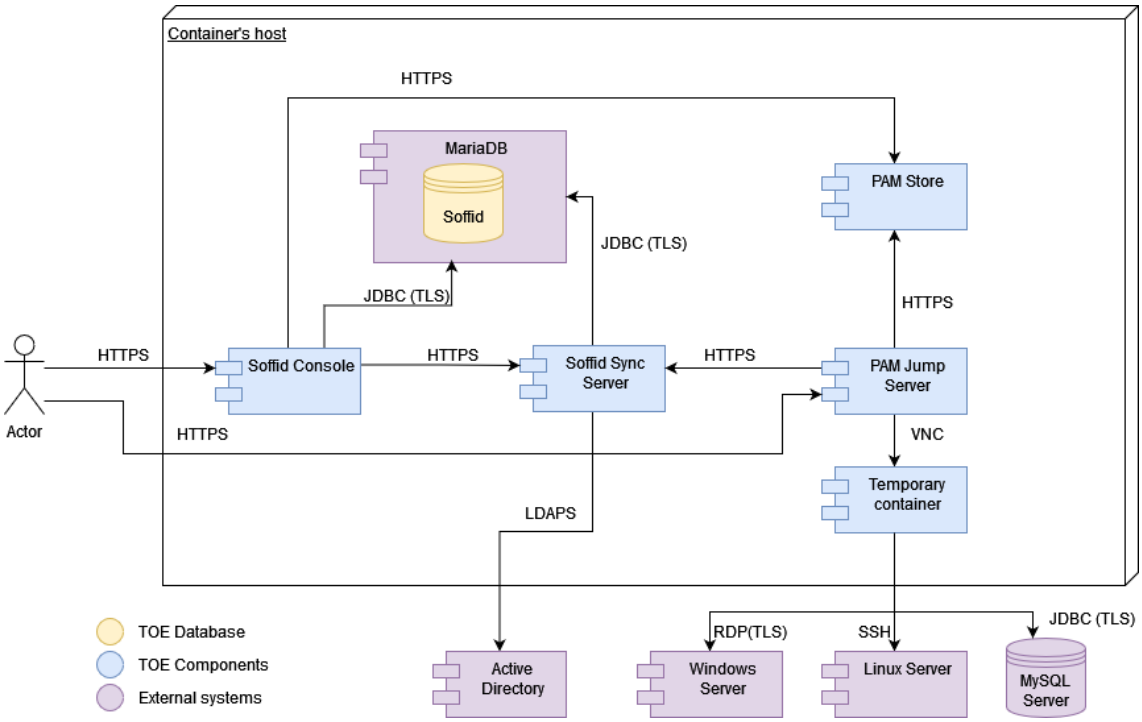

Figure 1: TOE Architecture

2 Conformance Claims

2.1 Common criteria Conformance Claim

This Security Target [ST] and the Target of Evaluation [TOE] are conformant to the following Common Criteria [CC] specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Conformant

2.2 Protection Profile Conformance Claim

The TOE for this ST does not claim conformance with any Protection Profile (PP).

2.3 Package Conformance Claim

This ST claims conformance with the following assurance package:

- Evaluation assurance level 2 (EAL2) — structurally tested. -Conformant

2.4 Conformance Rationale

This ST claims conformance to the assurance package Evaluation assurance level 2 (EAL2) — structurally tested.

The security assurance requirements of this ST are identical to those in the assurance package.

3 Security Problem Definition

3.1 Threats

This section identifies the possible threats that can be confronted by the TOE. The ones shown below have been taken from the [ICM PP].

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FALSIFY	A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment
T.FORGE	A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.
T. INSUFFATR	An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.RAWCRED	A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.

Threat Name	Threat Definition
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

Table 4: TOE Threats

3.2 Organizational Security Policies

This section identifies the OSPs which are expected to be implemented by the organization that deploys the TOE. These policies have been taken from the [ICM PP].

Policy	Policy Definition
P.BANNER	The TOE displays an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

Table 5: Organizational Security Policies

3.3 Assumptions

This section covers the assumptions applied to the TOE. These assumptions have been taken from the PP.

Assumption Name	Assumption Definition
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.FEDERATE	Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.
A.ENROLLMENT	There will be a defined enrolment process that confirms user identity before the assignment of credentials.
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment.
A.TRUSTED_ADMIN	The TOE administrator is considered competent, well-trained, and non-hostile.

Table 6: TOE Assumptions

4 Security Objectives

This chapter defines the security objectives for the TOE and the operational environment. These objectives have been extracted from the [ICM PP].

4.1 Security Objectives for the TOE

This section covers the security objectives established in the [ICM PP] for the TOE.

Objective	TOE Security Objective Definition
O.ACCESSID	The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.EXPORT	The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels
O.IDENT	The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.
O.INTEGRITY	The TOE will provide the ability to assert the integrity of identity, credential, or authorization data
O.MANAGE	The TOE will provide Assignment Managers with the capability to manage the TSF.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities

Objective	TOE Security Objective Definition
O.PROTECTED	The TOE will be able to protect stored credentials.
O.ROBUST	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment

Table 7: TOE Security Objectives

4.2 Security Objectives for the Operational Environment

This section identifies the security objectives established in the [ICM PP] for the operational environment.

Objective	Environmental Security Objective Definition
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic mechanisms that are used to ensure the confidentiality and integrity of communications
OE.ENROLLMENT	The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.
OE.FEDERATE	Data the TOE exchanges with trusted external entities is trusted.
OE.INSTALL	Those responsible for the TOE ensures that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security

Objective	Environmental Security Objective Definition
OE.PERSON	Personnel working as TOE administrators are carefully selected and trained for proper operation of the TOE.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.

Table 8: Security Objectives of the Operational Enviroments

4.3 Security Objectives Rationale

The assumptions, threats, OSPs, and objectives that are defined in this ST represent the assumptions, threats, OSPs, and objectives that are specified in the [ICM PP] to which the Security Target is based on. The associated mappings of assumptions to environmental objectives, SFRs to TOE objectives, and OSPs and objectives to threats are therefore identical to the mappings that are specified in said Protection Profile.

5 Extended Components Definition

Since this ST based on [ICM PP], the definition of functional classes is the same as in [ICM PP]. Likewise, family behavior, components leveling, management and audit from functional families are the same as in [ICM PP].

5.1 Extended Security Functional Requirements

5.1.1 ESM_EAU Enterprise Authentication

5.1.1.1 ESM_EAU.2 Reliance on Enterprise Authentication

Hierarchical to:	No other components.
Dependencies:	ESM_EID.2 Reliance on Enterprise Identification
ESM_EAU.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject authentication***], [***assignment: identified Operational Environment component(s) responsible for subject authentication***]] for subject authentication.
ESM_EAU.2.2	The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

5.1.2 ESM_EID Enterprise Identification

5.1.2.1 ESM_EID.2 Reliance on Enterprise Identification

Hierarchical to:	No other components.
Dependencies:	No dependencies.
ESM_EID.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject identification***], [***assignment: identified Operational Environment component(s) responsible for subject identification]***] for subject identification.

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

5.1.3 ESM_ICD Identity and Credential Definition

5.1.3.1 ESM_ICD.1 Identity and Credential Definition

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_ICD.1.1 The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2 The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, [***assignment: list of any additional security-relevant identity and credential attributes the TSF is able to associate with enterprise users***].

ESM_ICD.1.3 The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4 The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5 The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8 The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

a) For password-based credentials, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: [***assignment: list of character sets that are supported by the TSF for password entry***] that include the following values [***assignment: list of the supported characters for each supported character set***]; and
2. Minimum password length shall be settable by an administrator, and support passwords of 15 characters or greater; and
3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and
4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

5.1.4 ESM_ICT Identity and Credential Transmission

5.1.4.1 ESM_ICT.1 Identity and Credential Transmission

Hierarchical to:	No other components.
Dependencies:	ESM_ICD.1 Identity and Credential Definition

ESM_ICT.1.1	The TSF shall transmit [selection: “identity and credential data”, “identity, credential, and object attribute data”] to compatible and authorized Enterprise Security Management products under the following circumstances: [selection: choose one or more of: immediately following creation or modification of data, at a periodic interval, at the request of the product, [***assignment: other circumstances***]].

5.1.5 ESM_MPA_EXT Minimum Privileged Access

5.1.5.1 ESM_MPA_EXT.1 Minimum privileged access

Hierarchical to:	No other components.
Dependencies:	No other components.
ESM_MPA_EXT.1.1	The product shall have the ability to establish the privileged sessions with the managed IT resource on behalf of the user, so that the user does not know the privileged credentials for accessing the resource at any time.

5.1.6 FAU_STG_EXT External Audit Trail Storage

5.1.6.1 FAU_STG_EXT.1 External Audit Trail Storage

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit Data Generation FTP_ITC.1 Inter-TSF Trusted Channel
FAU_STG_EXT.1.1	The TSF shall be able to transmit the generated audit data to **[assignment: non-empty list of external IT entities and/or “TOE-internal storage”]**.
FAU_STG_EXT.1.2	The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3	The TSF shall ensure that any TOE-internal storage of generated audit data: 1) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and 2) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

5.1.7 FPT_APW_EXT Protection of Stored Credentials

5.1.7.1 FPT_APW_EXT.1 Protection of Stored Credentials

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_APW_EXT.1.1	The TSF shall store credentials in non-plaintext form.
FPT_APW_EXT.1.2	The TSF shall prevent the reading of plaintext credentials.

5.1.8 FPT_SKP_EXT Protection of Secret Key Parameters

5.1.8.1 FPT_SKP_EXT.1 Protection of Secret Key Parameters

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.9 FTA_SSL_EXT Session Locking and Termination

5.1.9.1 FTA_SSL_EXT.1 Session Locking and Termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL_EXT.1.1	The TSF shall, for local interactive sessions, [selection: • lock the session – clear or overwrite display devices, making the current contents unreadable, disable any activity of the user's data access/display devices other than unlocking the

session, and require that the user re-authenticate to the TSF prior to unlocking the session;

- terminate the session

] after an authorized administrator specified time period of inactivity.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This PP will highlight the four operations in the following manner:

- Assignment: allows the specification of an identified parameter. Indicated with bold and italicized text inside square brackets that contain the prompt "assignment:" if further operations are necessary by the Security Target author;
- Refinement: allows the addition of details. Indicated with italicized text. An SFR with a refinement is also preceded with "Refinement:" unless it is only an editorial refinement (i.e. only functional refinements are labeled in this way).
- Selection: allows the specification of one or more elements from a list. Indicated with underlined text inside square brackets that contain the prompt "selection:"
- Iteration: allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR.

For requirements taken from CC part 2 where selections and assignments have already been completed to ensure they apply to the PP, the conventions used are identical to the normal operations except that the "selection:" and "assignment:" prompts are not present.

6.2 Security Functional Requirements

The security functional requirements claimed by the TOE are:

Requirement Class	Component Identification	Component Name
ESM: Enterprise Security	ESM_EAU.2	Reliance on Enterprise Authentication

Requirement Class	Component Identification	Component Name
Management	ESM_EID.2	Reliance on Enterprise Identification
	ESM_ICD.1	Identity and Credential Definition
	ESM_ICT.1	Identity and Credential Transmission
	ESM_MPA_EXT.1	Minimum privileged access
FAU: Security audit	FAU_GEN.1	Audit Data Generation
	FAU_STG_EXT.1	TOE-internal Audit Trail Storage
FIA: Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_SOS.1	Verification of Secrets
	FIA_USB.1	User-Subject Binding
FMT: Security Management	FMT_MOF.1	Management of Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Management Roles
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Stored Credentials
	FPT_SKP_EXT.1	Protection of Secret Key Parameters
FTA: TOE access	FTA_SSL_EXT.1	TSF-initiated Session Locking

Requirement Class	Component Identification	Component Name
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	TOE Access Banner
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

Table 9: TOE Security Functional Requirements

The *refinements* in some of the SFRs are drawn from [ICM PP].

6.2.1 ESM_EAU.2 Reliance on Enterprise Authentication

ESM_EAU.2.1 The TSF relies on **[Soffid internal mechanism]** for subject authentication.

ESM_EAU.2.2 The TSF requires each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.2.2 ESM_EID.2 Reliance on Enterprise Identification

ESM_EID.2.1 The TSF relies on **[Soffid internal mechanism]** for subject identification.

ESM_EID.2.2 The TSF requires each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

6.2.3 ESM_ICD.1 Identity and Credential Definition

ESM_ICD.1.1 The TSF provides the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2 The TSF defines the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, **[user id, user password and user role]**.

ESM_ICD.1.3 The TSF provides the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4 The TSF provides the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5 The TSF provides the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF provides the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF provides the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8 The TSF ensures that the defined enterprise user credentials satisfy the following strength rules:

a) For password-based credentials, the following rules

apply:

1. Passwords shall be able to be composed of a subset of the following character sets: **[English character set]** that include the following values **[26 uppercase letters, 26 lowercase letters, 10 numbers, and the following 10 special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"]**; and
2. Minimum password length is settable by an administrator, and support passwords of 15 characters or greater; and
3. Password composition rules specifying the types and numbers of required characters that comprise the password is settable by an administrator; and
4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user.

b) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}

6.2.4 ESM_ICT.1 Identity and Credential Transmission

ESM_ICT.1.1 The TSF transmits [**identity and credential data**] to compatible and authorized Enterprise Security Management products under the following circumstances: [**immediately following creation or modification of data, at a periodic interval, at the request of the product]**,

6.2.5 ESM_MPA_EXT.1 Minimum Privileged Access

ESM_MPA_EXT.1.1 The product shall have the ability to establish and maintain the privileged sessions with the managed IT resource on behalf of the user, so that the user does not know the privileged credentials for accessing the resource at any time.

6.2.6 FAU_GEN.1 Audit Data Generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events identified in Table 10 for the **[not specified]** level of audit;

c) **[no other auditable events]**.

Component	Event	Additional Information
ESM_EAU.2	All use of the authentication mechanism	None
ESM_ICD.1	Creation or modification of identity and credential data	The attribute(s) modified
ESM_ICD.1	Enrollment or modification of	The subject created or modified,

Component	Event	Additional Information
	subject	the attribute(s) modified (if applicable)
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted
ESM_MPA_EXT.1	Session establishment and session activities.	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of TOE-internal audit server
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, theactions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached
FIA_SOS.1	Rejection or acceptance by the TSFof any tested secret	None
FIA_SOS.1	Identification of any changes to thedefined quality metrics	The change made to the quality metric
FIA_USB.1	User-Subject Binding	None
FMT_MOF.1	All modifications of TSF functionbehavior	None
FMT_MTD.1	Management of TSF Data	None
FMT_SMF.1	Use of the management functions	Management function performed
FMT_SMR.1	Security Management Roles	None
FTA_SSL_EXT.1	All session locking and unlockingevents	None
FTA_SSL.3	All session termination events	None
FTA_SSL.4	All session termination events	None
FTP_ITC.1	All use of trusted channel	Identity of the initiator and target of thetrusted channel

Component	Event	Additional Information
	functions	
FTP_TRP.1	All attempted uses of the trustedpath functions	Identification of user associated with alltrusted path functions, if available

Table 10: Auditable Events

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

a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, **[no other audit relevant information]**.

6.2.7 FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [***"TOE-internal storage"***].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

1) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

2) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

6.2.8 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **[3]** unsuccessful authentication attempts occur related to **[authentication of the GUI]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[surpassed]**, the TSF shall **[lock the account].**

6.2.9 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[the following:**

1. **Passwords shall be able to be composed of a subset of the following character sets: [upper case letters, lower case letters, numbers, and special characters] that include the following values: [A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z 1 2 3 4 5 6 7 8 9 0 ! @ # $ % ^ & * ( )]; and**
2. **Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and**
3. **Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and**
4. **Passwords shall have a maximum lifetime, configurable by an administrator; and**
5. **New passwords shall contain a minimum of an administrator-specified number of character changes from the previous password; and**
6. **Passwords shall not be reused within the last administrator-settable number of passwords used by that user.]**

6.2.10 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: **[user id, user password and user group]**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**the association of security attributes is done when the session is started and is linked to the user's identity**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users: [**the changes in security attributes are reflected immediately**].

6.2.11 FMT_MOF.1 Management of Functions Behavior

FMT_MOF_1.1 The TSF shall restrict the ability to **[determine the behavior of, disable, enable, modify the behavior of]** the functions: **[list of functions in Table 11]** to **[the administrator users in Table 11].**

Requirement	Management functions	Operation
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Determine/modify the behavior of
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Determine/modify the behavior of
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	Determine/modify the behaviour of: Full control over establishment, removal etc.. of enterprise user's (maintained in the TOE) and their credentials

Requirement	Management functions	Operation
		including the ability to activate (or define a user) and assign users to roles.
		Enable, Disable, Modify the behavior of the password management function
ESM_ICD.1	Management of credential status	Modify the behavior of
ESM_ICD.1	Enrollment of users into repository.	Determine the behavior of
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data is performed	Determine/modify the behavior of Enable/Disable
ESM_MPA_EXT.1	Management the establishment of the privileged session with the IT resource on behalf of the user	Determine/modify the behavior of
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts. Management of actions to be taken in the event of an authentication failure	Determine/modify the behavior of
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	Determine/modify the behavior of
FMT_MOF.1	Management of sets of users that can interact with security functions	Determine/modify the behavior of
FMT_SMR.1	Management of the users that belong to a particular role.	Determine/modify the behavior of
FTA_SSL_EXT.1	Configuration of the inactivity period for session termination	Determine/modify the behavior of
FTA_SSL.3	Configuration of the inactivity period for session termination	Determine/modify the behavior of

Requirement	Management functions	Operation
FTA_TAB.1	Maintenance of the banner	Enable/Disable the banner including the message that will be displayed
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	Enable/Disable
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	Enable/Disable

Table 11: Administrator Management of Functions

6.2.12 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [**change_default, query, modify, delete**] the **[username, password, role]** to **[administrators]**.

6.2.13 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[the management functions identified in Table 11].**

6.2.14 FMT_SMR.1 Security Management Roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrator, Basic User and PAM Access**]

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

6.2.15 FPT_APW_EXT.1 Protection of Stored Credentials

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

6.2.16 FPT_SKP_EXT.1 Protection of Secret Key Parameters

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.2.17 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, **[terminate the session]** after an authorized administrator specific time period of inactivity.

6.2.18 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after **[2 minutes]** of inactivity.

6.2.19 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

6.2.20 FTA_TAB.1 TOE Access Banner

FTA_TAB.1.1 *Refinement:* Before establishing a user session, the TSF shall display a *configurable* advisory warning message regarding unauthorized use of the TOE.

6.2.21 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 *Refinement:* The TSF shall *use* **[TLS]** *to* provide a *trusted* communication channel between itself and *authorized IT entities* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

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

FTP_ITC.1.3 *Refinement:* The TSF shall initiate communication via the trusted channel for *transfer of policy data*, **[audit data, user authentication]**.

6.2.22 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 *Refinement:* The TSF shall *use* **[TLS]** *to* provide a communication path between itself and **[remote]** users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from **[modification, disclosure]**.

FTP_TRP.1.2 The TSF shall permit **[remote users]** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *initial user authentication, execution of management functions*.

6.3 Security Assurance Requirements

The TOE assurance requirements for the ST must be in accordance with the EAL2 level. The following table describes the assurance requirements.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: ST evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements

Assurance class	Assurance components
	ASE_SPD.1 Security problem
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 12: Security Assurance Requirements

6.3.1 ADV_ARC.1 Security Architecture Description

6.3.1.1 Developer action elements

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

6.3.1.2 Content and presentation elements

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

6.3.1.3 Evaluator action elements

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.2 ADV_FSP.2 Security-enforcing Functional Specification

6.3.2.1 Developer action elements

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

6.3.2.2 Content and presentation elements

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

6.3.2.3 Evaluator action elements

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.3.3 ADV_TDS.1 Basic Design

6.3.3.1 Developer action elements

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

6.3.3.2 Content and presentation elements

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall provide the behaviour summary of each SFR-supporting or SFR-non-interfering TSF subsystem.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

6.3.3.3 Evaluator action elements

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.3.4 AGD_OPE.1 Operational User Guidance

6.3.4.1 Developer action elements

AGD_OPE.1.1D The developer shall provide operational user guidance.

6.3.4.2 Content and presentation elements

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security controls to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

6.3.4.3 Evaluator action elements

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5 AGD_PRE.1 Preparative Procedures

6.3.5.1 Developer action elements

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

6.3.5.2 Content and presentation elements

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

6.3.5.3 Evaluator action elements

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.3.6 ALC_CMC.2 Use of a CM System

6.3.6.1 Developer action elements

ALC_CMC.2.1D The developer shall provide the TOE and a unique reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

6.3.6.2 Content and presentation elements

ALC_CMC.2.1C The TOE shall be labelled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

6.3.6.3 Evaluator action elements

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

6.3.7 ALC_CMS.2 Parts of the TOE CM Coverage

6.3.7.1 Developer action elements

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

6.3.7.2 Content and presentation elements

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

6.3.7.3 Evaluator action elements

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.8 ALC_DEL.1 Delivery Procedures

6.3.8.1 Developer action elements

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

6.3.8.2 Content and presentation elements

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

6.3.8.3 Evaluator action elements

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.9 ASE_CCL.1 Conformance Claims

6.3.9.1 Developer action elements

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

6.3.9.2 Content and presentation elements

ASE_CCL.1.1C The conformance claim shall identify the edition of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The conformance claim shall describe the conformance of the ST as either “CC Part 3 conformant” or “CC Part 3 extended”.

ASE_CCL.1.4C The conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify a PP-Configuration, or all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim shall describe any conformance of the ST to a PP as PP-Conformant.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PP-Configuration or PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PP-Configuration, PPs and any functional packages for which conformance is being claimed.
ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PP-Configuration, PPs, and any functional package for which conformance is being claimed.
ASE_CCL.1.11C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PP-Configuration, PPs, and any functional packages for which conformance is being claimed.
ASE_CCL.1.12C	The conformance claim for PP(s) or a PP-Configuration shall be exact, strict, or demonstrable or a list of conformance types.
ASE_CCL.1.13C	If the conformance claim identifies a set of Evaluation methods and Evaluation activities derived from CEM work units that shall be used to evaluate the TOE then this set shall include all those that

are included in any package, PP, or PP-Module in a PP-Configuration to which the ST claims conformance, and no others.

6.3.9.3 Evaluator action elements

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.10ASE_ECD.1 Extended Components Definition

6.3.10.1 Developer action elements

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

6.3.10.2 Content and presentation elements

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements may be demonstrated.

6.3.10.3 Evaluator action elements

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component may be clearly expressed using existing components.

6.3.11 ASE_INT.1 ST Introduction

6.3.11.1 Developer action elements

ASE_INT.1.1D The developer shall provide an ST introduction.

6.3.11.2 Content and presentation elements

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C For a multi-assurance ST, the TOE overview shall describe the TSF organization in terms of the sub-TSFs defined in the PP-Configuration the ST claims conformance to.

ASE_INT.1.8C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.9C The TOE description shall describe the logical scope of the TOE.

6.3.11.3 Evaluator action elements

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

6.3.12 ASE_OBJ.2 Security Objectives

6.3.12.1 Developer action elements

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

6.3.12.2 Content and presentation elements

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

6.3.12.3 Evaluator action elements

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.13 ASE_REQ.2 Derived Security Requirements

6.3.13.1 Developer action elements

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

6.3.13.2 Content and presentation elements

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C For a single-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE. The sets of SARs shall be consistent with the PPs or PP-Configuration to which the ST claims conformance.

ASE_REQ.2.3C For a multi-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE and the sets of SARs that apply to each sub-TSF. The sets of SARs shall be consistent with the multi-assurance PP-Configuration to which the ST claims conformance.

ASE_REQ.2.4C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.5C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.6C All operations shall be performed correctly.

ASE_REQ.2.7C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

SE_REQ.2.8C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.9C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.10C The statement of security requirements shall be internally consistent.

ASE_REQ.2.11C If the ST defines sets of SARs that expand the sets of SARs of the PPs or PP-Configuration it claims conformance to, the security requirements rationale shall include an assurance rationale that justifies the consistency of the extension and provides a rationale for the disposition of any Evaluation methods and Evaluation activities identified in the conformance statement that are affected by the extension of the sets of SARs.

6.3.13.3 Evaluator action elements

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.14 ASE_SPD.1 Security Problem

6.3.14.1 Developer action elements

ASE_SPD.1.1D The developer shall provide a security problem definition.

6.3.14.2 Content and presentation elements

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

6.3.14.3 Evaluator action elements

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.15 ASE_TSS.1 TOE Summary Specification

6.3.15.1 Developer action elements

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

6.3.15.2 Content and presentation elements

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

6.3.15.3 Evaluator action elements

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.3.16 ATE_COV.1 Evidence of Coverage

6.3.16.1 Developer action elements

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

6.3.16.2 Content and presentation elements

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

6.3.16.3 Evaluator action elements

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.17ATE_FUN.1 Functional Testing

6.3.17.1 Developer action elements

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

6.3.17.2 Content and presentation elements

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

6.3.17.3 Evaluator action elements

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.18ATE_IND.2 Independent Testing – Sample

6.3.18.1 Developer action elements

ATE_IND.2.1D The developer shall provide the TOE for testing.

6.3.18.2 Content and presentation elements

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

6.3.18.3 Evaluator action elements

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.3.19 AVA_VAN.2 Vulnerability Analysis

6.3.19.1 Developer action elements

AVA_VAN.2.1D The developer shall provide the TOE for testing.

AVA_VAN.2.2D The developer shall provide a list of third party components included in the TOE and the TOE delivery.

6.3.19.2 Content and presentation elements

AVA_VAN.2.1C The TOE shall be suitable for testing.

AVA_VAN.2.2C The list of third party components shall include components provided by third parties, and that are part of the TOE or otherwise part of the TOE delivery.

6.3.19.3 Evaluator action elements

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE the components in the list of third party components, and specific IT products in the environment that the TOE depends on.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional

specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.4 Security Requirements Rationale

The Security Requirements in this ST are drawn from those in the PP this ST is based on. An additional requirement ESM_MPA_EXT has been added to denote the Privileged Access Management (PAM) capabilities of the TOE and to comply with [CCN-STIC-140-A6]. Additionally, the requirement FAU_STG_EXT.1.2 has been deleted because the TOE does not store audit data to any external IT entity.

The selected SAR package EAL2 is selected to fulfil the assurance level required by [CCN-STIC-140-A7].

The following table presents a mapping of TOE Security Functional Requirements to Objectives. The selected Security Functional Requirements are considered sufficient and required as they have been copied from the Protection Profile this ST is based on.

Objective	SFR
O.ACCESSID	FTP_ITC.1
O.AUDIT	FAU_GEN.1 FAU_STG_EXT.1
O.AUTH	ESM_EAU.2 ESM_EID.2 FIA_USB.1 FMT_SMR.1 FTP_TRP.1
O.BANNER	FTA_TAB.1

Objective	SFR
O.EXPORT	ESM_ICD.1 ESM_ICT.1
O.IDENT	ESM_ICD.1 ESM_ICT.1
O.INTEGRITY	FTP_ITC.1
O.MANAGE	ESM_EAU.2 ESM_EID.2 FIA_USB.1 FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FTP_TRP.1
O.PROTCOMMS	FPT_SKP_EXT.1 FTP_ITC.1 FTP_TRP.1
O.PROTCRED	FPT_APW_EXT.1 ESM_MPA_EXT.1
O.ROBUST	FIA_AFL.1 FIA_SOS.1 FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4 FTA_TSE.1
O.SELFID	ESM_EID.2 FTP_ITC.1

Table 13: Mapping of objectives to SFRs

7 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR.

7.1 Enterprise Security Management (ESM)

7.1.1 ESM_EAU.2, ESM_EID.2

The TOE requires the users to properly authenticate with valid credentials before any management actions can be done in the TOE. To do so, users interact with the Console component, the users need to enter a valid username and password, these credentials are checked locally against Soffid Repository (where the credentials are stored hashed). The component inside the TOE that is responsible for authenticating TOE users is the Console component which is in charge of validating user's credentials. The Console communicates with Soffid Repository using the JDBC API, which is securely protected with TLS.

7.1.2 ESM_ICD.1

The TOE has the ability to configure and store credential attributes for the different users inside the system. These attributes are what enable users to perform different actions inside the TOE's scope of actions. The different actions users can make, are determined by the attributes defined in the different roles that are created and assigned to users inside the system. The TOE first user, when the system is first deployed, is an administrative user. This user has the ability to create new users or import different users from an external agent into Soffid Repository. This administrative user will be responsible for the creation of the roles, each of these roles could later be associated with each of the users. The three by-default roles and their attributes are:

- Administrative role: This role will give permissions to access and manage all the functionalities of the system, these management functions are defined in Table 11. Administrative User is in charge of establishing the initial password for other users, passwords must comply with the password policy established. The

password policy that will be applied to every password-based credential account from an external agent linked is composed of the following rules: 26 uppercase letters, 26 lowercase letters, 10 numbers, and the following 10 special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”; the minimum length of a password must be 15 characters; the password must be composed of a mix of lowercase letters, uppercase letters, numbers and special characters; password cannot not be reused for at least the last 10 passwords history.

- Basic User role: This role is assigned to users without any privileged permissions. It allows users to access their own information and linked accounts in the console, as well as modify their password.
- Access PAM: This role can be assigned to Basic Users, enabling them to access specific remote systems through the PAM process.

These roles can be given to any user that is created inside the system, and they will define the user’s identity and credential attributes.

Users can be created in the system in two different ways, the first way is manually by administrative user. This administrative user will determine the new user’s security relevant identity and credential attributes.

The second way for user creation is by importing already created users from an external Active Directory agent, this agent communicates with the TOE and transmits the accounts into the TOE’s user’s database. The accounts within this agent are transmitted securely to the TOE using LDAPS to synchronize with the TOE and JDBC to send the accounts information into the TOE’s database where they are stored. The JDBC API uses TLS to make the communication secure, once these accounts are transmitted, they are linked to the corresponding user inside the Soffid’s users list, if the account that is imported from the agent doesn´t have a user inside the TOE users list, a new user will be created by the administrator to link the account to. From the Active Directory agent, the following data is imported: username id, user password and roles. These users will then have linked

accounts with the different agents connected to the TOE. Each of the users inside the TOE will be uniquely identified by the user id.

7.1.3 ESM_ICT.1

The TOE communicates with Soffid Repository for transmitting credential identity attribute data. This communication uses the JDBC API which ensures the safe transmission of data using TLS. When any identity or credential data of a user is modified inside the TOE, the changes are transmitted into the database. The transmission of identity and credential data between the TOE and an external agent such as Active Directory is done using LDAPS to synchronize the user data from the TOE with the external agent that is being imported.

7.1.4 ESM_MPA_EXT.1

The users that can access another device using the PAM process do not have knowledge of the privileged credentials of the administrative user of the system.

7.2 Security Audit

7.2.1 FAU_GEN.1

The TOE is able to generate an auditable record of the relevant events that occur. The auditable events are listed in Table 10. One of the most important features of the TOE is the storage of audit logs, in this way actions performed inside the TOE will be recorded. The most important actions that are recorded and stored are: the authentication of administrators into the TOE, the modification of attributes, the interaction with external third-party software, and remote connections with other devices. Activities performed outside the TOE but in use of the Privileged Access Management feature are also recorded and stored.

7.2.2 FAU_STG_EXT.1

The TOE stores audit data locally, each event will be stored, either inside the same container where the actions were performed, or inside Soffid Repository, if the actions performed are related to attributes or TOE`s configurations.

In Soffid Repository, all actions regarding the following data records are stored: creation of new users, assignment of permissions, integration of different agents, changes in the user's credentials, etc. The communication with the database is done using JDBC and the communication is secured with the use of TLS.

The recordings of PAM sessions are stored in PAM-store container. Those recordings are stored for 90 days by default configuration. The persistence of those recordings could be modified.

In the container's data store, the information recorded regards the depuration and management of the containerized systems.

All the audited data stored is protected and can only be accessed by Administrator Users. These administrative users can access the logs that have been stored from the Console component, this component also has a functionality that allows the Administrative Users to search and consult specific logs.

The administrative user from the CentOS system can also access these logs by accessing the local directory of each container where the logs have been placed.

The administrative user from database can also access the database where these logs have been stored. This administrative user is the one that was used to create and configure the database at first instance.

7.3 Identification and Authentication

7.3.1 FIA_AFL.1

The TOE requires the user to authenticate before they can access any of the functionalities offered by the TOE. If an authentication is rejected repeatedly, the TOE implements a policy which establishes that the account will be blocked for some time before a new authentication attempt can be made. The configuration of the number of unsuccessful attempts and the time the account is blocked before a new attempt can be made, is determined by the administrator user from inside the password policy directory of the TOE. This configuration establishes that after 3 unsuccessful authentication

attempts, the user account that is trying to be accessed will be blocked for 20 seconds before new attempts can be performed.

7.3.2 FIA_SOS.1

The Administrator User is in charge of creating the following password policy that will be applied to every user inside the TOE: Passwords shall be composed of the following values:

- Passwords shall be composed of the following characters: 26 uppercase letters, 26 lowercase letters, 10 numbers, and the following 10 special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"
- The minimum length of a password must be 15 characters.
- The password must be composed of a mix of lowercase letters, uppercase letters, numbers, and special characters.
- Passwords cannot not be reused for at least the last 10 passwords history; passwords will expire in 30 days.

For authenticating against the PAM store component, a password is automatically created by securely generating 48 random bytes and encoding them using base64. Even though that violates the aforementioned password policy, as it doesn't ensure one character from each group is present, the resulting password has a very large Shannon Entropy (384 bits[1]), and a greater one compared to the minimum Entropy accepted by the policy (93 bits[2]). Therefore, it is considered that the generated password is secure.

7.3.3 FIA_USB.1

The TOE associates user's security attributes with the subjects acting on her behalf. The roles and the security attributes linked to each role (Basic User or Administrator User) are

[1] $H = 48\ bytes \times 8\frac{bits}{byte} = 384\ bits$

[2] $H = log_2((26\ lowercase + 26\ uppercase + 10\ number + 10\ special\ characters)^{15\ characters\ long}) = 92.54\ bits$

determined by the Administrator User and assigned to each user manually through the Console GUI.

The initial association of users' security attributes with subjects acting on their behalf occurs only if the users have successfully authenticated to the TOE.

When a user's attributes change, the changes are reflected immediately: the new permissions apply from the moment the attributes are changed, including the ongoing user session, if any.

7.4 Security Management

7.4.1 FMT_MOF.1

The TOE only allows administrators to perform management functions. A user is an administrator if she successfully authenticates to the TOE and she possesses the Administrator User role.

7.4.2 FMT_MTD.1

The TOE stores authentication data in Soffid Repository, which is a database installed in a database manager in the operational environment. The TOE checks the users' permissions before accessing the database, and it only allows administrators to change default, query, modify or delete the username and password of other users.

7.4.3 FMT_SMF.1

The TOE implements the management functions defined in Table 11. The TSF acting on behalf of administrator users to perform Table 11 functionalities.

7.4.4 FMT_SMR.1

The TOE has three roles: Basic user, Administrator User and Access PAM. Upon authentication, the TSF associates the user with her role, which determines their accessibility to functionalities. These roles provide the following privileges:

- Administrator User: This role gives the user the ability to manage and modify all the functionalities and security attributes of the system.

- Basic User: This role is assigned to users without any privileged permissions. It allows users to access their own information and linked accounts in the console, as well as modify their password.
- PAM Access: This role can be assigned to Basic Users, enabling them to access specific remote systems through the PAM process.

7.5 Protection of the TSF

7.5.1 FPT_APW_EXT.1

The TOE protects credentials in a way that they are not accessible in plaintext. Instead, SHA256 hash values of passwords are stored. The passwords that need to be obscured in a reversible way are encrypted using RSAES-OAEP 3072.

7.5.2 FPT_SKP_EXT.1

The TOE certificates and associated private keys are protected. The public key used for encrypting the passwords is stored in the database and the corresponding private key is protected inside the keystore of the Sync Server. These keys are stored and can only be accessed by the keystore manager user.

7.6 TOE Access

7.6.1 FTA_SSL_EXT.1 / FTA_SSL.3

The TOE can be configured by an authorized administrative user to terminate an interactive session after a time period of inactivity. After the determined inactivity period, a message will be shown alerting that in 60 seconds the session will be terminated, and after those 60 seconds the session will be closed and terminated.

7.6.2 FTA_SSL.4

The TOE allows an administrator to terminate its own interactive session by logging out. Once terminated, the user must enter her credentials again to authenticate herself to the TOE and start a new session.

7.6.3 FTA_TAB.1

The TOE can be configured to display a warning banner with a message regarding the unauthorized use of the TOE before a session can be established through the Console GUI. The configuration of this warning message can only be done by administrators.

7.7 Trusted Path/Channels

7.7.1 FTP_ITC.1

The TOE provides trusted channels of communication between all the components that make up the system. All these components communicate inside a private virtual network. The components communicate between themselves and with the user through the Console component using HTTPS, TLS. The certificates that are used to ensure secure communications between components are provided by an external CA (Certificate Authority) that guarantees Certificates. The relation between components is the following:

- User -> Console: This is done via HTTPS connection.
- User -> IDP: This is done via HTTPS connection.
- User -> PAM Jump Server: It is done through HTTPS connection.
- Console -> Soffid Repository. It is done through standard JDBC connection with TLS.
- Sync server -> Soffid Repository: This is done via standard JDBC connection with TLS.
- Console -> Sync server. It is done through RPC calls encapsulated in HTTPS.
- Console -> PAM Store. It is done through REST calls with HTTPS.
- PAM Jump Server -> PAM Store. It is done through REST with HTTPS.
- PAM Jump Server -> Sync server. It is done via HTTPS connection.

The TOE also establishes the following connections with external components:

- From the Sync server to the Active Directory the connection and transmission of data is performed through LDAP using TLS.
- From The PAM Jump Server there can be three possible connections to different external systems, these are:
    - From PAM Jump Server to Windows Server, the connection is established through RDP using TLS.
    - From PAM Jump Server to Linux Server, the connection is established through SSH.
    - From PAM Jump Server to MySQL, the connection is established through JDBC using TLS.

All connection parameters are configured so that they comply with [CCN-STIC-807].

7.7.2 FTP_TRP.1

The TOE provides trusted communication paths using HTTPS, TLS accessing the GUI.

The TOE requires all users to initiate communication via the trusted path for initial user authentication, and execution of management functions.

8 References

Reference	Document
[CCN-STIC-140-A7]	Taxonomía de productos STIC- Anexo A7: Gestión de Identidades (IM) – August 2020
[CCN-STIC-140-A6]	Taxonomía de productos STIC- Anexo A.6: Gestión de acceso privilegiado (PAM)– July 2019
[CCN-STIC-807]	Criptología de empleo en el Esquema Nacional de Seguridad – May 2020
[PES-SOFFID]	Procedimiento de empleo seguro Soffid IAM. Versión 7 – 05/03/2025
[ICM PP]	Protection Profile for Enterprise Security Management - Identity and Credential Management Version 2.1 – October 2013
[CCMB-2017-04-002]	Common Criteria Part 2: Security functional components Version 3.1 Revision 5 – April 2017

Table 14: References

9 Glossary of Terms

Term	Definition
Access Control Product	An Enterprise Security Management product that is responsible for enforcing defined access control policies.
Assignment Manager	An individual authorized to use the TSF to define and maintain subject identity and credential data.
Credential	A collection of one or more pieces of information associated with an identity that can be used to assert that identity.
End User	An individual that is managed by the ESM system in order to have their authorizations clearly delineated and their activities unambiguously accounted.
Enrollment	The act of defining a new user in the ESM system.
Enterprise Security Management	Systems and personnel required to order, create, disseminate, modify, suspend, and terminate security management controls.
Federation	Two or more domains that have mutual assurance that a subject authenticated by one domain will be similarly valid on the other(s).
Identity	A unique identifier that is assigned to an individual that remains static for the duration of the user's lifecycle.
Managed Repository	A data store that is used to contain identity and credential attribute data. A managed repository does not have to be part of the TSF, but the TSF should be the only subject that is allowed to alter its contents.
Non-Person Entity	An identified subject that serves some function in an organization's operational environment that does not represent a human user, such as hardware or software.
Operational	The collection of hardware and software resources in an

Term	Definition
Environment	enterprise that are not within the TOE boundary. This may include but is not limited to third-party software components the TOE requires to operate, resources protected by the TOE, and the hardware upon which the TOE is installed.
Policy Administrator	An individual that uses a Policy Management product to define access control policies for the ESM.
Policy Management Product	An Enterprise Security Management product that is responsible for defining and transmitting access control policies that are subsequently implemented by Access Control products.
User	See End User.

Table 15: Terms and Definitions