ARCON PAM

(Previously known as ARCOS)

Version 4.8

Security Target

Version 1.6

May 15, 2023

Prepared for

ARCON TechSolutions Pvt. Ltd.

901, Kamla Executive Park,
Off Andheri-Kurla Road, JB Nagar, Andheri (E),
Mumbai – 400059
www.arconnet.com

Revision History

Version	Date	Author	Description
1.0	26th April 2019	Niranjan Nandodkar	First version of the document submitted to STQC
1.1	24th October 2019	Niranjan Nandodkar	Document modified based on the observations provided by STQC
1.2	4th November 2019	Niranjan Nandodkar	Changes in section 7.1 against the observations
1.3	6th November 2019	Niranjan Nandodkar	Changes against the response provided by STQC on the raised queries
1.4	18th July 2020	Niranjan Nandodkar	Changes against the observations provided by STQC
1.5	12th April 2021	Niranjan Nandodkar	Changes made against observations provided by STQC
1.6	15th May 2023	Niranjan Nandodkar	Minor changes made against suggestions provided by STQC validator

Table of Contents

List of Tables

List of Figures

1. Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE) identification information and an overview.

1.1. Security Target Reference

This section provides information necessary to identify and control the ST and the TOE.

ST Title	ARCON PAM Version 4.8 Security Target
Version	1.6
ST Date	May 15, 2023
ST Author	ARCON TechSolutions Pvt. Ltd.

Table 1: Security Target Reference

1.2. TOE Reference

TOE Identification	ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8
TOE Vendor	ARCON TechSolutions Pvt. Ltd.

Table 2: TOE Reference

1.3. TOE Overview

1.3.1. Usage and Major Security Features of TOE

The Target of Evaluation (TOE) is a software only Privilege Account Management solution which serves as a security layer between a user and organizations datacenter and is responsible for associating users with different sets of privileges to access the operational environments resources and services based on the pre-determined or customized policies as per organizations requirements.

TOE maintains accountability of individual users by implementing a comprehensive audit log system for execution of each a business process or system function which are configured in system. The service that manages an audit trail runs in a privileged mode to have access to each service and system of TOE to supervise entire activities of individual accounts. TOE implements adequate security to protect audit logs from unauthorized access through system or using direct access to database. TOE can be integrated with any SIEM (Security Information and Event Management) tool if API is available with the SIEM tool.

TOE secures privileged account's password by, making it cryptographically complex, introducing frequent change, and by avoiding sharing among independent systems and applications. TOE ensures that the sensitive data, including user's personal information, is protected by means of encryption and restriction, while stored in the database, implementing 256bit AES encryption model.

TOE implements an independent but interrelated set of technologies and services which include, but not limited to, Active Directory, Web Services, Access control, Digital Identities, Password Managers, Single-

Sign-On, Security Tokens, Security Token Services (STS) and dual factor authentication for user identification and authorization.

TOE allows the monitoring and management of identified privilege users or group of users, including their authentication, authorization, password management and activity auditing by a designated administrator. TOE ensures that minimum level of authority is provided to a user upon creation and as mentioned earlier, a designated administrator provides management authorization to an exclusively identified user. TOE also implements Maker-Checker concept that allows multilevel approval before any user is added with a specific set of authorization in the TOE.

Before allowing access to TOE itself and IT resource or system, TOE identifies and authorizes a user, that is required to associate accountability for the activities performed. Based on the successful authentication of a user, access to IT resources is provided depending on the authorizations configured for the authenticated user. Access to IT resources and systems is secured using additional authorization mechanism's which includes but may not be limited to Mobile OTP (using app) and SMS OTP. Also, TOE can secure access to IT resources and systems based on unique identifiers (viz. IP address, MAC address and BIOS id) of a system to prevent any unauthorized access.

TOE ensures that the communication channels established between TOE components and target systems are secured using HTTPS and TLS 1.2. All the data which transits through the established channel is encrypted by implementing various standard encryption mechanisms to mitigate any possible external interference.

TOE allows an enterprise to establish compliance to the regulatory and other requirements while mitigating possible internal data breaches using privileged accounts. In a nutshell, as a solution, which falls under the Privilege Account Management domain, TOE includes management of privileged accounts and their access control and audit.

Following is the list of major security features of the TOE,

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- trusted Path/Channel

Further details about the security requirements are mentioned in section 6. All the above-mentioned features are under evaluation.
This Security Target (ST) defines the Information Technology (IT) security requirements for the TOE. The TOE is being evaluated at assurance level EAL2+.

Refer section 1.4.2.1 for the lists of the components that describe the TOE and are under evaluation. Also refer to section 1.4.2.2 for the list of dependencies (hardware/software) needed by the TOE but are excluded from the evaluation.

1.3.2. TOE Type

The TOE is software application that performs Privilege Access Management (PAM) within an organization.

1.3.3. TOE Build number

TOE has the following identification details:

- Build Number: 4850U4 SP2
- Build date: 18th May 2022
- Version Number: 4.8

1.3.3.1. Identification Method

The TOE is a composite package inclusive of all TOE components (Vault Server, Application Server). Hence, each TOE component does not have a separate build number and is identified by the common TOE build number.

1.3.3.2. Platform Versioning

The TOE can be identified by the unique reference provided as the platform version. Versions of the TOE is classified into the following releases:

Major Release: These are the major updates of the platform provided by the development team. Versions v4.x and so on are assigned to the major releases. Major release of the TOE is comprised of any change to the security implementation within TOE.

Minor release: These are the minor updates within a major release provided by the development team. Versions vX.8 and so on are assigned to the minor releases. Minor Release of the TOE is comprised of a rollup of several enhancements/extensions to existing features or interfaces driven by various requirements.

1.4. TOE Description

1.4.1. Acronyms

ACL	Access Control List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ASP	Active Server Pages
CC	Common Criteria
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
EAL2+	Evaluation Assurance Level 2 extended
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IETF	Internet Engineering Task Force
IT	Information Technology
MD5	Message Digest 5
NIST	National Institute of Standards and Technology
OSP	Organizational Security Policy
PAM	Privilege Access Management
PP	Protection Profile
PUB	Publication
RAM	Random Access Memory
RMI	Remote Method Invocation
ROM	Read Only Memory
SACL	System Access Control List
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm 1 (NIST)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SQL	Structured Query Language for data base access
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UI	User Interface
VPN	Virtual Private Network

Table 3: Acronyms

1.4.2. Physical Scope of the TOE

The following diagram illustrates the physical scope and the physical boundary of TOE and connects together all of the components of the TOE and the constituents of the TOE Environment.

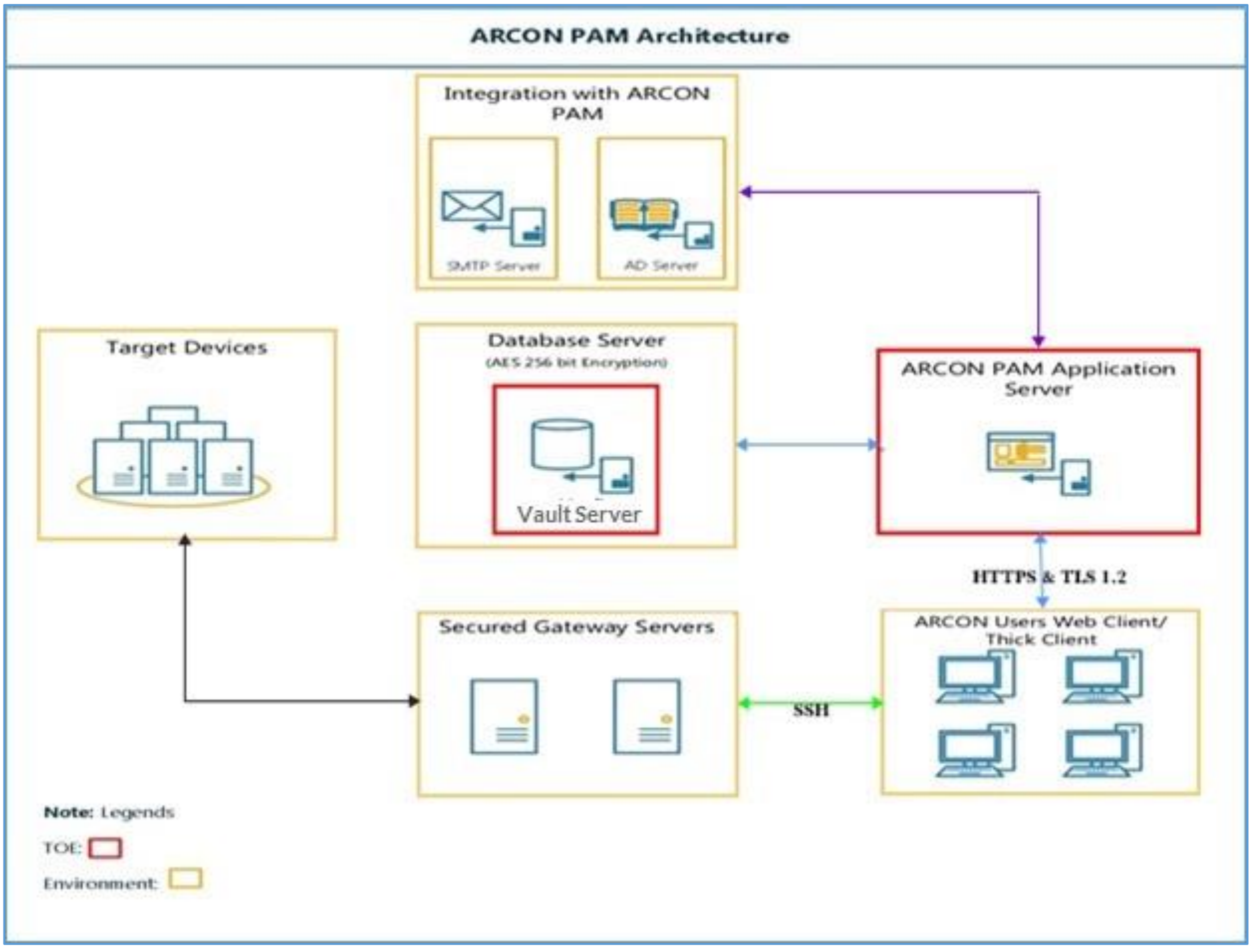

Figure 1: TOE Architecture

1.4.2.1. Components included in the TOE

The scope of the evaluation includes the following product components (marked in red bordered box in Figure 1)

- Vault Server
- Application Server

Following are the details of the components included in the TOE:

- **Vault Server**

Vault server is a core component of TOE which is the actual database. Following are the activities performed by Vault component:

- Passwords generated for privilege ID's managed by PAM are stored in encrypted format in Database.
- Text logs generated during operations are stored in encrypted format for analysis in case of an incident.

- **Application Server**

Application server provides tools to manage / configure TOE and mechanism to access target servers. Application server is an ActiveX based component which gets downloaded on end user's system once the TOE website is loaded.

Following are the services managed by Application server:

  - **Client Manager Online Service:** Client Manager Online is a web-based application interface to access authorized target servers.
  - **Server Manager**: Server Manager is an ActiveX based interface that enables and allows only TOE administrator to configure TOE. In this component administrator of TOE can perform various management activities.
  - **SPC Service**: Scheduled Password Change Service is a windows-based service that performs scheduled password change for privileged users. Time between password change is configurable.
  - **PWD Change Service:** PWD Change Service is windows-based service that is installed on all windows-based servers which are registered in TOE and is responsible to change password of users which are running windows dependency services like windows service, scheduled tasks and DCOM components.

1.4.2.2. Required Components Excluded from TOE

Features/Functionality that are required but are not part of the evaluated configuration of the TOE:

- Required hardware.
- Supported Windows Operating Systems.
- NT/Windows Authentication.
- .NET Framework components.
- ActiveX base components.
- Microsoft SQL Server.
- Internet Information Server.
- Video converter.
- Video Player.
- Image viewer.
- Text Viewers.
- Email clients.
- Client Browser.

1.4.2.3. TOE Guidance and Reference Documentation

The following guidance and reference documents are provided to customer and are considered as a part of the TOE:

Reference Title	ID
ARCON PAM Administrative Guide	[ADMIN]
ARCON PAM Client Manager Guide	[Client]

Table 4: Guidance and Reference Documents

1.4.3. Logical Scope of the TOE

TOE provides following security features,

- **Security Audit:**

TOE generates audit records with the help of Security Audit function. These audit records can be accessed by a user with the appropriate authorizations. Audit trail is maintained for each, and every activity performed by users, while accessing TOE including management of TOE. Generated audit logs are stored in a database. Such audit logs are protected as it can only be accessed through TOE. TOE allows us to filter the results which are generated with general filters, filters by target system, activities, and user-based activity. Only users with the appropriate authorizations and permission can access the audit log. Unauthorized access, deletion, and modification of the records is not possible.

- **Cryptographic Support:**

The TOE implements FIPS PUB 140-2 approved cryptographic algorithms to support various cryptographic functions. The cryptographic module within the TOE encrypts the sensitive data using a unique AES 256-bit key. Access to TOE using internet browsers is protected using SSL/TLS 1.2. The TOE is responsible for destroying all transient keying material generated within the TOE boundary.

- **User Data Protection:**

The TOE enforces access control policies that limit access to the user data and TOE configuration information. User account authorizations and permissions are enforced to protect user data from unauthorized access. Only users with the correct authorizations can manage the TOE. This includes the creation of users and overall management of TOE.

- **Identification and Authentication:**

TOE users must provide the username and password associated with an external authentication server or Local database. The TOE successfully identifies users by passing the username and password combination to the authentication server or to the TOE database, for validation prior allowing any actions on their behalf.

- **Security Management:**

Each TOE user that is granted access to the TOE is provided with a profile that defines the user's access rights, management rights, and action rights within the TOE. While first creating a user in the TOE and providing the user specific access, the TOE enforces restrictive default values by not providing the user with any authorizations or permissions. Exclusive security roles can also be defined and assigned to a TOE user based on organizational requirements. TOE implements maker-checker concept to restrict access to user and involve approver before allowing user to access TOE.

- **Protection of the TSF:**

The TOE employs an encryption mechanism to protect the credentials stored within the TOE database. Entire sensitive information is encrypted with unique encryption keys using 256bit AES algorithm. All TOE components communicate with one another over secure channel established using HTTPS and TLS 1.2.

- **TOE Access:**

TOE users attempting to access the TOE through web browser or windows application will encounter a display banner prior to being able to log into the TOE. The banner provides access to an advisory warning message regarding the unauthorized use of the TOE. TOE limits access to users who provide valid username and password combination to authenticate themselves. Restrictions are placed on a TOE user that deny them access to the TOE. TOE implements session time-out to make it mandatory for a user to actively interact with TOE to avoid session termination. If the user has not interacted with the TOE for an administrator-defined inactivity period, the TOE will initiate session termination and the user will be forced to provide login password to reestablish a session.

- **Trusted Path/Channel:**

Communication between all TOE components are established over secured channels. A user accesses the TOE Application server component over HTTPS using TLS 1.2. Authentication of user, in case of ADS authentication is done, over LDAP using the inherent security methods provided by Microsoft Windows operating system. All communication with the target IT resource is established using SSH Secured Gateway component. All communication between Application server and database is established using inherent security methods provided by Microsoft SQL server and Microsoft Windows operating system.

1.4.4. Operational Environment

TOE components run on top of Microsoft Windows Server and has following requirements,

- Vault Server requires Microsoft SQL Server
- Application Server requires Internet Information Server

The operational environment of TOE includes:

- Physical or Virtual Server platform based on the deployment requirement,
- External management workstations
- Managed devices
- Platform Services
    - Operating Systems
        - Basic networking features and libraries
        - Basic security features and libraries
    - Microsoft SQL Server Database with Required database components, features, and extensions
    - Internet Information Server (IIS) Required IIS components, features, and extensions.
    - External IT Systems
        - SIEM servers (optional)
        - Active Directory Server (optional)
        - SMTP Server (optional)

1.4.5. User Description

When a user account is created a default authorization must be applied. The user account inherits the access levels that are assigned to that role. The TOE contains the following predefined user roles,

Role	Access
Administrator	Full access to perform all configurational and management activities within TOE
Client	Minimal access to view approved target servers and access the same based on provided authorization

Table 5: User Description

A designated administrator provides required authorization to the identified user exclusively to elevate its role to operate in TOE logical boundary.

1.4.6. Delivery Method

TOE is delivered as a composite package compressed with password protection by team identified and based on email request by relevant team within ARCON. TOE delivery package password is available only with the team which is responsible to perform the deployment.

Entire TOE is uploaded on the external hosting server and link to the package is provided to the customers designated email address by authorizing the same for download.

TOE delivery package consists of binaries like executables (.exe), Dynamic Link Libraries (.DLL) and Basic database as backup for restoring (.BKP).

Guidance documents are provided as separate parts of TOE implementation and is in form of .PDF document.

1.4.7. Excluded Functionality

TOE supports multiple features which are not part of the core TOE functionality. All such features and any third-party source code or software that the TOE relies upon is excluded from the scope of evaluation:

- Use of Authentication mechanisms like LDAP, RADIUS, TACACS, ADS, etc.
- Use of SMTP
- Microsoft Core Networking components
- Video encoder and player

2. Conformance Claims

Following is the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims.

Common Criteria (CC) Identification and Conformance	• Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017 ○ CC Part 2 Extended • Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017 ○ CC Part 3 Conformant
Protection Profile Identification	This ST does not claim conformance to any existing Protection Profile.
Evaluation Assurance Level	EAL 2+ augmented with ALC_DVS.1

Table 6: CC and PP conformance

3. Security Problem Definition

3.1. Threats

The threat agents are broadly assumed into following four categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- TOE failure: The threat of the TOE failing in its operations or exhausting its resources which leads to a failure of TOE operations.
- External IT Entities: External IT entities that are being used by malicious attackers to adversely affect the security of the TOE.

TOE Security Functions (TSF) and user data saved on or transitioning through the TOE and the hosts on the protected network requires protection from the threats listed in following table:

Name	Description
T.ADMIN_ERROR	An administrator may incorrectly configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future records from being recorded, thus masking a user’s actions.
T.DATA_COMPROMISE	An unauthorized user may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.
T.MASQUERADE	A malicious user, process, or external IT entity may masquerade as an authorized entity to gain unauthorized access to data or TOE resources.
T.UNAUTHORIZED _ACCESS	A user may gain unauthorized access (view, modify, delete) to user data.
T.UNIDENTIFIED _ACTIONS	The administrator may fail to notice potential security violations, thus preventing the administrator from acting against a possible security violation.
T.DISASTER	Operation or access to the TOE may suddenly fail, rendering the TOE useless.

Table 7: Threats

3.2. Organizational Security Policies

There are no Organizational Security Policies defined for TOE deployment.

3.3. Assumptions

Following table lists the assumptions that are required to ensure the security of the environment where this TOE is employed.

Name	Description
A.PHYSICAL	Physical security is assumed to be provided by the environment.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMP	The base IT environment where TOE is hosted provides the TOE with the necessary reliable timestamps.
A.TRUSTED_ADMIN	TOE Administrators are non-hostile and are trusted to follow and apply all administrator guidance.
A.HARDEN	The TOE will be installed on a hardened instance of Windows.
A.ACCESS	Access to the TOE will be provided through a reliable network connection.
A.INSTALL	TOE components will be installed onto a compatible Operating System
A.INTERNAL_SERVICES	All LDAP and remote systems that the TOE communicates with should be located on the same internal network as the TOE. Users on this network are assumed to be non-hostile.

Table 8: Assumptions

4. Security Objectives

4.1. Security Objectives for the TOE

The specific security objectives for the TOE are listed in following table:

Name	Description
O.ACCESS	The TOE will ensure that only authorized users may gain access to it and the resources that it controls.
O.AUDIT	The TOE will provide the capability to detect security relevant events and record them to the audit trail.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit information for only authorized users.
O.AUDIT_STORAGE	The TOE will provide a secure method of storing generated audit logs.
O.BANNER	*The TOE will present an access banner to TOE users prior to accessing the TOE that defines acceptable use of the TOE.*
O.CRYPTO	The TOE will implement cryptography algorithms and procedures while handling critical information during operation of the TOE.
O.FAIL_SECURE	The TOE will provide a method to continue secure operations during a catastrophic TOE failure
O.PERMISSIONS	The TOE will ensure segregation of duties by restricting the abilities of individual TOE users.
O.PROTECT_COMM	The TOE will provide protected communication channels for distributed components of the TOE.
O.ROBUST_ACCESS	The TOE will monitor validity of sessions to deny or suspend session establishment.
O.TOE_ADMIN	The TOE will ensure that only authorized administrators are able to configure the TOE security functions attributes.
O.USER_AUTHEN	The TOE will uniquely identify and authenticate user prior allowing access to TOE functions and data.

Table 9: Security Objectives for the TOE

4.2. Security Objectives for the Operational Environment

The security objectives listed in following table are to be satisfied by the environment:

Name	Description
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.HARDENED	The TOE environment must be hardened adequately for the installation of TOE components.
OE.NETWORK	The TOE environment must provide a consistent, reliable network connection to the TOE.
OE.OS	The TOE environment must provide a compatible Windows Operating System version for the installation of TOE components.
OE.TRUSTED_ADMIN	Trusted TOE Administrators must follow and apply all administrator and configuration guidance.
OE.INTERNAL_SERVICES	LDAP servers and remote systems accessed by the TOE are located on the same internal network as the TOE. Users on this network are non-hostile.
OE.PHYSICAL	The TOE environment must provide physical security to the TOE and the data it contains.

Table 10: Security Objectives for the operational Environment

4.3. Security Objectives Rationale

4.3.1. Security Objectives Rationale Relating to Threats

The following table maps all threats to all objectives.

Threats	Objectives	Rationale
T.ADMIN_ERROR An administrator may incorrectly configure the TOE resulting in ineffective security mechanisms.	OE.TRUSTED_ADMIN Trusted TOE Administrators must follow and apply all administrator and configuration guidance.	OE.TRUSTED_ADMIN satisfies this threat by ensuring that administrators follow all administrative guidance.
T.AUDIT_COMPROMISE A malicious user or process may view audit records, cause harm to integrity of audit records or prevent future records from being recorded, thus masking a user's actions.	O.AUDIT The TOE will provide the capability to detect security relevant events and record them to the audit trail.	O.AUDIT satisfies this threat by ensuring that unauthorized attempts to access the TOE are recorded.
	O.AUDIT_STORAGE The TOE will provide a secure method of storing local audit records.	O.AUDIT_STORAGE satisfies this threat by ensuring that only authorized users are allowed to access stored audit records.

Threats	Objectives	Rationale
T.DATA_COMPROMISE An unauthorized user may read, modify, delay, or destroy security critical TOE data stored on the TOE or being transmitted between physically separated parts of the TOE.	O.CRYPTO The TOE will provide FIPS PUB FIPS 186-4, FIPS 180-4, FIPS 197, FIPS PUB 198-1 based cryptographic algorithms and procedures to TOE users during operation of the TOE.	O.CRYPTO satisfies this threat by providing encryption services available to authorized users and/or user applications.
	O.PROTECT_COMM The TOE will provide protected communication channels for parts of the distributed TOE.	O.PROTECT_COMM satisfies this threat by providing protected communication channels for parts of the distributed TOE.
	O.TOE_ADMIN The TOE will provide mechanisms to ensure that only authorized administrators are able to configure the TOE security functions attributes.	O.TOE_ADMIN satisfies this threat by ensuring that only trusted administrators are able to change the security functions and attributes stored on the TOE.
T.MASQUERADE A malicious user, process, or external IT entity may masquerade as an authorized entity to gain unauthorized access to data or TOE resources.	O.USER_AUTHEN The TOE will uniquely identify and authenticate each user's prior allowing access to TOE functions and data.	O.USER_AUTHEN satisfies this threat by ensuring that the TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
	O.BANNER The TOE will present an access banner to TOE users prior to accessing the TOE that defines acceptable use of the TOE	O.BANNER satisfies this threat by providing a warning message to users about unauthorized use of the TOE prior to logging in.
T.UNAUTHORIZED _ACCESS A user may gain unauthorized access (view, modify, delete) to user data.	O.ACCESS The TOE will ensure that only authorized users may gain access to it and the resources that it controls.	O.ACCESS satisfies this threat by ensuring that only authorized users gain access to it and to resources that it controls.

Threats	Objectives	Rationale
	O.ROBUST_ACCESS The TOE will implement mechanisms that can deny or suspend session establishment	O.ROBUST_ACCESS satisfies this threat by ensuring only authorized users are allowed to connect to the TOE and by automatically closing inactive sessions.
	O.PERMISSIONS The TOE will provide a method to maintain segregation of duties of individual TOE users	O.PERMISSIONS satisfies this threat by assigning users different permissions that relate to the data they are allowed to access.
T.UNIDENTIFIED _ACTIONS The administrator may fail to notice potential security violations, thus preventing the administrator from taking action against a possible security violation.	O.AUDIT_REVIEW The TOE will provide the capability for only authorized users to view audit information.	O.AUDIT_REVIEW satisfies this threat by providing the capability for only authorized administrators to view audit information.
T.DISASTER Operation or access to the TOE may suddenly fail, rendering the TOE useless	O.FAIL_SECURE The TOE will provide a method to continue secure operations during a catastrophic TOE failure	O.FAIL_SECURE satisfies this threat by providing a seamless transition to a working version of the TOE.

Table 11: Security Objective Rationale

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

4.3.2. Security Objectives Rationale Relating to Assumptions

Following table maps all assumptions to environmental objectives.

Assumptions	Objectives	Rationale
A.PHYSICAL Physical security is assumed to be provided by the environment.	OE.PHYSICAL The TOE environment must provide physical security to TOE and the data it contains.	OE.PHYSICAL satisfies the assumption by ensuring that the TOE environment provides physical security to TOE and the data it contains.
A.PROTECT	OE.PROTECT The TOE environment must protect itself and the TOE from	OE.PROTECT satisfies the assumption by performing integrity checks to ensure

Assumptions	Objectives	Rationale
The TOE software will be protected from unauthorized modification.	external interference or tampering.	external interference or tampering has not occurred.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption by providing reliable timestamps provided by the TOE environment hardware clock.
A.TRUSTED_ADMIN TOE Administrators are non-hostile and are trusted to follow and apply all administrator guidance.	OE.TRUSTED_ADMIN Trusted TOE Administrators must follow and apply all administrator and configuration guidance.	OE.TRUSTED_ADMIN satisfies the assumption by ensuring that only trusted administrators follow and apply all administrator guidance.
A.HARDEN The components of the TOE, which are considered under evaluation (refer section 1.4.2.1), will be installed on a hardened instance of Microsoft Windows Server and Microsoft SQL Server.	OE.HARDENED The TOE environment must provide a hardened version of Microsoft Windows Server and Microsoft SQL Server for the installation of TOE.	OE.HARDENED satisfies the assumption by ensuring a hardened version of Microsoft Windows Server and Microsoft SQL Server is provided for the installation of the TOE.
A.ACCESS Access to the TOE will be provided by a reliable network connection	OE.NETWORK The TOE environment must provide a consistent network connection to the TOE.	OE.NETWORK satisfies the assumption by ensuring a consistent network connection to the TOE will always be provided.
A.INSTALL TOE components will be installed onto a compatible Operating System	OE.OS The TOE environment must provide a compatible Windows Operating System version for the installation of TOE.	OE.OS satisfies the assumption by ensuring that a compatible Window Operating System will be provided for the installation of TOE.
A.INTERNAL_SERVICES All LDAP and remote systems that the TOE communicates with should be located on the same internal network as the TOE. Users on this network are assumed to be non-hostile.	OE.INTERNAL_SERVICES LDAP servers and remote systems accessed by the TOE are located on the same internal network as the TOE. Users on this network are non-hostile.	OE.INTERNAL_SERVICES satisfies this assumption by ensuring that LDAP and remote systems accessed by the TOE are located within the same internal network as the TOE. Users on this network are non-hostile.

Table 12: Security Objectives Rationale Relating to Assumptions

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined assumptions.

5. Extended Components Definition

The component defined below is modelled on components from Part 2 of the CC Version 3.1. The extended components are denoted by adding "_EXT" in the component name.

Item	SFR ID	SFR Title
1	FPT_SKP_EXT.1	Protection of Secret Key from Disclosure

Table 13: Extended Components

5.1. FPT_SKP_EXT.1 Protection of Secret Key from Disclosure

5.1.1. Class FPT: Protection of the TSF

See Section 15 of the Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017 Version 3.1 Revision 5.

5.1.2. Family: Secret Key Protection (FPT_SKP_EXT)

5.1.2.1. Family Behavior

The requirements of this family ensure that the TSF will protect secret key from disclosure.

5.1.2.2. Component Leveling

FPT_SKP_EXT Secret Key Protection
1

This family consists of only one component, FPT_SKP_EXT.1 Protection of Secret Key from Disclosure, which requires that the TSF ensures no mechanism for reading secret cryptographic data is available.

5.1.2.3. Management

There are no management actions foreseen.

5.1.2.4. Audit

There are no auditable actions foreseen.

5.1.3. Definition

FPT_SKP_EXT.1 Protection of Secret Key from Disclosure

Hierarchical to:	No other components.
Dependencies:	No Dependencies.

FPT_SKP_EXT.1.1

Hierarchal to: No other components

The TSF shall prevent reading of all pre-shared keys, Asymmetric keys, and private keys.

5.1.4. Rationale

FPT_SKP_EXT.1.1 describes the behavior of the TSF when handling pre-shared, Asymmetric, and private keys, collectively referred to here as secret key parameters. FPT_SKP_EXT.1.1 was needed to be defined as an explicit requirement as there is no equivalent requirement in the Common Criteria.

5.2. Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified below:

6.1. Conventions

The CC allows for assignment, refinement, selection, and iteration operations to be performed on security functional requirements. All these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets]. In keeping with these conventions, in the event an assignment is within a selection, it will be depicted as *italicized*, underlined text.
- Refinements are identified using **bold** text. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.

6.2. Security Functional Components

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Following table identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable Audit Review		✓		
FAU_SEL.1	Selective Audit	✓	✓		
FAU_STG.1	Protected Audit Storage	✓			
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_ETC.1	Export of user data without security attributes		✓		
FDP_RIP.2	Full residual information protection	✓			
FDP_SDI.1	Stored data integrity monitoring		✓		
FIA_AFL.1	Authentication Failure Handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.1	Timing of identification		✓		
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_ITT.1	Basic Internal TSF Data Transfer Protection	✓			
FPT_RPL.1	Replay Detection		✓		
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)				
FTA_SSL.3	TSF-Initiated Termination		✓		
FTA_SSL.4	User-initiated Termination				
FTA_TAB.1	Default TOE Access Banners				
FTA_TSE.1	TOE Session Establishment		✓		
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted Path	✓	✓		

Table 14: Security Functional Requirements

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1. Class FAU: Security Audit

FAU_GEN.1	Audit Data Generation
Hierarchical to:	No other components
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions b) All auditable events, for the [Not Specified] level of audit; and c) [*All auditable events identified in Table 15*].

Component	Auditable Events	Additional Audit Record Contents
FDP_ACF.1	*All requests to perform an operation on an object covered by the SFP*	*Subject identity, object identity, requested operation*
FIA_AFL.1	*The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state*	*Action taken when threshold is reached*
FMT_SMF.1	*Use of the management functions*	*Management function performed*
FMT_SMR.1	*Modification to the members of the management roles*	*No Additional Information*
FTA_SSL.3	*Termination of an interactive session by the session locking mechanism.*	*No Additional Information*
FTA_SSL.4	*Termination of an interactive session by the user.*	*No Additional Information*
FTA_TSE.1	*Denial of session establishment*	*No Additional Information*

Table 15: List of Auditable Events

Application Note:	The TSF is comprised of several components that are registered as Windows services and therefore the start-up and shutdown events are captured in the Windows Event Log.
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: no other audit relevant information].

FAU_GEN.2	User identity association
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1	Audit review
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [*users with the "View logs" authorization*] with the capability to read [*operational reports and audit/compliance reports*] 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.

FAU_SAR.2	Restricted audit review
Hierarchical to:	No other components
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3	Selectable audit review
Hierarchical to:	No other components
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.3.1	The TSF shall provide the ability to apply [*filters*] of audit data based on [*general filters, target systems, activities, and userid, IP address*].

FAU_SEL.1	Selective Audit
Hierarchical to:	No other components
Dependencies:	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data
FAU_SEL.1.1	The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: a) [user identity, host identity, ll even types identified in table 16] b) [*None*]

Auditable Events
All requests to perform an operation on an object covered by the SFP
The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state
Use of the management functions
Modification to the members of the management roles
Termination of an interactive session by the session locking mechanism.
Termination of an interactive session by the user.
Denial of session establishment

Table 16: Auditable Events

FAU_STG.1	Protected Audit Storage
Hierarchical to:	No other components
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

6.2.2. Class FCS: Cryptographic Support

FCS_CKM.1	Cryptographic key generation
Hierarchical to:	No other components
Dependencies:	FCS_COP.1 Cryptographic operation FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*AES*] and specified cryptographic key sizes [*256-bit*] that meet the following: [*FIPS PUB 140-2*].

FCS_CKM.4	Cryptographic key destruction
Hierarchical to:	No other components.
Dependencies:	FCS_CKM.1 Cryptographic key generation
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [Zeroize] that meets the following: [*FIPS 140-2*].

FCS_COP.1(1)	Cryptographic operation (for data encryption/decryption)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(1) The TSF shall perform [*encryption/decryption]* in accordance with a specified cryptographic algorithm [*AES operating in CBC*] and cryptographic key sizes [*256 bits*] that meet the following: [*FIPS PUB 197, "Advanced Encryption Standard (AES)"*]

FCS_COP.1(2) Cryptographic operation (for cryptographic signature)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(2) The TSF shall perform [*cryptographic signature services]* in accordance with a specified cryptographic algorithm [*Self customized cryptographic algorithm based on AES*] and cryptographic key sizes [*256 bit*] that meet the following: [*FIPS PUB 186-4, "Digital Signature Standard"*]

FCS_COP.1(3) Cryptographic operation (for cryptographic hashing)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(3) The TSF shall perform [*cryptographic hashing services as defined in Table 16]* in accordance with a specified cryptographic hash algorithm [*as defined in Table 16*] and message hash sizes [*as defined in Table 16*] that meet the following: [*as defined in Table 16*]

Operation	Hash Algorithms	Standards
HTTPS	Client Specific; as the SSL certificate is provided by client	FIPS PUB 180-4 (Secured Hash Standard) FIPS PUB 198-1 (Keyed-Hash Message Authentication Code)
SSH	**KexAlgorithms:** ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256, diffie-hellman-group-exchange-sha256	
	MACs: hmac-sha2-512, hmac-sha2-256, hmac-ripemd160	
	Ciphers: aes256-ctr, aes192-ctr, aes128-ctr	

Table 17: Cryptographic hashing services

FCS_COP.1(4) Cryptographic operation (for keyed-hash message authentication)

Hierarchical to: No other components.

Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(4) The TSF shall perform [*keyed-hash message authentication]* in accordance with a specified cryptographic hash algorithm [*hmac-sha2-512, hmac-sha2-256, hmac-ripemd160*] and message hash sizes [*512, 256, 160*] that meet the following: [*FIPS PUB 198-1, "Keyed-Hash Message Authentication Code"*]

6.2.3. Class FDP: User Data Protection

FDP_ACC.1	Subset access control
Hierarchical to:	No other components
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the [*Access Control Policy*] on [*Subjects: users accessing TOE Data* *Objects: database tables* *Operations: view, create, modify, delete*].

FDP_ACF.1	Security attribute based access control
Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1	The TSF shall enforce the [*Access Control Policy*] to objects based on the following: [*Subject attributes (users)* *User ID, Password, Role, LoB, IP Address, user account expiration date and time, user access allowed date and time*]
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*all operations between subjects and objects defined in Table 17 below based upon some set of organizational attributes*].

Subject	Object	Operation
User	*Processes*	*Execute | Delete | Terminate | Change Permissions*
	Files	*Create | Read | Modify | Delete| Change Permissions*
	Host Configuration	*Read | Modify | Delete*
	Authentication Functions	*Login*

Table 18:FDP Requirement Table for Access Control

FDP_ACF.1.3	The TSF shall explicitly authorize 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*].

FDP_ETC.1	Export of user data without security attributes
Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
FDP_ETC.1.1	The TSF shall enforce the [*access control List*] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes

FDP_RIP.2	Full residual information protection
Hierarchical to:	No other components
Dependencies:	FDP_RIP.1 Subset residual information protection
FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to, deallocation of the resource from] all objects.

FDP_SDI.1	Stored data integrity monitoring
Hierarchical to:	No other components
Dependencies:	No dependencies.
FDP_SDI.1.1	The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*user data attributes*].

6.2.4. Class FIA: Identification and Authentication

FIA_AFL.1	Authentication Failure Handling
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [*an administrator configurable positive integer* within *[range]*] unsuccessful authentication attempts occur related to [*attempted logins to the TSF*].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*Lock the account for a set number of minutes as defined by the Administrator until manually unlocked by administrator or reset lockout period is met*].

FIA_ATD.1	User attribute definition
Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [*Email Address, User Name, Password, Associated Groups, User Active checkbox, Account Locked checkbox, and Two Factor Authentication settings*].

FIA_SOS.1	Verification of secrets
Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [*The following password requirements within BI for local accounts:* • *Administrator-defined complexity requirements when creating a password.* • *A maximum length for the password.* • *Administrator-defined integer for the maximum number of days before a password must be changed.* • *Administrator-defined integer for the minimum number of days that a password must be used before it can be changed.*

The following password requirements when resetting a password through the UI:

- *The password does not contain all or part of the user's account name.*
- *The minimum length for a password*
- *The password is not a previously used password.*
- *The password contains characters from three of the following four categories: Upper case characters, lower case characters, numbers 0-9, non-alphanumeric characters*].

FIA_UAU.1	Timing of authentication
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_UAU.1.1	The TSF shall allow [*the following TSF mediated actions:* *Access the guides provided by TSF providing information on authentication procedure*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.2	User authentication before any action
Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification
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.

FIA_UAU.5	Multiple authentication mechanisms
Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_UAU.5.1	The TSF shall provide [*any of the following authentication mechanisms:* • *Local authentication mechanisms* • *AD/LDAP authentication mechanisms* • *Two-factor authentication mechanisms* • *SMS verification mechanisms*] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the [*following rules:* • ***Local authentication:*** *User sends their credentials to the Application Server. Application server compares the user's password to the value stored in the user's account information. If they match, the user is authenticated and allowed access to the TOE.* • ***AD/LDAP authentication:*** *A user sends their credentials to the application server. Application server forwards the credentials to the AD/LDAP server. The AD/LDAP server evaluates the credentials and if the username corresponds to a valid domain user and the password matches the stored password, then the AD/LDAP server sends back to application server that the account is authenticated.* • ***Two-factor authentication:*** *A user sends their credentials to the Application Server. These credentials are first checked following the local or AD/LDAP authentication method, depending on the account used. If the first check is successful, BI will then send the username, username/password, or username/token to the RADIUS server depending on which setting is used for*

the RADIUS server. When the options for username/token is chosen, Application server will prompt the user to enter their token to be sent to the RADIUS server. The RADIUS server will respond to any request with Accept, Reject, or Challenge. Application server acts upon services and services parameters bundled with Accept or Reject.

- ***SMS verification mechanisms:*** *A user sends their credentials to the Application Server. Application server sends an OTP to user's registered mobile number. User is prompted to type in the received OTP number. Application server compares the OTP with the user's username. If the provided information matches user is authenticated.*]

FIA_UAU.7	Protected authentication feedback
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication
FIA_UAU.7.1	The TSF shall provide only [*asterisks ("*") as feedback when accessing the Application server's Console UI*] to the user while the authentication is in progress.

FIA_UID.1	Timing of identification
Hierarchical to:	No other components.
Dependencies:	No dependencies
FIA_UID.1.1	The TSF shall allow [the following TSF mediated actions: *Download the guides stored in TSF*] on behalf of the user to be performed before the user is identified.

FIA_UID.2	User identification before any action
Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any actions on behalf of that user.

6.2.5. Class FMT: Security Management

FMT_MOF.1	Management of security functions behavior
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MOF.1.1	The TSF shall restrict the ability to [determine the behavior of, modify the behavior of] the functions: [*specified in Table 18*] to [*administrator*].

Requirement	Management Functions	Role allowed
FIA_AFL.1	*TSF shall restrict a user to perform management of the threshold for unsuccessful authentication attempts.*	Administrator
FMT_SMR.1	*TSF shall allow to specify users which are allowed to modify privileges of other users. The user who can use the management function shall be restricted to a specific role.*	*Administrator*
FTA_TAB.1	*TSF shall restrict a user which is allowed to maintain he banner.*	*Administrator*

Table 19: Management of Functions within TOE

FMT_MSA.1	Management of security attributes
Hierarchical to:	No other components
Dependencies:	FDP_ACC.1 Subset access control FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
FMT_MSA.1.1	The TSF shall enforce the [*Access Control Policy*] to restrict the ability to [change default, query, modify, delete, [*create*]] the security attributes [*user role and group assignment, level for exception approval*] to [*Administrator*]

FMT_MSA.3	Static attribute initialization
Hierarchical to:	No other components
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the [*access control 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 [*Administrator*] to specify alternative initial values to override the default values when an object or information is created

FMT_MTD.1	Management of TSF data
Hierarchical to:	No other components
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [change_default, query, modify, delete, clear] the [*Not specified*] to [*Administrator*].

FMT_SMF.1	Specification of Management Functions
Hierarchical to:	No other components.
Dependencies:	No Dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [*management functions listed in Table 19*].

Requirement	Management Functions
FAU_SEL.1	*Configuration of auditable events*
FIA_AFL.1	*Management of the threshold for unsuccessful authentication attempts*
	Management of actions to be taken in the event of an authentication failure
FMT_MOF.1	*Management of sets of users that can interact with security functions*
FMT_SMR.1	*Management of the users that belong to a particular role*
FTA_SSL.3	*Configuration of the inactivity period for session termination*
FTA_TAB.1	*Maintenance of the banner*
FTP_ITC.1	*Configuration of actions that require trusted channel (if applicable)*
FTP_TRP.1	*Configuration of actions that require trusted path (if applicable)*

Table 20: List of Management Functions

FMT_SMR.1	Security roles
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1	The TSF shall maintain the roles [*Administrator, client*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.2.6. Class FPT: Protection of the TSF

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to:	No other components.
Dependencies:	No other components.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [*Loss in network connectivity, catastrophic service failure*].
Application Note:	TOE is a conduit between End user device and Target server. TOE does not maintain any security information related to the session establishment like session id, session logs, etc., other than the captured screenshot from the end user device only. In such a case where TOE becomes unavailable due to any reason, no session related information is exposed and hence the security state remains preserved.

FPT_ITT.1	Basic Internal TSF Data Transfer Protection
Hierarchical to:	No other components.
Dependencies:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

FPT_RPL.1	Replay Detection
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_RPL.1.1	The TSF shall detect replay for the following entities: [*secured tasks*].

FPT_RPL.1.2	The TSF shall perform [*reject the secured task*] when replay is detected.
Application Note:	The TOE relies on the implementation of TLS in the operational environment to provide secure transmission, including replay detection, of secured tasks.

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 key, and private keys

6.2.7. Class FTA: TOE Access

FTA_SSL.3	TSF-Initiated Termination
Hierarchical to:	No other components.
Dependencies:	No other components.
FTA_SSL.3.1	The TSF shall terminate an interactive session after: [*For the web-based Client: an administrator-defined period of inactivity;* *For the windows-based Interface: an administrator-defined period of inactivity*].

FTA_SSL.4	FTA_SSL.4 User-initiated Termination
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.4.1	The TSF shall allow user-initiated termination of the user's own interactive session.

FTA_TAB.1	Default TOE Access Banners
Hierarchical to:	No other components.
Dependencies:	No other components.
FTA_TAB.1.1	Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

FTA_TSE.1	TOE Session Establishment
Hierarchical to:	No other components.
Dependencies:	No other components.
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [*Incorrect User ID, incorrect Password, IP Address of the device attempting session establishment, MAC Address of the device attempting session establishment, BIOS ID of the device attempting session establishment, CPU ID of the device attempting session establishment, account expiration date, account restriction date and time*]

6.2.8. Class FTP: Trusted Paths/Channels

FTP_ITC.1	Inter-TSF trusted channel
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1	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, another trusted IT product] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [*communication with LDAP servers*].

FTP_TRP.1	Trusted Path
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_TRP.1.1	The TSF shall use [**TLS/HTTPS**] to provide a trusted 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, [*none*]].
FTP_TRP.1.2	The TSF shall permit [the TSF, local users, 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

This section defines the assurance requirements for the TOE. Assurance requirements listed in following table are derived from the CC Part 3 and are EAL 2 + augmented with ALC_DVS.1.

Assurance Requirements	
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class 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
	ALC_DVS.1 Identification of security measures
Class ASE: Security Target 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
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 21: Security Assurance Requirements

7. TOE Summary Specification

This section provides information to describe how the TOE meets the SFR's described in previous sections of this ST.

7.1. TOE Security Functions

Considering that each of the security requirements and the associated descriptions correspond to the security functions; this section describes how each function specifically satisfies each of its related requirements. This helps in describing the security functions and rationalize that the security functions satisfy the necessary requirements. Following table lists all SFRs claimed within this Security Target.

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable Audit Review
	FAU_SEL.1	Selective Audit
	FAU_STG.1	Protected Audit Storage
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic operation (for cryptographic signature)
	FCS_COP.1(3)	Cryptographic operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic operation (for keyed-hash message authentication)
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute-based access control
	FDP_ETC.1	Export of user data without security attributes
	FDP_RIP.2	Full residual information protection
	FDP_SDI.1	Stored data integrity monitoring
Identification and Authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
	FIA_UID.2	User identification before any action

TOE Security Functionality	SFR ID	Description
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
	FPT_RPL.1	Replay Detection
	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
TOE Access	FTA_SSL.3	TSF-Initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banner
	FTA_TSE.1	TOE Sessions Establishment
Trusted Path/Channel	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path

Table 22: TOE Security Functions

7.1.1. Security Audit

The Security Audit function allows the TOE to generate audit records. Typical audit records that can be accessed by a user with the correct authorizations include Process access, Command access, User activities, User access, Service access, User validity, Service reference and Service password status logs. As TOE user's access, manage, and configure the TOE, their activities are tracked. When an Auditor user generates an "ARCON PAM Log", the Auditor will see the various activities performed by TOE users in a specific LoB. The audit list contains the columns and information listed in the table below.

Column name	Content
User ID	User id that performed the activity
Object Type	Type of object accessed
Operation type	Information on activity performed (Add, Modify, Delete)
Transaction for	Target service or system
Old value	Original value
New Value	Changed value
Time Stamp	Timestamp of the activity performed

Table 23: Audit record contents

Further, once an Activity Log has been generated, the results can be filtered with from and to date, Object type, operation, and user id. Audit records when requested, is generated by the TOE and stored in the database. Only users with the appropriate authorizations and permission can access the contents of the database.

Log management, which may include log retention, rotation and movement of log files considering the disk size, is configurable and is under TOE administrator control.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_SEL.1, FAU_STG.1

7.1.2. Cryptographic Support

The TOE implements HTTPS and TLS 1.2 to establish a trusted communication channel between TOE and target machine while sensitive data is in transit. TOE also forces symmetric encryption, using FIPS PUB 140-2 based customized cryptographic algorithms using a unique AES 256-bit key over such data. TOE performs symmetric encryption and decryption using the Cryptographic Application Programming Interfaces (CAPI) implementation of the Advanced Encryption Standard (AES) algorithm.

The size of the symmetric key used for the encryption process is 256bits. The 128bit initialization vector (implemented through System.Security.Cryptography.SymmetricAlgorithm.IV) is implemented for FIPS PUB 140-2 based symmetric encryption. Further, the encryption method implements the block size of 128 bit and padding used is PKCS7.

Any data which is stored in database is also encrypted using available default Microsoft encryption methods using a unique AES 256-bit key. Communications initiated between TOE and database also implements TLS 1.2.

The TOE is responsible for destroying all transient keys generated and any data which resides in kernel allocated memory spaces within the TOE boundary while TOE is in operation. The TOE destroys all keys and other critical data generated by the TOE, when all the processes and communication channels established are stopped using operational methods provided by TOE and operating environment.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4)

7.1.3. User Data Protection

The TOE provides the User Data Protection security function to manage user access and interaction with TOE data. Access to the TOE data is enforced by user account authorizations and permissions. A user attempting to access the TOE data with the incorrect authorizations and permissions will be denied access.

Users can access the safe through one of the many TOE component interfaces including: Windows based tool and Web Client. Access to the TOE data through these interfaces requires the correct access type associated with each TOE user. Once granted access to the TOE data, the users with the correct authorizations can manage the TOE configuration within the TOE. TOE users can be denied access to the TOE data if they are attempting to access the TOE data from an interface with invalid access type. Additionally, TOE access can be limited to TOE users based on the time of day, location of access, or account expiration date.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_ETC.1, FDP_RIP.2, FDP_SDI.1

7.1.4. Identification and Authentication

TOE users must provide the correct username and password associated with an external LDAP account. The TOE must successfully identify and authenticate a user prior to allowing any actions on their behalf. The TOE identifies and authenticates the user by passing the username and password combination to the Microsoft Active Directory Service or TACACS service, which needs to be configured in TOE by an administrator, for validation.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.1, FIA_UID.2

7.1.5. Security Management

Each TOE user having granted access to the TOE is mapped with a user type that defines the user's access rights, management rights, and action rights within the TOE. Further users are mapped in a user group that has collection of authorizations to perform activities. The TOE enforces restrictive default values by not providing the user with any authorizations or permissions. Authorizations are added by the TOE user creating the new user within the TOE and permissions are given to the new user by mapping them to groups and services. The TOE does not inherently define security roles.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.6. Protection of the TSF

The TOE employs a dual encryption mechanism to protect the credentials stored in database by TOE. All user credentials are by default encrypted with unique encryption keys. In addition to the default mechanism, TOE allows client to provide its own encryption key which further encrypts the credential while stored in database. TOE also provides an option to change the customized encryption key on a timely basis based on customers discretion. The TOE provides a trusted internal channel for all components of the TOE. This ensures mitigation of any external interference while communicating with database. The TOE employs AES-256 for confidentiality and integrity. The TOE components communicate with one another through a variety of ports which ensures that all their communication is secure and logically separate. Allowing communication using different port than default allows us protection against logical tampering of data at rest.

The TOE stores all pre-shared keys, symmetric keys, and private keys encrypted using AES-256 in the Microsoft SQL Server database in the operational environment. The encryption key is stored in the Database, protected by an ACL and by encrypting the secret key using the Cryptographic Application Programming Interfaces (CAPI). Any user is unable to read or view any keys through any interfaces other than so provided by TOE.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_ITT.1, FPT_RPL.1, FPT_SKP_EXT.1.1

7.1.7. TOE Access

TOE users attempting to access the TOE through the web client or windows-based tools need to identify itself by providing valid credentials. Such credentials are authenticated by implementing Microsoft Active Directory Service or TACACS service provided by third party vendors. Once the initial authentication is successful, the user will be displayed with a banner prior to being able to log into the TOE. The banner provides access to an advisory warning message regarding the unauthorized use of the TOE. Access to the TOE will be limited to users that provide the correct username and password combination.

Restrictions can be placed on a TOE user that will deny them access to the TOE. The location from which a TOE user is attempting to access the TOE, can be used to limit access to the TOE. Administrators can also place an account expiration date onto a user account. Once the account has expired, the user will not be allowed to access the TOE. Lastly, if the user does not have the correct access type to access the TOE from a given interface, they will be denied access to the TOE.

Users must actively interact with the TOE to avoid session termination. If the user account has not interacted with the TOE for an administrator-defined inactivity period, the session will terminate, and the user will be logged out of the TOE. The user must proceed with the login process to regain access to the TOE.

TOE implements a TSPlugin agent on the servers which are onboarded agent to prevents session bypassing. If a connection with the target Server, bypassing TOE, is established, TSPlugin checks for its origin and disconnects the session. This restricts bypassing of TOE to establish session with target servers (which are onboarded in TOE).

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1, FTA_TSE.1

7.1.8. Trusted Path/Channel

The TOE requires TOE users and TOE Administrators to initiate communication via the trusted path for initial user authentication, and execution of management functions. The TOE allows integration with Microsoft Active Directory Service and TACACS service to perform the initial user authentication. TOE ensures that the user is provided access to the management functions and operational features based on the response to the initial authentication and further by confirming the authorizations provided to the identified user. All the management functions and operational features such as executing configuration of TOE, connecting to target servers are accessed through the interface provided by Application Server post initial authentication. The communication channel is protected using HTTPS in the operational environment.

The TOE uses HTTPS/TLS 1.2 for secure administrative access which is provided by the third-party Microsoft Server Operating system platform cryptographic libraries.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1

8. Rationale

8.1. Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 conformant of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5, April 2017.

This ST does not conform to a PP.

8.2. Security Functional Requirements Rationale

The following section provides evidence of coverage for each security objective.

8.2.1. Rationale for Security Functional Requirements of the TOE Objectives

The following table maps all TOE objectives to SFRs.

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE will ensure that only authorized users may gain access to it and the resources that it controls.	FDP_ACC.1 Subset access control	The requirement meets the objective by enforcing the Access Control Policy for accessing TOE data. While authorized users are trusted to some extent, this requirement ensures only authorized access is allowed to TOE components.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by specifying the Access Control Policy rules that will be enforced by the TSF and determines if an operation among TOE components is allowed. Furthermore, it specifies the rules to explicitly authorize or deny access to a TOE user based upon security attributes.
	FDP_ETC.1 Export of user data without security attributes	The requirement meets the objective by controlling information which is exported outside the limit of TSF
	FDP_RIP.2 Full residual information protection	The requirement meets the objective by controlling information assigned to resources or objects to ensure that no information is available to other resource once the existing resource or object is not in use.
	FDP_SDI.1 Stored data integrity monitoring	The requirement meets the objective by monitoring the integrity of the stored data to avoid any security incident due to stored data modification.
O.AUDIT The TOE will provide the capability to detect security relevant events and record them to the audit trail.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	The requirement meets the objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT_REVIEW The TOE will provide the capability for only authorized users to view audit information.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.2 Restricted audit review	The requirement meets the objective by ensuring that only authorized users can review logs.
	FAU_SAR.3 Selectable Audit Review	The requirement meets the objective by ensuring the TOE provides an organized method to review audit records
	FAU_SEL.1 Selective Audit	The requirement meets the objective by allowing selection of audit records based on criteria
O.AUDIT_STORAGE The TOE will provide a secure method of storing local audit records.	FAU_STG.1 Protected Audit Storage	The requirement meets the objective by ensuring that only authorized users are allowed to access stored audit records.
O.CRYPTO The TOE will provide FIPS PUB 186-4 Approved cryptographic algorithms and procedures to TOE users during operation of the TOE.	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE can generate FIPS-Approved cryptographic keys for use during cryptographic operations.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that the TOE destroys cryptographic keys when no longer in use using FIPS-Approved methods
	FCS_COP.1 (1) Cryptographic Operation (for data encryption/decryption)	The requirement meets the objective by ensuring that the TOE performs encryption/decryption in accordance with AES operating in CBC mode using cryptographic key size of 256 bits that meets FIPS PUB 197, “Advanced Encryption Standard (AES)” standard
	FCS_COP.1 (2) Cryptographic Operation (for cryptographic signature)	The requirement meets the objective by ensuring that TOE performs cryptographic signature services in accordance with a Self-customized cryptographic algorithm based on AES using cryptographic key size of 256 bit that meets the FIPS PUB 186-4, “Digital Signature Standard” standard
	FCS_COP.1 (3) Cryptographic Operation (for cryptographic hashing)	This requirement meets the objective by ensuring that the TOE performs the cryptographic hashing services in

Objective	Requirements Addressing the Objective	Rationale
		accordance with a specified cryptographic hash algorithm that meets the FIPS standards as defined in Table 16.
	FCS_COP.1 (4) Cryptographic operation (for keyed-hash message authentication)	This requirement meets the objective by ensuring that the TOE performs keyed-hash message authentication in accordance with a specified cryptographic hash algorithm that meet the FIPS PUB 198-1 standard.
	FPT_SKP_EXT.1 Protection of Secret Key from Disclosure	The requirement meets the objective by ensuring that the TOE encrypts all the secret keys while at rest in database.
O.USER_AUTHEN The TOE will uniquely identify and authenticate user prior allowing access to TOE functions and data.	FIA_AFL.1 Authentication Failure Handling	The requirement meets the objective by ensuring that TSF handles failures resulted during user authentication.
	FIA_ATD.1 User attribute definition	The requirement meets the objective by maintaining user attributes to identify user entity explicitly.
	FIA_SOS.1 Verification of secrets	The requirement meets the objective by implementing complexity in password to ensure and improve security in user authentication
	FIA_UAU.1 Timing of authentication	The requirement meets the objective by providing information on authentication procedure before a user is authenticated.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that every user is authenticated before the TOE performs any TSF-mediated actions on behalf of that user.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by providing multiple authentication mechanisms which can be used in conjunction of each other to introduce additional level of security in the user authentication process.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by hiding the password characters entered in the UI by a user while following the authentication process.
	FIA_UID.1 Timing of identification	The requirement meets the objective by providing information on

Objective	Requirements Addressing the Objective	Rationale
		authentication procedure before a user is identified.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that every user is identified before the TOE performs any TSF-mediated actions on behalf of that user.
O.PROTECT_COMM The TOE will provide protected communication channels for parts of the distributed TOE.	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the objective by providing a trusted communication channel between itself and authorized IT entities which are logically distinct from other communication channels while assuring identification of its end points and protecting data from modification and disclosure.
	FPT_ITT.1 Basic Internal TSF Data Transfer Protection	The requirement meets the objective by protecting data being transferred between TOE components from disclosure and modification
	FTP_TRP.1 Trusted Path	The requirement meets the objective by providing a trusted communication path between itself and remote user by allowing them to initiate communication via the used trusted path for the management and authentication operations.
O.BANNER The TOE will present an access banner to TOE users prior to accessing the TOE that defines acceptable use of the TOE	FTA_TAB.1 Default TOE Access Banner	The requirement meets this objective by presenting an access banner to all TOE users prior to being able to login to the TOE
O.TOE_ADMIN The TOE will provide mechanisms to ensure that only authorized administrators are able to	FMT_MOF.1 Management of security functions behavior	The requirement meets the objective by restricting the ability determine and modify the behavior of the management functions.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that only administrators with the ability to manage security attributes for the TOE are allowed to manage TOE.

Objective	Requirements Addressing the Objective	Rationale
configure the TOE security functions attributes.	FMT_MSA.3 Static attribute initialization	The requirement meets the objective by ensuring that the TOE provides restrictive default values for security attributes and specifies alternative initial values to override the default values when an object or information is created.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by controlling access to the configuration parameter of TSF
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.ROBUST_ACCESS The TOE will implement mechanisms that can deny or suspend session establishment	FPT_RPL.1 Replay Detection	The requirement meets the objective by denying access to secured tasks when a replay attack is detected
	FTA_SSL.3 TSF-Initiated Termination	The requirement meets the objective by suspending currently active sessions that have been inactive for a configurable amount of time
	FTA_SSL.4 User-initiated Termination	The requirement meets the objective by allowing user to suspend currently active session that have been initiated by self.
	FTA_TSE.1 TOE Sessions Establishment	The requirement meets the objective by denying users access to the TOE based on user attributes
O.FAIL_SECURE The TOE will provide a method to continue secure operations during a catastrophic TOE failure	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by providing seamless failover over when a failure of the TOE occurs by preserving a secure state.
O.PERMISSIONS The TOE will provide a method to separate and	FMT_SMR.1 Security roles	The requirement meets the objective by associating the permissions of a TOE user to a defined role that provides access to different TSF management functions and data

Objective	Requirements Addressing the Objective	Rationale
restrict the abilities of individual TOE users		

Table 24: Objectives: SFRs Mapping

8.3. Security Assurance Requirements Rationale

The EAL2 extended is chosen to provide a low to moderate level of assurance that is consistent with industry best practices. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment.

The augmentation of ALC_DVS.1 was chosen to give greater assurance of the processes set by the developer that provides the insight of the security measures implemented to provide development security.

8.3.1. Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements,

Security Assurance Requirement	Evidence Title
ASE_CCL.1 Conformance claims	ARCON PAM Security Target
ASE_ECD.1 Extended components definition	
ASE_INT.1 ST introduction	
ASE_OBJ.2 Security objectives	
ASE_REQ.2 Derived security requirements	
ASE_SPD.1 Security problem definition	
ASE_TSS.1 TOE summary specification	
ALC_CMC.2 Use of a CM system	ARCON PAM Configuration Management
ALC_CMS.2 Parts of the TOE CM Coverage	
ALC_DEL.1 Delivery procedures	ARCON PAM Delivery Procedure
ALC_DVS.1 Identification of security Measures	ARCON PAM Development Security
ADV_ARC.1 Security architecture description	ARCON PAM Security Architecture
ADV_FSP.2 Security-enforcing functional specification	ARCON PAM Functional Requirement Specification
ADV_TDS.1 Basic design	ARCON PAM Design Document
AGD_OPE.1 Operational user guidance	ARCON PAM Administrative Guide ARCON PAM Client Manager Guide
AGD_PRE.1 Preparative procedures	ARCON PAM Installation and Configuration Guide
ATE_COV.1 Evidence of coverage	ARCON PAM Security Test Summary Report
ATE_FUN.1 Functional testing	

Table 25: Security Assurance Requirements Evidence

8.4. Dependency Rationale

This ST satisfy all the requirement dependencies of the Common Criteria. The following table lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As per the below table, all dependencies have been met, or rationale has been provided as to why a particular dependency cannot be met.

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	No	FPT_STM.1 is not included because time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable timestamps.
FAU_GEN.2	FAU_GEN.1	Yes	
	FIA_UID.1	Yes	
FAU_SAR.1	FAU_GEN.1	Yes	
FAU_SAR.2	FAU_SAR.1	Yes	
FAU_SAR.3	FAU_SAR.1	Yes	
FAU_SEL.1	FAU_GEN.1	Yes	
	FMT_MTD.1	Yes	
FAU_STG.1	FAU_GEN.1	Yes	
FCS_CKM.1	FCS_CKM.4	Yes	
	FCS_COP.1	Yes	
FCS_CKM.4	FCS_CKM.1	Yes	
FCS_COP.1	FCS_CKM.1	Yes	
	FCS_CKM.4	Yes	
FDP_ACC.1	FDP_ACF.1	Yes	
FDP_ACF.1	FDP_ACC.1	Yes	
	FMT_MSA.3	Yes	
FDP_ETC.1	FDP_ACC.1	Yes	
	FDP_IFC.1	No	No information flows from to and from the controlled objects
FDP_RIP.2	No dependencies	NA	
FDP_SDI.1	No dependencies	NA	
FIA_AFL.1	FIA_UAU.1	Yes	
FIA_ATD.1	No dependencies	NA	
FIA_SOS.1	No dependencies	NA	
FIA_UAU.1	FIA_UID.1	Yes	
FIA_UAU.2	FIA_UID.1	Yes	
FIA_UAU.5	No dependencies	NA	
FIA_UAU.7	FIA_UAU.1	Yes	
FIA_UID.1	No dependencies	NA	
FIA_UID.2	No dependencies	NA	
FMT_MOF.1	FMT_SMR.1	Yes	
	FMT_SMF.1	Yes	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MSA.1	FDP_ACC.1	Yes	
	FMT_SMF.1	Yes	
	FMT_SMR.1	Yes	
FMT_MSA.3	FMT_MSA.1	Yes	
	FMT_SMR.1	Yes	
FMT_MTD.1	FMT_SMR.1	Yes	
	FMT_SMF.1	Yes	
FMT_SMF.1	No dependencies	NA	
FMT_SMR.1	FIA_UID.1	Yes	
FPT_FLS.1	No dependencies	NA	
FPT_ITT.1	No dependencies	NA	
FPT_RPL.1	No dependencies	NA	
FPT_SKP_EXT.1	No dependencies	NA	
FTA_SSL.3	No dependencies	NA	
FTA_SSL.4	No dependencies	NA	
FTA_TAB.1	No dependencies	NA	
FTA_TSE.1	No dependencies	NA	
FTP_ITC.1	No dependencies	NA	
FTP_TRP.1	No dependencies	NA	

Table 26: Functional Requirements Dependencies