# Indian CC Certification Scheme (IC3S)

## Certification Report

| | | |
|---|---|---|
| **Report Number** | **:** | **IC3S/BG01/ARCON/EAL2/0119/0015/CR** |
| **Product / system** | **:** | **ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8** |

**Dated: 30-08-2023**

**Version: 1.0**

**Government of India**
**Ministry of Electronics & Information Technology**
**Standardization, Testing and Quality Certification Directorate**
**6. CGO Complex, Lodi Road, New Delhi – 110003**
**India**

*This report contains a total of 19 pages. In case it needs to be reproduced, all the pages must be included.*

**Product developer:** **ARCON TechSolutions Pvt. Ltd. 901, Kamla Executive Park,**
**Off Andheri-Kurla Road, JB Nagar, Andheri (E), Mumbai –**
**400059**

**TOE evaluation sponsored by**: **ARCON TechSolutions Pvt. Ltd. 901, Kamla Executive Park,**
**Off Andheri-Kurla Road, JB Nagar, Andheri (E), Mumbai –**
**400059**

**Evaluation facility**: **CCTL, ETDC (BG), Bengaluru**
**STQC Directorate, Govt. of India**
**Ministry of Electronics & Information Technology,**
**Peenya Industrial Estate, Ring Road, Bengaluru,**
**Karnataka, 560058, India**

**Evaluation Personnel:**

1) E Kamalakar Rao
2) Jaganath Gupta
3) Ziaul Hasan
4) Prashant Kumar

**Evaluation Technical Report: IC3S/BG01/ARCON/EAL2/0119/0015/ETR1 dated 26-06-2023**

**Validation Personnel:** **Tapas Bandyopadhyay, STQC**

# Table of Contents

## Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY ........... 4

A1 Certification Statement .......... 4

A2. About the Certification Body .......... 5

A3 Specifications of the Certification Procedure .......... 5

A4 Process of Evaluation and Certification .......... 5

A5 Publication .......... 6

PART B: CERTIFICATION RESULTS .......... 7

B.1 Executive Summary .......... 7

B 2 Identification of TOE .......... 9

B 3 Security policy .......... 10

Following is the list of security features available in the TOE: .......... 10

B.4 Assumptions .......... 11

B.5 Evaluated configuration .......... 11

The TSF maintains the roles Administrator, client .......... 12

B.6 Document evaluation .......... 13

B 7 Product Testing .......... 14

B 8 Evaluation Results .......... 17

Table 3: Assurance classes and components wise verdict .......... 18

B 9 Validator Comments .......... 19

B 10 List of Acronyms .......... 19

B 11 References .......... 19

# PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

## A1 Certification Statement

| **The product (TOE) below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.** | |
|---|---|
| Sponsor | **ARCON TechSolutions Pvt. Ltd. 901, Kamla Executive Park, Off Andheri-Kurla Road, JB Nagar, Andheri (E), Mumbai – 400059, India** |
| Developer | **ARCON TechSolutions Pvt. Ltd. 901, Kamla Executive Park, Off Andheri-Kurla Road, JB Nagar, Andheri (E), Mumbai – 400059, India** |
| The Target of Evaluation (TOE) | **ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8** |
| Security Target | **ARCON PAM Version 4.8 Security Target version 1.6** |
| Brief description of product | 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 user 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 privilege 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 log 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 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. |
| CC Part 2 [CC-II] | **Conformant to CC Part 2 Version 3.1 Rev 5** |
| CC Part 3 [CC-III] | **Conformant CC Part 3 Version 3.1 Rev 5** |
| EAL | **EAL2** |
| Evaluation Lab | **Common Criteria Test Laboratory, CCTL, ETDC, Bengaluru** |
| Date Authorized | **17 May 2019** |

## A2. About the Certification Body

**STQC IT Certification Services**, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are-

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/MeitY/Govt. of India);
c) Common Criteria Testing Laboratories (CCTL, ETDC (BG), Bengaluru).

## A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1 Rev 5
- Common Evaluation Methodology (CEM) Version 3.1.

## A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation body **Common Criteria Test Laboratory (CCTL,ETDC( BG), Bengaluru,STQC Directorate, Govt. of India, Ministry of Electronics & Information Technology, Peenya Industrial Estate, Ring Road, Bengaluru, Karnataka, 560058, India has** conducted the evaluation of the product. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

**ARCON TechSolutions Pvt. Ltd. 901, Kamla Executive Park, Off Andheri-Kurla Road, JB Nagar, Andheri (E), Mumbai – 400059, India** is the developer and sponsor of the TOE under certification.

The certification process is concluded with the completion of this certification report. This evaluation was completed on 26th June 2023 after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL 2) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version and release/build of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant apply for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

## A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

# PART B: CERTIFICATION RESULTS

## B.1 Executive Summary

### B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.
Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

Common Criteria Test Laboratory (**CCTL, ETDC, Bengaluru, STQC** Directorate, Govt. of India, Ministry of Electronics & Information Technology, Peenya Industrial Estate, Ring Road, Bengaluru, Karnataka, 560058, India has performed the evaluation. The information in the Certification Report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [**CCTL, ETDC, Bengaluru** STQC Directorate, Govt. of India, Ministry of Electronics & Information Technology, Peenya Industrial Estate, Ring Road, Bengaluru, Karnataka, 560058, India The evaluation team has evaluated and confirmed that the security target [ST] that is used for evaluation of the product is CC Version 3.1, Rev 5 Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL2) have been met.

### B 1.2 Evaluated product and TOE

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. The Evaluated Configuration, its security functions, assumed operational environment, architectural information and evaluated configuration are given below). The TOE & Its Physical Environments & Boundaries are depicted in Figure 1 and Figure 2.

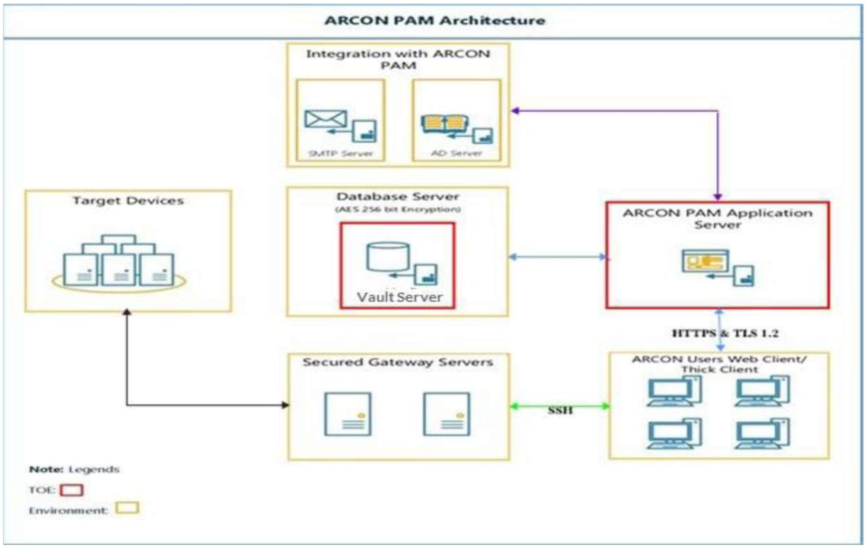

**Figure 1: TOE Boundary**

## B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter. The Security Functional Requirements (SFRs) are taken from CC Part 2.

## B 1.4 Conduct of Evaluation

The common criteria evaluation of the TOE was initiated by the **IC3S Certification** Scheme of STQC Certification Body vide communication no. IC3S/BG01/ARCON/EAL2/0119/0015 dated 30/04/2019.
The Target of Evaluation (TOE) is **ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8.**
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 user 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 privilege 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 log 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 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 was evaluated through evaluation of its documentation; independent testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM]. The Evaluation Assurance Level is **EAL 2+ (Augmented with ALC_DVS.1) as per Common Criteria Version 3.1 Rev 5.**

The evaluation has been carried out under written agreement [19-05-2019] between **CCTL, ETDC (BG), Bengaluru** and the developer/ sponsor **M/s ARCON TechSolutions Pvt. Ltd.**

## B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them, which might have an influence on this assessment.

## B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

## B 1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST document].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

## B 2 Identification of TOE

The TOE is the **ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8**

**TOE has the following identification details:**

- **• Build Number: 4850U4 SP2**
- **Build date: 18th May 2022**
- **Version Number: 4.8The SHA256 hash of the TOE as given below:**

| **Configuration Item** | **Version** | **Size** | **SHA256** |
|---|---|---|---|
| ARCOSServerManager.exe | 4.8.5.0 | 6,438 KB | ddb1414abbdfe486cc6623a509d8ce58b85864aff2fcba0f 617f7d012073818f |
| ARCOSClientManagerOnline.dll | 4.8.5.0 | 1,298 KB | bf6b01ebfb18e34df663026295280125afbc9e5615328bb 65607617f35a71bdb |
| ARCOSClientManagerActiveX.dll | 8.0.0.0 | 42 KB | 99d1483b704608b87148f249d3a3a64eba089fe86d96fc1 a2f7111cf5b48cdd4 |
| ARCON.Common.dll | 5.2.45.6171 | 113 KB | 07142854800b1260d144e35c81cfdb12c893d9d035151c d486203189fc36421e |
| ARCON.NetworkSecure.dll | 5.2.45.6171 | 373 KB | 015c3ef9ab1f8de7e3c3a44c99072356dbd24d81055838f 7e0fbe5bf32a7846a |
| ARCONSWinsockControl.dll | 4.0.0.0 | 76 KB | 23aa9a636c9289339213574daf551e1852e06d59a48cf2a f542f10422e8945b3 |
| ARCOSPasswordGenerator.dll | 4.7.9.1 | 22 KB | 0e2212dbdf8cd00979e49f5bb356baf7b5bc08097a22bb 673753cde1f05f9704 |
| ARCON.Network.DLL | 5.2.45.6171 | 90 KB | 49a4d1342ab9f007b75b55c11f59c459f43365e0e7bea16 e47877c9e843257a9 |
| ARCONACMOCommonFunctions.dll | 4.8.5.0 | 321 KB | 8e7613698ed82b461e086d5033b15ba74f41727da72c68 e9f66242ebfdd18a3f |
| ARCONCommonLibrary.dll | 1.0.0.0 | 1,825 KB | 74e61d9bd759b0ad7dd7645037ff5dd8ff86aa2da145a1 62b3a5db4b1421eaa5 |
| ARCONCommonLibrary.XmlSerializers.dll | 1.0.0.01 | 29 KB | a7f3c25e448c8129709be5d92f82feca651c05df74629cb 7ce38ea6e5495f536 |
| ARCONPAMSecurity.dll | 2.0.0.0 | 37 KB | 80e7b9c4f9700c7fdbe921a5ee171ecd3c0a78b802f63c33 f336d0ed8c96b50a |

## B 3 Security policy

Following is the list of security features available in the TOE:

- Audit Data Generation
- Audit Review
- Protected Audit Trail Storage
- Cryptographic Key Generation
- Cryptographic Key Distribution
- Cryptographic Key Destruction
- Cryptographic Operation
- Subset Access Con troll
- Security attribute based access control
- Export of user data without security attributes
- Full residual Information Protection
- Stored data integrity monitoring
- Authentication Failure Handling
- User attribute definition
- Verification of secrets
- Timing of authentication
- User authentication before any action
- Multiple user authentication
- Protected Authentication feedback
- Timing of Identification
- User identification before any action
- Management of Security Functions Behavior
- Specification of management function
- Management of Security Attributes
- Secure Security Attributes
- Static Attribute Initialization
- Security Roles
- Failure with preservation of secured state
- Basic Internal TSF data protection
- Replay Detection
- Protraction of TSF Data
- Default TOE access banner
- Reliable Time Stamps
- Toe Session establishment
- TSF-initiated termination
- Inter TSF trusted channel
- Trusted Path

## B.4 Assumptions

**There are following assumptions exist in the TOE environment.**

**Table 1: Assumptions**

| Item | Assumption Code | Assumption Description |
|---|---|---|
| 1 | A.PHYSICAL | Physical security is assumed to be provided by the environment. |
| 2 | A.PROTECT | The TOE software will be protected from unauthorized modification. |
| 3 | A.TIMESTAMP | The base IT environment where TOE is hosted provides the TOE with the necessary reliable timestamps. |
| 4 | A.TRUSTED_ADMIN | TOE Administrators are non-hostile and are trusted to follow and apply all administrator guidance. |
| 5 | A.HARDEN | The TOE will be installed on a hardened instance of Windows. |
| 6 | A.ACCESS | Access to the TOE will be provided through a reliable network connection. |
| 7 | A.INSTALL | TOE components will be installed onto a compatible Operating System |
| 8 | 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 |

## B.5 Evaluated configuration

The **Target of Evaluation (TOE)** is ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8.

**TOE description**

The TOE is identified as **ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8**

Product (TOE): **ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8)**

TOE Version: 4.8

The scope of the evaluation includes the following product components

- 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 in the course of 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 privilege 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.

## TOE 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

## Users of the TOE

The TSF maintains the roles Administrator, client

| 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 |

## B.6 Document evaluation

### B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility by the developer, are given below:

1. **Security Target: ARCON PAM Version 4.8 Security Target Version 1.6**
2. **TOE Functional Specification document**: ARCON PAM Functional Requirement Specification 1.7
3. **Design : ARCON PAM Design Document 2.2**
4. **Security Architecture : ARCON PAM Security Architecture Document 1.3**
5. **Preparative procedures**: ARCON PAM Preparative Procedure 2.2
6. **Operational User guidance**: ARCON PAM Operational User Guidance 2.1
7. **Configuration Management Capability: ARCON PAM Configuration Management Capabilities 2.1**
8. **CM scope: ARCON PAM Configuration Management Scope (ALC_CMS) 1.4**
9. **Delivery procedure :** ARCON PAM Delivery Procedure 2.0
10. **Development Security : ARCON PAM Development Security 1.2**
11. **Functional Test : ARCON PAM Functional testing (ATE_FUN) 1.7**
12. **Tests Coverage (ATE_FUN & ATE_COV) :** ARCON PAM Coverage Evidence (ATE_COV) 1.3

### B.6.2 Analysis of document

The developer's documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

**Development process:** The evaluators have analyzed the functional specification of the TOE and found that the TOE security function interfaces [TSFI} are described clearly and unambiguously. The evaluators have analyzed the Security Architecture and Design Documents. The security architecture description explains how the properties described below are exhibited by the TSF. It describes how domains are defined and how the TSF keeps them separate. It describes what prevents untrusted processes from getting to the TSF and modifying it. It describes what ensures that all resources under the TSF's control are adequately protected and all actions related to the SFRs are mediated by the TSF. It explains what role the environment plays in any of these. The security architecture description presents the TSF's properties of self-protection, domain separation, and non-bypassability to protect the TOE itself and the TSF.

**Guidance Documents:** The evaluators have analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information was also clear and unambiguous.

**Configuration management:** The evaluators have analyzed configuration management documentation and determined that the TOE and its associated components and documents are clearly identified as configurable items (CI).

**Delivery Procedure:**

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 part of TOE implementation and are in form of .PDF document.

## B 7 Product Testing

Testing at EAL2+ consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Vulnerability analysis and Penetration testing.

### B 7.1 IT Product Testing by Developer

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].The evaluators have analyzed the developer's test coverage and found them to be complete and satisfactory. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

### B 7.2 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of test results. The evaluators have examined the TOE and it is found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:

The TOE has been installed properly as per the preparative procedure document. While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements. Independent testing is designed to verify the correct implementation of security functionalities available to different categories of users and to check whether audit record is being generated for auditable events, also checked for the privilege escalation is prevented.

The tests were designed to cover following TSFs and associated TSFIs of the TOE:

a. **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.

b. **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.

c. **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.

d. **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.

e. **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.

f. **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.

g. **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.

h. **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.

## B 7.2 Vulnerability Analysis and Penetration testing

The evaluators have considered the threats identified in ST and conducted vulnerability search from the internal documents and the information available in the public domain in search of potential vulnerabilities from public domain. For this purpose scanning tools are used. The Nmap tools were used for scanning to find out open ports. Nessus Vulnerability scanning tool is used with the latest plug in to find out hypothesized potential vulnerabilities present in the TOE. The OWASP Top Ten 2021 – The Ten Most Critical Web Application Security Risks, CIS Benchmarks Standard was used to searched for vulnerabilities.

The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1

and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

The evaluator has analyzed the evaluation evidences like, the ST, the Functional Specification, the TOE Design, the Security Architecture Description and the Guidance Documentation and as well as the operational environment, stated in the ST and then hypothesized the security vulnerabilities considering five categories of attack to the Security functions, viz. 'Bypassing', 'Tampering', 'Direct Attacks', 'Monitoring' and 'Misuse'.

Considering the type of the TOE and its intended use, the possibility of "Direct Attack" is negligible; evaluator's judgement is justified and supported by analysis. The evaluator has identified the following Attack scenarios.

VS1. Cross Site Scripting (XSS) attacks on various input fields from application webpages

Attack Potential: 8 (Within Basic) Penetration Testing is required]

VS2. SQL Injection (SQLI) on input fields on Login page

Attack Potential: 9 (Within Basic) Penetration Testing is required]

VS3. Path traversal to find hidden directories and files

Attack Potential: 4 (Within Basic) Penetration Testing is required]

VS4. Local File Inclusion attack to upload malicious file to compromise the server

Attack Potential: 4 (Within Basic) Penetration Testing is required]

VS5. Distributed Denial of Service (DDoS) attacks through flooding of crafted packets

Attack Potential: 5 (Within Basic) Penetration Testing is required]

VS6. Microsoft's Data Access Component (MDAC) ActiveX vulnerability exploitation

Attack Potential: 11 (Beyond Basic) Penetration Testing is not required]

VS7. Fuzz Testing on various input fields to identify security issues

Attack Potential: 5 (Within Basic) Penetration Testing is required]

VS8. Brute Force Attack on the login page to identify basic/common accounts

Attack Potential: 2 (Within Basic) Penetration Testing is required]

VS9. SSL Stripping attacks

Attack Potential: 5 (Within Basic) Penetration Testing is required]

VS10. Denial of service through account lock-out

Attack Potential: 0 (Within Basic) Penetration Testing is required]

The relevant attack potentials, corresponding to the identified vulnerabilities have been estimated considering various factors like the 'time to identify & exploit', 'expertise required', 'knowledge of the TOE', 'windows of opportunity' and 'equipment required'. The calculated attack potentials are as follows:

The evaluator conducted **Penetration Testing**:

PT1: for attack scenario AT1: Cross Site Scripting (XSS) attacks on various input fields from application webpages. The TOE web interface has various user input fields. These input fields may be prone to XSS attacks if the fields are not sanitized properly for malicious values.

PT2: VS2. SQL Injection (SQLI) on input fields on Login page

PT3: Path traversal to find hidden directories and files.

The server hosting the TOE application may contain some hidden directories and files which can disclose some sensitive data which can be misused by the attacker

PT4: Local File Inclusion attack to upload malicious file to compromise the server after identifying if the application is vulnerable to LFI attack

PT5: Distributed Denial of Service (DDoS) attacks through flooding of crafted packets

PT7: Fuzz testing on various input fields to identify security issues.

PT8: Brute Force Attack on the login page to identify basic/common accounts

PT9: SSL Stripping attacks Man In the Middle (MiTM) attacks

PT10: Denial of service through account lock-out

The Evaluator could not able to exploit the hypothesized Security vulnerabilities/ concern of the TOE evolved through analysis of evaluation objects.

Hence, it is concluded that the TOE does not contain any exploitable vulnerability for 'Basic' Attack Potential.

As the target assurance level is EAL 2+, the evaluation team has restricted their Penetration Testing activities to the attack scenarios for which the estimated attack potential is less than 10. Considering the attack potential as 'Basic', the evaluators could exploit no identified vulnerabilities.

Hence, the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'. However, these Vulnerabilities may be exploited with higher attack potential.

The identified vulnerability, having attack potential more than 'Basic' was not considered for penetration Testing. Hence, this vulnerability may be considered as residual vulnerabilities. The residual vulnerabilities given below.

Subsequent to the independent review of public domain vulnerability databases and all evaluation evidences, potential vulnerabilities were identified with their attack potentials. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing.

The penetration testing could not exploit any vulnerability in the intended operational environment of the TOE. However, these vulnerabilities may be exploited with higher attack potential.

**Residual Vulnerabilities**

Considering the attack potential as 'Basic', the evaluators could exploit no identified vulnerabilities. Hence, the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'. However, these vulnerabilities may be exploited with higher attack potential.

The identified vulnerabilities, having attack potential more than 'Basic' were not considered for penetration testing. Hence, these vulnerabilities may be considered as residual vulnerabilities. The residual vulnerabilities are given below.

**VS6/AT6:** Microsoft's Data Access Component (MDAC) ActiveX vulnerability exploitation.

Attack Potential: 11 **(Beyond Basic**).

## B 8 Evaluation Results

The evaluation team has documented the evaluation results in the Evaluation Technical Report [ETR]. The TOE was evaluated through evaluation of its evaluation evidences, documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedures.

**Documentation evaluation results:**

The documents for TOE and its development life cycle have been analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CC Version 3.1 Revision 5 for Evaluation level EAL2+ (Augmented with ALC_DVS.1).

**Testing:**

The independent functional tests yielded the expected results, giving assurance that '**ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8**' behaves as specified in its [ST].

**Vulnerability assessment and penetration testing:**

The penetration testing with '**Basic**' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

**Table 3: Assurance classes and components wise verdict**

| Assurance classes and components | | | Verdict |
|---|---|---|---|
| Security target document evaluation | | ASE | PASS |
| 1. | ST introduction | ASE_INT.1 | PASS |
| 2. | Conformance claims | ASE_CCL.1 | PASS |
| 3. | Security problem definition | ASE_SPD.1 | PASS |
| 4. | Security objectives | ASE_OBJ.2 | PASS |
| 5. | Extended component definition | ASE_ECD.1 | PASS |
| 6. | Derived Security requirements | ASE_REQ.2 | PASS |
| 7. | TOE Summary Specification | ASE_TSS.1 | PASS |
| TOE Development evaluation | | ADV | PASS |
| 1 | Security architecture description | ADV_ARC.1 | PASS |
| 2 | Security-enforcing functional specification | ADV_FSP.2 | PASS |
| 3 | Basic design | ADV_TDS.1 | PASS |
| TOE Guidance document evaluation | | AGD | PASS |
| 1 | Operational user guidance | AGD_OPE.1 | PASS |
| 2 | Preparative procedure | AGD_PRE.1 | PASS |
| TOE Life cycle support evaluation | | ALC | PASS |
| 1 | Use of a CM system | ALC_CMC.2 | PASS |
| 2 | Parts of the TOE CM coverage | ALC_CMS.2 | PASS |
| 3 | Delivery procedures | ALC_DEL.1 | PASS |
| Testing of the TOE | | ATE | PASS |
| 1 | Evidence of coverage | ATE_COV.1 | PASS |
| 2 | Functional Testing | ATE_FUN.1 | PASS |
| 3 | Independent Testing - Sample | ATE_IND.2 | PASS |
| Vulnerability assessment of the TOE | | AVA | PASS |
| 1 | Vulnerability Analysis | AVA_VAN.2 | PASS |

## B 9 Validator Comments

The Validator has reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, worksheets, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] ARCON PAM Version 4.8 Security Target version 1.6 has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that 'ARCON PAM Version 4.8 comprising of Vault Server 4.8 and Application Server 4.8"satisfies all the security functional requirements ( SFR) and Security assurance requirements( SAR) as defined in the [ST]. Hence, the TOE is recommended for EAL2+ (augmented with ALC-DVS.1) Certification as per CC version 3.1 Revision 5.**

However, it should be noted that there are no **Protection Profile** compliance claims.

## B 10 List of Acronyms

ACL: Access Control List

CC: Common Criteria

CCTL: Common Criteria Test Laboratory

CEM: Common Evaluation Methodology

EAL: Evaluation Assurance Level

ETR: Evaluation Technical Report

FSP: Functional Specification

IC3S: Indian Common Criteria Certification Scheme

IT: Information Technology

PP: Protection Profile

ST: Security Target

TOE: Target of Evaluation

TDS: TOE Design Specification

TSF: TOE Security Function

TSFI: TOE Security Function Interface

## B 11 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [ST] : ARCON PAM Version 4.8 Security Target, Version 1.6
6. [ETR]: Evaluation Technical Report No. IC3S/BG01/ARCON/EAL2/0119/0015/ETR1