

Department of Veterans Affairs

Cardiac Rehab Provider System Integration with Identity and Access Management Services

Integration Requirements Specification Document



February 2015

Version 0.4

Revision History

The revision history cycle begins once changes or enhancements are requested after the integration Requirements Specification Document has been baselined.

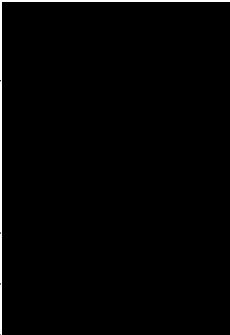
Date	Version	Description	Author
02/04/2014	0.4	Added signature line for Consuming Application Business Representative.	
12/11/2014	0.3	Updates to clarify Central Login screen version to use, authorization policy and added a note to trait list to indicate future state.	
12/09/2014	0.2	Updates with projected usage	
12/04/2014	0.1	Initial Draft – with questions noted	

Table of Contents

1.0	Introduction.....	1
1.1	Purpose.....	1
1.2	Scope	1
1.3	References.....	2
1.3.1	Requirements, Design, and Service Description Documentation	2
1.3.2	Business Policy Documentation	2
1.3.3	Abbreviations and Definitions	2
2.0	Functional Requirements	2
2.1	Functional Requirements for Cardiac Rehab Provider.....	2
2.1.1	Single Sign On Internal (SSOi)	2
2.2	Functional Requirements for IAM.....	6
2.2.1	SSOi	6
3.0	Other Specifications	6
3.1	Business Rules Specifications	6
3.2	Design Constraints Specifications.....	7
3.3	Disaster Recovery Specifications	7
3.4	Performance Specifications.....	7
3.5	Quality Attributes Specifications.....	7
3.6	Security Specifications	8
4.0	Attachment A: Approval Signatures.....	9

1.0 Introduction

1.1 Purpose

The purpose of this integration Requirements Specification Document (iRSD) is to provide the requirements that the Cardiac Rehab Provider Development team needs to integrate Cardiac Rehab Provider with Identity and Access Management (IAM) services, in accordance with the IAM service request: SR-457.

Integrations with IAM services are mandated by executive management via the following mandates:

- IAM Identity Services (IdS) mandate memorandum (VAIQ #7011145). All applications within VA must comply with IAM requirements to ensure that references to the identities of Veterans and their beneficiaries are accurate.
- IAM Access Services (AcS) functionality within VA is mandated by VAIQ #7060071 ([REDACTED]).

The target audiences for this iRSD include the following:

- **VHA Health Information Governance (HIG)/Data Quality (DQ):** This group is the business owner for Identity Services/Master Veteran Index, and is responsible for managing the IdS business requirements.
- **Office of Information Security (OIS) IAM Business Program Management Office (BPMO):** This group is responsible for managing the AcS business requirements.
- Cardiac Rehab Provider **Business Sponsor** and the Cardiac Rehab Provider **Development team**. These groups are responsible for fulfilling the IAM requirements within the Cardiac Rehab Provider system.
- **IAM Development Leads:** They are responsible for the implementation of IAM requirements and ensuring the correct integration of Cardiac Rehab Provider with IAM-approved requirements.

Note: This document does not contain the detailed requirements for the changes needed in the Cardiac Rehab Provider system to integrate with IAM services. The Cardiac Rehab Provider team should use this document as a guide for writing the detailed system and, if applicable, user interface design specifications. The Cardiac Rehab Provider team should include both IAM business and technical representatives as stakeholders regarding the Cardiac Rehab Provider design documents. The Quality Attributes Specification section of this document provides more information about the integration process.

1.2 Scope

The Cardiac Rehab Provider application allows VA clinicians to monitor progress of the cardiac rehabilitation patients and make updates to VistA. The application is being migrated within the VA firewall. As part of its integration to IAM services, Cardiac Rehab calls the following AcS service:

- SSOi SiteMinder pattern

Initially, the the SSOi data about the user will contain information from VA Active Directory (AD) only.

After IAM Provisioning has completed its integration with VistA, the SSOi information will be updated to include any VistA Site and DUZ information for the user that is known to Provisioning.

1.3 References

1.3.1 Requirements, Design, and Service Description Documentation

The applicable IAM requirements, design, and service description documentation are included in the following:

- [Designation of Identity and Access Management Business Sponsor \(VAIQ #7060071\)](#)
- [AcS Use Cases and Models](#)
- [VA IAM AcS Integration Patterns](#)
- VistA-IAM iRSD

1.3.2 Business Policy Documentation

The applicable IAM business policies are included in the following:

- [VA Directive 6500 Information Security Program](#)
- [Section 508 Standards Guide](#)

1.3.3 Abbreviations and Definitions

The applicable IAM Terms and Definitions can be found in the [Identity and Access Services Master Glossary](#).

2.0 Functional Requirements

2.1 Functional Requirements for Cardiac Rehab Provider

The functional requirements for the Cardiac Rehab Provider integration with IAM services are identified in this section.

Cardiac Rehab Provider shall integrate with IAM SSOi using the CA SiteMinder Web Agent Pattern.

2.1.1 Single Sign On Internal (SSOi)

Cardiac Rehab Provider will use IAM's Single Sign On Internal (SSOi) service. The IAM SSOi service is an authentication service specifically designed for controlling access for VA internal users (employees and contractors) accessing VA applications. This service enhances the user experience by reducing the time associated with multiple log on and log off activities that require

application-specific identifiers and passwords. The service also enables enriched password management and reduction in help desk support.

The operation that occurs between SSOi web agent and Cardiac Rehab Provider is described below.

- **Authenticate Internal User:** Allows a user to sign on once to an application, using PIV/PIN or VA Active Directory (AD) username/password, then allows the user to access other integrated applications using the sign-on credentials originally submitted

The SSOi service uses the following COTS product for web-based applications:

- **Computer Associates (CA) SiteMinder (SM):** Users access integrated web-based applications via CA SiteMinder.

Detailed below is the interface defined by the Cardiac Rehab Provider team and configured by SSOi services to SSOi-enable a Cardiac Rehab Provider user.

CA SiteMinder Web Agent: The web agent is used to intercept access requests for protected resources and work with the Policy Server to determine whether or not a user should have access. The web agent resides on a web server and intercepts requests for a resource to determine whether or not the resource is protected by SiteMinder. The web agent then interacts with the CA SiteMinder Policy Server to authenticate and authorize users who request access to the protected web server resources of Cardiac Rehab Provider

Qualifying Criteria

- For integration with CA SiteMinder SSO, Cardiac Rehab Provider must be a web-based application.
- For integration with CA SiteMinder SSO, Cardiac Rehab Provider must have infrastructure supporting integration of the web agent.
- For integration with CA SiteMinder SSO, the Cardiac Rehab Provider authentication process must work with identifiers passed to it from the web agent.

Process Flow

1. Cardiac Rehab Provider user logs on to the workstation with credentials.
2. Cardiac Rehab Provider user selects Cardiac Rehab Provider or navigates to the URL.
3. SSOi SiteMinder intercepts the request.
4. SSOi checks for the presence of the user's SSOi credential
 - a. If no SSOi credential is present, SSOi presents the IAM Centralized Login Page so the user can authenticate to SSOi using one of the following methods:
 - i. VA Network User ID/Password
 - ii. PIV/PIN
 - iii. Windows Authentication
(other option – PIV only)

5. If the user fails to authenticate to SSOi through the IAM Centralized Login Page, SSOi presents an error page.
6. SSOi performs authorization based on the authorization policy created in SSOi for Cardiac Rehab Provider Community of Interest
 - a. The user must be in Active Directory.
7. If the user fails the SSOi authorization check, SSOi presents an error message.
8. If the user passes the SSOi authentication and authorization, the user is forwarded to Cardiac Rehab Provider with SSOi credentials.
9. SSOi SiteMinder intercepts the request.
10. SSOi SiteMinder calls the SSOi Policy Server to check on whether the SSOi user session is active
 - a. The user session timeout is set at 15 minutes for Cardiac Rehab Provider
Note: The 15 minute timeout is set per VA 6500 policy. every time the user clicks a link within the application, this check is performed and the timeout is reset.
11. SSOi SiteMinder requests user attributes from the SSOi Policy Server.
12. SSOi SiteMinder passes the user data to Cardiac Rehab Provider
13. Cardiac Rehab Provider accepts the authenticated SSOi user as authenticated to Cardiac Rehab Provider.
 - a. Cardiac Rehab Provider authorizes the user based on traits passed from SSOi.

Diagram of Process Flow

- adDomain
- adSamAccountName
- adUpn
- adEmail
- firstName
- lastName

Note: IN a future update, IAM traits will include the user's VistA site and DUZ.

4. Cardiac Rehab Provider shall redirect the user to the to the IAM Authenticated Landing Page when user initiates logout.

2.2 Functional Requirements for IAM

The IAM functional requirements for the Cardiac Rehab Provider integration are identified in this section. IdS/AcS provides the following functionality.

2.2.1 SSOi

Requirements

1. IAM shall provide SSOi services using CA SiteMinder to Cardiac Rehab Provider.
2. SSOi shall provide the Centralized Login Page with the following authentication methods:
 - VA Network User ID/Password
 - PIV/PIN
 - Windows Authentication
3. SSOi shall perform authorization based on the authorization policy created in SSOi as defined by Cardiac Rehab Provider .
4. SSOi shall present an error message if the Cardiac Rehab Provider user fails to authenticate to SSOi.
5. SSOi shall present an error message if the Cardiac Rehab Provider user fails to authorize based on the authorization policy.

3.0 Other Specifications

3.1 Business Rules Specifications

The business rules are expressed in the functional requirements.

3.2 Design Constraints Specifications

The design constraints specifications are identified in the Functional Requirements section of this document and in the following documents:

- AcS Interface Control Documents

3.3 Disaster Recovery Specifications

There are no disaster recovery specifications for the Cardiac Rehab Provider integration with IAM services. The AcS disaster recovery specifications include the following:

- The AcS solution is hosted by Terremark and leverages the Disaster Recovery Plan and Concept of Operations (CONOPS) to support the systems that require continuous availability.

3.4 Performance Specifications

The Cardiac Rehab Provider team estimates the following usage pattern:

Initial implementation (Fall/Winter 2015)

- Number of users - 20
- Number of logins per week or day – 2/day
- Peak logins per hour - 5
- Time of peak logins (hour or hours of the day, days or months of the year if there is some sort of annual cycle – 9AM

After roll out to entire user population (2016)

- Number of users – 500 (an estimate of how many people I think may actually be using with any regularity)
- Number of logins per week or day – average will probably be 1/day, with some users logging in more frequently - probably 5/day
- Peak logins per hour - 100
- Time of peak logins (hour or hours of the day, days or months of the year if there is some sort of annual cycle – 9AM

3.5 Quality Attributes Specifications

Cardiac Rehab and IAM agree to participate in the following activities to ensure the quality of the system:

- Acceptance and baseline of the iRSD
- Change control
- Unit testing
- Integration/functional testing

- User acceptance testing

The following quality processes are followed:

a. Stakeholder Review and Oversight

The Cardiac Rehab development team shall include both IAM business and technical representatives as stakeholders for approval of the IAM-related detailed requirements and design.

b. Requirements Management Traceability

The IAM portion of the Cardiac Rehab Provider detailed system and user interface requirements and design specifications shall be traceable back to this iRSD.

c. Change Control

The baselined version of this iRSD is stored in IBM Rational ClearCase. Changes to this iRSD shall be accomplished by creating an IAM change request (CR) and shall follow standard Program Management Accountability System (PMAS) approval processes.

d. Integration Testing

Integration testing between Cardiac Rehab Provider and IAM

Note: An integration test schedule needs to be developed to identify the test environment.

3.6 Security Specifications

Cardiac Rehab Provider and IAM agree to meet the following requirements:

1. Cardiac Rehab Provider and IAM shall conform to the VA security standards detailed in VA Handbook 6500 Information Security Program.

4.0 Attachment A: Approval Signatures

REVIEW DATE

Signed: <[REDACTED] Representative> [REDACTED] <mm/dd/yyyy>

Signed: [REDACTED] [REDACTED] [REDACTED] <mm/dd/yyyy>

Signed: [REDACTED] [REDACTED] <mm/dd/yyyy>