

**Identity and Access Management  
Access Services 2.0 Increment 5  
Requirements Specification Document**



**Department of Veterans Affairs**

**March 2015**

**Version 1.6**

## Revision History

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

Date	Version	Description
3/31/2015	1.6	Completed a quality review. Replaced doc v1.3 with doc v1.6 on the AcS TSPR.
3/25/2015	1.5	Updated document with Rational Requirements Composer Feature tags to uniquely identify the traceable requirements.
3/06/2015	1.4	Updated 2.6.3.6 and Appendix C as per updated business rules for multiple EDI PI and SEC ID and i5 Kickoff action items.
3/06/2015	1.3	Completed a quality review. Replaced doc v1.0 with doc v1.3 on the AcS TSPR.
3/05/2015	1.2	Document updated with Rational Requirement Composer Feature tags for the new requirements.
1/27/2015	1.1	Per Work Item 150690, new Identity Proofing requirements entered in Section 2.6.6. Updated AccessVA UI requirements in Section 2.6.2.
12/31/2014	1.0	Completed a quality review. Document version changes to 1.0 upon stakeholder approval. Posted the PDF with email approval signatures on the AcS TSPR. Attached Word doc to CR EAuth 4982.
12/23/2014	0.8	Updated traceable requirements with Rational Requirements Composer Feature tags.
12/22/2014	0.7	Added 3 new Standard SSOi Trait requirements in section 2.6.3.1.
11/25/2014	0.6	Added support for 3 address lines in Provisioning Service Elimination of local Provisioning Search for CRISP on-boarding Update Performance requirements based upon VistA requirements
11/18/2014	0.5	Updated traceable requirements with Rational Requirements Composer Feature tags
10/24/2014	0.4	Updated with Formal Review Feedback
10/16/2014	0.3	Updated with Peer Review Feedback
10/05/2014	0.2	Completed a tech edit review
9/19/2014	0.1	Initial Draft

*Place latest revisions at top of table.*

*The Revision History pertains only to changes in the content of the document or any updates made after distribution. It does not apply to the formatting of the template.*

*Remove blank rows.*

## **Artifact Rationale**

The Requirements Specification Document (RSD) records the results of the specification gathering processes carried out during the Requirements phase. The RSD is generally written by the functional analyst(s) and should provide the bulk of the information used to create the test plan and test scripts. It should be updated for each increment.

The level of detail contained in this RSD should be consistent with the size and scope of the project. It is not necessary to fill out any sections of this document that do not apply to the project. The resources necessary to create and maintain this document during the life cycle of a large project should be acknowledged and clearly reflected in project schedules. Do not duplicate data that is already defined in another document or a section in this document; note in the section where the information can be found.

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Purpose .....	1
1.2	Scope.....	2
1.3	References .....	2
<b>2</b>	<b>Overall Description .....</b>	<b>5</b>
2.1	Accessibility Specifications .....	5
2.2	Business Rules Specification.....	5
2.3	Design Constraints Specification .....	5
2.4	Disaster Recovery Specification .....	5
2.5	Documentation Specifications .....	5
2.6	Functional Specifications .....	5
2.6.1	Single Sign-On – Internal (SSOi) .....	6
2.6.1.1	Security Token Service (STS) Support of JSON Web Token and Bearer Token.....	6
2.6.1.2	Expose STS Service with REST Interface .....	7
2.6.1.3	Standard SSOi Traits .....	7
2.6.1.4	SSOi Deferred Requirements .....	9
2.6.2	AccessVA .....	9
2.6.2.1	AccessVA UI Updates.....	9
2.6.2.2	AccessVA Future Vision Requirements.....	14
2.6.3	Single Sign-On – External.....	17
2.6.3.1	Support Imprecise Date of Birth from MVI.....	17
2.6.3.2	SSOe Accepts Address and Phone # from VDS.....	18
2.6.3.3	SSOe Accepts JSON Web Token and Bearer Token.....	18
2.6.3.4	Expose STS Service with REST Interface .....	18
2.6.3.5	OAuth Validation Service .....	19
2.6.3.6	SSOe Provides PID, BIRLS, SEC ID, and EDI PI IDs.....	19
2.6.3.7	Third-Party Credential Onboarding .....	20
2.6.4	Provisioning .....	21
2.6.5	Compliance Audit and Reporting (CAR) .....	26
2.6.5.1	Role Engineering and Compliance Tool Integration with CAR .....	26
2.6.6	Identity Proofing (IP).....	27
2.7	Graphical User Interface (GUI) Specifications .....	28
2.8	Multi-divisional Specifications .....	28
2.9	Performance Specifications .....	28
2.9.1	Example Performance Specification for AcS Service Component....	29
2.9.2	Single Sign-On – Internal (SSOi) .....	30
2.9.3	Single Sign-On – External (SSOe) and AccessVA .....	31
2.9.4	Provisioning (Prov).....	33

2.9.5	Compliance Audit and Reporting (CAR) .....	34
2.9.6	Specialized Access Control (SAC) .....	35
2.9.7	Electronic Signature (ESig).....	35
2.9.8	Identity Proofing (IP).....	36
2.9.9	Credential Service Provider (CSP) .....	37
2.10	Quality Attributes Specification .....	37
2.11	Reliability Specifications .....	38
2.12	Scope Integration .....	39
2.13	Security Specifications .....	39
2.14	System Features.....	39
2.15	Usability Specifications .....	39
3	Applicable Standards .....	39
4	Interfaces.....	41
4.1	Communications Interfaces .....	41
4.2	Hardware Interfaces .....	41
4.3	Software Interfaces .....	41
4.4	User Interfaces.....	41
5	Legal, Copyright, and Other Notices .....	41
6	Purchased Components.....	41
6.1	Defect Source (TOP 5).....	41
7	User Class Characteristics.....	41
8	Estimation .....	42
9	Approval Signatures.....	44
	Appendix A: Acronym List and Glossary.....	46
	Appendix B: Requirements Deferred to AcS 2.0 Increment 5.....	47
	Appendix C: SSOe Headers .....	50
	Appendix D: CRISP Onboarding Activity Diagram.....	54

## List of Figures

Figure 1: AccessVA Unauthenticated Home Page .....	12
Figure 2: AccessVA Unauthenticated Home Page (CSP Selection).....	13
Figure 3: AccessVA Sign-In Partners Page .....	14
Figure 4: AccessVA Login Button .....	15
Figure 5: AccessVA User Type Selector Pop-Up Widget.....	16
Figure 6: AccessVA User Type Selector Pop-Up Widget – Expanded.....	16
Figure 7: AccessVA CSP Selector Pop-Up Widget.....	17
Figure 8: Offboarding Screen.....	25
Figure 9: Error Messages Displayed on Search for User Screen .....	26
Figure 10: Cumulative Probability (“S-curve”) Chart.....	43

## List of Tables

Table 1: Document References.....	3
Table 2: SSOi Support of JSON Web Token and Bearer Token Business Needs and Requirements Enhancements .....	6
Table 3: Expose STS Service with REST Interface Business Needs and Requirements Enhancements.....	7
Table 4: Provisioning Business Needs and Requirements Enhancements.....	21
Table 5: Role Engineering and Compliance Tool Integration with the CAR Service Business Needs and Requirements Enhancements.....	26
Table 6: Name and Description of Reports to Reside in CAR .....	27
Table 7: Performance Specifications.....	28
Table 8: Service Availability Level 4 .....	38
Table 9: Applicable Standards .....	40
Table 10: LOA 2+ Authentication Traits Business Rules.....	50

# 1 Introduction

The Department of Veterans Affairs (VA) serves a vast enterprise of VA stakeholders, including the Veteran, the Veteran's Beneficiary, the Veteran Support Representative, business partners such as loan officers and providers, along with internal businesses and programs.

The Veterans Relationship Management (VRM) Program Management Office (PMO) has identified the need to further develop the core Access Services (AcS) to definitively and consistently identify VA stakeholders, and to establish supporting processes that provide the appropriate level of security required to protect and manage the identities, information, and interests of the VA stakeholders. AcS is currently developing and supporting these core authentication and authorization capabilities to provide uniform enterprise methods.

VA acknowledges the importance of providing a single, uniform method to identify and provide access for Veterans and their representatives who use VA services.

The VA lines of business (LOB) often cross departments and programs within and outside of VA. AcS protects the Veteran by safeguarding sensitive information viewed and retrieved by Veterans, their family members and caregivers, beneficiaries, employees and other VA stakeholders. AcS also provides a consistent experience for the Veteran or their representative across all LOB, by using a standard process to identify the requestor of Veteran information, and to retrieve the data from the authoritative source.

The AcS solution supports VA's mission to assure the Veteran or their representative that sensitive information is only retrievable by authorized personnel.

## 1.1 Purpose

The purpose of this RSD is to summarize the business and functional requirements that are required for the development and implementation of AcS 2.0 Increment 5.

The AcS 2.0 Increment 5 requirements described in this RSD are drawn from VA AcS FY15 Business Requirements Documents (BRDs). Additional AcS 2.0 Increment 5 requirements may be found in consuming application integration analysis efforts in the form of integration Requirements Specification Documents (iRSDs) approved by the Identity and Access Management (IAM) Integrated Project Team (IPT).

This RSD supports the development of the AcS 2.0 Increment 5 System Design Document (SDD), which provides guidance for the implementation and development of the AcS solution.

This RSD provides a foundation for establishing baseline test cases and identifies the capabilities and functionalities to be compared and assessed against the VA AcS requirements.

The target audiences for this RSD include the following:

- VRM IAM IPT
- AcS Business and Technical Stakeholders
- Health Information Governance/Data Quality
- Office of Information and Security

The AcS Development Partners are responsible for supporting the delivery, implementation, and maintenance of the system.

The current development partners include the following:

- The Development team responsible for implementing approved AcS 2.0 Increment 5 requirements
- IAM Program Office
- Product Support
- Master Veteran Index (MVI) Development Leads
- AcS Development Leads
- Other technical support personnel and product vendors

## 1.2 Scope

The scope of this RSD encompasses the AcS requirements that VA is requesting for AcS 2.0 Increment 5. The AcS requirements include the following components:

- Single Sign-On – Internal (SSOi)
- Single Sign-On – External (SSOe)
- AccessVA
- Provisioning (Prov)
- Virtual Directory Service (VDS)
- Compliance Audit and Reporting (CAR)

While AcS consists of additional components to those listed above, no new requirements for the following have been identified for this RSD:

- Identity Proofing (IP)
- Electronic Signature (ESig)
- Credential Service Provider (CSP)
- Specialized Access Control (SAC)
- Role Engineering and Compliance

Additionally, [Appendix B](#) contains a list of requirements that were stated in previous AcS RSDs but deferred to AcS 2.0 Increment 5 for delivery.

## 1.3 References

This section identifies additional project-specific documentation and external sources of information referenced or cited to support the development of this RSD. In the table below, a list of references, including the document title, publication date, and publisher, is provided.

**Table 1: Document References**

<b>Title</b>	<b>Date</b>	<b>Published By</b>
<a href="#">AcS FY15 BRD</a>	01/2014	OIS BPMO
<a href="#">Section 508 Standards Guide</a>	04/16/2010	General Service Administration
<a href="#">NIST Special Publication (SP) 800-63 Version 1.0.2: Electronic Authentication Guideline</a>	04/2006	National Institute of Standards and Technology (NIST)
<a href="#">VA Directive 6500: Information Security Program</a>	08/2006	VA
VA Directive 6501; VA Identity Verification In Person Proofing (IPP) Process; IAM Handbook	Last updated: 09/01/2010	VA
<a href="#">NIST Public Key Infrastructure (PKI) Program</a>	2/2001	National Institute of Standards and Technology (NIST)
VA IAM Handbook 6510	TBD	VA
<a href="#">VRM IAM Scope and Vision Document</a>	10/2012	VA
<a href="#">Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0</a>	12/2011	Federal CIO Council
<a href="#">OMB 04-04 E-Authentication Guidance for Federal Agencies</a>	12/2003	Office of Management and Budget (OMB)
<a href="#">Security Assertion Markup Language (SAML) Artifact Profile as an Adopted Scheme for E-Authentication, Version 1.0.0</a>	6/2004	GSA
Security Assertion Markup Language (SAML) Artifact Profile as an Adopted Scheme for E-Authentication, Version 1.1.0	9/2005	GSA
<a href="#">Sec-ID MVI iRSD</a>	9/2012	IAM Integration Analysis Team
<a href="#">AcS i3 RSD</a>	9/2012	IAM Access Service Analysis Team

<b>Title</b>	<b>Date</b>	<b>Published By</b>
<a href="#">AcS i4 RSD</a>	3/2013	IAM Access Services Analysis Team
<a href="#">AcS 2.0 Increment 2 RSD</a>	8/2013	IAM Access Services Analysis Team
<a href="#">AcS SDD</a>	12/2013	AcS Development Contractors
AcS 2.0 Increment 2 UC Model	TBD	
<a href="#">AcS 2.0 Increment 3 RSD</a>	4/2013	IAM Access Services Analysis Team
AcS 2.0 Increment 4 RSD		IAM Access Services Analysis Team
<a href="#">Role Management in IdentityIQ</a>	9/2013	SailPoint
<a href="#">Role Models and Methodology</a>	3/2010	SailPoint
<a href="#">Lifecycle of a Certification</a>	7/2013	SailPoint
<a href="#">SailPoint Best Practices – Certification Generation on large deployments</a>	12/2013	SailPoint
<a href="#">Delimited File Application Set-up and Configuration</a>	2/2014	SailPoint
<a href="#">Managing Extended Attributes</a>	2/2014	SailPoint
<a href="#">IAM Portal Strategy</a>	2/2013	IAM Technical Lead
<a href="#">IAM IP-MVI Integration iRSD</a>	11/2013	IAM Access Services Analysis Team
<a href="#">MVI Service Description Document</a>	1/2013	IAM Identity Services Team
<a href="#">Initial AccessVA RSD (Listed as EAG)</a>	3/2013	IAM Access Services Team
<a href="#">AccessVA Use Case Specification (Listed as EAG)</a>	1/2013	AccessVA Development Contractors
<a href="#">SSOe AccessVA AcS Increment 2 RSD</a>	12/2013	IAM Services Analysis Team
<a href="#">SSOe VAAFI AccessVA 2.0 Increment 3 RSD</a>	5/2014	IAM Services Analysis Team
<a href="#">SSOe VAAFI AccessVA 2.0 Increment 4 RSD</a>	5/2014	IAM Services Analysis Team
<a href="#">AcS 2.0 Increment 3 SDD</a>	5/2014	AcS Development Contractors
<a href="#">SSOe VAAFI AccessVA 2.0</a>	11/2013	SSOe AccessVA

Title	Date	Published By
<a href="#">Increment 2 SDD</a>		Development Contractors
SSOe VAAFI AccessVA 2.0 Increment 3 SDD	5/2014	SSOe AccessVA Development Contractors

## 2 Overall Description

The scope and functionality for AcS 2.0 Increment 5 are limited to the AcS services specified in this RSD.

### 2.1 Accessibility Specifications

The AcS solution aligns its accessibility specifications to be in compliance with relevant guidelines and regulations set forth by Section 508 of the Rehabilitation Act of 1973.

The Accessibility Requirements for the AcS solution identified for Section 508 Compliance consist of the 1194.21 Software Applications and Operating; 1194.22 Web-based Intranet and Internet Information and Applications; and Subpart D – Information, Documentation and Support – Section 1194.31 Information, Documentation, and Support. These specific checklists have been documented within the enterprise-level requirements by the Section 508 Office for the purpose of being used within applicable projects.

### 2.2 Business Rules Specification

The business rules specifications are identified in section 2.6.

### 2.3 Design Constraints Specification

The AcS solution complies with the approved [Enterprise Service Level Agreement \(SLA\)](#).

### 2.4 Disaster Recovery Specification

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

### 2.5 Documentation Specifications

The documentation to support the AcS solution complies with existing PMAS policies and uses [ProPath templates](#).

### 2.6 Functional Specifications

The functional specifications are identified in the following subsections. Requirement clarifications pertaining to particular subcomponents or partial requirements that are realized in the final production implementation of the AcS solution are provided.

The AcS Requirements Traceability Matrix (RTM) traces each system requirement mentioned in this RSD to a business need from the AcS FY15 BRD and is a separate deliverable.

## 2.6.1 Single Sign-On – Internal (SSOi)

### 2.6.1.1 Security Token Service (STS) Support of JSON Web Token and Bearer Token

To improve integration options, SSOi needs to accept a wider range of security tokens (e.g., JavaScript Object Notation [JSON] and Bearer tokens), as currently SSOi only accepts Security Assertion Markup Language (SAML) tokens. The acceptance of more security tokens also helps to set up SSOi for future enhancements to SSOi's Representational State Transfer (REST) capabilities.

**Table 2: SSOi Support of JSON Web Token and Bearer Token Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: As an application partner, I want to be able to know who accessed my user's data.		
BRD BN12. Centralized Enterprise Single Sign-On – Internal (SSOi): Provide a capability to allow a user to sign on once to an application, then allow the user to access another application		
12.0	Support for JSON Web Token and Bearer Token	<b>[FEAT461870]</b> SSOi shall provide a JSON web token within the Open Authorization Standard (OAuth) framework.
		<b>[FEAT461871]</b> SSOi shall provide a JSON web token within the STS framework.
		<b>[FEAT461872]</b> SSOi shall be able to digitally sign and encrypt JSON web tokens.
		<b>[FEAT461873]</b> SSOi shall be able to verify digitally signed JSON web tokens and decrypt encrypted JSON web tokens.
		<b>[FEAT461874]</b> SSOi shall accept JSON Web tokens.
		<b>[FEAT461875]</b> SSOi shall accept JSON Bearer tokens.

### 2.6.1.2 Expose STS Service with REST Interface

SSOi exposes the STS service with a REST interface. SSOi can then interface with clients that want a REST interface instead of a Simple Object Access Protocol (SOAP) interface.

**Table 3: Expose STS Service with REST Interface Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: As an application partner, I want to be able to know who accessed my user's data.		
BRD BN12. Centralized Enterprise Single Sign-On – Internal (SSOi): Provide a capability to allow a user to sign on once to an application, then allow the user to access another application		
12.0	Expose STS Service with REST interface	[FEAT461877] SSOi shall expose the STS service with a REST interface.
		[FEAT461878] SSOi shall secure the REST STS service with mutual Transport Layer Security (TLS).

### 2.6.1.3 Standard SSOi Traits

To improve integration options and consistency across integrations, three standard trait bundles will be provided to applications integrating with SSOi in the SiteMinder and Federated patterns: General VA, VHA, and VBA.

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: As an application partner, I want to be able to know who accessed my user's data.		
BRD BN12. Centralized Enterprise Single Sign-On – Internal (SSOi): Provide a capability to allow a user to sign on once to an application, then allow the user to access another application		
12.0	Provide standard user traits to integrating applications	[FEAT474250] SSOi shall provide General VA traits. See table below.
		[FEAT474251] SSOi shall provide VHA traits, which are the General VA traits plus user identity in VHA systems. See table below.
		[FEAT474252] SSOi shall provide VBA traits, which are the General VA traits plus user identity in VBA system. See table below.

The following table identifies the SSOi traits:

Authentication Trait (HTTM Header for SiteMinder or Federated)	Source Primary (Secondary)	General VA Default	VHA	VBA	Source Attribute/Trait Name
sessionScope		X	X	X	The Scope of Service attribute is intended to bind the user's interaction with backend systems to self-service or business type request. Values: B, S (case insensitive)
transactionId	SSOi	X	X	X	
issueInstant	SSOi	X	X	X	
authnType	SSOi	X	X	X	Values: Direct, Indirect (case insensitive)
proofingAuth	SSOi	X	X	X	Values: FICAM, DMDC, DoDCAC, VA
assurLevel	SSOi	X	X	X	For SSOi will be 2 (AD) or 3 (PIV)
adDomain	AD	X	X	X	
adSamAccountName	AD	X	X	X	
adUpn	AD	X	X	X	
adEmail	AD	X	X	X	
extensionattribute6 – VistA Unique Identifier (VAUID)	AD	X	X	X	
firstName	Prov	X	X	X	Initially, will be from AD pending CRISP. After CRISP, Prov becomes the source.
lastName	Prov	X	X	X	Initially, will be from AD pending CRISP. After CRISP, Prov becomes the source.
secId	Prov	X	X	X	SecID largely null pre-CRISP
mvilcn	MVI		X		MVI's ICN
vistald	MVI		X		VHA VistA user identifier – a combination of Site+DUZ to capture VistA instance and identifier within that instance
corpId	MVI			X	VBA Corporate user identifier
dodEdiPnId	MVI	X	X	X	DOD identifier
Role	Prov	Null or roles defined in Prov integration	Null or roles defined in Prov integration	Null or roles defined in Prov integration	Role, Organization, and Organization ID only passed if the target if the app target of authentication is integrated with Provisioning
Organization	Prov	X	X	X	Value: Department of Veterans Affairs
Organization ID	Prov	X	X	X	Value:urn:oid:2.16.840.1.113883.4.349

### 2.6.1.4 SSOi Deferred Requirements

[Appendix B](#) contains a list of SSOi requirements that were stated in previous AcS RSDs but deferred to AcS 2.0 Increment 5 for delivery.

## 2.6.2 AccessVA

AccessVA is a portal to several VA sites for Veterans, beneficiaries, and affiliates. It allows users to log in once with a VA accepted credential to gain access to all AccessVA-enabled websites and applications. AccessVA is a graphical user interface (GUI) for authenticating Veterans and other members of VA's external user community of interest with the SSOe capability. AccessVA establishes a unified authentication system that can be used between various agencies that provide services to our Veterans

The focus of AccessVA enhancements in AcS 2.0 Increment 5 is to redesign AccessVA, enable AccessVA to become a more seamless function with IAM's integrated partners, and increase the range of partners by reducing technical roadblocks to integration.

This section identifies the AccessVA functional requirements that improve the AccessVA design. The AccessVA design includes the GUI requirements in the following areas with embedded mock screens:

- AccessVA Unauthenticated Home Page
- AccessVA Processing Page
- AccessVA CSP Selection Page
- AccessVA Authenticated Page
- AccessVA Future Vision

**Note:** The entire AccessVA website including pop-up widgets are required to comply with Section 508 Accessibility Requirements (see section 3 regarding applicable standards).

### 2.6.2.1 AccessVA UI Updates

This section outlines the requirements for the GUI for AccessVA and organizes them into a top-level design.

**User Story:** As a Veteran, Beneficiary or VA Partner, I want to be able to sign on to my desired VA website with my preferred credential.

#### 1.1 AccessVA Unauthenticated Home Page

- 1.1.1. **[FEAT461883]** On the AccessVA Unauthenticated Home Page, the AccessVA logo shall be displayed on the top left of the screen.
- 1.1.2. **[FEAT461884]** On the AccessVA Unauthenticated Home Page, the IAM logo shall be displayed on the top right of the screen.
- 1.1.3. **[FEAT506032]** On the AccessVA Unauthenticated Home Page, the IAM and AccessVA logos shall be in the same banner.
- 1.1.4. **[FEAT506033]** The AccessVA Home Page banner shall be a 2-color gradient starting in blue (#1677bd) and ending in white (FFFFFF).

- 1.1.5. **[FEAT506034]** The AccessVA Unauthenticated Home Page banner shall contain the text “Securing your Access to the VA.”
- 1.1.6. **[FEAT506035]** The AccessVA Unauthenticated Home Page banner shall have a top and bottom thin outline in red (#E31B23).
- 1.1.7. **[FEAT506036]** The AccessVA Unauthenticated Home Page introductory paragraph “Welcome to AccessVA, your solution for accessing VA’s many web resources. AccessVA provides login capability to website and applications as part of VA’s Identity and Access Management (IAM) Enterprise.”
- 1.1.8. **[FEAT461885]** On the AccessVA Unauthenticated Home Page, the wording, “Please select a VA web site below to logon with AccessVA,” shall be displayed.
- 1.1.9. **[FEAT506037]** On the AccessVA Unauthenticated Home Page, AccessVA shall display buttons with application logos for the AccessVA Partner web sites integrated with AccessVA.
- 1.1.10. **[FEAT461892]** On the AccessVA Unauthenticated Home Page, when the user selects a partner website, they are taken to the AccessVA CSP selection page.
- 1.2 AccessVA Processing Page
  - 1.2.1 **[FEAT461894]** On the AccessVA Processing Page, AccessVA shall display a processing notification page during third-party onboarding (3POB).
  - 1.2.2 **[FEAT461895]** On the AccessVA Processing Page, AccessVA’s 3POB Processing notification page shall inform the user that their request is processing and may take up to the 30 seconds.
- 1.3 AccessVA CSP Selection Page
  - 1.3.1 **[FEAT461897]** On the AccessVA CSP Selection Page, AccessVA shall have a CSP selection page displaying the accepted CSPs for the selected target application.
  - 1.3.2 **[FEAT461898]** On the AccessVA CSP Selection Page, the AccessVA CSP selection page shall display a logo for each accepted CSP.
  - 1.3.3 **[FEAT461899]** On the AccessVA CSP Selection Page, the AccessVA CSP Selection page shall have a “select another VA Application” button.
  - 1.3.4 **[FEAT461900]** On the AccessVA CSP Selection Page, the “select another VA Application” button on the AccessVA CSP Selection page shall return the user to the AccessVA Unauthenticated page.
  - 1.3.5 **[FEAT499971]** On the AccessVA CSP Selection Page, the logo for the application selected shall be displayed in the top left corner

- 1.3.6 **[FEAT499972]** On the AccessVA CSP Selection Page, the AccessVA CSP selection page CSP logos shall dynamically disappear to allow additional space for the text box, when the browser size is reduced.
- 1.4 AccessVA Authenticated Page
  - 1.4.1 **[FEAT461902]** On the AccessVA Authenticated Page, the AccessVA Authenticated page shall be redesigned to be more consistent with the style of the redesigned AccessVA Unauthenticated page.
  - 1.4.2 **[FEAT461903]** On the AccessVA Authenticated Page, the AccessVA Authenticated page shall be updated to feature the log out capability.
- 1.5 Addition of an AccessVA Sign-In Partners Page
  - 1.5.1 **[FEAT499973]** A new menu selection for Sign-In Partners shall be displayed in the AccessVA menu bar
  - 1.5.2 **[FEAT499974]** The Sign-In Partners page shall display “Sign-In Partners:” at the top of the page
  - 1.5.3 **[FEAT499975]** The Sign-In Partners page shall display a button with the logo for each Sign-In Partner available via AccessVA
  - 1.5.4 **[FEAT499976]** Upon selection of one of a Sign-In Partner button, information about that Sign-In Partner will be displayed under the wording, “About Sign-In Partner”
  - 1.5.5 **[FEAT499977]** “About Sign-In Partner” shall display the Sign-In Partner logo, and information to include; 1) Who Qualifies for the Sign-In Partner; 2) Which applications are accessible after logging in with the selected Sign-In Partner; 3) and links to logon, or register for the selected Sign-In Partner
  - 1.5.6 **[FEAT499978]** Upon logon or registering from the AccessVA Sign-In Partner page, the user will be returned to the AccessVA Authenticated Page.
- 1.6 AccessVA Widget
  - 1.6.1 **[FEAT499979]** The AccessVA widget AccessVA logo shall be updated to the most current AccessVA logo.
  - 1.6.2 **[FEAT499981]** The AccessVA widget CSP logos shall be increased in size.

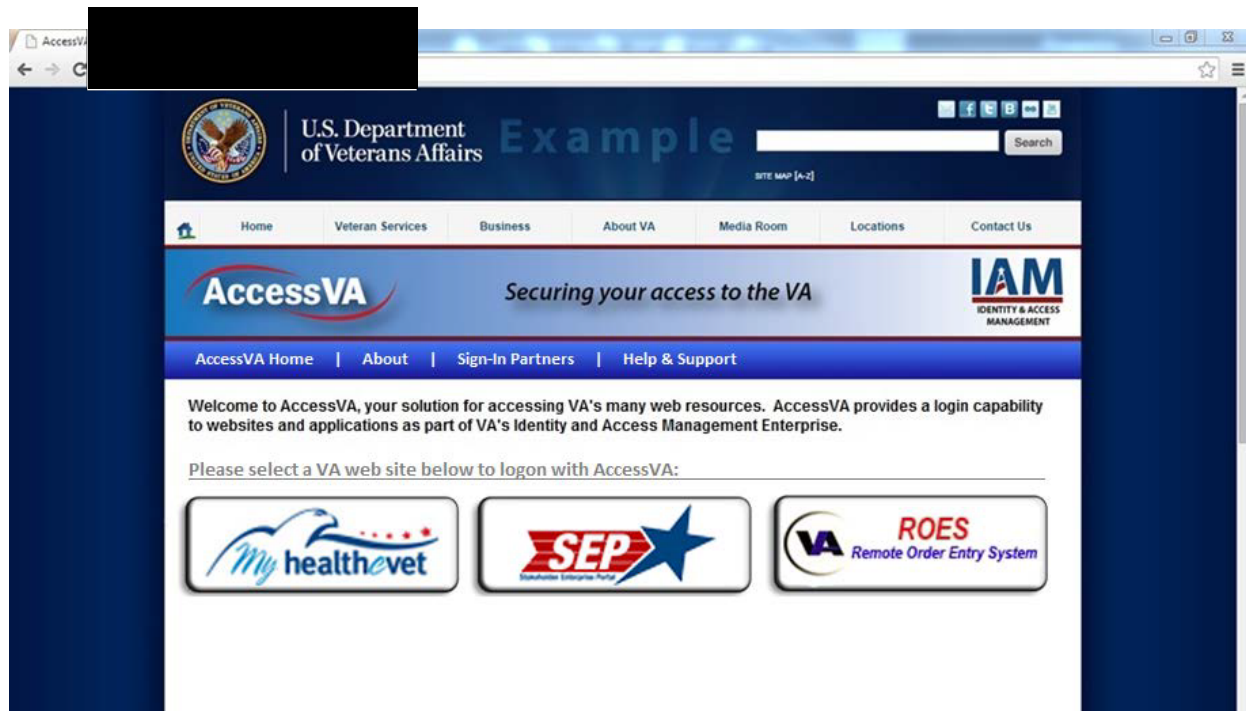


Figure 1: AccessVA Unauthenticated Home Page



**Figure 2: AccessVA Unauthenticated Home Page (CSP Selection)**



**Figure 3: AccessVA Sign-In Partners Page**

### 2.6.2.2 AccessVA Future Vision Requirements

This section outlines the GUI requirements for AccessVA for creating a single login button to provide a common user experience across all VA sites.

**Note:** Refer to the SSOf VAAFI AccessVA 2.0 Increment 4 RSD for CSP selection pop-up widget requirements (see section 1.3).

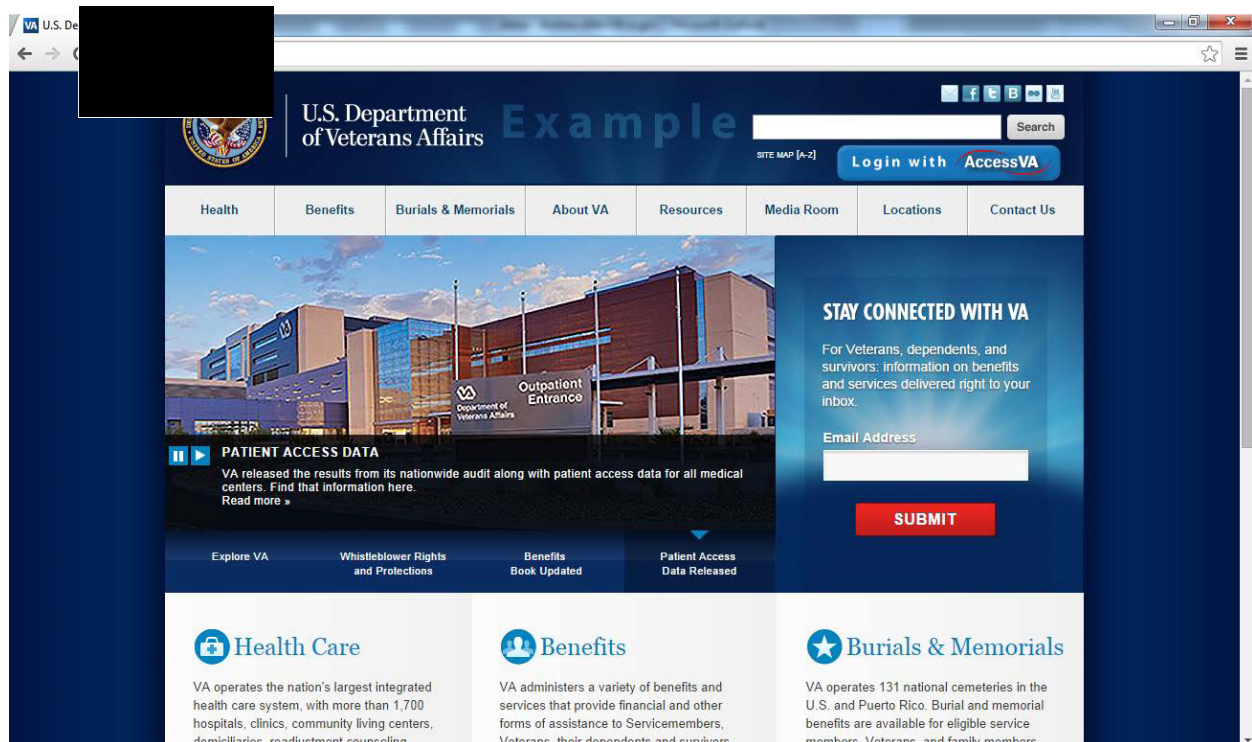
#### 1.1.1 AccessVA Login Button

- 1.1.1.1 **[FEAT461906]** An AccessVA login button shall appear on the partner website.

#### 1.1.2 AccessVA User Selector Pop-Up Widget

- 1.1.2.1 **[FEAT461908]** The AccessVA User Selector Pop-Up Widget shall display on the partner website after the user selects the AccessVA login button.
- 1.1.2.2 **[FEAT461909]** The AccessVA User Selector Pop-Up Widget shall darken the partner website underneath it.

- 1.1.2.3 **[FEAT461910]** The AccessVA User Selector Pop-Up Widget User Type buttons shall display asking the user to identify themselves as by one of the following user types: Veteran, Family Member, Service Member, or VSO.
- 1.1.2.4 **[FEAT461911]** The AccessVA User Selector Pop-Up Widget shall display buttons for the AccessVA Partner websites relevant to the selected user type when the user type button is selected.
- 1.1.2.5 **[FEAT461912]** When the user selects a partner website from the AccessVA User Selector Pop-Up Widget, the AccessVA CSP Selection Pop-Up Widget shall appear.



**Figure 4: AccessVA Login Button**

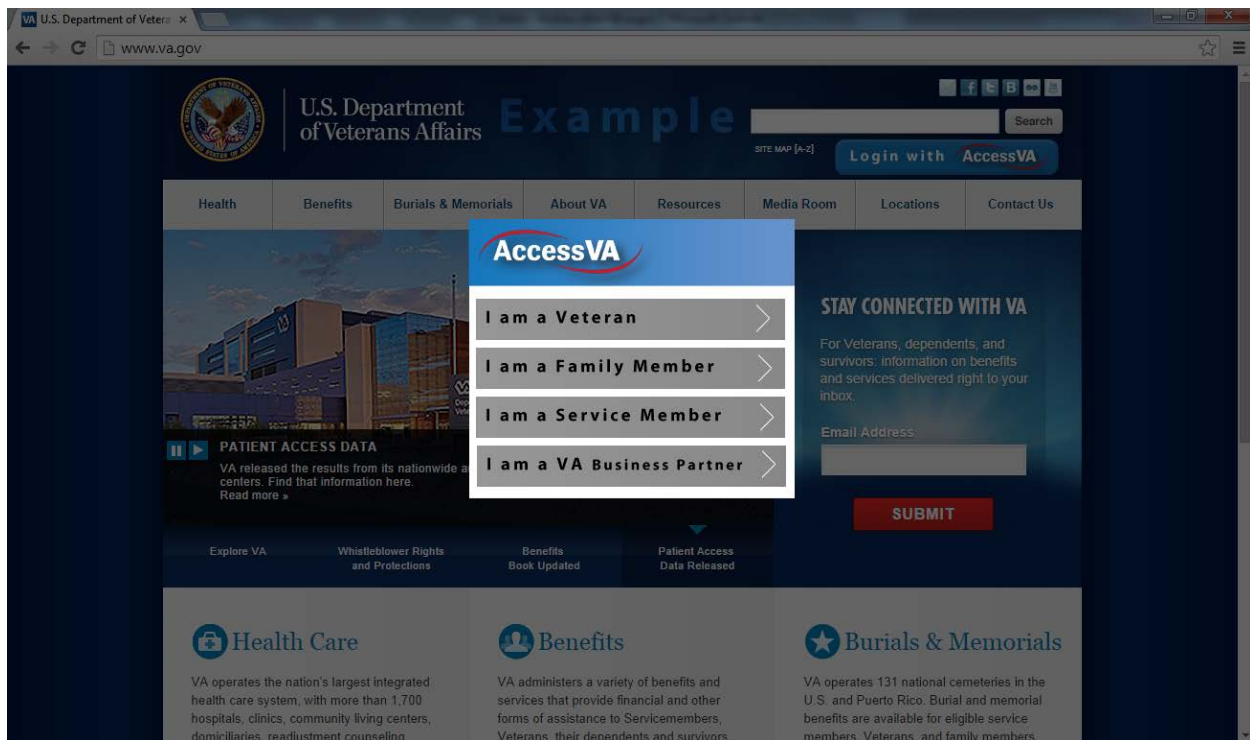


Figure 5: AccessVA User Type Selector Pop-Up Widget

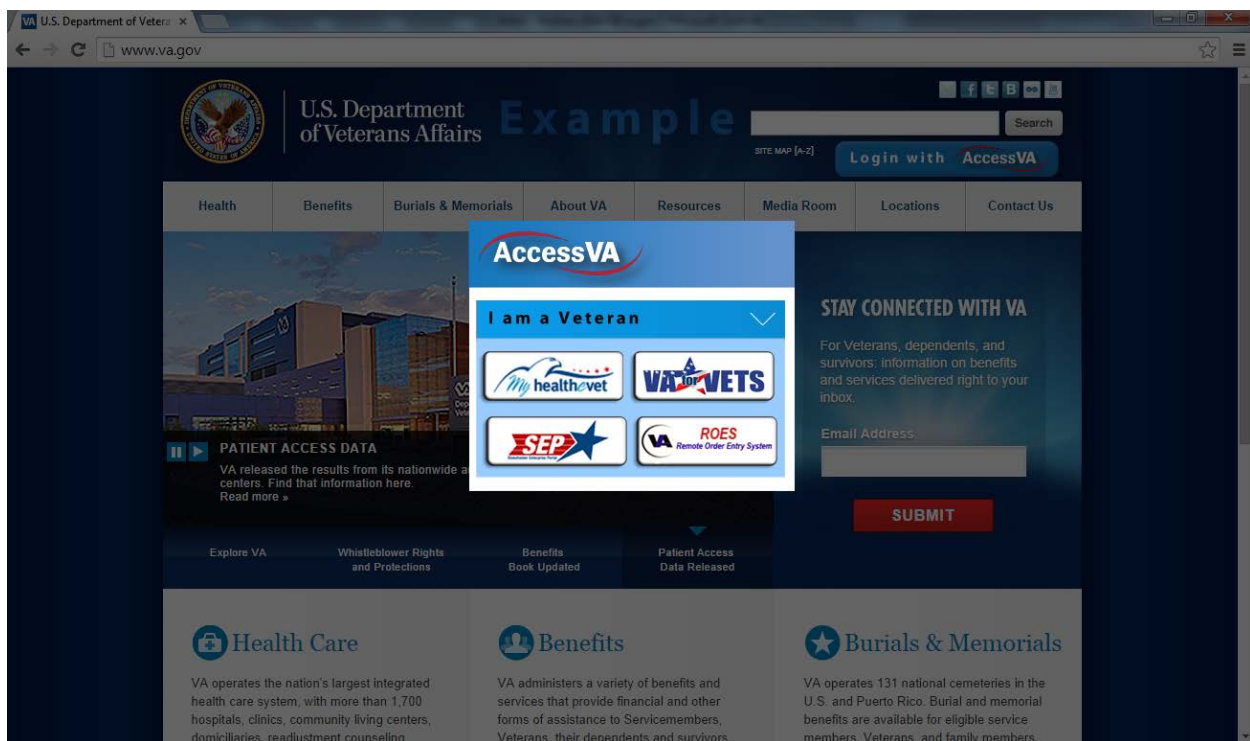
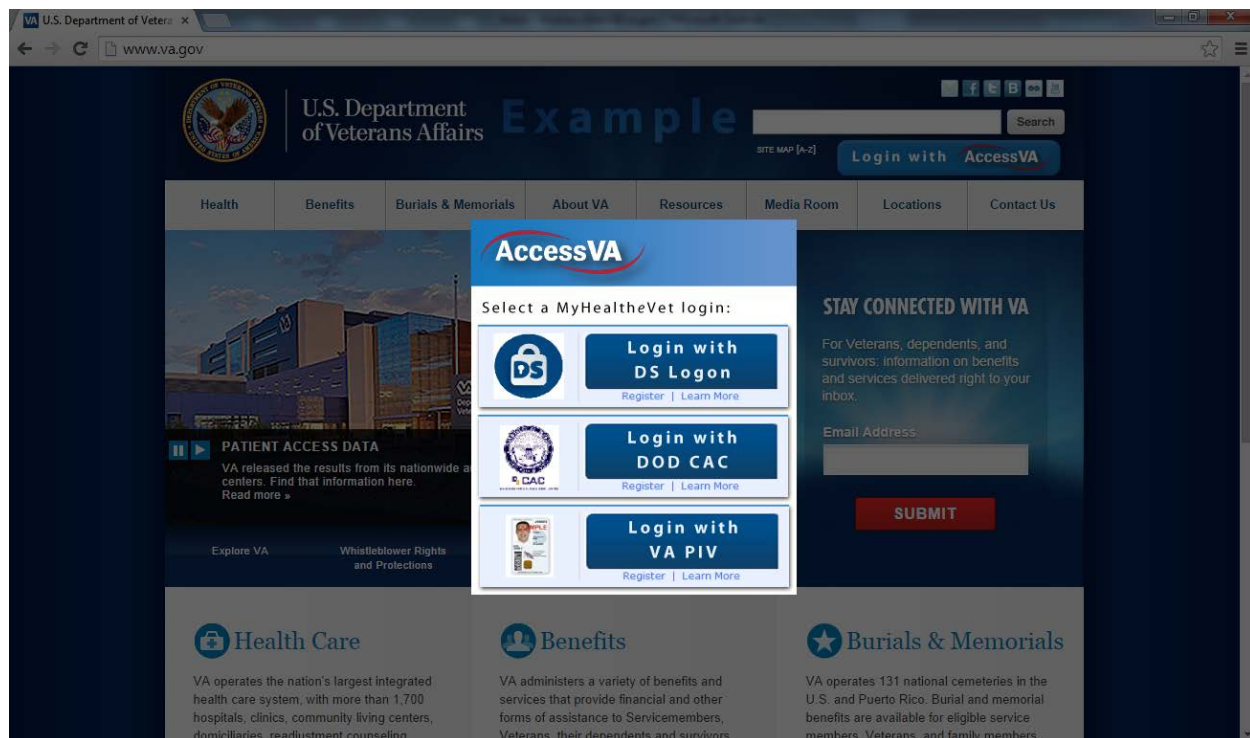


Figure 6: AccessVA User Type Selector Pop-Up Widget – Expanded



**Figure 7: AccessVA CSP Selector Pop-Up Widget**

## 2.6.3 Single Sign-On – External

Single Sign-On – External (SSOe) performs as an abstraction layer between the operational components of the VA authentication federation credentials and public-facing VA applications that are suited for federated authentication. SSOe eliminates the need for each VA application to develop interfaces to a complex set of security and policy requirements. The SSOe infrastructure is designed with the use of application-level input, lessons learned, and industry best practices in an effort to support multiple agency application needs and requirements.

This section identifies the functional requirements that enhance the SSOe service. The SSOe requirements in this section support capability enhancement in the following areas:

- 3POB addresses functionality
- Imprecise Date of Birth
- Support the JSON Web Token and the Bearer Token
- STS Service with REST interface
- Auth Validation Service

### 2.6.3.1 Support Imprecise Date of Birth from MVI

**User Story:** As a Veteran, Beneficiary or VA Partner, I want my identity data to be available after authentication for use in the business process.

MVI supports an imprecise date of birth as it contains records for some users who are unable to provide an exact date.

1. **[FEAT461915]** SSOe shall accept an imprecise date of birth from MVI.

### 2.6.3.2 SSOe Accepts Address and Phone # from VDS

**User Story:** As a Veteran, Beneficiary or VA Partner, I want my identity data to be available after authentication for use in the business process.

SSOe currently adds attributes to the Virtual Directory Service (VDS) during 3POB. This requirement is to have an address added to the list of attributes that SSOe provides to VDS. This improves the chances of success during 3POB registration and softboarding.

1. **[FEAT461917]** SSOe shall accept an address from VDS during authentication.
2. **[FEAT473909]** SSOe shall support a 3-line formatted street address.
3. **[FEAT473910]** SSOe shall accept a phone number from VDS during authentication.

For the full SSOe header trait list, see [Appendix C](#).

### 2.6.3.3 SSOe Accepts JSON Web Token and Bearer Token

**User Story:** As an application partner, I want to be able to know who accessed my user's data.

To improve integration options, SSOe needs to accept a wider range of security tokens (e.g., JavaScript Object Notation [JSON] and Bearer tokens), as currently SSOe only accepts Security Assertion Markup Language (SAML) tokens. The acceptance of more security tokens also helps to set SSOe up for future enhancements to SSOe's Representational State Transfer (REST) capabilities.

1. **[FEAT461919]** SSOe shall provide a JSON web token within the Open Authorization Standard (OAuth) framework.
2. **[FEAT461920]** SSOe shall provide a JSON web token within the Security Token Service (STS) framework.
3. **[FEAT461921]** SSOe shall be able to digitally sign and encrypt JSON web tokens.
4. **[FEAT461922]** SSOe shall be able to verify digitally signed JSON web tokens and decrypt encrypted JSON web tokens.
5. **[FEAT461923]** SSOe shall accept JSON Web tokens.
6. **[FEAT461924]** SSOe shall accept JSON Bearer tokens.

### 2.6.3.4 Expose STS Service with REST Interface

**User Story:** As an application partner, I want to be able to know who accessed my user's data.

SSOe exposes the STS service with a REST interface. SSOe can then interface with clients that want a REST interface instead of a Simple Object Access Protocol (SOAP) interface.

1. **[FEAT461926]** SSOe shall expose the STS service with a REST interface.
2. **[FEAT461927]** SSOe shall secure the REST STS service with mutual Transport Layer Security (TLS).
3. **[FEAT473911]** SSOe shall exchange the user session data when presented with a valid REST SSO user token.

### 2.6.3.5 OAuth Validation Service

**User Story:** As an application partner, I want to validate the user's access credential and obtain the user's identity data.

For clients that cannot provide token validation on their own, SSOe provides OAuth validation. SSOe also provides the artifact verification and resolution.

1. **[FEAT461929]** SSOe shall provide an access token validation service.
2. **[FEAT461930]** SSOe shall provide a validation service for the STS SAML token.
3. **[FEAT461931]** SSOe shall provide a validation service for the JSON web token.
4. **[FEAT461932]** SSOe's validation services shall be supported by SOAP and REST interfaces.
5. **[FEAT461933]** SSOe's access token validation service shall provide both Extensible Markup Language (XML) and JSON responses.
6. **[FEAT473912]** SSOe shall secure the OAuth service with mutual Transport Layer Security (TLS).
7. **[FEAT473913]** SSOe shall exchange the user session data when presented with a valid OAuth user access token.
8. **[FEAT473914]** SSOe's OAuth validation service REST response messages shall support the JSON format.

### 2.6.3.6 SSOe Provides PID, BIRLS, SEC ID, and EDI PI IDs

**User Story:** As a Veteran, Beneficiary or VA Partner, I want my identity data to be available after authentication for use in the business process.

SSOe previously only provided two corresponding Person Identification (PID) and Beneficiary Identification Records Locator Subsystem (BIRLS) IDs with other databases. This requirement removes that restriction. Target applications will be provided all known IDs.

1. **[FEAT461935]** SSOe shall provide all instances of PID IDs to target applications during authentication.
2. **[FEAT461936]** SSOe shall provide all instances of BIRLS file number ID to target applications during authentication.
3. SSOe shall provide all instances of Security Identifier (SEC ID) to target applications during authentication.
4. SSOe shall provide all instances of Electronic Data Interchange (EDI) Personal Identifier (PI) to target applications during authentication.

Authentication Trait (HTTP Header)	Required/Optional	Source	Source Attribute/Trait Name	Action If Trait Not Provided	Additional Business Rules
va_eauth_PID	O	MVI	Person ID (Corporate DB)	Pass Null Value	If 2 or more PIDs are returned, then provide all in

Authentication Trait (HTTP Header)	Required/Optional	Source	Source Attribute/Trait Name	Action If Trait Not Provided	Additional Business Rules
					headers
va_eauth_filenummer	O	MVI	File Number (BIRLS)	Pass Null Value	If 2 or more BIRLS file numbers are returned, then provide all in headers
va_eauth_secID	R	Prov	secID	Pass User to Third-Party Credential Onboarding	If 2 or more secID are returned, then provide all in headers
va_eauth_dodedipnid	O	MVI	va_eauth_dodedipnid	1. If CSP is DS LOGON a. and EDI PI returned from MVI is different, then pass value from CSP b. and EDI PI not in MVI, then pass EDIPI from CSP 2. If CSP is not DSLOGON, and EDI PI is not in MVI, then pass null	If 2 or more EDI PI are returned, then provide all in headers

For the full SSOe header trait list, see [Appendix C](#).

### 2.6.3.7 Third-Party Credential Onboarding

**User Story:** As a Veteran, Beneficiary or VA Partner, I want to be able to sign on to my desired VA website with my preferred credential.

Third-party credential onboarding is triggered when the user attempting to authenticate is not known to VA or based on LOA 2+ business rules. VAAFI attempts to identify the user as defined in the portal strategy. Users who cannot be identified by the existing Portal Strategy may be presented with a Third-Party Credential Onboarding registration screen.

1. **[FEAT473917]** AccessVA shall collect street address in 3-line format.

**Address:**

Street – Line 1	String	3 – 35
Street – Line 2	String	3 – 30
Street – Line 3	String	3 – 30

## 2.6.4 Provisioning

The Provisioning (Prov) service provides portions of the Federal Identity, Credential, and Access Management (FICAM)-defined Digital Identity and Privilege Management services. The Prov service includes the following FICAM service components:

- **Digital Identity Lifecycle Management:** This is the process of establishing and maintaining the attributes that make up an individual's digital identity. It supports general updates to an identity such as a name change or biometric update.
- **Linking / Association:** This is the process of linking one identity record with another across multiple systems. It involves the activation and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications in response to an automated or interactive process, and is used in conjunction with Authoritative Attribute Exchange.
- **Privilege Administration:** This is the process of establishing and maintaining the entitlement or privilege attributes that make up an individual's access profile. Because an individual's access needs to be changed, it supports updates to privileges over time.
- **Centralized Account Management:** This is the process of requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions.
- **Bind / Unbind:** This is the process of building or removing a relationship between an entity's identity and further attribute information on the entity (e.g., properties, status, or credentials).
- **Provisioning:** This is the capability of creating user access accounts and assigning privileges or entitlements within the scope of a defined process or interaction, and providing users with access rights to applications and other resources that may be available in an environment and may include the creation, modification, deletion, suspension, or restoration of a defined set of privileges.

The Prov service is being enhanced to support additional capabilities to support the Portal Strategy. Additionally, the Prov service user interface is being enhanced to improve the user experience during the Continuous Readiness in Information Security Program (CRISP) onboarding/offboarding process.

**User Story:** As a Veteran, Beneficiary or VA Partner, I want to be able to sign on to my desired VA website with my preferred credential.

**Table 4: Provisioning Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: As a Veteran, Beneficiary or VA Partner, I want my identity data to be available after authentication for use in the business process.		
3.0 Digital Identity Lifecycle Management Onboarding/Offboarding: Provide a digital process of establishing and maintaining the attributes that make up an individual digital identity and support general updates to an identity such as a name change or biometric update.		
3.0	Portal Strategy	[FEAT461939] When the Date of Birth is not provided by the user or

BRD BN	Requirement	In-Scope Requirement Clarification
	Enhancements	the credential during third-party credential onboarding, the Provisioning service shall retrieve the date of birth from MVI and populate the corresponding date of birth in the Virtual Directory Service (VDS).
		<b>[FEAT461940]</b> The Provisioning service shall support the ability to retrieve and store an imprecise date of birth from MVI when the user or the credential does not provide a date of birth during third-party credential onboarding.
		<b>[FEAT461941]</b> VDS shall support the ability to store an imprecise date of birth.
		<b>[FEAT461942]</b> VDS shall support the ability to store the home address (street, city, state, postal code, country, province/region).
		<b>[FEAT461943]</b> The Provisioning service shall populate the home address with the address provided on the credential in the case of Third-Party Credential Onboarding provided that the address is provided by the call to the Provisioning service.
		<b>[FEAT461944]</b> The Provisioning service shall retrieve the home address from MVI when creating a record in VDS in the event the address is not provided by the Third-Party Credential Onboarding call.
		<b>[FEAT461945]</b> Existing VDS records shall be populated with the home address from MVI.
		<b>[FEAT461946]</b> When receiving a Third-Party Credential onboarding request, the Provisioning service shall first retrieve the credential using the CSP ID. If the CSP ID exists, the Provisioning service shall only update traits that are unpopulated within the Provisioning service with data provided on the request (e.g., if the SSN is unpopulated in the Provisioning datastore and the SSN is populated on the request, the Provisioning service will update the data with the provided SSN.) If the CSP ID is not found, the Provisioning service shall perform the existing Third-Party Credential onboarding logic.
		<b>[FEAT472918]</b> The Provisioning Service shall support street address in 3-line format.  <b>Address:</b> Street – Line 1   String   3 – 35 Street – Line 2   String   3 – 30 Street – Line 3   String   3 – 30
User Story: As a User who onboards and offboards people, I want to have a consistent way to search for records in Provisioning.		
3.0	User Interface	<b>[FEAT461948]</b> The Provisioning service shall present a consistent set of search criteria and search results for all search screens

BRD BN	Requirement	In-Scope Requirement Clarification
	Enhancements	<p>presented during the CRISP on/offboarding processes. These search screens include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Offboard Employee Search Screen</li> <li>• Offboard Contractor Search Screen</li> <li>• Offboard Health Professions Trainee Search Screen</li> <li>• Offboard Volunteer Search Screen</li> <li>• Emergent Offboard Employee Search Screen</li> <li>• Emergent Offboard Contractor Search Screen</li> <li>• Emergent Offboard Health Professions Trainee Search Screen</li> <li>• Emergent Offboard Volunteer Search Screen</li> <li>• Update Employee Search Screen</li> <li>• Update Contractor Search Screen</li> <li>• Update Health Professions Trainee Search Screen</li> <li>• Update Volunteer Search Screen</li> <li>• CRISP Checklist Search Screen</li> <li>• Manager Search Screen</li> <li>• AD Facility CIO Search Screen</li> <li>• AD ISO Search Screen</li> <li>• Company POC Search Screen</li> <li>• COR Search Screen</li> <li>• Supervisor Search Screen</li> <li>• Project Manager Search Screen</li> <li>• Sponsor Search Screen</li> </ul>
		<p><b>[FEAT461949]</b> The Provisioning service shall only present the following default search criteria when searching for a user:</p> <ul style="list-style-type: none"> <li>• First Name</li> <li>• Last Name</li> <li>• Email</li> </ul>
		<p><b>[FEAT461950]</b> The Provisioning service shall allow the user to add the following additional search criteria:</p> <ul style="list-style-type: none"> <li>• SEC ID</li> <li>• Middle Name</li> </ul>
		<p><b>[FEAT461951]</b> The Provisioning service shall present the following data in the search results when available:</p> <ul style="list-style-type: none"> <li>• SEC ID</li> <li>• First Name</li> <li>• Last Name</li> <li>• Middle Name</li> <li>• Email Address</li> </ul>
		<p><b>[FEAT461952]</b> The Provisioning service shall not display the Enabled Checkbox when a user has been selected for Offboarding. Refer to Figure 8 for an example.</p>

BRD BN	Requirement	In-Scope Requirement Clarification
		<p><b>[FEAT461953]</b> The Provisioning service shall suppress error messages on the search for user screens when a user is completing the Onboarding forms. Refer to Figure 9 for an example.</p> <p><b>[FEAT461954]</b> The Provisioning service shall not display the CSP ID and LOA on the On-Boarding screens.</p> <p><b>[FEAT473919]</b> The following requirements pertain to the elimination of a local search into the Provisioning User Store for CRISP onboarding. (See <a href="#">Appendix D</a> for the CRISP Onboarding activity diagram.)</p> <ol style="list-style-type: none"> <li>1. When a requestor is onboarding a user (Employee, Contractor, etc.), the Provisioning service shall prompt the requestor for the following attributes: <ul style="list-style-type: none"> <li>• First Name (required)</li> <li>• Middle Name (optional)</li> <li>• Last Name (required)</li> <li>• SSN (required)</li> <li>• Date of Birth (required)</li> <li>• Gender (required)</li> </ul> </li> <li>2. Once the requestor has entered the required traits and submitted a search, the Provisioning service shall utilize the MVI Search for Person (Unattended, Returning Corresponding IDs) Service.</li> <li>3. If the MVI Search for Person (Unattended, Returning Corresponding IDs) Service does not find the person, the Provisioning service shall prompt the requestor to enter the additional attributes for the user needed to complete the onboarding process.</li> <li>4. If the MVI Search for Person (Unattended, Returning Corresponding IDs) Service finds the person and that person is not assigned a SEC ID, the Provisioning service shall prompt the requestor to enter the additional attributes for the user needed to complete the onboarding process.</li> <li>5. If the MVI Search for Person (Unattended, Returning Corresponding IDs) Service finds the person and that person is assigned a SEC ID, the Provisioning service shall retrieve the user with the SEC ID provided by MVI. The Provisioning service shall prompt the requestor to update the existing Provisioning record to complete the onboarding process.</li> </ol>
User Story: As a user of Provisioning, I want to be able to use my PIV card to digitally sign submissions and/or approvals.		

BRD BN	Requirement	In-Scope Requirement Clarification
3.0	General Enhancements	<b>[FEAT461957]</b> The Provisioning service shall support the ability to capture the digital signature (using the PIV card) at any point in the workflow (submission and/or approvals). The specific impacted workflows will be identified in separate iRSDs.

VA Provisioning Service

VA Employee Emergent OffBoarding: 0000027668

• = Required

User ID

Enabled

First Name

Last Name

Full Name

Email

Offboarding Justification (required)

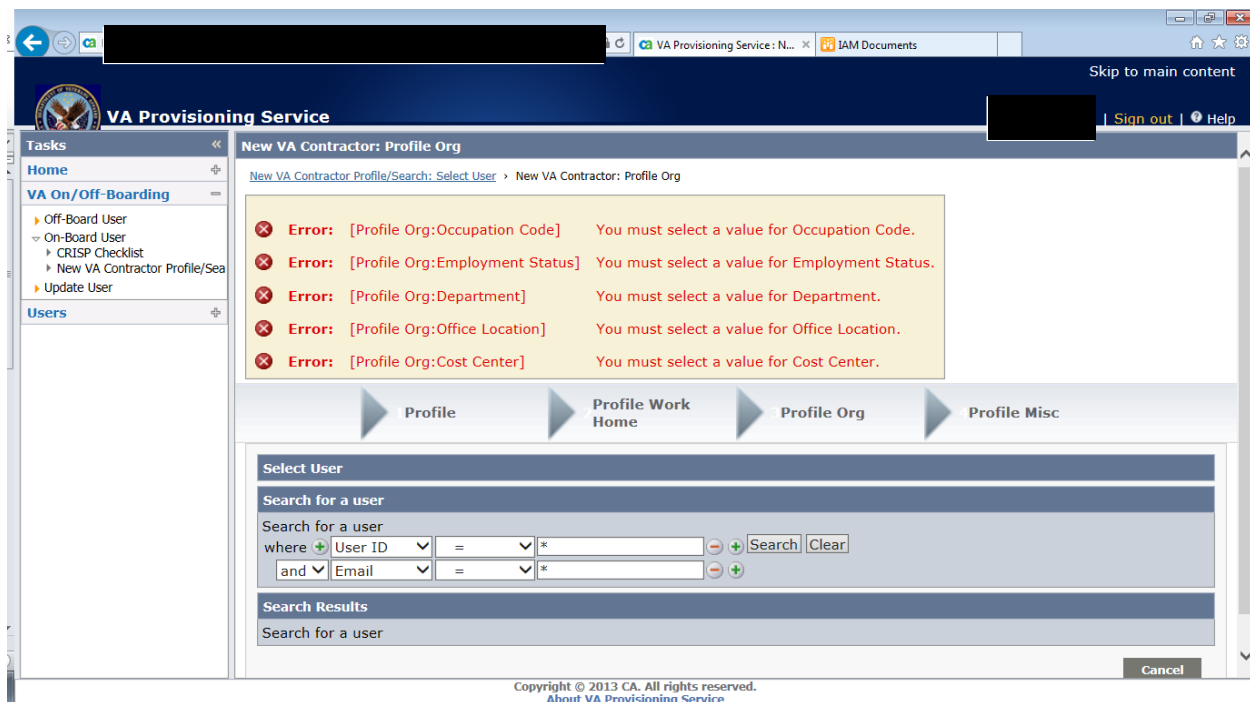
**IMPORTANT INFORMATION**

Select Submit to validate the off-board of this VA personnel.  
This action will start the Termination Process Immediately.

Submit Cancel

Copyright © 2013 CA. All rights reserved.  
About VA Provisioning Service

**Figure 8: Offboarding Screen**



**Figure 9: Error Messages Displayed on Search for User Screen**

## 2.6.5 Compliance Audit and Reporting (CAR)

### 2.6.5.1 Role Engineering and Compliance Tool Integration with CAR

The role engineering and compliance tool gathers and analyzes access control information to support and model roles and attribute-based policies for IT systems. The tool is able to extract data from a variety of systems to consolidate data in a form that can be used to create roles for enterprise use and to ensure compliance to VA security policies.

The tool is envisioned to gather and analyze access control information from operational systems and identity and access data repositories, model roles, and support enforcement of role- and attribute-based policies for IT systems. As such, the tool is able to extract data from a variety of systems and to consolidate that data in a form that can be used by analysts to create roles for enterprise use and ensure compliance to VA security policies.

To fulfill the business need of providing a single point of auditing and reporting capability for all IAM services, the role engineering and compliance tool shall be integrated with the CAR service for the purpose of providing role engineering and compliance transactional data within the CAR interface. The requirements for the integration are depicted in the following table.

**Table 5: Role Engineering and Compliance Tool Integration with the CAR Service Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
	User Story: As a user of CAR, I want to be able to produce reports from Role Engineering and Compliance transactions.	

BRD BN	Requirement	In-Scope Requirement Clarification
23.01 The CAR Service will provide a single point of auditing and reporting capability (only user and access management data) for all IAM services.		
23.01	SailPoint/CAR Integration	<b>[FEAT461962]</b> The Role Engineering and Compliance tool and the CAR Service shall integrate to produce reports on provisioning and de-provisioning activities.

**Table 6: Name and Description of Reports to Reside in CAR**

Report Title	Description and Elaboration
Provisioned Users as a result of role mining and certification activities Report	Displays information about provisioned users that were a result of a role mining and/or a certification activity
De-Provisioned Users as a result of role mining and certification activities Report	Displays information about de-provisioned users that were a result of role mining and/or a certification activity
Provisioned Users imported from an Authoritative Source Report	Displays information about provisioned users that were imported from an authoritative source
Privileged User who imported identities from Authoritative Source Report	Displays information about a privileged user that imported identities from an authoritative source

### 2.6.6 Identity Proofing (IP)

The In-Person Proofing (IPP) process confirms the identity of an individual through review of identification documents and artifacts provided during a visit to a VA Regional Office or at any location where IPP is being conducted.

The Identity Proofing service is being enhanced to allow the capture of new expiration date requirements when a military identification card is used as a proofing document.

**Table 7: Identity Proofing Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: As a user, I want to be able to capture the expiration date of a military identification cardholder's proofing document as a specific date through year 2150, or indefinite.		
1.0 Identity Proofing: Provide a digital process that vets and verifies the information (e.g., identity history, credentials, documents) that is used to establish the identity of a system entity, initiate a chain of trust in establishing a digital identity, and bind it to an individual.		

BRD BN	Requirement	In-Scope Requirement Clarification
1.11	Identity Proofing	<b>[FEAT499983]</b> The Identity Proofing Service shall be able to collect an expiration date through year 2150 when the military identification card is presented as a proofing document.
1.11	Identity Proofing	<b>[FEAT499984]</b> The Identity Proofing Service shall be able to collect an expiration date of "INDEF" (indefinite) when the military identification card is presented as a proofing document.

## 2.7 Graphical User Interface (GUI) Specifications

The GUI specifications include the following:

- User acceptance training and testing tools include user prompts to guide the use of the application so that minimal technical support is needed by the user.
- User interfaces are built with the VA logo and color scheme to the fullest extent possible. The VA 6102 Handbook or the [VA Media Management Office](#) is used as a reference.
- The required web pages are available on the Internet and compatible with VA-defined and -supported versions of web browsers such as Mozilla and Internet Explorer.

## 2.8 Multi-divisional Specifications

There are no multi-divisional specifications for this RSD.

## 2.9 Performance Specifications

The performance specifications are targeted for the planned consumption of AcS services for the following year; however, the performance specifications are easily scalable for future implementations. The following are the specifications as defined in the [AcS FY15 BRD](#), Section 7.2.1 Performance, Capacity, and Availability Requirements. For a detailed performance specification for each service, refer to the following subsections.

**Table 7: Performance Specifications**

<b>How many users does the current system support?</b>
<p>The IAM system supports the current and future (forecasted) user base of relying applications and systems. The system is expected to support a minimum of the following:</p> <ul style="list-style-type: none"> <li>▪ 700,000 contractors</li> <li>▪ 350,000 employees</li> <li>▪ 28 million Veterans</li> <li>▪ Hundreds of internal and external VA applications</li> </ul>
<b>How many users does the new system (or system modification) support?</b>

<b>How many users does the current system support?</b>
The new system is scalable to accommodate an internal and external user base of approximately 29 million.
<b>What is the predicted annual growth in the number of system users?</b>
The new system supports at least 10 million users during the initial year (full production deployment of IAM suite) with at least 100% increase in numbers annually. Integration of applications on a monthly basis via IAM Governance process (process support up to 200 applications over an annual basis).

The performance specifications include the following:

- The online application screens contained in the user interface render less than ten seconds with an average rendering of three seconds within the budgeted resource utilization constraints.
- The online procedures prompted from a user interface execute under five seconds with an average of four seconds within the budgeted resource utilization constraints.
- The metric data indicating the performance characteristics of the system to support application monitoring is provided.

## 2.9.1 Example Performance Specification for AcS Service Component

This subsection provides a template and defines the performance specification to be identified for each AcS Service Component.

**User Profile:** *<Identify the types of internal and/or external users for the AcS Service Component.>*

*<Provide any bulleted performance goals for the complete enterprise implementation of the service when fully integrated with the VA enterprise.>*

The *<AcS Service Component>* for this increment shall support the following:

Operation	
<b>Name</b>	<i>&lt;AcS Service Component&gt;</i>
<b>Usage Profile</b>	<i>&lt;Define the type of service usage event&gt;</i>
Mean Daily volume	<i>&lt;Define the average Daily number of the service usage events &gt;</i>
Projected Growth	<i>&lt;Define the Project Growth Amount for the Mean Daily Volume of the service usage events&gt;/year</i>
Peak Daily volume	<i>&lt;Define the Peak Daily number of service usage events.&gt;</i>
Projected Growth	<i>&lt;Define the Projected Growth Amount of the Peak Daily value</i>

Peak Hourly volume	<i>of service usage events&gt;/year &lt;Define the Peak Hourly number of service usage events.&gt;</i>
Days of operation	<i>&lt;Define the days of operation this service should support. For example Sunday-Saturday&gt;.</i>
Hours of operation	<i>&lt;Define the hours of operation this service should support. For example 24/7&gt;</i>
Peak Hours	<i>&lt;Define the hours of peak usage this service should support. For example 9am-7p.m.Eastern&gt;</i>
Maximum Response Time	<i>&lt;Maximum Response Time for the service usage event. &gt;</i>

#### **Architect and Developer Notes:**

*The service performance should be able to support and performance should be tested against:*

- *Mean Daily Volume + Projected Growth*
- *Peak Daily Volume + Projected Growth*
- *Peak Hourly Volume*

*The bullets provided for complete enterprise performance requirements should be used as a guide when architecting the solution to ensure the solution is scalable to the expected performance requirements.*

### **2.9.2 Single Sign-On – Internal (SSOi)**

**User Profile:** VA Employee or Contractor who wants to gain access to an SSOi-protected application

The performance specifications for the SSOi service include the following:

- SSOi shall support 20 million authentications per day.
- VDS shall support 20 million authentications by SSOi per day.
- The IAM Binding Application shall support 1 million authentications per day.
- The IAM Binding Application shall support 1 million users.
- SSOi shall be able to handle an increase of 1 million users with integration to VistA.

The SSOi service for this increment shall support the following:

Operation	
<b>Name</b>	SSOi User Authentication (CA SiteMinder Web Agent, CA SiteMinder SPS and IdP to SP Federation)
<b>Usage Profile (User Authentication Events)</b>	

Mean Daily volume	40000
Projected Growth	8000/year
Peak Daily volume	50000
Projected Growth	10000/year
Peak Hourly volume	8000
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

Operation	
Name	SSOi STS
Usage Profile (Token Requests)	
Mean Daily volume	0
Projected Growth	10000/year
Peak Daily volume	0
Projected Growth	25000/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	1 second

### 2.9.3 Single Sign-On – External (SSOe) and AccessVA

**User Profile:** External users who want to gain access to an SSOe-protected VA resource

The target end state for AccessVA and SSOe should support the following:

- SSOe supports up to 4 million authentications per month.
- SSOe supports up to 7,500 concurrent users.
- AccessVA shall support threshold average page load Essential time under light load conditions (10 requests/minute) <= 5 seconds.
- AccessVA shall support threshold average page load Essential time under normal load conditions (100 requests /minute) <= 8 seconds.
- AccessVA shall support threshold average page load Essential time under peak load conditions (1000 requests /minute) <= 10 seconds.

AccessVA and SSOe for this increment shall support the following:

Operation	
Name	SSOe (Application Junction, Reassertion Provider, CSP/IdP Federation Partner)

<b>Usage Profile (User Authentication Events)</b>	
Mean Daily volume	80000
Projected Growth	20000/year
Peak Daily volume	120000
Projected Growth	30000/year
Peak Hourly volume	10000
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	10 seconds

<b>Operation</b>	
<b>Name</b>	SSOe STS
<b>Usage Profile (Token Requests)</b>	
Mean Daily volume	0
Projected Growth	20000/year
Peak Daily volume	0
Projected Growth	50000/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	10 seconds

<b>Operation</b>	
<b>Name</b>	SSOe oAuth
<b>Usage Profile (Token Requests)</b>	
Mean Daily volume	0
Projected Growth	20000/year
Peak Daily volume	0
Projected Growth	50000/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	10 seconds

Operation	
<b>Name</b>	SSOe (Webservice Client, Webservice Producer)
<b>Usage Profile (Webservice Calls)</b>	
Mean Daily volume	6000
Projected Growth	1500/year
Peak Daily volume	6800
Projected Growth	1700/year
Peak Hourly volume	950
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	10 seconds

## 2.9.4 Provisioning (Prov)

### User Profile:

- VA Employee or Contractor on the VA Network Provisioning/Modifying/De-provisioning a user for application access
- VA Employee or Contractor on the VA Network Approving or Rejecting a Provisioning/Modification/De-provisioning Request
- VA Employee or Contractor accessing the VA Network remotely to Provision/Modify/De-provision User Access
- VA Employee or Contractor accessing the VA Network remotely to Approve or Reject a Provision/Modify/De-provision Request
- VA Employee or Contractor accessing the VA Network remotely to Administer the Provisioning Application

The performance specifications for the Prov service include the following:

- VDS shall support 20 million authentications by SSOi per day.
- VDS shall support an additional 1 million users with integration to VistA.
- Provisioning supports 500,000 onboarding / offboarding requests per day.
- The provisioning repository / data store supports 10 million queries per day (300,000 from the VistA Evolution program).
- The response time for queries to the provisioning repository / data store has an average response time of five seconds and a maximum response time of ten seconds.
- The IAM Binding Application shall support 1 million authentications per day.
- The IAM Binding Application shall support 1 million users.

The Prov service for this increment shall support the following:

Operation	
Name	Provisioning
Usage Profile (Provisioning Events – On-board/Off-board, Provision, Deprovision, and Modify Events)	
Mean Daily volume	500
Projected Growth	1000/year
Peak Daily volume	1000
Projected Growth	2000/year
Peak Hourly volume	50
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

Operation	
Name	VDS
Usage Profile (Service Calls)	
Mean Daily volume	80000
Projected Growth	20000/year
Peak Daily volume	120000
Projected Growth	30000/year
Peak Hourly volume	10000
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am-10p.m.Eastern
Maximum Response Time	10 seconds

## 2.9.5 Compliance Audit and Reporting (CAR)

**User Profile:** VA Employee or Contractor accessing CAR to run standard and ad hoc reports

The CAR service for this increment shall support the following:

Operation	
Name	CAR
Usage Profile (Log Entries)	

Mean Daily volume	1,000,000
Projected Growth	250,000/year
Peak Daily volume	2,000,000
Projected Growth	500,000/year
Peak Hourly volume	100,000
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	Data must be returned at no more than 1 minute for every 10,000 records

## 2.9.6 Specialized Access Control (SAC)

**User Profile:** Users of an External System that checks SAC to determine whether a Veteran has given permission to see their health information

The target end state for the SAC service should support 325,000 transactions per day.

The SAC service for this increment shall support the following:

Operation	
<b>Name</b>	<b>SAC</b>
Usage Profile (Webservice Calls)	
Mean Daily volume	200
Projected Growth	200/year
Peak Daily volume	300
Projected Growth	300/year
Peak Hourly volume	25
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	5 seconds

## 2.9.7 Electronic Signature (ESig)

**User Profile:** External User accessing VA systems via the web and applying their electronic signature to a document

The Electronic Signature (ESig) service for this increment shall support the following:

Operation	
<b>Name</b>	<b>ESig</b>
Usage Profile (Webservice Calls)	

Mean Daily volume	100
Projected Growth	1000/year
Peak Daily volume	250
Projected Growth	2500/year
Peak Hourly volume	25
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am-10p.m.Eastern
Maximum Response Time	10 seconds

## 2.9.8 Identity Proofing (IP)

**User Profile:** VA Employee or Contractor on the VA Network proofing a person for a VA business process such as the issuance of a Veteran Health Identification Card (VHIC) card

The IP service for this increment shall support the following:

Operation	
Name	IP (Proofing UI)
Usage Profile (Proofing Events)	
Mean Daily volume	3500
Projected Growth	350/year
Peak Daily volume	4000
Projected Growth	400/year
Peak Hourly volume	500
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

Operation	
Name	IP (Webservice)
Usage Profile (Webservice Calls)	
Mean Daily volume	3500
Projected Growth	350/year
Peak Daily volume	4000
Projected Growth	400/year
Peak Hourly volume	500
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

### 2.9.9 Credential Service Provider (CSP)

**User Profile:** VA Employee or Contractor on the VA Network accessing the CSP service to update, upgrade, suspend, or revoke a credential to be used to access a VA application

The CSP service for this increment shall support the following:

Operation	
Name	CSP (Credential Registration)
Usage Profile (Registration Events)	
Mean Daily volume	0
Projected Growth	1000/year
Peak Daily volume	0
Projected Growth	1000/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am-10p.m.Eastern
Maximum Response Time	10 seconds

Operation	
Name	CSP (Authentication)
Usage Profile (User Authentication Events)	
Mean Daily volume	0
Projected Growth	10000/year
Peak Daily volume	0
Projected Growth	10000/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am-10p.m.Eastern
Maximum Response Time	10 seconds

## 2.10 Quality Attributes Specification

The AcS solution complies with the quality specifications set forth by the VA IAM Project Management Plan (PMP), Quality Management Approach section. The following types of testing are performed to assess the quality of the solution:

- Unit testing
- Integration / functional testing

- User acceptance testing (UAT)
- Section 508 testing
- Performance testing

The AcS solution also consists of the following quality specifications:

- The system is composed of tools, applications, and software that conform to VA's standard server and database operating systems. The VA [Technical Reference Model \(TRM\)](#) provides more information.
- The system is designed to operate in VA's standard virtualized operating system environment according to the VA [TRM](#).

## 2.11 Reliability Specifications

The AcS solution is hosted within the Terremark environment as required by VA. Terremark is responsible for reliability and monitoring when the AcS solution becomes operational. The tools, methods, and specifications for monitoring the reliability of the AcS solution are at the discretion of Terremark.

**Table 8: Service Availability Level 4**

<b>Service Availability Level 4</b> <b>*Standards adopted from specification created by Application Structure and Integration Services (ASIS)</b>	
<b>Description</b>	Mission Critical Information
<b>Minimum Availability</b>	99.99%
<b>Maximum Downtime Per Month</b>	4.4 minutes
<b>Business Value</b>	Essential to fundamental business operations – outage seriously impairs functioning of business.
<b>System Response</b>	In the absence of any system superseding requirements, the system responds to user actions in three seconds or less in 90% of the attempts, and never more than 10 seconds.
<b>Operational Hours</b>	Required 24 hours a day, every day.
<b>Significant Outage</b>	More than five minutes of downtime is considered significant at any time and requires an ANR to be sent out to the appropriate teams.
<b>Outage Impact</b>	Interruption of service may result in severe financial, regulatory, patient safety, patient health, or other business issues.
<b>Scheduled Maintenance</b>	Maintenance, including maintenance of externally developed software incorporated into the IAM system, is scheduled during off-peak hours (evenings and weekends) or in conjunction with relevant maintenance schedules.

Additional reliability specifications (response times, monitoring, maintenance periods, and operational support) may be viewed in the [IAM SLA](#).

## 2.12 Scope Integration

The scope of the integration for this AcS solution increment is identified in section 1.2.

## 2.13 Security Specifications

The security specifications include the following:

- AcS is deployed inside the VA firewall.
- AcS conforms to the VA security standards detailed in VA Handbook 6500 Information Security Program.
- Designated ports are opened between systems. All other ports are blocked to provide secure server-to-server communication.
- The Hypertext Transfer Protocol Secure (HTTPS) communication protocol is used for outbound and inbound traffic for external-facing applications.
- AcS communication channels are TLS/Secure Sockets Layer (SSL)-enabled and -encrypted.
- The AcS data layer is within the internal firewall zone to provide security of the data.
- AcS meets all Veterans Health Administration (VHA) security, privacy, and identity management requirements and those listed in VA Handbook 6500 (Enterprise Requirements Appendix).
- AcS databases, user information stores, and information tied to individuals are secured and/or encrypted while at rest and in motion.
- Access to the administrative, management, and internal user interfaces of the authorization service is controlled through the use of SSOi.
- The system must store and transmit Personally Identifiable Information (PII) or sensitive information such as passwords in an encrypted or one-way hashed format and on the SSL channel.
- The web servers providing access to VA applications for external users over the Internet must reside in the demilitarized zone (DMZ).

## 2.14 System Features

The AcS system features are included in the functional requirements.

## 2.15 Usability Specifications

The usability specifications include the following:

- The implementation plan conforms and adapts to VA's CRISP.
- The system integrates with VA business applications (as determined feasible) across heterogeneous environments and platforms.

# 3 Applicable Standards

The AcS solution complies with the applicable standards as specified in the following:

- Align processes and solutions with Federal mandates, industry standards, and VA policy

**Table 9: Applicable Standards**

<b>Applicable Standards</b>
<a href="#">NIST SP 800-63 Version 1.0.2; Electronic Authentication Guideline</a>
<a href="#">OASIS XACML 2.0</a>
<a href="#">Section 508 Standards Guide</a>
<a href="#">VA Directive 6500; Information Security Program</a>
VA Directive 6501; VA Identity Verification In-Person Proofing (IPP) Process
<a href="#">World Wide Web Consortium (W3C) SOAP Standard</a>
<a href="#">World Wide Web Consortium (W3C) XML Standard</a>
FICAM Roadmap and Implementation Guidance
OMB 04-04 E-Authentication Guidance for Federal Agencies
Aligns with the VA Enterprise Shared Services directive and strategy
Supports <a href="#">HSPD-12</a> specifications where applicable (i.e., Personal Identification Verification (PIV))
Follows the documentation specifications provided by the <a href="#">ProPath website</a> and VA Program Management Accountability System (PMAS)
<a href="#">6102 Handbook and the VA Web Best Practices Guide</a>
<a href="#">Approved and In-Process Devices</a>
<a href="#">Screen Resolution for Mobile Devices</a>

The eXtensible Access Control Markup Language (XACML) 3.0 standard is leveraged by the SAC service. XACML provides the following capabilities:

- XACML 3.0 is an Organization for the Advancement of Structured Information Standards (OASIS) standard. XACML provides a flexible policy management framework to achieve a consistent security implementation and alignment with VA's goals.
- XACML provides common, reusable security services that form the Service Oriented Architecture (SOA) foundational building blocks. These building blocks provide the ability to secure data and applications that are used by the different SOA components.
- XACML enables access control policies. XACML stores policies or provides a request and response model (based on XML format) for communication between enforcement and decision points.

The AccessVA development contractor shall conduct an audit of the AccessVA web pages, including pop-up widgets to ensure compliance with the abovementioned VA web standards, as well as Section 508. The AccessVA development contractor shall correct all items in the AccessVA web pages found not to be in compliance with the published VA web standards. See published VA web standards for compliance guidance.

## 4 Interfaces

Technical specifications and interfaces relating to communication, hardware, and software are defined in the specified design documents as outlined in the following subsections.

### 4.1 Communications Interfaces

The following documents provide information regarding communications interfaces:

- VA AcS Solution SDD
- VA AcS Solution Interface Control Document (ICD)

### 4.2 Hardware Interfaces

The VA AcS Solution SDD provides information regarding hardware interfaces.

### 4.3 Software Interfaces

The VA AcS Solution SDD provides information regarding software interfaces.

### 4.4 User Interfaces

The user interfaces are described in section 2.6.5.1 and section 2.14.

## 5 Legal, Copyright, and Other Notices

Independent and product-specific information pertaining to legal, copyright, and other notices is available externally (e.g., organization/product websites and guides).

## 6 Purchased Components

The AcS solution uses existing VA-approved and -procured components. The VA AcS Solution SDD provides information regarding purchased components.

### 6.1 Defect Source (TOP 5)

Not applicable

## 7 User Class Characteristics

The user community consists of the following classes:

- Internal users (internal VA personnel, employees, administrators, and contractors, etc.)
- External users (DoD, Veterans, doctors, beneficiaries, etc.)

The user community receives sufficient training to have the basic knowledge and technical skills required to successfully use the AcS solution technology:

- A technical training curriculum is developed and delivered to all levels of staff users. This may include user guidelines, in-person training, and computer-based training.

- The training curriculum states the expected task completion time for primary and secondary users.

## **8 Estimation**

The estimation information is not available at this time.

# Project Software Functional Size and Size-Based Effort and Duration Estimate

## Application

Item	A	B	C	D	E	Total
Counted Function Points						
Estimated Scope Growth						
Estimated Size at Release						

Size-Based Effort Estimates	Labor Hours	Probability
Low-Effort Estimate – With indicated probability, project will consume no more than:		
High-Effort Estimate – With indicated probability, project will consume no more than:		

Size-Based Duration Estimates	Work Days	Probability
Low-Duration Estimate – With indicated probability, project will consume no more than:		
High-Duration Estimate -- With indicated probability, project will consume no more than:		

**Figure 10: Cumulative Probability (“S-curve”) Chart**

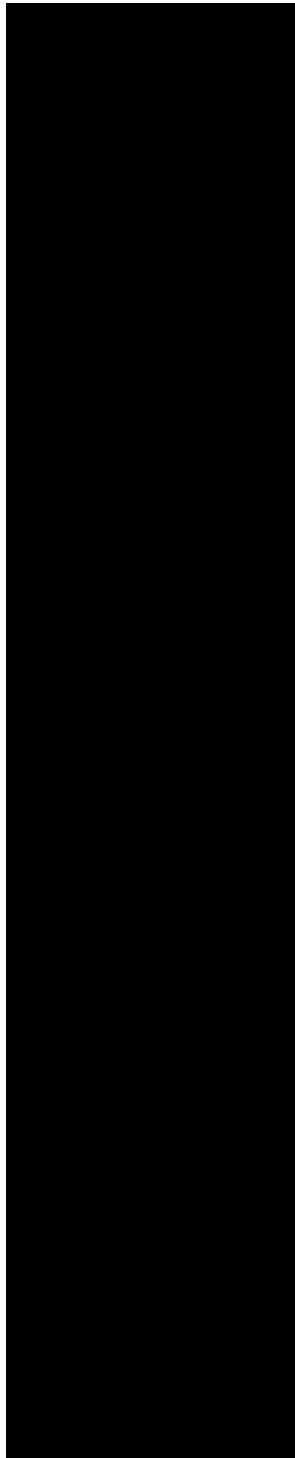
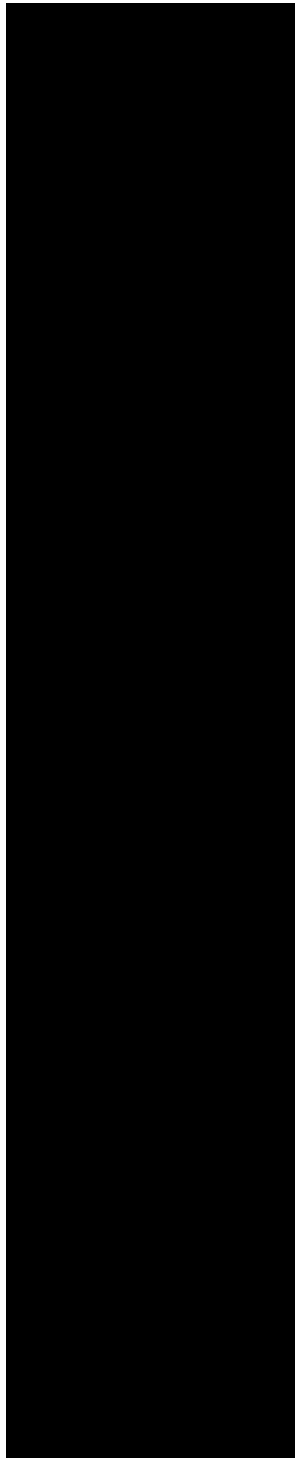
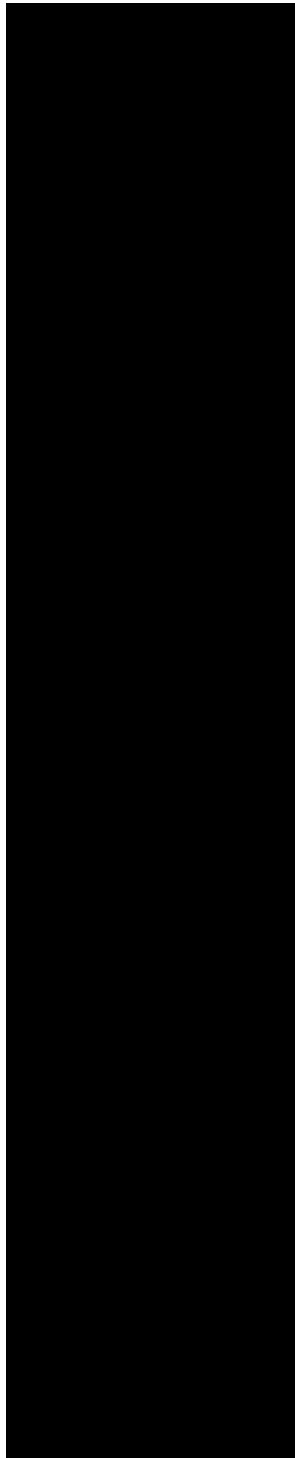
*[Insert Cumulative Probability (“S-curve”) Charts here]*

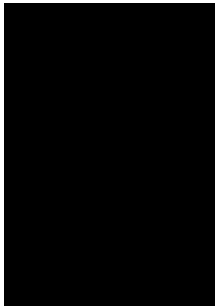
## 9 Approval Signatures

REVIEW DATE: <date>

SCRIBE: <name>

Signed:

		03/25/2015
	Integrated Project Team (IPT) Chair	Date
		02/13/2015
	Integrated Project Team (IPT) Chair	Date
		12/30/2014
	Integrated Project Team (IPT) Chair	Date
		11/17/2014
	Acting Integrated Project Team (IPT) Chair	Date
		10/30/2014
	Business Sponsor, IAM BPMO	Date
		10/30/2014
	IAM Program Manager	Date



10/30/2014

AcS Project Manager

Date

## Appendix A: Acronym List and Glossary

The abbreviations and terms used in this RSD are defined in the [Identity and Access Services Master Glossary](#).

### Glossary

Term	Meaning
3POB	Third-Party Onboarding
JSON	JavaScript Object Notation
OAuth	Open Authorization Standard
STS	Security Token Service

## Appendix B: Requirements Deferred to AcS 2.0 Increment 5

The following requirements were stated in previous AcS RSDs but were not delivered. They are delivered in AcS 2.0 Increment 5.

Requirements Document	REQ ID	REQ Text	Change Request ID	Code Change Request ID
AcS 2.0 Increment 2	SPEC570.6.1.1.3.1	SSOi shall support LOA-4 user authentication with holder-of-key implementation	AcS CR 2139	AcS CCR 3135
AcS 2.0 Increment 2	SPEC570.6.1.1.4.1	SSOi shall support mobile client registration	AcS CR 2146	AcS CCR 2499
AcS 2.0 Increment 2	SPEC570.6.1.1.4.3	SSOi shall support management and enforcement of oAuth policies	AcS CR 2174	No Associated CCR
AcS 2.0 Increment 2	SPEC570.6.1.1.4.4	SSOi shall support fine-grained revocation	AcS CR 2175	No Associated CCR
AcS 2.0 Increment 2	SPEC570.6.1.1.4.5	SSOi shall support limiting the number of access or refresh tokens	AcS CR 2176	AcS CCR 2731
AcS 2.0 Increment 2	SPEC570.6.1.1.4.6	SSOi shall support self-registration of clients	AcS CR 2177	No Associated CCR
AcS 2.0 Increment 2	SPEC570.6.1.1.5.2	SSOi shall support LOA-4 token exchange with holder of key	AcS CR 2179	AcS CCR 3140
AcS 2.0 Increment 2	SPEC570.6.1.2.1.1	SSOi shall support LOA-4 user authentication	AcS CR 2184	AcS CCR 3141
AcS 2.0 Increment 2	SPEC570.6.1.2.3	SSOi shall support VA internal user LOA-4 authentication into the SSOi environment	AcS CR 2223	AcS CCR 2523
AcS 2.0 Increment 2	SPEC570.6.1.2.4	SSOi shall support VA application integration at LOA-4	AcS CR 2224	AcS CCR 2524
AcS 2.0 Increment 2	SPEC570.6.1.2.6.1	SSOi shall support oAuth from the provider perspective	AcS CR 2226	AcS CCR 2526
AcS 2.0 Increment 2	SPEC570.6.1.2.6.2	SSOi shall support oAuth enforcement from application perspective	AcS CR 2227	AcS CCR 2527
AcS 2.0 Increment 2	SPEC570.6.1.2.6.3	SSOi shall support mobile client registration	AcS CR 2228	AcS CCR 2528
AcS 2.0 Increment 2	SPEC570.6.1.2.6.5	SSOi shall support management and enforcement of oAuth policies	AcS CR 2230	AcS CCR 2530
AcS 2.0 Increment 2	SPEC570.6.1.2.6.6	SSOi shall support fine-grained revocation	AcS CR 2231	AcS CCR 2531

Requirements Document	REQ ID	REQ Text	Change Request ID	Code Change Request ID
AcS 2.0 Increment 2	SPEC570.6.1.2.6.7	SSOi shall support limiting the number of access or refresh tokens	AcS CR 2232	AcS CCR 2532
AcS 2.0 Increment 2	SPEC570.6.1.2.6.8	SSOi shall support self-registration of clients	AcS CR 2233	AcS CCR 2533
AcS 2.0 Increment 2	SPEC570.6.1.2.7.5	SSOi IdP shall support issuance of LOA-4 SAML token with holder of key	AcS CR 2238	AcS CCR 3107
AcS 2.0 Increment 3	SPEC1448.6.1.4	<p>The Identity Proofing service shall require only one Primary ID in order to be In-Person Proofed</p> <p>Primary ID documents for Identity Proofing LOA 2:</p> <ul style="list-style-type: none"> <li>• U.S. Passport or U.S. Passport Card</li> <li>• Permanent Resident Card or Alien Registration Receipt Card (Form I-551)</li> <li>• Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa</li> <li>• Employment Authorization Document that contains a photograph (Form I-766)</li> <li>• Foreign passport with Form I-94 or Form I-94A that has the same name as the passport</li> <li>• Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address, ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address (includes PIVs)</li> <li>• U.S. Military ID card (both active and retired acceptable) or draft record</li> <li>• U.S. Military dependent's ID card</li> </ul>	AcS CR 3671	No Associated CCR

Requirements Document	REQ ID	REQ Text	Change Request ID	Code Change Request ID
		<p>References:</p> <ul style="list-style-type: none"> <li>• <i>NIST SP 800-63-2, Electronic Authentication Guideline</i>, August, 2013</li> <li>• <i>Federal Information Processing Standards Publication 201-2, Personal Identity Verification of Federal Employees and Contractors</i>, September, 2013</li> <li>• VA Directive 6510, <i>VA Identity and Access Management (Draft)</i></li> </ul>		

## Appendix C: SSOe Headers

The LOA 2+ authentication traits have been updated for this increment.

**Table 10: LOA 2+ Authentication Traits Business Rules**

Authentication Trait (HTTP Header)	Required/Optional	Source Primary (Secondary)	Source Attribute/Trait Name	Action If Trait Not Provided	Additional Business Rules
va_eauth_ICN	R	MVI	ICN	Pass User to Third-Party Credential Onboarding	
va_eauth_PID	O	MVI	Person ID (Corporate DB)	Pass Null Value	1. If 2 or more PIDs are returned, then provide all in headers
va_eauth_filenumbr	O	MVI	File Number (BIRLS)	Pass Null Value	1. If 2 or more BIRLS file numbers are returned, then provide all in headers
va_eauth_secID	R	Prov	secID	Pass User to Third-Party Credential Onboarding	1. If 2 or more secID are returned, then provide all in headers
va_eauth_dodedipnid	O	MVI	va_eauth_dodedipnid	1. If CSP is DS LOGON a. and EDI PI returned from MVI is different, then pass value from CSP b. and EDI PI not in MVI, then pass EDI PI from CSP 2. If CSP is not DSLOGON, and EDI PI is not in MVI, then	1. If 2 or more EDI PI are returned, then provide all in headers

Authentication Trait (HTTP Header)	Required/Optional	Source Primary (Secondary)	Source Attribute/Trait Name	Action If Trait Not Provided	Additional Business Rules
				pass null	
va_eauth_csid	R	CSP	va_eauth_csid	Do Not Authenticate	
va_eauth_uid	R	CSP	va_eauth_uid	Do Not Authenticate	
va_eauth_hash	R	CSP	va_eauth_hash	Do Not Authenticate	
va_eauth_assurancelevel	R	CSP	va_eauth_assurancelevel	Do Not Authenticate	
va_eauth_authenticationmethod	O	CSP	va_eauth_authenticationmethod	Pass Null Value	
va_eauth_authenticationauthority	O	CSP	va_eauth_authenticationauthority	Pass Null Value	
va_eauth_commonname	O	CSP	va_eauth_commonname	Pass Null Value	
va_eauth_email	O	CSP (Prov)	email	Pass Null Value	<ol style="list-style-type: none"> <li>1. If email is provided by CSP, then pass CSP</li> <li>2. If email is not provided by CSP, then pass Prov value</li> </ol>
va_eauth_LastName	R	MVI	va_eauth_LastName	Do Not Authenticate	
va_eauth_FirstName	O	MVI	va_eauth_FirstName	Pass Null Value	
va_eauth_MiddleName	O	MVI	MiddleName	Pass Null Value	
va_eauth_PNID	O	MVI (CSP)	va_eauth_PNID	Pass Null Value	<ol style="list-style-type: none"> <li>1. If SSN is provided by MVI, then pass MVI</li> <li>2. If SSN is not provided by MVI, then pass CSP</li> </ol>
va_eauth_Prefix	O	MVI	Prefix	Pass Null Value	
va_eauth_Suffix	O	MVI	Suffix	Pass Null Value	
va_eauth_Gender	O	MVI	Gender	Pass Null Value	
va_eauth_DOB	O	MVI	Date of Birth (DOB)	Pass Null Value	

Authentication Trait (HTTP Header)	Required/Optional	Source Primary (Secondary)	Source Attribute/Trait Name	Action If Trait Not Provided	Additional Business Rules
va_eauth_transactionID	R	SSOe	Transaction ID for session user	Do Not Authenticate	
va_eauth_IssueInstant	R	CSP	The time of authentication to the CSP	Do Not Authenticate	
va_eauth_csp_object	O	CSP	Derived JSON package of CSP's additional traits*	Pass Null Value	
va_eauth_mhvien	O	MVI	MHV IEN (MHV)	Pass NOT_FOUND	1. If two or more MHV IENs are returned, then put all in headers
va_eauth_street	O	MVI (CSP)	va_eauth_street	Pass Null Value	
va_eauth_street_2	O	MVI (CSP)	va_eauth_street	Pass Null Value	
va_eauth_street_3	O	MVI (CSP)	va_eauth_street	Pass Null Value	
va_eauth_city	O	MVI (CSP)	va_eauth_city	Pass Null Value	
va_eauth_state	O	MVI (CSP)	va_eauth_state	Pass Null Value	
va_eauth_country	O	MVI (CSP)	va_eauth_country	Pass Null Value	
va_eauth_postalcode	O	MVI (CSP)	va_eauth_postalcode	Pass Null Value	
CSP Data Only	R	SSOe		N/A	
IAM Service Down	R	SSOe		N/A	

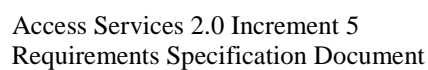
\*Data elements from the va\_eauth\_csp\_object must not be used to override the elements provided in the common authentication traits.

**Notes:**

- a. Required means that if this data element is not available from the Primary Source, do not authenticate the user
- b. Optional means that if this data element is not available from the Primary Source take alternative action
- c. Pass User to Third-Party Credential Onboarding
  - o Pass Null Value in header

- Pass Value from secondary source
- Other as specified in the business rules table

The following activity diagram describes the IAM Prov-enabled CRISP onboarding process.



## Template Revision History

Date	Version	Description	Author
December 2014	1.4	Updated to conform with latest Section 508 guidelines and remediated with Common Look Office tool	Process Management
May 2014	1.3	Reordered cover sheet to clarify results of artifact searches	Process Management
May 2013	1.2	Add Appendix for acronyms and glossary	Process Management
March 2013	1.1	Formatted to current ProPath documentation standards and edited to conform with latest Alternative Text (Section 508) guidelines	Process Management
January 2013	1.0	Initial Version	PMAS Business Office