

**Identity and Access Management  
Access Services 2.0 Increment 7  
Requirements Specification Document**



**April 2016  
Version 1.2**

**Department of Veterans Affairs**

## 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	Author
4/14/2016	1.2	Completed a quality review. Posted the PDF on the AcS Phase 2 TSPR.	
3/28/2016	1.1	Updated document with Rational Requirements Composer Feature tags to reflect added and deleted requirements.	
3/14/2016	1.1	Removed On/Off-Boarding Requirements. These requirements are now being managed in a separate document. Adding AccessVA requirements approved by the CCB. Adding SSOi UI Enhancements to focus on 2FA.	
1/05/2016	1.0	Document version changes to 1.0 upon stakeholder approval. Posted the PDF on the AcS Phase 2 TSPR.	
1/04/2016	0.5	Updated document with Rational Requirements Composer Feature tags to uniquely identify the AcS traceable requirements.	
12/01/2015	0.4	Completed a quality review.	
11/20/2015	0.3	Updated with formal review feedback.	
11/12/2015	0.2	Completed a tech edit review.	
10/30/2015	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. Introduction .....</b>	<b>1</b>
1.1. Purpose.....	1
1.2. Scope .....	2
1.3. References.....	2
<b>2. Overall Description .....</b>	<b>4</b>
2.1. Accessibility Specifications.....	4
2.2. Business Rules Specification .....	4
2.3. Design Constraints Specification.....	4
2.4. Disaster Recovery Specification.....	4
2.5. Documentation Specifications.....	4
2.6. Functional Specifications .....	5
2.6.1. SSOi .....	5
2.6.1.1. STS Support of NPE.....	5
2.6.1.2. Preserve POST Data .....	6
2.6.1.3. IdP to SP SiteMinder Cookie Refresh .....	6
2.6.1.4. IdP to SP Federation Partner SAML SDK Package .....	7
2.6.1.5. SSOi External Error Page .....	7
2.6.1.6. SSOi UX/UI Enhancements .....	9
2.6.1.7. SSOi Audit Logging .....	11
2.6.2. SSOe and AccessVA.....	12
2.6.2.1. SSOe PIV Parsing .....	12
2.6.2.2. Re-Assertion Partner Session Refresh .....	12
2.6.2.3. oAuth Access Token Status Tracking .....	13
2.6.2.4. Re-Assertion Partner SAML SDK Package.....	14
2.6.2.5. SSOe DOB Attribute .....	14
2.6.2.6. DS Logon CSP ID Update .....	15
2.6.2.7. SSOe Last Login Tracking .....	15
2.6.2.8. SSOe Changed Data Tracking.....	15
2.6.2.9. SSOe Delegation Tool Support.....	16
2.6.2.10. Enabling Widget for Re-Assertion and oAuth Partners .....	16
2.6.2.11. AccessVA UX/UI Enhancements.....	17
2.6.2.12. SSOe Audit Logging.....	18
2.6.3. Provisioning .....	18
2.6.3.1. General Enhancements .....	20
2.6.3.2. SSOe User Attribute for AMS in VDS.....	21
2.6.3.3. Off-Boarding Third-Party Credential.....	22
2.6.3.4. Trait Updates for Third-Party Credentials.....	22
2.6.3.5. NPE .....	24
2.6.3.6. Delete CSP .....	28
2.6.3.7. Provisioning UX/UI Enhancements .....	31
2.6.4. Authorization Management Service (Delegation).....	31
2.6.4.1. Invitation to Act as Delegate Flow .....	31
2.6.4.2. IAM AMS Web Service .....	35

2.6.4.3.	IAM AMS Integration with Relationship Management.....	36
2.6.4.4.	IAM Delegation Self-Service User Interface .....	38
2.6.4.5.	IAM Delegation Staff-Facing User Interface .....	42
2.6.4.6.	AMS Audit Logging .....	43
2.6.5.	IP .....	43
2.6.5.1.	Decoupling VA IP and VA VHIC.....	43
2.6.6.	CSP .....	44
2.6.6.1.	VA CSP UX/UI Enhancements .....	44
2.6.6.2.	CSP Audit Logging .....	44
2.6.7.	eSig.....	44
2.6.7.1.	eSig Service Security Enhancement .....	44
2.6.7.2.	eSig Audit Logging.....	46
2.6.8.	Audit Logging Requirements.....	47
2.7.	Graphical User Interface (GUI) Specifications.....	50
2.8.	Multi-divisional Specifications.....	50
2.9.	Performance Specifications.....	50
2.9.1.	Templates for AcS Service Components .....	51
2.9.2.	SSOi .....	52
2.9.3.	SSOe and AccessVA.....	55
2.9.4.	Prov .....	58
2.9.5.	CAR .....	60
2.9.6.	SAC .....	60
2.9.7.	AMS.....	61
2.9.8.	eSig.....	62
2.9.9.	IP .....	63
2.9.10.	CSP .....	64
2.10.	Quality Attributes Specification.....	66
2.11.	Reliability Specifications.....	66
2.12.	Scope Integration .....	67
2.13.	Security Specifications .....	68
2.14.	System Features .....	68
2.15.	Usability Specifications .....	68
2.16.	External System Enablements .....	68
<b>3.</b>	<b>Applicable Standards .....</b>	<b>69</b>
<b>4.</b>	<b>Interfaces.....</b>	<b>70</b>
4.1.	Communications Interfaces.....	70
4.2.	Hardware Interfaces .....	71
4.3.	Software Interfaces .....	71
4.4.	User Interfaces.....	72
<b>5.</b>	<b>Legal, Copyright, and Other Notices .....</b>	<b>72</b>

<b>6. Purchased Components.....</b>	<b>72</b>
<b>7. User Class Characteristics.....</b>	<b>72</b>
<b>8. Estimation .....</b>	<b>72</b>
<b>9. Approval Signatures .....</b>	<b>74</b>
<b>Appendix A: Non-Functional Requirements .....</b>	<b>76</b>
<b>Appendix B: Acronym List and Glossary.....</b>	<b>82</b>
<b>Appendix C: Requirements Deferred to AcS 2.0 Increment 7.....</b>	<b>83</b>

## List of Figures

Figure 1: SSOi External Error Page .....	8
Figure 2: Third-Party Credential On-Boarding.....	23
Figure 3: Provisioning NPE .....	25
Figure 4: Delete CSP .....	29
Figure 5: Patient-Initiated Invitation Scenario for VAHP Delegation .....	32
Figure 6: Staff-Initiated Invitation Scenario for VAHP Delegation .....	33
Figure 7: Creating VA Healthcare Proxy for Delegator .....	39
Figure 8: eSig Service Security Enhancement .....	45

## List of Tables

Table 1: Document References .....	2
Table 2: Performance Specifications.....	51
Table 3: Availability Level Specifications .....	67
Table 4: AcS Services and Availability Levels.....	67
Table 5: Applicable Standards .....	69

# 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 Enterprise Shared Services (ESS) 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 requester 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 7.

The AcS 2.0 Increment 7 requirements described in this RSD are drawn from VA AcS FY16 Business Requirements Documents (BRDs). Additional AcS 2.0 Increment 7 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 7 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:

- ESS 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 7 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 7. The AcS requirements include the following components:

- Single Sign-On – Internal (SSOi)
- Single Sign-On – External (SSOe) and AccessVA
- Provisioning (Prov)
- Specialized Access Control (SAC)
- Authorization Management Service (AMS)
- Identity Proofing (IP)
- Credential Service Provider (CSP)
- Electronic Signature (eSig)

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

- Compliance Audit and Reporting (CAR)

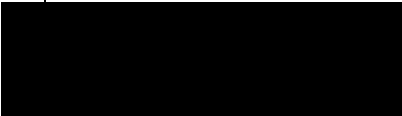
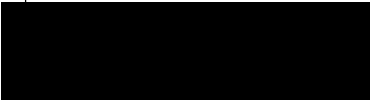
Additionally, [Appendix C](#) contains a list of requirements that were stated in previous AcS RSDs but deferred to AcS 2.0 Increment 7 for delivery.

## 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**

Title	Date	Published By
AcS FY16 BRD	1/2015	OIS BPMO
Section 508 Standards Guide	4/16/2010	General Service Administration

<b>Title</b>	<b>Date</b>	<b>Published By</b>
NIST Special Publication (SP) 800-63-2; Electronic Authentication Guideline	8/2013	National Institute of Standards and Technology (NIST)
VA Directive 6500; Information Security Program	8/2006	VA
VA Directive 6501; VA Identity Verification In Person Proofing (IPP) Process; IAM Handbook	Last updated: 09/01/2010	VA
NIST Public Key Infrastructure (PKI) Program	2/2001	National Institute of Standards and Technology (NIST)
VA IAM Handbook 6510	TBD	VA
VRM IAM Scope and Vision Document	10/2012	VA
Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0	12/2011	Federal CIO Council
OMB 04-04 E-Authentication Guidance for Federal Agencies	12/2003	Office of Management and Budget (OMB)
Security Assertion Markup Language (SAML) Artifact Profile as an Adopted Scheme for E-Authentication, Version 1.0.0	6/2004	GSA
Security Assertion Markup Language (SAML) Artifact Profile as an Adopted Scheme for E-Authentication, Version 1.1.0	9/2005	GSA
AcS RSDs at the following links: 		IAM Access Service Analysis Team
AcS SDDs at the following links: 		AcS Development Contractors

Title	Date	Published By
AcS 2.0 Increment 2 UC Model	TBD	
[REDACTED]	8/2015	IAM Identity Services Team
AccessVA Use Case Specification (Listed as EAG) at the following links: [REDACTED]	1/2013	AccessVA Development Contractors

## 2. Overall Description

The scope and functionality for AcS 2.0 Increment 7 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](#). Refer to the Common Business Rules document for additional business rules.

### 2.3. Design Constraints Specification

The AcS solution complies with the approved [REDACTED]

### 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 [REDACTED]

## 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 FY16 BRD and is a separate deliverable.

### 2.6.1. SSOi

#### 2.6.1.1. STS Support of NPE

To improve IAM security support both internally and externally, the IAM Secure Token Service (STS) will be enhanced to provide three additional token types to support Non-Person Entities (NPE). The NPE Types include the following:

- NPE with Enterprise Identity (Ent ID): Connected User with Application Determined Enterprise Identity content
- NPE with Non-Enterprise User: Connected User without Enterprise Identity content
- NPE with No User: Business Process running with no associated connected user.

The business process/entity will be represented by a set of traits/attributes allowing it to be recognizable by the enterprise when communicating externally.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. 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 using the sign on credentials originally submitted.		
	Non Person Entity (NPE) Token Types	<b>[FEATURE 650123]</b> STS shall be enhanced to provide a standard set of SSO authentication traits for the following non person entity (NPE) token types: <ul style="list-style-type: none"><li>• NPE with Enterprise Identity (Ent ID) only</li><li>• NPE with Non-Enterprise User</li><li>• NPE with No User</li></ul> See [REDACTED]
	IAM Standard STS Token Input Parameters	<b>[FEATURE 650124]</b> STS shall provide the capability to accept a standard set of input parameters based on the entity token type as identified in the STS SAML Token Definition. See [REDACTED]
	Data Mapping	<b>[FEATURE 650125]</b> STS shall support the data mapping for the STS Token Traits as identified in the STS SAML Token Definition.

BRD BN	Requirement	In-Scope Requirement Clarification
		<b>Note:</b> STS shall retrieve System Metadata from a Provisioning component. See [REDACTED]

### 2.6.1.2. Preserve POST Data

Enhance SSOi to preserve the data the user has entered in the event of session timeout. This will ensure that the data is still available when the user logs back into the application.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12.75: SSOi shall preserve the data entered in the current session to prevent inadvertent loss due to time out or session interruption.		
12.75	Preserve POST Data	<b>[FEATURE 650127]</b> SSOi shall preserve the Hypertext Transfer Protocol Secure (HTTP) POST data entered in the current session to prevent inadvertent loss due to timeout.

### 2.6.1.3. IdP to SP SiteMinder Cookie Refresh

Enhance SSOi to allow a SAML Identity Provider (IdP) to Service Partner (SP) Federation partner to keep the SSOi SiteMinder cookie alive. This will prevent SAML IdP to SP Federation partner users from being logged out of their applications due to timeouts when they are still in fact active users.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. 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 using the sign on credentials originally submitted.		
12.0	IdP to SP Federation Partner SiteMinder Cookie Refresh	<b>[FEATURE 650129]</b> SSOi shall allow SAML IdP to SP Federation partners to keep our SSOi SiteMinder Cookie alive.
		<b>[FEATURE 650130]</b> SSOi shall place a max expiration time on the refresh capability on the SAML IdP to SP Federation refresh capability.
		<b>[FEATURE 650131]</b> SSOi shall allow SAML IdP to SP Federation partner to terminate the refresh token.
		<b>[FEATURE 650132]</b> SSOi shall allow SAML IdP to SP Federation partner to terminate the refresh token and logout (i.e. terminate SiteMinder Cookie).

BRD BN	Requirement	In-Scope Requirement Clarification
		[FEATURE 650133] SSOi shall terminate the user's refresh token on all global logout calls when a SAML IdP to SP Federation assertion partner terminates refresh token and logs out.
		[FEATURE 650134] SSOi shall on a periodic basis remove all expired refresh tokens.

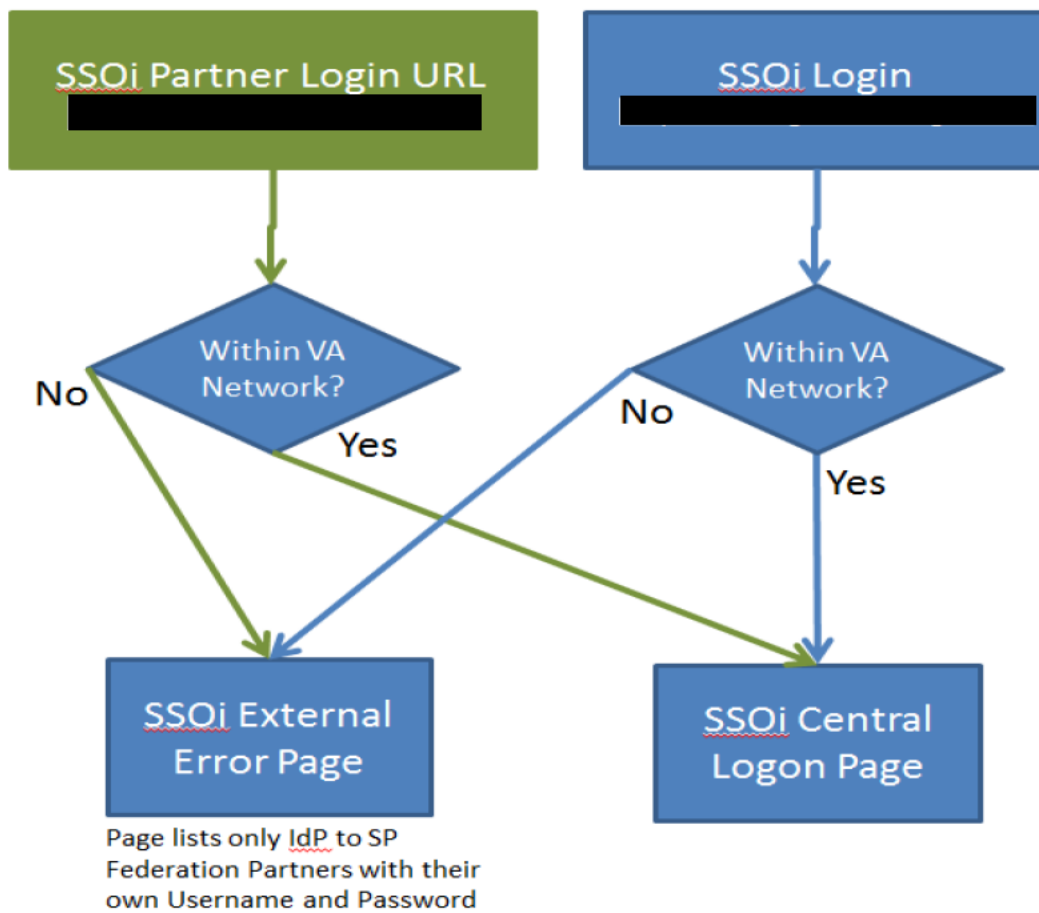
#### 2.6.1.4. IdP to SP Federation Partner SAML SDK Package

The IdP to SP Federation Partner SAML Software Development Kit (SDK) package improves integration efficiency and the speed of the integration with SSOi IdP to SP Federation partners. By providing SDK packages with examples to partner applications, it will be easier to understand the IAM SAML solution and adapt their application to accept it.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. 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 using the sign on credentials originally submitted.		
12.0	IdP to SP Federation Partner SAML SDK Package	[FEATURE 650136] SSOi shall create an SDK package with examples to support the integration of IdP to SP Federation partners SAML messaging and SAML consumption.
		[FEATURE 650137] SSOi shall create the "IdP to SP Federation Partner" SDK package for Java language.
		[FEATURE 650138] SSOi shall create the "IdP to SP Federation Partner" SDK package for JavaScript.
		[FEATURE 650139] SSOi shall create the "IdP to SP Federation Partner" SDK package for Ruby.
		[FEATURE 650140] SSOi shall create the "IdP to SP Federation Partner" SDK package for .Net.
		[FEATURE 650141] SSOi shall create installation documentation and example running documentation for the "IdP to SP Federation Partner" SDK package.

#### 2.6.1.5. SSOi External Error Page

An SSOi External Error Page will be provided for users who attempt to access an SSOi resource (i.e., Talent Management System [TMS] SSOi link) while not connected to the VA network.



**Figure 1: SSOi External Error Page**

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. 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 using the sign on credentials originally submitted.		
12.0	SSOi External Error Page	<b>[FEATURE 650143]</b> If a user attempts to access an SSOi resource (i.e., TMS SSOi link) while not connected to the VA network, SSOi shall display the SSOi External Error Page.
		<b>[FEATURE 650144]</b> The SSOi External Error Page shall provide the message “Users must be on the VA network (i.e. VPN or in a VA facility) in order to access an SSOi resource via the Centralized Login Screen.”
		<b>[FEATURE 650145]</b> The SSOi External Error Page shall display a list of IdP to SP Federation Partners which have their own independent log in method in addition to SSOi.
		<b>[FEATURE 650146]</b> The SSOi External Error Page shall display a list of IdP to SP Federation Partners as user-friendly, configurable application names (for example, TMS, E-Gov Travel Service (ETS2), Pulse) as hyperlinks to target URLs for the user to login with a non SSOi login.
		<b>[FEATURE 650147]</b> The SSOi External Error Page shall have the same header, footer, Government warning and Help Desk information as the IAM Central Logon Page.

#### 2.6.1.6. SSOi UX/UI Enhancements

These requirements aim to improve the user experience (UX) and the user interface (UI) for users throughout the logging in process and across SSOi.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. 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 using the sign on credentials originally submitted.		
12.0	SSOi UX/UI Enhancements	<b>[FEATURE 650149]</b> All SSOi pages shall be updated to match the AcS Style Guide.
		<b>[FEATURE 650150]</b> SSOi shall receive UX/UI improvements identified during user testing and

BRD BN	Requirement	In-Scope Requirement Clarification
	Update SSOi Centralized Login Page	wireframing sessions.
		<b>[FEATURE 650151]</b> The Centralized Login Page shall have an “About” link to launch the About Page.
		<b>[FEATURE 650152]</b> The Centralized Login Page shall contain a target statement “Select Log In Method to Access: [user-friendly application name]”
		<b>[FEATURE 650153]</b> The Centralized Login Page shall display a target URL “[target URL, if IdP to SP consumer application URL (SPID)]” under the user-friendly application name.
		<b>[FEATURE 650154]</b> The Centralized Login Page shall be formatted to be readable on a screen without zooming or scrolling.
		<b>[FEATURE 695006]</b> The SSOi Central Login page shall be enhanced to focus on Two Factor Authentication. <b>Note:</b> Screen mockups will be provided as a starting point to support wireframing sessions.
BRD BN12.22 Single Sign-On – Internal (SSOi): SSOi shall receive user request for individual application log off.		
BRD BN12.23 Single Sign-On – Internal (SSOi): SSOi shall generated request for individual application log off.		
12.22	Update IAM Authenticated Landing Page	<b>[FEATURE 650155]</b> The IAM Authenticated Landing Page shall have an “About” link to launch the About Page.
12.23		<b>[FEATURE 650156]</b> The IAM Authenticated Landing Page shall contain the following text: “You have been logged out of [user-friendly application name]. You can navigate to another application protected by IAM SSOi without logging in.”
		<b>[FEATURE 650157]</b> The IAM Authenticated Landing Page shall display the user-friendly application name as a hyperlink to target URL.
		<b>[FEATURE 650158]</b> The IAM Authenticated Landing Page shall contain the following text: “You are logged in to IAM Single Sign On Internal (SSOi). If you are finished working, log out of SSOi and close any secure sessions that may still be open by clicking the ‘Logout’ button

BRD BN	Requirement	In-Scope Requirement Clarification
		immediately above. To protect your privacy, please close your browser after completing the log off.”
BRD BN12.20 Single Sign-On – Internal (SSOi): SSOi shall receive user request for global application log off. BRD BN12.21 Single Sign-On – Internal (SSOi): SSOi shall generate request for global application log off.		
12.20 12.21	Update IAM Logout Page	<b>[FEATURE 650159]</b> The IAM Logout Page shall have an “About” link to launch the About Page.
		<b>[FEATURE 650160]</b> The IAM Logout Page shall contain the following text: “To protect your privacy, please close your browser after completing the log off.”
	Update Timeout Page	<b>[FEATURE 650161]</b> The IAM Timeout Page shall have an “About” link to launch the About Page.
		<b>[FEATURE 650162]</b> The IAM Timeout Page shall contain the following text: “To protect your privacy, please close your browser after completing the log off.”
		<b>[FEATURE 650163]</b> The IAM Timeout Page shall contain the following text: “For general questions regarding the IAM authentication service, please contact the National Service Desk Support, [REDACTED]”

#### 2.6.1.7. SSOi Audit Logging

These requirements aim to ensure each service conforms to the audit logging requirements.

BRD BN	Requirement	In-Scope Requirement Clarification
23. Audit Trail: Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.		
23.0	SSOi Audit Logging	<b>[FEATURE 650165]</b> The SSOi service complies with the auditing requirements specified in the <b>Audit Logging Requirements</b> section.

## 2.6.2. SSOe and AccessVA

### 2.6.2.1. SSOe PIV Parsing

Enhancement to SSOe Personal Identity Verification (PIV) parsing to improve the reliability of parsing the data elements needed for user identification for PKI users. This will help prevent incorrect or missed user identity mappings during third-party on-boarding.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	SSOe PIV Parsing	<b>[FEATURE 650168]</b> SSOe shall create a parsing algorithm for the subject DN of a user's PKI certificate with preference given to the following data items in order: 1. coordinated id (May be obtained from FASC-N) 2. lastname 3. firstname 4. middle 5. generational qualifiers
		<b>[FEATURE 650169]</b> SSOe shall create a test suite that includes all subject DN naming combinations to validate the parsing success and error capability.

### 2.6.2.2. Re-Assertion Partner Session Refresh

Enhance SSOe to allow a SAML re-assertion partner to keep our SSOe PDSESSION alive. This will prevent SAML re-assertion users from being logged out of their applications due to timeouts when they are still in fact active users (e.g., still active on a standard junction AccessVA partner site).

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	Re-Assertion Partner Session Refresh	<b>[FEATURE 650171]</b> SSOe shall allow SAML re-assertion partners to keep our SSOe PDSESSION active by using a refresh call.
		<b>[FEATURE 650172]</b> SSOe shall place a max expiration time on the refresh capability on the SAML re-assertion refresh capability.
		<b>[FEATURE 650173]</b> SSOe shall allow SAML re-assertion partners to terminate the refresh token.
		<b>[FEATURE 650174]</b> SSOe shall allow SAML re-assertion partners to terminate the refresh token and logout (i.e., terminate PDSESSION).

BRD BN	Requirement	In-Scope Requirement Clarification
		<b>[FEATURE 650175]</b> SSOe shall terminate the users refresh token on all global logout calls when a SAML re-assertion partner terminates refresh token and logs out.
		<b>[FEATURE 650176]</b> SSOe shall on a periodic basis remove all expired refresh tokens.

### 2.6.2.3. oAuth Access Token Status Tracking

Allows partner applications to provide warning messages to their users that a session idle timeout will occur (e.g., “Your session has been idle. Please click here to keep your session active”). This also eliminates the need for partner applications to store and track “lastAccessedTime” per user identifier on its Authorization services Database and delegates any requests to the IAM endpoint instead.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	oAuth Access Token Status Tracking	<b>[FEATURE 650178]</b> SSOe OAuth shall provide a REST based service that accepts a valid access token and returns the lastAccessedTime, lastLoginTime, timeToExpireInSeconds, UserId, and SecID.
		<b>[FEATURE 650179]</b> SSOe OAuth Access Token Status service shall return responses in a JSON format.
		<b>[FEATURE 650180]</b> SSOe OAuth Access Token Status service shall error response with properties "error" and "error_description."
		<b>[FEATURE 650181]</b> SSOe OAuth Access Token Status service shall use the following values for the "error" property: <ul style="list-style-type: none"> <li>• ACCESS_DENIED</li> <li>• DESCRIPTION</li> <li>• ERROR</li> <li>• INSUFFICIENT_SCOPE</li> <li>• INVALID_CLIENT</li> <li>• INVALID_GRANT</li> <li>• INVALID_REQUEST</li> <li>• INVALID_SCOPE</li> <li>• INVALID_TOKEN</li> <li>• REDIRECT_URI_MISMATCH</li> <li>• UNAUTHORIZED_CLIENT</li> <li>• UNSUPPORTED_GRANT_TYPE</li> </ul>

BRD BN	Requirement	In-Scope Requirement Clarification
		<ul style="list-style-type: none"> <li>• UNSUPPORTED_RESPONSE_TYPE</li> <li>• URI</li> </ul>

#### 2.6.2.4. Re-Assertion Partner SAML SDK Package

The Re-Assertion Partner SAML SDK package improves integration efficiency and the speed of the integration with SSOe re-assertion partners. By providing SDK packages with examples to partner applications, it will be easier to understand the IAM SAML solution and adapt their application to accept it.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	Re-Assertion Partner SAML SDK Package	<b>[FEATURE 650183]</b> SSOe shall create an SDK package with examples to support the integration of Re-Assertion partners SAML messaging and SAML consumption.
		<b>[FEATURE 650184]</b> SSOe shall create the "Re-Assertion Partner" SDK package for Java language.
		<b>[FEATURE 650185]</b> SSOe shall create the "Re-Assertion Partner" SDK package for JavaScript.
		<b>[FEATURE 650186]</b> SSOe shall create the "Re-Assertion Partner" SDK package for Ruby.
		<b>[FEATURE 650187]</b> SSOe shall create the "Re-Assertion Partner" SDK package for .Net.
		<b>[FEATURE 650188]</b> SSOe shall create installation documentation and example running documentation for the "Re-Assertion Partner" SDK package.

#### 2.6.2.5. SSOe DOB Attribute

SSOe Date of Birth (DOB) was previously split into 2 attributes to support imprecise DOB. The format of the DOB attribute was updated to support imprecise DOB. The second attribute is no longer needed.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	SSOe Date of Birth Attribute	<b>[FEATURE 650190]</b> SSOe shall retire the "Imprecise DOB" attribute once imprecise DOB is managed by the existing "DOB"

BRD BN	Requirement	In-Scope Requirement Clarification
		attribute.

#### 2.6.2.6. DS Logon CSP ID Update

Change the current Department of Defense Self-Service Logon (DS Logon) CSP ID to using Electronic Data Interchange Personal Identifier (EDIPI) only.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	DS Logon CSP ID Update	<b>[FEATURE 650192]</b> SSOe shall change the current DS Logon and CAC CSPID to the new EDIPI only format for all processing and data calls (this includes Virtual Directory Service [VDS] and Third-Party On-Boarding [3POB] calls).
		<b>[FEATURE 650193]</b> SSOe shall check for known credentials for DS Logon and CAC users by calling VDS with EDIPI as the CSPID.
		<b>[FEATURE 650194]</b> SSOe shall call Provisioning 3POB, when VDS does not contain an EDIPI and provide EDIPI as CSPID.

#### 2.6.2.7. SSOe Last Login Tracking

To support the IAM Provisioning services de-provisioning functionality, SSOe will track the user's login times and provide those times to Provisioning. This ensures the Provisioning services is always aware of the users last login time, which will improve the ability of Provisioning to enforce de-provisioning business rules based on period of inactivity.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	SSOe Last Login Tracking	<b>[FEATURE 650196]</b> SSOe shall make available user's last login time (per CSP) to IAM Provisioning service at time of user authentication.
		<b>[FEATURE 650197]</b> SSOe last login time shall match MVI time format: CCYYMMDDHHMMSS.SSSS+ZZZZ.

#### 2.6.2.8. SSOe Changed Data Tracking

This will help identify when a change has occurred in the CSP identity data and provide support for corresponding VA reporting or business logic.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	SSOe Changed Data Tracking	<b>[FEATURE 650199]</b> SSOe shall compare CSP traits to VDS traits based on list of required trait comparisons and configurable at run time.
		<b>[FEATURE 650200]</b> SSOe shall log differences identified when comparing CSP traits to VDS traits.
		<b>[FEATURE 650201]</b> SSOe shall make an update call to Provisioning when differences are identified when comparing authentication traits to VDS traits.

#### 2.6.2.9. SSOe Delegation Tool Support

SSOe will add an attribute to the Portal Strategy Data set to indicate to an application that this person can act as a delegate.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.5: Provide SSO capabilities to enable external users to seamlessly access VA web applications.		
11.5	SSOe Delegation Tool Support	<b>[FEATURE 650203]</b> SSOe shall provide a Boolean attribute identifying if the user is set up for delegation (to be added to the SSOe LOA 2 + Authentication trait set). <b>Note:</b> See the AcS Common Business Rules document for the full trait set.

#### 2.6.2.10. Enabling Widget for Re-Assertion and OAuth Partners

AccessVA currently provides a widget CSP selector for standard junction integration partners. However, AccessVA has not been able to provide this widget to Re-Assertion and OAuth partners. Expanding the capabilities of AccessVA to be able to offer the widget to all integration partners will improve user experience and consistency for AccessVA's partners.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.1: System shall provide a single web-based entry portal for external users to access VA subscribing applications. (including mobile support)		
11.1	Enabling Widget for Re-Assertion and OAuth Partners	<b>[FEATURE 650205]</b> SSOe shall update the AccessVA login widget and SSOe infrastructure to support use from an external partner site.
		<b>[FEATURE 650206]</b> SSOe shall demo the AccessVA login widget from an external non-va.gov domain site in all non-PreProd/Prod

BRD BN	Requirement	In-Scope Requirement Clarification
		environments.
		<b>[FEATURE 650207]</b> SSOe shall update installation and integration guides with corresponding updates to assist partners.

### 2.6.2.11. AccessVA UX/UI Enhancements

AccessVA is a public facing online portal, which acts as the user interface for SSOe. AccessVA allows users to access online VA services by logging in with a VA Sign-In Partner. These requirements aim to improve the user experience (UX) and user interface (UI) for users throughout the logging in process and across the AccessVA Portal, as well as to other pages hosted by AccessVA (e.g., Third-Party Onboarding and eSig).

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN 11.1: System shall provide a single web-based entry portal for external users to access VA subscribing applications. (including mobile support)		
11.1	AccessVA UX/UI Enhancements	<b>[FEATURE 650209]</b> All AccessVA pages shall be updated to match the AcS Style Guide. (Note: This includes all AccessVA hosted pages such as eSig Attestation.)
		<b>[FEATURE 650210]</b> All AccessVA pages shall receive UX/UI improvements identified during user testing and wireframing sessions. (Note: This includes all AccessVA hosted pages such as eSig Attestation.)
		<b>[FEATURE 650211]</b> The AccessVA common HTML style sheets shall be updated as part of the wireframing sessions.
		<b>[FEATURE 650212]</b> All AccessVA pages shall be updated to use the AccessVA common HTML style sheets (to include all pages hosted on Access.VA.Gov [e.g. Authenticated Page, Unauthenticated page, CSP selection pages, all information pages, contact us, eSig attestation, third-party onboarding, success pages, and error pages] and AccessVA pages still on eauth.va.gov [e.g., [REDACTED]
		<b>[FEATURE 650213]</b> AccessVA's front page shall be updated to include logical categorization of applications improving usability.
		<b>[FEATURE 650214]</b> AccessVA shall make use of dynamic tables, lists, and menu toolbars where applicable.

BRD BN	Requirement	In-Scope Requirement Clarification
		<p><b>[FEATURE 644904]</b> The AccessVA Contact Us page text shall be updated to the following:</p> <p>Contact Us Please see the AccessVA Frequently Asked Questions (FAQs) for more information and answers to common questions.</p> <p>Not able to sign into an AccessVA enabled website? Contact the [REDACTED]</p> <p>Hours of operation: 7:00am to 7:00pm (eastern) Monday to Friday.</p> <p>For questions about use of VA websites after you've successfully signed in, please use the contact information provided by that website.</p>
		<p><b>[FEATURE 645447]</b> The AccessVA CSP selection button for "Anonymous Access" will be updated to state "Guest Access" and "Visit with Guest Access."</p>
		<p><b>[FEATURE 645457]</b> The AccessVA Learn More pages shall rename "Anonymous" to "Guest Access."</p>
		<p><b>[FEATURE 645458]</b> The AccessVA Learn More page for "Anonymous Access" shall be updated to replace "Anonymous" with "Guest Access" — "Guest Access can be used for generic situations which do not require personal identification. To access your website without logging in simply select the button for Guest Access." <input type="checkbox"/></p>

### 2.6.2.12. SSOe Audit Logging

These requirements aim to ensure each service conforms to the audit logging requirements.

BRD BN	Requirement	In-Scope Requirement Clarification
23. Audit Trail: Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.		
23.0	SSOe Audit Logging	<p><b>[FEATURE 650216]</b> The SSOe service complies with the auditing requirements specified in the <b>Audit Logging Requirements</b> section.</p>

### 2.6.3. Provisioning

The Provisioning service provides portions of the Federal Identity, Credential, and Access Management (FICAM)-defined Digital Identity and Privilege Management services. The Provisioning 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 Provisioning service is being enhanced to support the IAM integration with the VBA Common Security System (CSS). The Provisioning service will also support the registration of Non-Person Entities. Several enhancements related to the maintenance of Third-Party Credentials are also included. Inactive Third-Party Credentials will be off-boarded after one year of inactivity. The Provisioning service will also capture trait updates from Third-Party Credential Providers. Additionally, privileged users will have the capability to delete a Third-Party Credential from the Provisioning data store.

Additionally, the Provisioning service is being enhanced to accommodate the business requirements of the Identity, Credential, and Access Management (ICAM) Program Management Office (PMO). The ICAM PMO has issued a BRD outlining requirements pertaining to establishing a standardized, integrated, and enterprise-wide VA on-boarding solution. The on-boarding solution leverages existing Provisioning capabilities. The employee and contractor on-boarding/off-boarding requirements presented in this document reflect the first iteration of the solution and supersede previous CRISP on-boarding/off-boarding requirements. Future AcS increments will enhance the on-boarding solution to include additional system interfaces (e.g., eCMS) as well as additional capabilities (e.g., employee transfers, escalation notifications).

### 2.6.3.1. General Enhancements

BRD BN	Requirement	In-Scope Requirement Clarification
3.0 Digital Identity Lifecycle Management On-boarding/Off-boarding: 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	Third Party On-Boarding Enhancements	<p><b>[FEATURE 650219]</b> The Provisioning service shall perform a one-time bulk archival of all DS Logon and CAC CSPs from the Provisioning data store. The bulk deletion shall only archive the CSP ID data leaving the SEC ID and user profile intact. The CSP ID data includes the following:</p> <ul style="list-style-type: none"> <li>• First Name</li> <li>• Last Name</li> <li>• Middle Name (or Initial), if available</li> <li>• SSN</li> <li>• Prefix</li> <li>• Suffix</li> <li>• Address</li> <li>• Date of Birth</li> <li>• Email</li> <li>• Gender</li> <li>• EDIPI</li> <li>• CSP ID</li> <li>• LOA</li> </ul> <p>Self Asserted Flags are associated with the above list.</p> <p>The bulk archival shall occur after the VAAFI changes to the Third-Party Credential On-Boarding process have been deployed.</p>
3.0	IAM CSS Integration	<p><b>[FEATURE 650220]</b> The Provisioning service shall add a Sensitivity Level attribute to the User Profile. The Sensitivity Level attribute is a single digit with valid values of 0 through 9. The CSS IAM iRSD will elaborate the usage of this attribute in detail.</p>
3.0	Audit Logging	<p><b>[FEATURE 650221]</b> The Provisioning service shall generate an audit log that conforms to the AcS Auditing Logging Requirements and includes the following events:</p> <ul style="list-style-type: none"> <li>• User Profile Created</li> <li>• User Profile Updated</li> <li>• User Profile Disabled</li> <li>• User Profile Deleted</li> </ul>

BRD BN	Requirement	In-Scope Requirement Clarification
		<ul style="list-style-type: none"> <li>• CSP ID Created</li> <li>• CSP ID Update</li> <li>• CSP ID Deleted</li> <li>• CSP ID Moved</li> <li>• PIV record created</li> <li>• PIV record updated</li> <li>• AD Account created</li> <li>• AD Account updated</li> <li>• AD Account disabled</li> <li>• AD Account deleted</li> <li>• Integrated System Account Provisioned</li> <li>• Integrated System Account Modified</li> <li>• Integrated System Account De-provisioned</li> </ul>

### 2.6.3.2. SSOe User Attribute for AMS in VDS

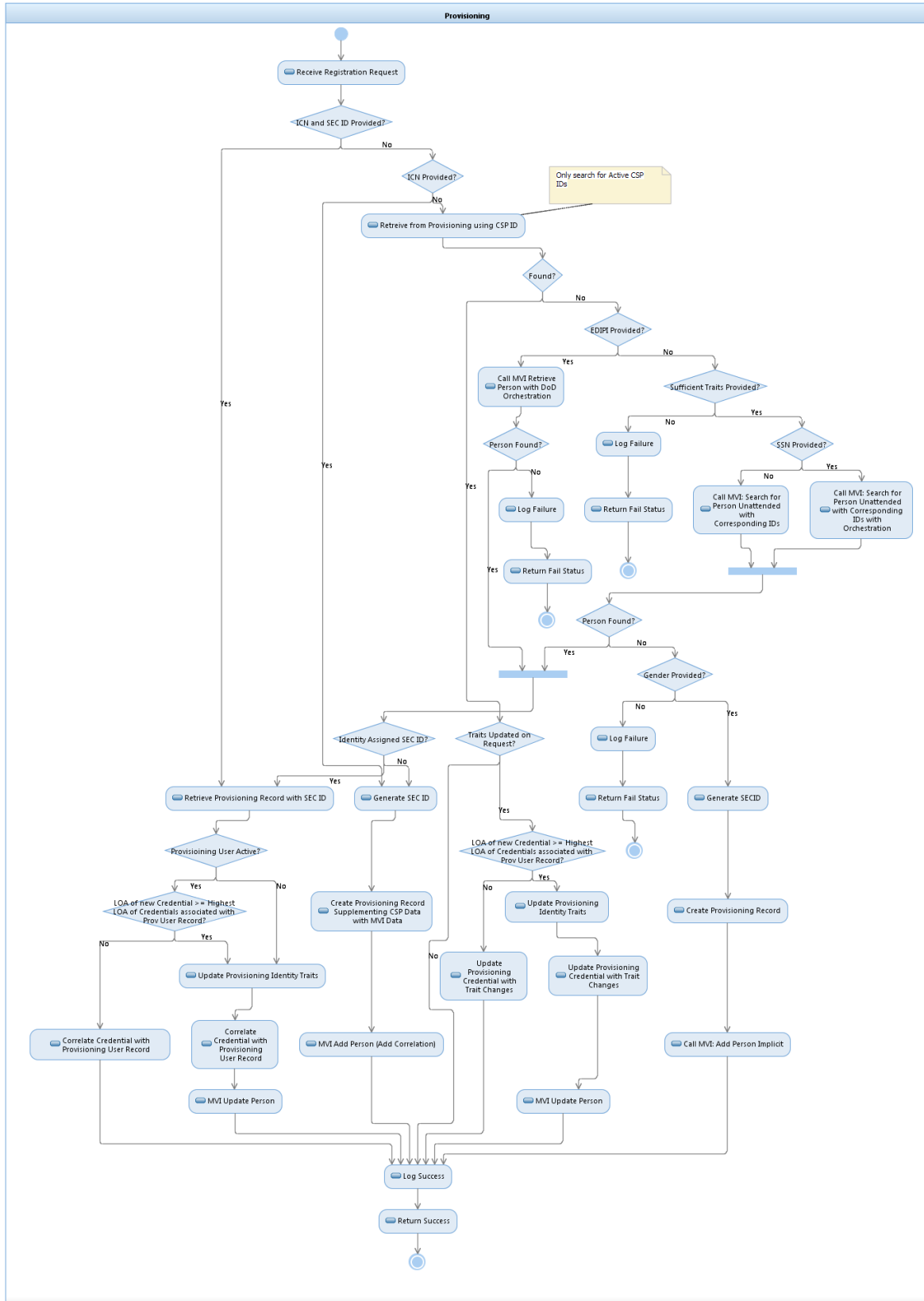
BRD BN	Requirement	In-Scope Requirement Clarification
<p>BRD 14. Backend Attribute Retrieval: Provide a capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access-based decision.</p> <p>14.61 The SAC Service shall provide the ability for a SAC System Administrator to manage the delegation/surrogacy process concerning access to clients' records.</p> <p>14.63 The SAC Service shall support the surrogacy process to allow clients to authorize others to act in their name and/or access their records.</p>		
14	VDS shall retrieve the "Is a Delegate" attribute	<b>[FEATURE 650223]</b> VDS shall provide a Boolean attribute identifying if the user is set up for delegation.

### 2.6.3.3. Off-Boarding Third-Party Credential

BRD BN	Requirement	In-Scope Requirement Clarification
3.0 Digital Identity Lifecycle Management On-boarding/Off-boarding: 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	3POB Off-Boarding	<b>[FEATURE 650225]</b> The IAM Provisioning service shall capture and store the date/time stamp provided by SSOe every time a user authenticates to an SSOe enabled application.
3.0	3POB Off-Boarding	<b>[FEATURE 650226]</b> The IAM Provisioning service shall archive a CSP ID after one year of inactivity. The IAM Provisioning service shall archive the data associated with the CSP ID, which includes the following: <ul style="list-style-type: none"><li>• First Name</li><li>• Last Name</li><li>• Middle Name (or Initial), if available</li><li>• SSN</li><li>• Prefix</li><li>• Suffix</li><li>• Address</li><li>• Date of Birth</li><li>• Email</li><li>• Gender</li><li>• EDIPI</li><li>• CSP ID</li><li>• LOA</li></ul> Self Asserted Flags are associated with the above list.
3.0	3POB Off-Boarding	<b>[FEATURE 650227]</b> The IAM Provisioning service shall not disable a CSP ID related to a PIV card based upon the user's activity.
3.0	3POB Off-Boarding	<b>[FEATURE 650228]</b> If the user profile associated with the archived third-party credential is not associated with any other active credentials or an active internal user profile, the IAM Provisioning service shall disable associated user profile.

### 2.6.3.4. Trait Updates for Third-Party Credentials

The Third-Party Credential On-Boarding flow diagram is shown below.

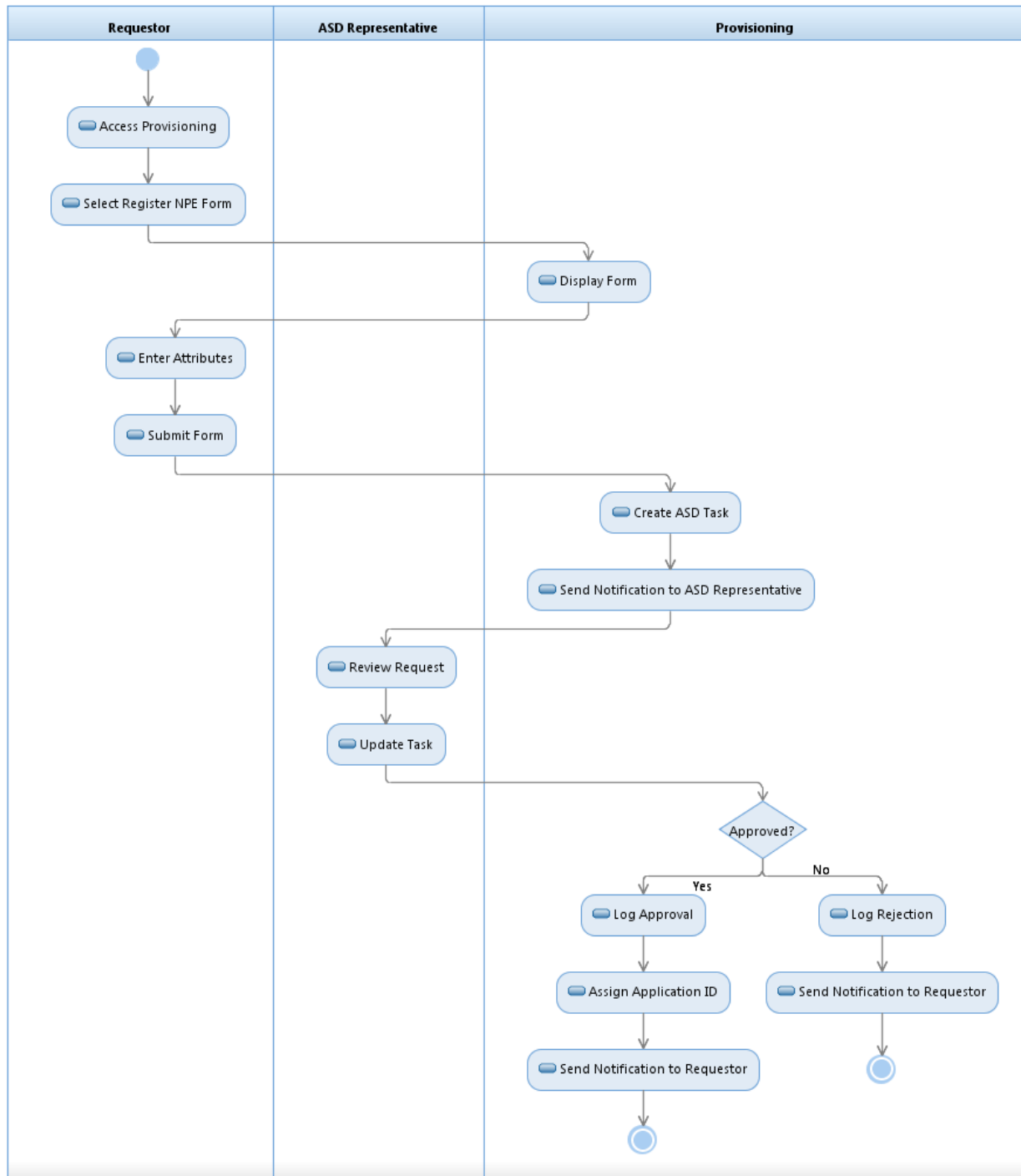


**Figure 2: Third-Party Credential On-Boarding**

BRD BN	Requirement	In-Scope Requirement Clarification
3.0 Digital Identity Lifecycle Management On-boarding/Off-boarding: 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	Trait Updates	<b>[FEATURE 650230]</b> Upon receipt of a Third-Party Credential Registration Request from VAAFI, the Provisioning service shall only search for CSP IDs among the active CSP IDs present in the Provisioning user store.
3.0	Trait Updates	<b>[FEATURE 650231]</b> When the retrieve using the CSP ID locates an active CSP ID, the Provisioning service shall evaluate the following traits from the registration request to determine if they have changed: <ul style="list-style-type: none"> <li>• First Name</li> <li>• Last Name</li> <li>• Middle Name (or Initial), if available</li> <li>• SSN</li> <li>• Prefix</li> <li>• Suffix</li> <li>• Address</li> <li>• Date of Birth</li> <li>• Email</li> <li>• Gender</li> </ul>
3.0	Trait Updates	<b>[FEATURE 650232]</b> If the identity traits have been updated, the Provisioning service shall update the identity traits associated with the credential in the Provisioning user store.
3.0	Trait Updates	<b>[FEATURE 650233]</b> The Provisioning service shall retrieve all active credentials associated from the user profile and choose the credential having this highest LOA that was on-boarded at the earliest point in time. If the identity traits on the third-party credential registration request differ from the identity traits of the retrieved credential, the Provisioning service shall update the identity traits on the Provisioning User Profile record and call MVI Update Person.

### 2.6.3.5. NPE

The Provisioning Non-Person Entities (NPE) flow diagram is shown below.



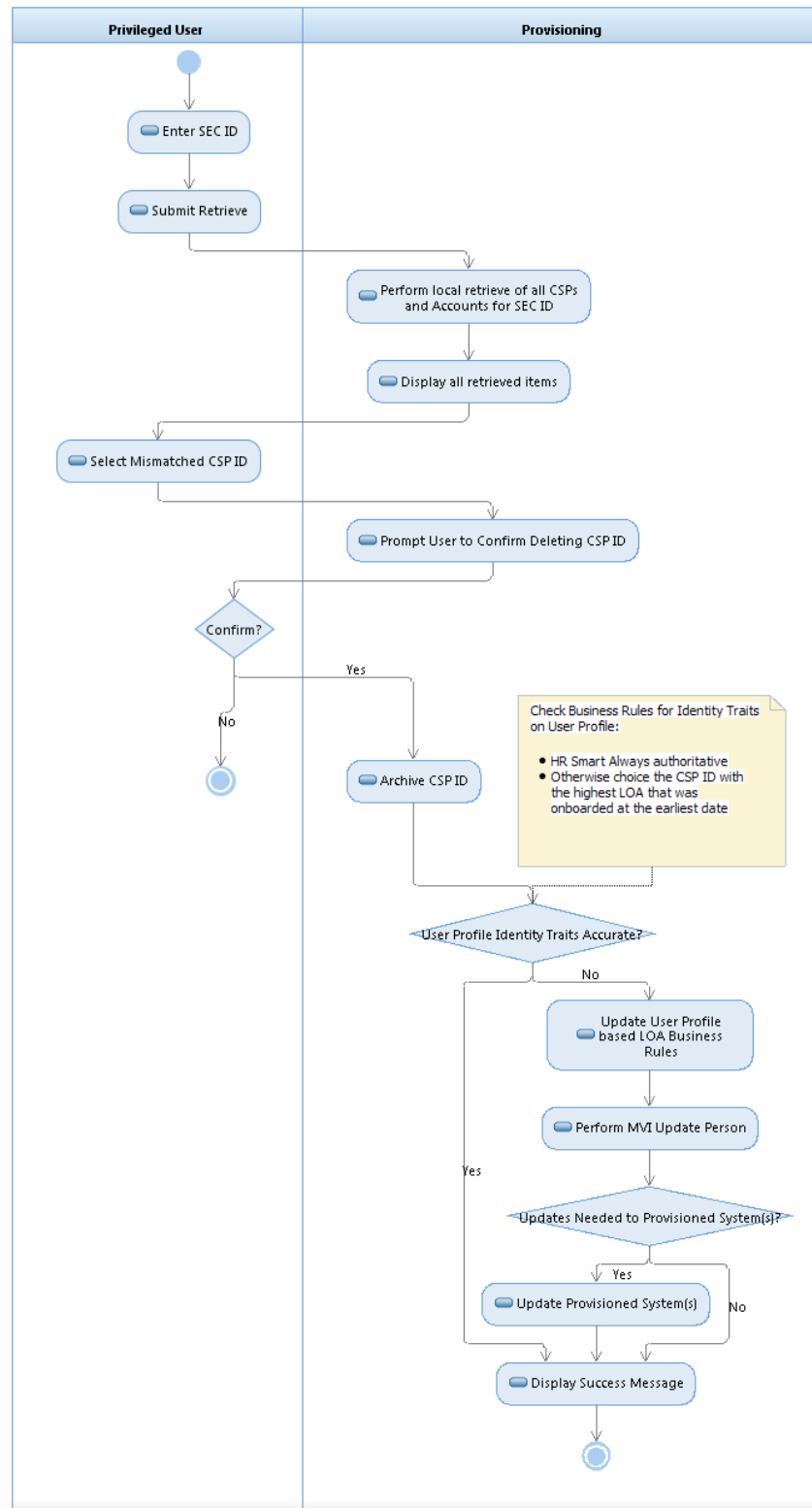
**Figure 3: Provisioning NPE**

BRD BN	Requirement	In-Scope Requirement Clarification
3.0 Digital Identity Lifecycle Management On-boarding/Off-boarding: 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	Non-Person Entities	<b>[FEATURE 650235]</b> The Provisioning service shall provide a user interface allowing a requester to submit a request to register a system as a Non-Person Entity.
3.0	Non-Person Entities	<b>[FEATURE 650236]</b> The Provisioning service shall require the user to enter the following data on the registration request: <ul style="list-style-type: none"> <li>• Application/Business Process Name</li> <li>• Application/Business Process Organization</li> <li>• Application/Business Process Email Address</li> <li>• Application Certification DN (optional)</li> <li>• STS Type</li> </ul>
3.0	Non-Person Entities	<b>[FEATURE 650237]</b> The Provisioning service shall capture the following data associate the data with the registration request: <ul style="list-style-type: none"> <li>• Requester Name</li> <li>• Requester SEC ID</li> <li>• Requester VA Email Address</li> <li>• Organization ID</li> </ul>
3.0	Non Person Entities	<b>[FEATURE 650238]</b> The Provisioning service shall reject requests for duplicated Applicate/Business Process Names.
3.0	Non-Person Entities	<b>[FEATURE 650239]</b> Once the requester submits the registration request, the Provisioning service shall route the request to an ASD Representative for review.
3.0	Non-Person Entities	<b>[FEATURE 650240]</b> The Provisioning service shall send the following email notification to the ASD Representative once the request has been routed for review: Subject: Provisioning Service – New Request in Queue Body: A new provisioning request has been submitted. Please review the request and provide a response at your earliest convenience by accessing the link below and logging into the Provisioning service. <a href="#">Link</a>
3.0	Non-Person	<b>[FEATURE 650241]</b> If the ASD Representative rejects the request, the Provisioning service shall log the rejection and send the following email

BRD BN	Requirement	In-Scope Requirement Clarification
	Entities	<p>notification to the requester:  Subject: Provisioning Service – Request Rejected  Body: (&lt;Application/Business Process Name&gt;) registration request has been rejected.</p> <p>You can review the details of your request by accessing the link below and logging into the Provisioning service.</p> <p><u><a href="#">Link</a></u></p> <p>If you need assistance, or have any questions, please contact the helpdesk at (<u><a href="#">helpdesk email</a></u>).</p>
3.0	Non-Person Entities	<p><b>[FEATURE 650242]</b> If the ASD Representative approves the request, the Provisioning service shall assign a unique 10 digit application identifier to the registration request and create a record for the NPE in the NPE metadata repository. The Provisioning service shall store the following data in the NPE metadata repository:</p> <ul style="list-style-type: none"> <li>• Application/Business Process Name</li> <li>• Application/Business Process Organization</li> <li>• Application/Business Process Email Address</li> <li>• Application Certification DN (optional)</li> <li>• STS Type</li> <li>• Application/Business Process Organization ID</li> <li>• Home Community ID</li> <li>• Application ID</li> <li>• Requester SEC ID</li> <li>• Approver SEC ID</li> <li>• Date Approved</li> </ul>
3.0	Non-Person Entities	<p><b>[FEATURE 650243]</b> If the ASD Representative approves the request, the Provisioning service shall log the approval and send the following email notification to the requester:  Subject: Provisioning Service – Registration Approved  Body: (&lt;Application/Business Process Name&gt;) registration has been approved. The application has been assigned the following Application ID: &lt;Application ID&gt;</p> <p>Please review the details of your registration request by accessing the link below and logging into the Provisioning service.</p> <p><u><a href="#">Link</a></u></p> <p>If you need assistance, or have any questions, please contact the helpdesk at (<u><a href="#">helpdesk email</a></u>).</p>

#### **2.6.3.6. Delete CSP**

The Delete CSP flow diagram is shown below.



**Figure 4: Delete CSP**

BRD BN	Requirement	In-Scope Requirement Clarification
3.0 Digital Identity Lifecycle Management On-boarding/Off-boarding: 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	Delete CSP	<b>[FEATURE 650245]</b> The Provisioning service shall provide a user interface allowing a privileged user to initiate the Delete CSP function by retrieving by a SEC ID.
3.0	Delete CSP	<b>[FEATURE 650246]</b> The Provisioning service shall perform a local retrieve to obtain all items (CSP IDs and accounts) associated with the input SEC ID.
3.0	Delete CSP	<b>[FEATURE 650247]</b> The Provisioning service shall display all items (CSP IDs and accounts) retrieved and the following data elements: <ul style="list-style-type: none"> <li>• Identifier (CSP ID, or Account ID)</li> <li>• Account Name (e.g., JLV, VHIC)</li> <li>• First Name</li> <li>• Middle</li> <li>• Last Name</li> <li>• SSN</li> <li>• DoB</li> <li>• Gender</li> </ul>
3.0	Delete CSP	<b>[FEATURE 650248]</b> For CSP IDs, the Provisioning service shall display an indicator that identifies if the value of the data was provided by the CSP or self-asserted by the user.
3.0	Delete CSP	<b>[FEATURE 650249]</b> The Provisioning service shall allow the user to select a CSP ID to delete.
3.0	Delete CSP	<b>[FEATURE 650250]</b> The Provisioning service shall present a notification to the user to confirm that the selected CSP ID should be deleted.
3.0	Delete CSP	<b>[FEATURE 650251]</b> Once the user confirms the deletion, the Provisioning service shall archive the CSP and the associated data.
3.0	Delete CSP	<b>[FEATURE 650252]</b> If the user confirms that the CSP ID should be deleted, the Provisioning service shall select the remaining credential having the highest LOA.
3.0	Delete CSP	<b>[FEATURE 650253]</b> In the event that there are no other credentials associated with the user profile, the Provisioning service shall display a success message to the user.
3.0	Delete CSP	<b>[FEATURE 650254]</b> In the event that multiple credentials have the highest LOA, the Provisioning service shall select from that subset, the credential that was on-boarded at the earliest point in time.

BRD BN	Requirement	In-Scope Requirement Clarification
3.0	Delete CSP	<b>[FEATURE 650255]</b> If the identity traits associated with the selected credential differ from the identity traits of the user profile, the Provisioning service shall update the identity traits on the user profile.
3.0	Delete CSP	<b>[FEATURE 650256]</b> If the identity traits associated with the selected credential differ from the identity traits of the user profile, the Provisioning service shall update the person's identity in MVI.
3.0	Delete CSP	<b>[FEATURE 650257]</b> If the user profile has been provisioned to any internal VA systems (e.g., JLV), the Provisioning service shall update the Provisioned systems as necessary. ( <b>Note:</b> This function is addressed in the ongoing reconciliation requirements for the integrated systems).
3.0	Delete CSP	<b>[FEATURE 650258]</b> The Provisioning service shall display a success message to the user.

### 2.6.3.7. Provisioning UX/UI Enhancements

These requirements aim to improve the user experience (UX) and user interface (UI) for users throughout the logging in process and across Provisioning.

BRD BN	Requirement	In-Scope Requirement Clarification
BRD 20. Provisioning: Provide an automated capability of creating user access accounts and assigning privileges or entitlements within the scope of a defined process.		
	Provisioning UX/UI Enhancements	<b>[FEATURE 650363]</b> Provisioning shall receive UX/UI improvements identified during user testing and wireframing sessions.

## 2.6.4. Authorization Management Service (Delegation)

The IAM Authorization Management Service (AMS) is a generalized service to manage authorizations of all types. The initial business driver has been person-to-person delegation for access to VA self-service healthcare applications. As a result, the term “Delegation” is widely used. The term “Delegation” is used in this RSD to refer to user interfaces and workflows related to delegation. The core services are referred to as “IAM AMS.”

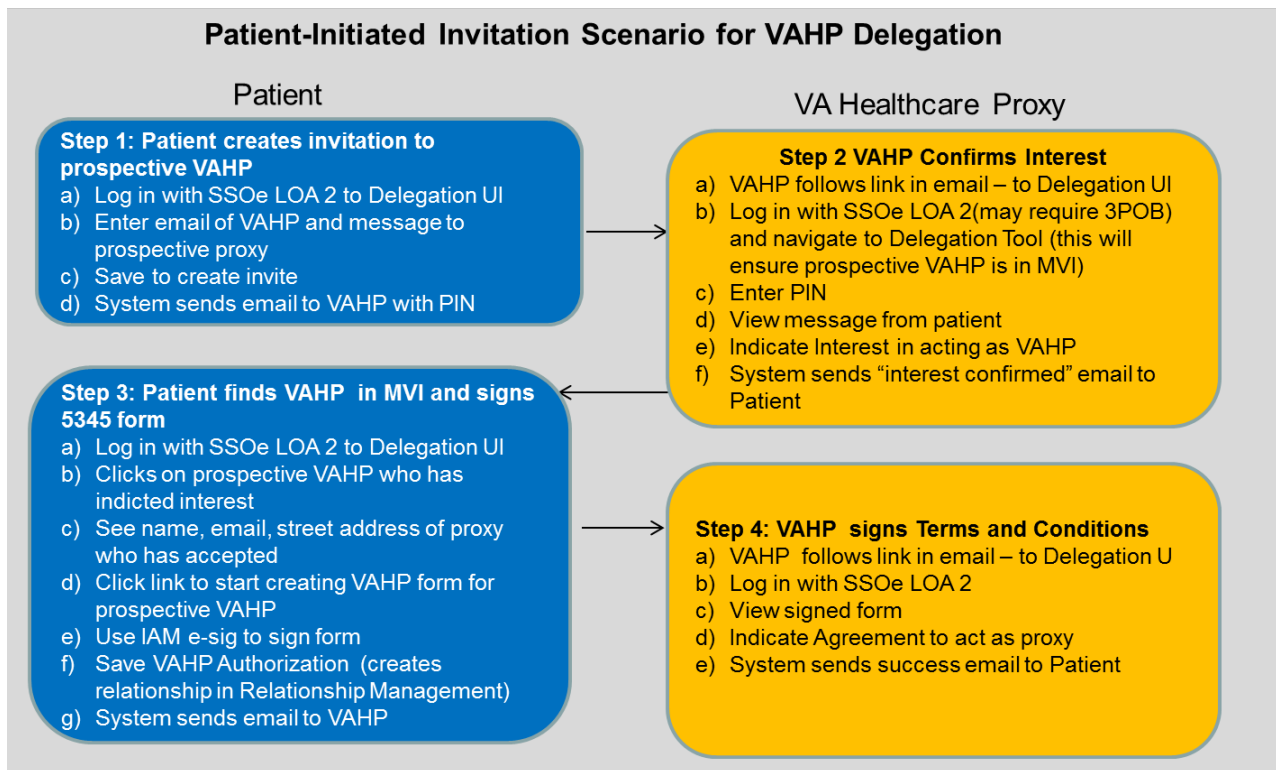
### 2.6.4.1. Invitation to Act as Delegate Flow

The invitation flow starts with the creation of an invitation to a prospective Delegate. The invitation flow increases usability of the self-service delegation user interface in several ways:

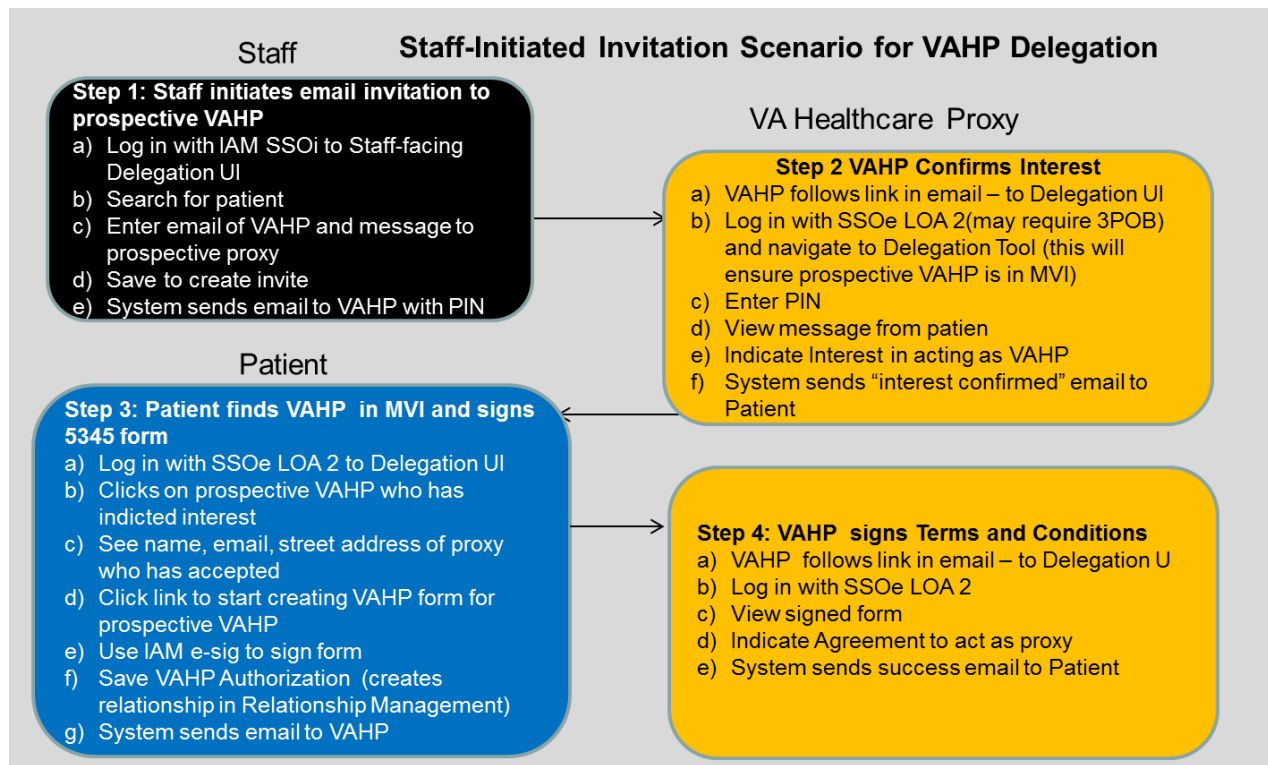
- The Veteran or Staff member can get the flow started by providing an email address, rather than needing to enter all the traits required for a successful MVI unattended search for the prospective delegate.

- The prospective delegate does not need to be known to MVI at the start of the process; following the link in the email will lead to the prospective delegate to get a CSP account, get that account on-boarded with VA, and be entered into MVI.
- Once the prospective delegate confirms interest in acting as a delegate, the veteran can initiate the process of creating the authorization based on the confirmed invitation, bypassing the need for a search.
- The remainder of the process is identical to the existing flow: the veteran completes and signs the authorization form, and then the delegate reviews and accepts.

The patient-initiated and staff-initiated invitation scenarios for VA Healthcare Proxy (VAHP) delegation are depicted in the following diagrams.



**Figure 5: Patient-Initiated Invitation Scenario for VAHP Delegation**



**Figure 6: Staff-Initiated Invitation Scenario for VAHP Delegation**

BRD BN	Requirement	In-Scope Requirement Clarification
<p>BRD 14. Backend Attribute Retrieval: Provide a capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access-based decision.</p> <p>14.61 The SAC Service shall provide the ability for a SAC System Administrator to manage the delegation/surrogacy process concerning access to clients' records.</p> <p>14.63 The SAC Service shall support the surrogacy process to allow clients to authorize others to act in their name and/or access their records.</p>		
14	Support invitation flow with an email sent to a prospective delegate prompting that person to log in to the self-service user interface to confirm interest in acting as a delegate.	<b>[FEATURE 650366]</b> The IAM Delegation System shall have the capability of an invitation flow to allow self-service user to generate an invitation to a person to act as their Delegate.
		<b>[FEATURE 650367]</b> The IAM Delegation System shall have the capability of an invitation flow to allow a staff user who has selected a Veteran to generate an invitation to a person to act as the Veteran's Delegate.
		<b>[FEATURE 650368]</b> The IAM Delegation System invitation flow shall create invitation that the prospective

BRD BN	Requirement	In-Scope Requirement Clarification
		delegate can view in the self-service user interface.
		<b>[FEATURE 650369]</b> The IAM Delegation System invitation flow shall accept input from the self-service user of an email address of the prospective delegate and a note field created by the self-service Veteran user for display in the invitation to the prospective Delegate.
		<b>[FEATURE 650370]</b> The IAM Delegation System invitation flow shall accept input from the staff user of an email address and note field related to the Veteran for display in the invitation to the prospective Delegate.
		<b>[FEATURE 650371]</b> The IAM Delegation System invitation flow shall create a 4 digit Personal Identification Number (PIN) associated with a specific invitation that the self-service user must enter in order to view the invitation.
		<b>[FEATURE 650372]</b> The IAM Delegation System invitation flow shall send the 4-digit PIN associated with a specific invitation to the prospective delegate in e-mail.
		<b>[FEATURE 650373]</b> The IAM Delegation System invitation flow shall associate the invitation with the self-service user's SecID after the self-service user logs in to the Delegation self-service portal and correctly enters the 4-digit PIN.
		<b>[FEATURE 650374]</b> The IAM Delegation flow shall display the Veteran's email and note to prospective delegate after the self-service user correctly enters the 4 digit PIN
		<b>[FEATURE 650375]</b> The IAM Delegation System invitation flow shall support input of "Not Interested" from the prospective delegate through the self-service user interface. In response to the input of "Not Interested," the Delegation System shall trigger an email to the Veteran.
		<b>[FEATURE 650376]</b> The IAM Delegation System invitation flow shall support input of "Confirming Interest" from the prospective delegate through the self-service user interface. In response to the input of "Confirming," the Delegation System shall trigger an email to the Veteran.

BRD BN	Requirement	In-Scope Requirement Clarification
		<b>[FEATURE 650377]</b> The IAM Delegation System invitation flow shall support display of the prospective delegate's response to invitation to the Veteran in the self-service user interface.
		<b>[FEATURE 650378]</b> The IAM Delegation System invitation flow shall support display of the prospective delegate's response to invitation to a staff user who has selected a Veteran in the staff user interface.
		<b>[FEATURE 650379]</b> The IAM Delegation System invitation flow shall support use of the self-service interface to initiate an individual authorization for a prospective delegate who has confirmed interest.
		<b>[FEATURE 650380]</b> The IAM Delegation System invitation flow shall support use of the staff interface to initiate an individual authorization for a prospective delegate who has confirmed interest.
		<b>[FEATURE 650381]</b> The IAM Delegation System shall support the existing flow to fill out, sign and complete an authorization after initiation based on user selection of a prospective delegate who has confirmed interest in acting as a Delegate for the Veteran.
		<b>[FEATURE 650382]</b> The IAM Delegation System shall support the existing flow to fill out, sign and complete an authorization after initiation based on user selection of a person who has an existing relationship with the Veteran.

#### 2.6.4.2. IAM AMS Web Service

BRD BN	Requirement	In-Scope Requirement Clarification
<p>BRD 14. Backend Attribute Retrieval: Provide a capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access-based decision.</p> <p>14.61 The SAC Service shall provide the ability for a SAC System Administrator to manage the delegation/surrogacy process concerning access to clients' records.</p> <p>14.63 The SAC Service shall support the surrogacy process to allow clients to authorize others to act in their name and/or access their records.</p>		
14	Update the Delegation web service to accept requests for delegations by type.	<b>[FEATURE 650384]</b> The AMS web service shall have the capability to provide a list of authorizations of a specified type or types for a person based on the submission of the following:

BRD BN	Requirement	In-Scope Requirement Clarification
		<ul style="list-style-type: none"> <li>• A SecID or ICN to identify the user</li> <li>• One or more authorization types to specify the type(s) of authorizations to be returned</li> <li>• Specification of whether to return active or all authorizations</li> </ul>
		<p><b>[FEATURE 650385]</b> The AMS web service shall have the capability to provide a list of active delegation relationships for a person based on the submission of the following:</p> <ul style="list-style-type: none"> <li>• A SecID or ICN to identify the user</li> <li>• One or more authorization types to specify the type(s) of authorizations to be returned</li> </ul>

#### 2.6.4.3. IAM AMS Integration with Relationship Management

This section is to be refined based on integration requirements with MVI Relationship Management. The “Relationships” categorization includes family and other relationships stored in MVI Relationship Management. Relationship Management will also store Delegation Relationships—those relationships that are created and managed by IAM AMS.

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: A partner application wants to implement a delegation flow with IAM.		
BRD 14. Backend Attribute Retrieval: Provide a capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access-based decision.		
14.61 The SAC Service shall provide the ability for a SAC System Administrator to manage the delegation/surrogacy process concerning access to clients’ records.		
14.63 The SAC Service shall support the surrogacy process to allow clients to authorize others to act in their name and/or access their records.		
14	Integrate with MVI Relationship Management to retrieve a person’s relationships and create, update or inactivate delegation relationships	<b>[FEATURE 650387]</b> The IAM AMS shall provide the capability to retrieve all of a person’s relationships from the Relationship Management Service.
		<b>[FEATURE 650388]</b> The IAM AMS shall provide the capability to retrieve a person’s active relationships from Relationship Management Service.
		<b>[FEATURE 650389]</b> The IAM AMS shall provide the capability to display a person’s active non-delegation relationships in the self-service user interface.
		<b>[FEATURE 650390]</b> The IAM AMS shall provide the capability to display a person’s active non-delegation

BRD BN	Requirement	In-Scope Requirement Clarification
		relationships in the staff-facing user interface.
		<b>[FEATURE 650391]</b> The IAM AMS shall provide the capability to create Delegation Relationships in the Relationship Management Service.
		<b>[FEATURE 650392]</b> The IAM AMS shall provide the capability to update Delegation Relationships in Relationship Management. Updates shall include the following: <ul style="list-style-type: none"> <li>• Setting Inactive Date to a new value</li> <li>• Setting Inactive Date to null</li> </ul>

#### 2.6.4.4. IAM Delegation Self-Service User Interface

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: A partner application wants to implement a delegation flow with IAM.		
BRD 14. Backend Attribute Retrieval: Provide a capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access-based decision.		
14.61 The SAC Service shall provide the ability for a SAC System Administrator to manage the delegation/surrogacy process concerning access to clients' records.		
14.63 The SAC Service shall support the surrogacy process to allow clients to authorize others to act in their name and/or access their records.		
14	Enhancements to the self-service user interface.	<b>[FEATURE 650394]</b> The IAM Delegation System shall provide a self-service user interface to support the invitation flow.
		<b>[FEATURE 650395]</b> The IAM self-service user interface shall support removal of the existing trait search functionality to identify a person in MVI to act as delegate.
		<b>[FEATURE 650396]</b> Delegation self-service pages shall be updated to match the AcS style guide.
		<b>[FEATURE 650397]</b> Delegation self-service pages shall receive UX/UI improvements identified during user testing and wireframing sessions.
		<b>[FEATURE 650398]</b> The Delegation self-service interface shall provide a web-based Help system. Links on every page will lead to a Help system that will have instructions on how to perform the following: <ul style="list-style-type: none"> <li>• Manage the list of delegations</li> <li>• View existing delegations</li> <li>• Create an Authorization</li> <li>• Revoke an authorization</li> <li>• Accept an Authorization</li> <li>• Decline an Authorization</li> <li>• Invite another person to act as a Delegate</li> <li>• Confirm interest in acting as a Delegate</li> <li>• Indicate "Not Interested" In acting as a Delegate</li> </ul>

The following flow diagram shows how the Personal Representative creates a VA Healthcare Proxy for a Delegator.



BRD BN	Requirement	In-Scope Requirement Clarification
User Story: A partner application wants to implement a delegation flow with IAM.		
BRD 14. Backend Attribute Retrieval: Provide a capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access-based decision.		
14.61 The SAC Service shall provide the ability for a SAC System Administrator to manage the delegation/surrogacy process concerning access to clients' records.		
14.63 The SAC Service shall support the surrogacy process to allow clients to authorize others to act in their name and/or access their records.		
14	Support of a Personal Representative using the self-service user interface on behalf of the person for whom the user is a Personal Representative.	<b>[FEATURE 650399]</b> The IAM Delegation System self-service user interface shall check IAM Delegation to see if the user has an active Personal Representative delegation.
		<b>[FEATURE 650400]</b> The IAM Delegation System self-service user interface shall display a link to allow a user who has an active Personal Representative delegation to navigate to see the Delegation data of the Veteran for whom the user is a Personal Representative.
		<b>[FEATURE 650401]</b> The IAM Delegation System shall perform an authorization check against the SAC Policy Decision Point (PDP) at the time the user navigates to see Delegation data of the Veteran for whom the user is a Personal Representative.
		<b>[FEATURE 650402]</b> The IAM Delegation System self-service user interface shall provide a user who has an active Personal Representative delegation navigation capabilities to allow the user to view Delegation data the Veteran for whom the user is a Personal Representative: <ul style="list-style-type: none"> <li>• Navigation to view the data of the person for whom the user is a Personal Representative</li> <li>• A consistent visual indication that the user is viewing another person's date</li> <li>• Navigation out of the data of the Veteran for whom the user is a Personal Representative back to a view of the user's own data</li> </ul>
		<b>[FEATURE 650403]</b> The IAM Delegation System self-service user interface shall provide a user who has an active Personal Representative delegation the same view and update capabilities for the Delegation data of the Veteran for whom the user is a Personal Representative that the

BRD BN	Requirement	In-Scope Requirement Clarification
		Veteran themselves would have.
		<b>[FEATURE 650404]</b> The IAM Delegation System self-service user interface shall allow a user who has an active Personal Representative delegation to initiate a VA Healthcare Proxy authorization for the Veteran for whom the user is a Personal Representative.
		<b>[FEATURE 650405]</b> The IAM Delegation System self-service user interface shall allow a user who has an active Personal Representative delegation to view and update an in-progress VA Healthcare Proxy authorization for the Veteran for whom the user is a Personal Representative.
		<b>[FEATURE 650406]</b> The IAM Delegation System self-service user interface shall allow a user who has an active Personal Representative delegation to electronically sign an in-progress VA Healthcare Proxy authorization for the Veteran for whom the user is a Personal Representative.
		<b>[FEATURE 650407]</b> The IAM Delegation System self-service user interface shall allow a user who has an active Personal Representative delegation to initiate a revocation of an existing VA Healthcare Proxy authorization for the Veteran for whom the user is a Personal Representative.
		<b>[FEATURE 650408]</b> The IAM Delegation System self-service user interface shall allow a user who has an active Personal Representative delegation to view and update an in-progress VA Healthcare Proxy revocation for the Veteran for whom the user is a Personal Representative.
		<b>[FEATURE 650409]</b> The IAM Delegation System self-service user interface shall allow a user who has an active Personal Representative delegation to electronically sign an in-progress VA Healthcare Proxy revocation for the Veteran for whom the user is a Personal Representative.
		<b>[FEATURE 650410]</b> The IAM Delegation System self-service user interface shall allow a user who has an active Personal Representative delegation to generate an invitation for a person to act as the Delegate for the Veteran for whom the user is a Personal Representative.

#### 2.6.4.5. IAM Delegation Staff-Facing User Interface

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: A partner application wants to implement a delegation flow with IAM.		
BRD 14. Backend Attribute Retrieval: Provide a capability that acquires additional information not found in the authenticated credential that is required by a relying party to make an access-based decision.		
14.61 The SAC Service shall provide the ability for a SAC System Administrator to manage the delegation/surrogacy process concerning access to clients' records.		
14.63 The SAC Service shall support the surrogacy process to allow clients to authorize others to act in their name and/or access their records.		
14	Enhancements to the staff-facing user interface.	<b>[FEATURE 650412]</b> The IAM Delegation System shall provide a user interface to allow the staff user who has selected a Veteran to execute the invitation to act as delegate flow.
		<b>[FEATURE 650413]</b> The IAM Delegation System shall provide a user interface to allow the staff user who has selected a Veteran to record a paper VA Healthcare Proxy authorization for the Veteran.
		<b>[FEATURE 650414]</b> The IAM Delegation System shall provide a user interface to allow the staff user who has selected a Veteran to record a paper VA Healthcare Proxy revocation for the Veteran.
		<b>[FEATURE 650415]</b> Delegation staff-facing pages shall be updated to match the AcS Style Guide.
		<b>[FEATURE 650416]</b> Delegation staff-facing pages shall receive UX/UI improvements identified during user testing and wireframing sessions.
		<b>[FEATURE 650417]</b> The Delegation staff interface shall provide a web-based Help system. Links on every page will lead to a Help system that will have instructions on how to perform the following: <ul style="list-style-type: none"> <li>• Search for Veterans</li> <li>• Manage a Veteran's list of delegations</li> <li>• View existing delegations for a Veteran</li> <li>• Record authorizations for a Veteran</li> <li>• Record revocations for a Veteran</li> <li>• Invite a person to act as a delegate for a Veteran</li> </ul>

BRD BN	Requirement	In-Scope Requirement Clarification
		<b>[FEATURE 650418]</b> The Delegation staff interface shall prevent a staff user from using the staff interface to access their own Delegation data.
		<b>[FEATURE 650419]</b> The Delegation staff interface shall prevent a staff user from using the staff interface to create or edit any authorization that grants themselves access to another person's data.

#### 2.6.4.6. AMS Audit Logging

These requirements aim to ensure each service conforms to the audit logging requirements.

BRD BN	Requirement	In-Scope Requirement Clarification
23. Audit Trail: Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.		
23.0	AMS Audit Logging	<b>[FEATURE 650421]</b> The AMS service complies with the auditing requirements specified in the <b>Audit Logging Requirements</b> section.

### 2.6.5. IP

#### 2.6.5.1. Decoupling VA IP and VA VHIC

BRD BN	Requirement	In-Scope Requirement Clarification
BN1. Identity Proofing (IDP): 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; initiates chain of trust in establishing a digital identity and binding it to an individual.		
1.0	Decoupling VA IP and VA VHIC	<b>[FEATURE 650424]</b> The VA IP system and the VA VHIC system shall be decoupled.
		<b>[FEATURE 650425]</b> The current VA IP system records shall be migrated to MVI TK to keep proofing records intact.

## 2.6.6. CSP

### 2.6.6.1. VA CSP UX/UI Enhancements

These requirements aim to improve the user experience (UX) and user interface (UI) for users throughout the logging in process and across VA CSP.

BRD BN	Requirement	In-Scope Requirement Clarification
BN 9. Credentialing Lifecycle Management: Provide a digital process of maintaining a credential and associated support over the full credential life cycle.		
9.0	VA CSP UX/UI Enhancements	<b>[FEATURE 650428]</b> All VA CSP UIs shall be updated to match the AcS Style Guide.
		<b>[FEATURE 650429]</b> VA CSP shall receive UX/UI improvements identified during user testing and wireframing sessions.

### 2.6.6.2. CSP Audit Logging

These requirements aim to ensure each service conforms to the audit logging requirements.

BRD BN	Requirement	In-Scope Requirement Clarification
23. Audit Trail: Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.		
23.0	CSP Audit Logging	<b>[FEATURE 650431]</b> The CSP service complies with the auditing requirements specified in the <b>Audit Logging Requirements</b> section.

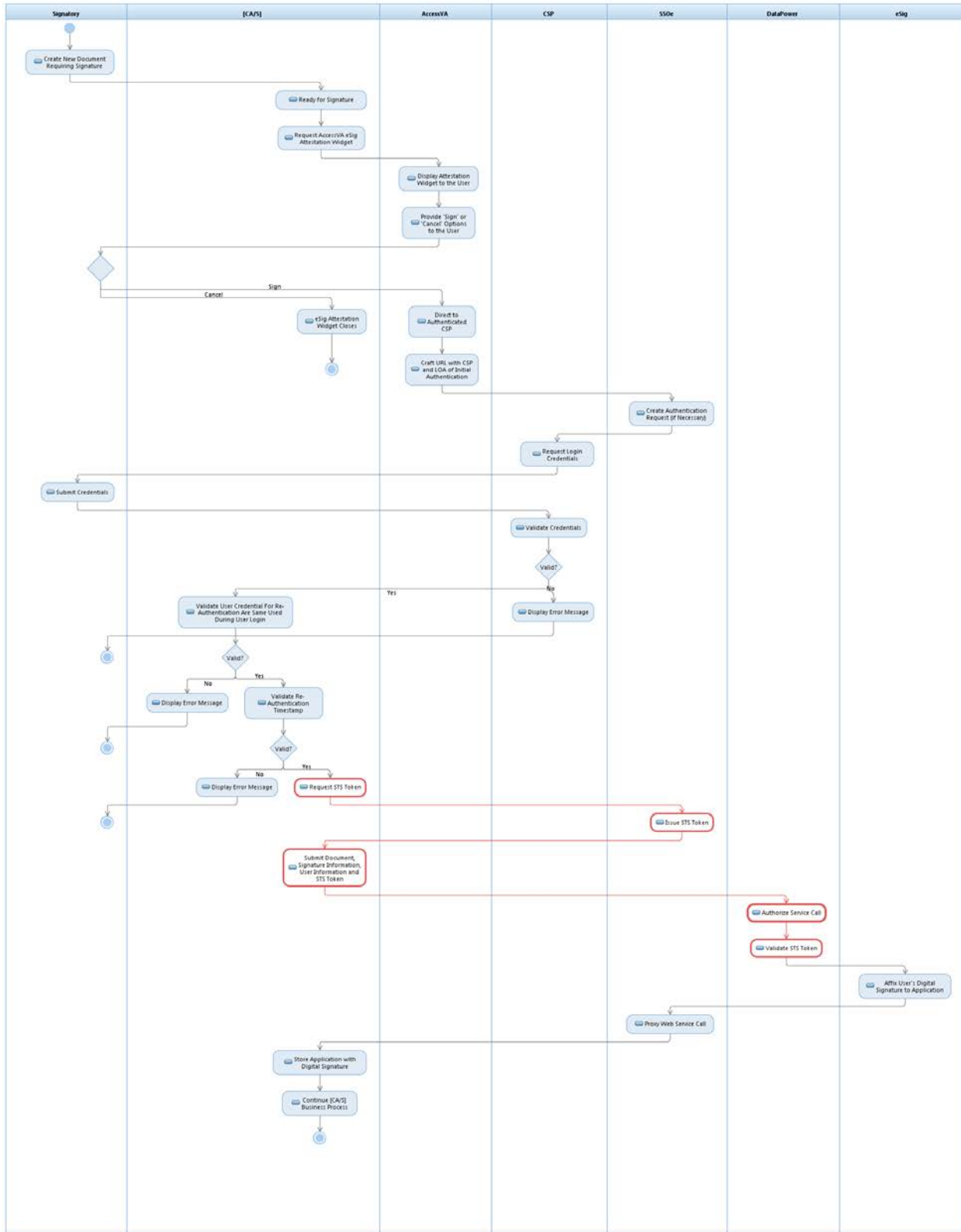
## 2.6.7. eSig

### 2.6.7.1. eSig Service Security Enhancement

To enhance the security of the eSig service, the eSig gateway shall offer an additional interface which will require use of SSOe STS token. This enhancement will ensure that the user parameters submitted by the consuming application match to an authenticated user.

Current eSig consumers will need to update to use the STS integration pattern.

The enhancements to the eSig process are identified in red in the following diagram.



**Figure 8: eSig Service Security Enhancement**

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN13. The eSig service shall accept a request to apply an electronic signature.		
13.0	Enhance eSignature Service Security	<b>[FEATURE 650434]</b> eSig gateway shall offer an additional interface that will require use of the SSOe STS token.
		<b>[FEATURE 650435]</b> eSig gateway shall continue to support the current interface while existing consumers are transitioned.
	Validate STS Token	<b>[FEATURE 650436]</b> eSig shall compare the SSOe token user parameter against the eSig user parameters to ensure a match.
		<b>[FEATURE 650437]</b> eSig shall validate the token issuer to ensure the token issuer is SSOe STS.
		<b>[FEATURE 650438]</b> eSig shall validate that the token digital signature using XML Digital Signature standard to process the signature element within the token.
		<b>[FEATURE 650439]</b> eSig shall validate the timestamps to ensure the token is within the validity period.
		<b>[FEATURE 650440]</b> eSig shall validate the endpoint as follows: <ul style="list-style-type: none"> <li>a. Validate Subject::SubjectConfirmation::SubjectConfirmationData@Address matches the requester (e.g., common name in this attribute matches that from the certificate which secured the session)</li> <li>b. Validate Service Endpoint using Subject::SubjectConfirmation::SubjectConfirmationData@Recipient (e.g., token issued for VSA use only)</li> <li>c. Validate audience restrictions in Conditions@AudienceRestriction. (e.g., audience restricted to eMI services)</li> <li>d. Validate one-time use restriction (e.g., token has not be used prior to this request)</li> </ul>
	Enhance eSig Demo Application	<b>[FEATURE 650441]</b> The eSig Demo application shall be enhanced to use the eSig gateway interface requiring use of SSOe STS token.

### 2.6.7.2. eSig Audit Logging

These requirements aim to ensure each service conforms to the audit logging requirements.

BRD BN	Requirement	In-Scope Requirement Clarification
23. Audit Trail: Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.		
23.0	eSig Audit Logging	<b>[FEATURE 650443]</b> The eSig service complies with the auditing requirements specified in the <b>Audit Logging Requirements</b> section.

### 2.6.8. Audit Logging Requirements

This section defines the audit logging requirements for each of the AcS services. These requirements are derived from multiple sources and include the following:

- AcS system security classification of High-impact/High-risk category
- Information Security Handbook 6500
- Federal standards and regulations for auditing and reporting (e.g., HIPAA)

BRD BN	Requirement	In-Scope Requirement Clarification
23. Audit Trail: Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.		
23.0	Frequency of Audit Logging	<b>[FEATURE 650445]</b> Each service shall log all auditable events immediately.
	Audit Events	<b>[FEATURE 650446]</b> Each service shall generate audit records for the following audit events (as applicable to the service): <ul style="list-style-type: none"> <li>• Actions of system administrators and operators</li> <li>• Production of printed output</li> <li>• New objects and deletion of objects in user address space</li> <li>• Security-relevant events</li> <li>• System configuration activities and events</li> <li>• Events relating to use of privileges</li> <li>• All events relating to user identification and authentication</li> <li>• The setting of user identifiers</li> <li>• Access to all audit trails</li> <li>• Valid or invalid logical access attempts</li> <li>• Initialization of audit logs</li> <li>• Creation and deletion of system-level objects</li> </ul>
	Content of	<b>[FEATURE 650447]</b> Each service shall generate audit records

BRD BN	Requirement	In-Scope Requirement Clarification
	Audit Records	<p>containing information that establishes the following:</p> <ul style="list-style-type: none"> <li>• What type of event occurred</li> <li>• When the event occurred</li> <li>• Where the event occurred</li> <li>• The source of the event</li> <li>• The outcome of the event</li> <li>• The identity and role of any individuals or subjects associated with the event</li> <li>• Individual identities of group account users</li> </ul>
	Content of Audit Records	<b>[FEATURE 650448]</b> Each service shall, as applicable, include in the content of the audit logs time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.
	Content of Audit Records	<b>[FEATURE 650449]</b> Each service shall not include any Highly Restricted data (e.g., PCI, HIPPA), passwords, or other PII (e.g., SSN, TaxID) in the content of the audit logs.
	Audit Log Maintenance	<p><b>[FEATURE 650450]</b> Audit logs shall be maintained as follows:</p> <ul style="list-style-type: none"> <li>• Must be sufficient in detail to facilitate reconstruction of events if a compromise or malfunction is suspected or has occurred.</li> <li>• Must be treated as restricted information/limited access and protected from unauthorized access, modification, or destruction and reviewed periodically for action. Access to logs must be granted based upon need-to-know and least privilege.</li> <li>• Must be backed up and stored securely.</li> <li>• Must be retired according to approved Records Schedule.</li> </ul>
	Response to Audit Processing Failure	<p><b>[FEATURE 650451]</b> Audit processing failures include, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.</p> <p>The services shall send system alerts to the roles/positions defined by the IAM System Owner.</p>
	Response to Audit Processing Failure	<b>[FEATURE 650452]</b> The services shall immediately alert designated organizational officials/positions in the event of an audit processing failure.
	Response to	<b>[FEATURE 650453]</b> In the event of audit processing failure, the

BRD BN	Requirement	In-Scope Requirement Clarification
	Audit Processing Failure	<p>services shall</p> <ul style="list-style-type: none"> <li>• Notify system administrator by email when approaching capacity</li> <li>• Overwrite oldest audit records</li> <li>• Stop generating audit records</li> </ul>
	Response to Audit Processing Failure	<b>[FEATURE 650454]</b> The services shall provide a warning to designated organizational officials/positions immediately when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.
	Audit Reduction and Report Generation	<p><b>[FEATURE 650455]</b> The services shall provide an audit reduction and report generation capability that does the following:</p> <ul style="list-style-type: none"> <li>• Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and</li> <li>• Does not alter original content or time ordering of audit</li> <li>• Processes audit records for events of interest based on defined audit fields within audit records</li> </ul>
	Auditing Time Stamps	<p><b>[FEATURE 650456]</b> The services, for the purposes of timekeeping and timestamps in audit records, shall include the following:</p> <ul style="list-style-type: none"> <li>• Use internal system clocks to generate time stamps for audit records</li> <li>• Record time stamps for audit records that can be mapped to Greenwich Mean Time (GMT) and meets granularity of milliseconds (hour:min:sec:milsec)</li> <li>• Compare the internal information system clocks with a defined authoritative time source (GMT)</li> <li>• Adjust settings to time zone and if time sync varies by more than two minutes, reset to default authoritative source</li> <li>• Include both date and time in the time stamp</li> </ul>
	Protection of Audit Information	<b>[FEATURE 650457]</b> The services shall protect audit information and audit tools from unauthorized access, modification, and deletion. Audit information constitutes all information (e.g., audit records, audit settings, and audit reports needed to successfully audit information system activity).
	Protection of Audit Information	<b>[FEATURE 650458]</b> The services shall back up audit records onto a physically different system or system component than the system or component being audited.
	Protection of Audit	<b>[FEATURE 650459]</b> The services shall implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

BRD BN	Requirement	In-Scope Requirement Clarification
	Information	Cryptographic mechanisms used for protecting the integrity of audit information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality the secret key used to generate the hash.
	Protection of Audit Information	<b>[FEATURE 650460]</b> The services shall authorize access to management of audit functionality to only a subset of privileged users identified by the IAM system owner. Access by Subset of Privileged Users, requires that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.
	Audit Record Retention	<b>[FEATURE 650461]</b> The services shall retain audit logs which describe a security breach for 6 years. The services shall retain all other audit records for a minimum of one year.
	Audit Generation	<b>[FEATURE 650462]</b> The services shall provide the capability for designated organizational officials/positions (defined by IAM system owner) to change the auditing to be performed on information system components based on selectable event criteria within time thresholds.

## 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 [REDACTED] 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 Explorers.
- User interfaces shall match the AcS Style Guide.

## 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 FY16 BRD, Section

7.2.1 Performance, Capacity, and Availability Requirements. For a detailed performance specification for each service, refer to the following subsections.

**Table 2: Performance Specifications**

<b>How many users does the current system support?</b>
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: <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>
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:

- a. 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.
- b. 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. Templates for AcS Service Components**

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	
<hr/>	
<b>Name</b>	<i>&lt;AcS Service Component&gt;</i>
<hr/>	
<b>Usage Profile</b>	<i>&lt;Define the type of service usage event&gt;</i>
<hr/>	
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 of service usage events&gt;/year</i>
Peak Hourly volume	<i>&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>
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. 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.

- b. VDS shall support 20 million authentications by SSOi per day.
- c. The IAM Binding Application shall support 1 million authentications per day.
- d. The IAM Binding Application shall support 1 million users.
- e. 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)
Usage Profile (User Authentication Events)	
Mean Daily volume	50,000
Projected Growth	8,000/year
Peak Daily volume	60,000
Projected Growth	10,000/year
Peak Hourly volume	8,000
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

Operation	
<b>Name</b>	SSOi STS
Usage Profile (Token Requests)	
Mean Daily volume	500,000
Projected Growth	10,000/year
Peak Daily volume	900,000
Projected Growth	25,000/year
Peak Hourly volume	72,000
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	1 second

- SSOi STS shall be capable of generating and exchanging 20 tokens per second for each token type.

Operation	
<b>Name</b>	SSOi oAuth
<b>Usage Profile (Token Requests)</b>	
Mean Daily volume	5,000
Projected Growth	5,000/year
Peak Daily volume	10,000
Projected Growth	10,000/year
Peak Hourly volume	1,000
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	1 second

- SSOi oAuth shall be capable of issuing 10 oAuth tokens per second for each token model.
- SSOi oAuth shall be capable of validating 20 oAuth tokens per second for each token model.

Operation	
<b>Name</b>	Authentication and SSO Token Issuance (SSOi Central Login Page)
<b>Usage Profile (User Authentication Events)</b>	
Concurrent Users	500
Mean Daily volume	50,000
Projected Growth	8,000/year
Peak Daily volume	500,000
Projected Growth	10,000/year
Peak Hourly volume	40,000
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

- SSOi Central Login Page shall support 15 authentications per second for each authentication method.

Operation	
<b>Name</b>	SSO Token Validation (CA SiteMinder Web Agent, CA SiteMinder SPS and IdP to SP Federation)
<b>Usage Profile (User Authentication Events)</b>	
Concurrent Users	500
Mean Daily volume	50,000
Projected Growth	8,000/year
Peak Daily volume	650,000
Projected Growth	10,000/year
Peak Hourly volume	54,000
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

- SSOi Central Login Page shall support 20 SSO token validations per second for each authentication method.

### 2.9.3. 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)  $\leq$  5 seconds.
- AccessVA shall support threshold average page load Essential time under normal load conditions (100 requests /minute)  $\leq$  8 seconds.
- AccessVA shall support threshold average page load Essential time under peak load conditions (1000 requests /minute)  $\leq$  10 seconds.

AccessVA and SSOe for this increment shall support the following:

Operation	
<b>Name</b>	SSOe (Application Junction, Reassertion Provider, CSP/IdP Federation Partner)
<b>Usage Profile (User Authentication Events)</b>	

Mean Daily volume	90,000
Projected Growth	20,000/year
Peak Daily volume	130,000
Projected Growth	30,000/year
Peak Hourly volume	10,000
Days of operation	Sunday-Saturday
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	10 seconds

- SSOe shall be capable of processing 10 SAML tokens per second for known on-boarded users.

Operation	
<b>Name</b>	SSOe STS
<b>Usage Profile (Token Requests)</b>	
Mean Daily volume	20,000
Projected Growth	20,000/year
Peak Daily volume	50,000
Projected Growth	50,000/year
Peak Hourly volume	72,000
Days of operation	Sunday-Saturday
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	1 seconds

- SSOe STS shall be capable of generating and exchanging 20 tokens per second.

Operation	
<b>Name</b>	SSOe oAuth
<b>Usage Profile (Token Requests)</b>	

Mean Daily volume	20,000
Projected Growth	20,000/year
Peak Daily volume	50,000
Projected Growth	50,000/year
Peak Hourly volume	5,000
Days of operation	Sunday-Saturday
Peak Hours	8am-10p.m.Eastern
Maximum Response Time	1 seconds

- SSOe oAuth shall be capable of issuing 10 oAuth tokens per second for each token model.
- SSOe oAuth shall be capable of validating 20 oAuth tokens per second for each model.

Operation	
<b>Name</b>	SSOe (Webservice Client, Webservice Producer)
<b>Usage Profile (Webservice Calls)</b>	
Mean Daily volume	10,000
Projected Growth	1,500/year
Peak Daily volume	1,5000
Projected Growth	2,000/year
Peak Hourly volume	1,500
Days of operation	Sunday-Saturday
Peak Hours	8am-10p.m.Eastern
Maximum Response Time	10 seconds

Operation	
<b>Name</b>	AccessVA User Interface (Full Site and Widget)
<b>Usage Profile (User Authentication Events)</b>	

Concurrent Users	500
Mean Daily volume	90,000
Projected Growth	20,000/year
Peak Daily volume	130000
Projected Growth	30,000/year
Peak Hourly volume	10,000
Days of operation	Sunday-Saturday
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	10 seconds

## 2.9.4. 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 Provisioning 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 on-boarding / off-boarding 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 Provisioning service for this increment shall support the following:

<b>Operation</b>	
<b>Name</b>	<b>Provisioning</b>
<b>Usage Profile (Provisioning Events – On-board/Off-board, Provision, De-provision, and Modify Events)</b>	
Mean Daily volume	1,500
Projected Growth	1,000/year
Peak Daily volume	2,000
Projected Growth	2,000/year
Peak Hourly volume	100
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

<b>Operation</b>	
<b>Name</b>	<b>VDS</b>
<b>Usage Profile (Service Calls)</b>	
Mean Daily volume	120,000
Projected Growth	50,000/year
Peak Daily volume	20,5000
Projected Growth	105,000/year
Peak Hourly volume	20,000
Days of operation	Sunday-Saturday
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	10 seconds

Operation	
Name	Provisioning User Interface
Usage Profile (Provisioning Events – On-board/Off-board, Provision, De-provision, and Modify Events)	
Concurrent Users	500
Mean Daily volume	1,500
Projected Growth	1,000/year
Peak Daily volume	2,000
Projected Growth	2,000/year
Peak Hourly volume	100
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

### 2.9.5. 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
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. 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>
<b>Usage Profile (Webservice Calls)</b>	
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
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	5 seconds

## 2.9.7. AMS

### User Profile:

- Veterans and beneficiaries who want to use a self-service interface to grant or revoke access to their VA record to another user
- Family members, caregivers and others who want to use a self-service interface to accept or revoke the right to access a Veteran's or beneficiary's VA record
- VA staff who want to be able to assist a Veteran or Beneficiary's Personal Representative, by using a staff-facing interface to perform the following;
  - Record the documentation that makes them a Personal Representative (Durable Power of Attorney, Legal Guardian, etc.) and
  - Create the right for the Personal Representative to access a Veteran's or beneficiary's VA record
- VA Staff who need to know whether a self-service user has the right to access another user's data, and the specific rights granted

The AMS for this increment shall support the following:

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

<b>Mean Daily volume</b>	<b>0</b>
<b>Projected Growth</b>	10000/year
<b>Peak Daily volume</b>	0
<b>Projected Growth</b>	20000/year
<b>Peak Hourly volume</b>	1000
<b>Days of operation</b>	Sunday-Saturday
<b>Peak Hours</b>	9am-7p.m.Eastern
<b>Maximum Response Time</b>	5 seconds

<b>Operation</b>	
<hr/>	
<b>Name</b>	AMS
<hr/>	
<b>Usage Profile (Self-Service/Staff UI)</b>	
<hr/>	
<b>Mean Daily volume</b>	<b>0</b>
<b>Projected Growth</b>	250/year
<b>Peak Daily volume</b>	0
<b>Projected Growth</b>	500/year
<b>Peak Hourly volume</b>	50
<b>Days of operation</b>	Sunday-Saturday
<b>Peak Hours</b>	9am-7p.m.Eastern
<b>Maximum Response Time</b>	5 seconds

### 2.9.8. 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	
Name	eSig
Usage Profile (Webservice Calls)	
Mean Daily volume	750
Projected Growth	1,000/year
Peak Daily volume	2,000
Projected Growth	2,500/year
Peak Hourly volume	100
Days of operation	Sunday-Saturday
Peak Hours	8am-10p.m.Eastern
Maximum Response Time	10 seconds

### 2.9.9. 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	0
Projected Growth	0/year
Peak Daily volume	0
Projected Growth	0/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

Operation	
Name	IP (Webservice)
Usage Profile (Webservice Calls)	

Mean Daily volume	0
Projected Growth	0/year
Peak Daily volume	0
Projected Growth	0/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

Operation	
Name	IP User Interface
Usage Profile (Proofing Events)	
Concurrent Users	0
Mean Daily volume	0
Projected Growth	0/year
Peak Daily volume	0
Projected Growth	0/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

## 2.9.10. 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:

<b>Operation</b>	
<b>Name</b>	<b>CSP (Credential Registration)</b>
<b>Usage Profile (Registration Events)</b>	
Mean Daily volume	100
Projected Growth	1,000/year
Peak Daily volume	250
Projected Growth	1,000/year
Peak Hourly volume	50
Days of operation	Sunday-Saturday
Peak Hours	8am- 10p.m.Eastern
Maximum Response Time	10 seconds

<b>Operation</b>	
<b>Name</b>	<b>CSP (Authentication)</b>
<b>Usage Profile (User Authentication Events)</b>	
Mean Daily volume	10,000
Projected Growth	10,000/year
Peak Daily volume	15,000
Projected Growth	10,000/year
Peak Hourly volume	10,000
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>	<b>CSP User Interface</b>
<b>Usage Profile (Proofing Events)</b>	

Concurrent Users	250
Mean Daily volume	10,000
Projected Growth	10,000/year
Peak Daily volume	15,000
Projected Growth	10,000/year
Peak Hourly volume	10,000
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.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 [REDACTED] (TRM) provides more information.
- The system is designed to operate in VA's standard virtualized operating system environment according to the VA [REDACTED]

## 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 3: Availability Level Specifications**

<b>Availability Level</b>	<b>1 (Important for Operations, Downtime Tolerant)</b>	<b>2 (Important for Productivity)</b>	<b>3 (Business Vital Information)</b>	<b>4 (Mission Critical Information)</b>	<b>5 (High Availability)</b>	<b>6 (Optimal Availability)</b>
<b>Minimum Availability Annually</b>	90.0%	95.0%	99.0%	99.9%	99.99%	99.999%
<b>Maximum Downtime Per Month</b>	73 hours	36 hours	7 hours 18 minutes	43 minutes 45 seconds	4 minutes 22 seconds	26 seconds
<b>Operational Hours</b>	Required during business hours	Required during business hours and some extended hours	Required for extended hours daily	Required 24/7	Required 24/7	Required 24/7
<b>Scheduled Maintenance</b>	Permits scheduled downtime operations on a regular basis	Permits brief scheduled downtime operations weekly or monthly	Permits brief scheduled downtime operations monthly	Continuity of service—little interruption	Continuity of service—minimal interruption	Virtually uninterrupted continuity of service

**Table 4: AcS Services and Availability Levels**

<b>Service</b>	<b>Classification</b>
Single Sign-On – Internal (SSOi)	4
Single Sign-On – External (SSOe)	4
Credential Service Provider (CSP)	2
Electronic Signature (eSig)	3
Provisioning (Prov)	2
Virtual Directory Service (VDS)	5
Specialized Access Control (SAC)	4
Compliance Audit and Reporting (CAR)	2
Authorization Management Service (AMS)	3

## 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.

## 2.16. External System Enablements

A system enablement effort supports authorized activity by an external system to consume information from the AcS system. Typically, enablements to external systems do not require functional or technical changes to the AcS system. However, joint analysis and design support are often required so that the consuming application can modify its system accordingly. An

external system wishing to consume AcS data must first [REDACTED] (SR) so that IAM resources and schedule may be allocated to support the enablement in advance of the consumption of AcS data. Full and complete instructions to consuming applications wishing to consume AcS data are provided.

The [REDACTED] document contains a high-level overview of the AcS service and service interfaces.

This document contains requirements for the VHIC application only. To comply with VA mandate [REDACTED] consuming applications shall follow the process outlined above to submit an IAM SR, and an integration RSD will be produced following analysis with the consuming application.

The On/Off-Boarding requirements are dependent on the following integrations:

- Provisioning HR Smart
- Provisioning AD
- Provisioning PIV
- Provisioning eCMS
- Provisioning TMS
- Provisioning VA-PAS
- Provisioning MVI

### 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 5: Applicable Standards**

Applicable Standards
<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>
[REDACTED]
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

Applicable Standards	
Identification Verification (PIV))	
Follows the documentation specifications provided by the [REDACTED] and VA Program Management Accountability System (PMAS)	
[REDACTED]	
[REDACTED]	
<a href="#">Screen Resolution for Mobile Devices</a>	
AcS Style Guide	

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 VA AcS Solution System Design Documents (SDDs) and Interface Control Documents (ICDs) provide information regarding communications interfaces:

- AcS eSig SDD
- AcS CSP SDD
- AcS IP SDD
- AcS CAR SDD
- AcS SAC SDD
- AcS SSOe SDD

- AcS SSOi SDD
- AcS Prov SDD
- AcS AMS SDD
- AcS eSig Master ICD
- AcS IP Master ICD
- AcS CAR Master ICD
- AcS SAC Master ICD
- AcS SSOe Master ICD
- AcS SSOi Master ICD
- AcS Prov Master ICD

## **4.2. Hardware Interfaces**

The following VA AcS Solution SDDs provide information regarding hardware interfaces:

- AcS eSig SDD
- AcS CSP SDD
- AcS IP SDD
- AcS CAR SDD
- AcS SAC SDD
- AcS SSOe SDD
- AcS SSOi SDD
- AcS Prov SDD
- AcS AMS SDD

## **4.3. Software Interfaces**

The following VA AcS Solution SDDs provide information regarding software interfaces:

- AcS eSig SDD
- AcS CSP SDD
- AcS IP SDD
- AcS CAR SDD
- AcS SAC SDD
- AcS SSOe SDD
- AcS SSOi SDD
- AcS Prov SDD
- AcS AMS SDD

## 4.4. User Interfaces

The user interfaces are described in [section 2.6](#).

## 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 following VA AcS Solution SDDs provide information regarding purchased components:

- AcS eSig SDD
- AcS CSP SDD
- AcS IP SDD
- AcS CAR SDD
- AcS SAC SDD
- AcS SSOe SDD
- AcS SSOi SDD
- AcS Prov SDD
- AcS AMS SDD

## 7. User Class Characteristics

The user community consists of the following classes:

- Internal users (internal VA personnel, employees, administrators, and contractors, etc.)
- External users (the Department of Defense [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:		

## Cumulative Probability (“S-curve”) Chart

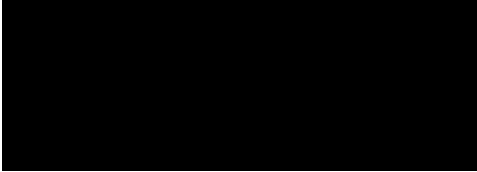



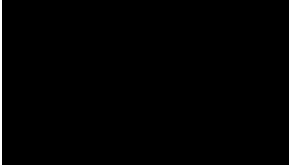





*[Insert Cumulative Probability (“S-curve”) Charts here]*

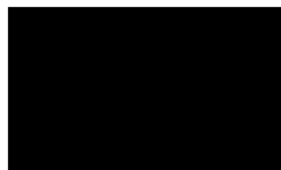
## 9. Approval Signatures

REVIEW DATE: <date>


SCRIBE: <name>

Signed:

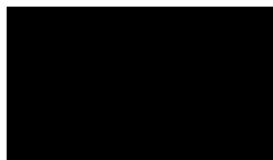
	mm/dd/yyyy
 Integrated Project Team (IPT) Chair	Date
	12/02/2015
 , Integrated Project Team (IPT) Chair	Date
	12/07/2015
 Director, Identity, Credential and Access Management (ICAM)	Date
	12/17/2015
 Data Quality Business Product Manager	Date
	12/07/2015
 , Business Sponsor, IAM BPMO	Date




12/07/2015

, IAM Program Manager

Date



12/13/2015

, AcS Project Manager

Date

# Appendix A: Non-Functional Requirements

The following non-functional requirements should be reviewed and accessed while developing the requirements for the project.

## System Performance Reporting Requirements

(Note: Each system developed by the Department of Veterans Affairs (VA) Office of Information and Technology (OI&T) must comply with the following mandatory requirements.)

1. Include instrumentation to measure all performance metrics specified in the Non-Functional Requirements section of the Requirements Traceability Matrix (RTM). At a minimum, systems will have the ability to measure reporting requirements for Responsiveness, Capacity, and Availability as defined in the non-functional requirements section of the RTM.
2. Make the performance measurements available to the Information Technology (IT) Performance Dashboard to enable display of “actual” system metrics to customers and IT staff.

## Operational Environment Requirements

1. System response times and page load times shall be consistent with \_\_\_\_\_ standards (for example, My HealtheVet or HealtheVet). (Comment: There may be different expectations for an external display vs. a query. Need to address these different uses. Also indicate if this information is unknown).
2. Maintenance, including maintenance of externally developed software incorporated into the \_\_\_\_\_ application(s), shall be scheduled during off peak hours or in conjunction with relevant maintenance schedules. The business owner should provide specific requirements for establishing system maintenance windows when planned service disruptions can occur in support of periodic maintenance.
3. Information about response time degradation resulting from unscheduled system outages and other events that degrade system functionality and/or performance shall be disseminated to the user community within 30 minutes of the occurrence. The notification shall include the information described in the current Automated Notification Reporting (ANR) template maintained by the VA Service Desk. The specific business impact must be noted in order for OIT to provide accurate data in the service impact notice of the ANR.
4. Provide a real-time monitoring solution to report agreed/identified critical system performance parameters.
5. Critical business performance parameters shall be identified e.g., transaction speed, response time for screen display/refresh, data retrieval, etc. in a manner that data capture can occur to support metric reporting and support the OI&T performance dashboard display. If no such performance metrics are required or provided there will be no program specific Service Level Agreements (SLA) created, nor shall there be any active/real time monitoring through OI&T Performance Dashboard to provide the business owners any performance metrics.

6. Notification of scheduled maintenance periods that require the service to be offline or that may degrade system performance shall be disseminated to the business user community a minimum of 48 hours prior to the scheduled event.

## Documentation Requirements

1. The training curriculum shall state the expected training time for primary users and secondary users to become proficient at using the \_\_\_\_\_ application(s).
2. All training curricula, user manuals and other training tools shall be developed/updated by \_\_\_\_\_ <<insert name of Program Office>> and delivered to all levels of users \_\_\_\_\_. If known, insert how much time in advance the training tools will be delivered and via what mechanism(s); for example, 2-4 weeks in advance of the release of the enhancement through nationwide conference calls and PowerPoint presentations). The curricula shall include all aspects of the enhanced \_\_\_\_\_ application(s) and all changes to processes and procedures.
3. The training curriculum developed by the Program Office shall state the expected task completion time for primary and secondary users.
4. User manuals and training tools shall be developed. If they already exist, updates shall be made, as necessary, to them and they shall be delivered to all levels of users.
5. IT will provide the level of documentation required to support the system and maintain operations and continuity. Documentation shall represent minimal programmatic and lifecycle operations support documentation artifacts as defined by VA standards in ProPath and as required by the VA Enterprise System Engineering Lifecycle and Release Management office for sustained operations, maintenance, and support (<http://vaww.eie.va.gov/lifecycle/default.aspx>) prior to approval by any VA change control board and release into production.

## Implementation Requirements

1. Technical Help Desk support for the application shall be provided for users to obtain assistance with \_\_\_\_\_.
2. The IT solution shall be designed to comply with the applicable approved Enterprise SLA.
3. The implementation must be complete by \_\_\_\_\_. (Enter date - dd-mm-yyyy)

## Data Protection/Back-up/Archive Requirements

1. Based upon the criticality of the system, provide a back-up and data recovery process for when the system is brought off-line for maintenance or technical issues/problems.
2. Data protection measures, such as back-up intervals and redundancy shall be consistent with systems categorized as routine (30 day restoration), mission essential (72 hour restoration), or mission critical (12 hour restoration).

Business owners are required to state the mission criticality of the IT services required in order to assist the planners and developers in determining best strategies for engineering an IT solution to meet their business objectives/needs. The business owner needs to state the criticality of the data and the impact to the business during a service disruption so appropriate technologies can be considered.

## Levels for Disaster Recovery

Classification	Recovery Time Objective	Recovery Point
Objective Routine	30 day restoration	TBD
Mission Essential	72 hour restoration	24 hours
Mission Critical	12 hour restoration	2 hours

Recovery Time Objective (RTO) – RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.

Maximum Tolerable Downtime (MTD) - The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.

Recovery Point Objective (RPO) - The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage.

## Data Quality/Assurance Requirements

A monitoring process shall be provided to ensure that data is accurate and up-to-date and provides accurate alerts for malfunctions while minimizing false alarms.

## User Access/Security Requirements

Ensure the proposed solution meets all Veterans Health Administration (VHA) Security, Privacy, and Identity Management requirements including VA Handbook 6500 (see the Enterprise Requirements section of the RTM).

## Usability/User Interface Requirements

Adhere to good User Interface/User Centered Design (UI/UCD) principles as outlined in the Usability Appendix of the BRD.

## Conceptual Integrity

Provide standards based messaging and middleware infrastructure needed to support both Legacy Veterans Health Information Systems Technology Architecture (VistA) and future VistA 4 deployments.

## Availability

1. Maintenance window, including maintenance of externally developed software incorporated into the VistA 4 application(s), will be by mutual agreement between OI&T and the VHA Point of Contact (POC) for the affected facility (ies). VHA will provide POCs for each facility.

2. VistA application unavailability due to an unplanned outage or planned outages that exceed the defined maintenance window will not exceed 8.76 hours per year and will not exceed 43.8 minutes per month (99.9% availability).
3. The application shall be available 24 hours a day, seven days a week, with an uptime of 99.9%.
4. All system updates and scheduled maintenance should occur between the hours of 1800 and 0600 (per local time zone), when clinical usage would be lightest.

## **Interoperability**

1. The system shall support all recognized health system standards i.e., Health Level 7 (HL7), Fast Healthcare Interoperability Resources (FHIR).
2. Systems must be heterogeneous and agnostic for operating systems and code bases.
3. Provide the ability to securely transfer large files (of 4-8 gigabyte) from an external source to VA systems.
4. Provide access to the system over a remote access solution.

## **Manageability**

1. Provide Service Desk/Incident and Problem Management tracking related to maintenance events of patient care systems with priority over non-patient care systems.
2. Provide data related to maintenance events, both routine and exceptional, including key metadata:
  - Predicted routine work
  - Occurrences where maintenance is completed, including restart from down time
  - Identity of the organization performing maintenance
  - User performing maintenance (if available)
  - Identity of the system
  - Date/time, physical location
  - Systems impacted
  - Does it affect patient care
  - Non-urgent or emergent
3. Provide audit capabilities for system access and usage with settings that are configurable to support internal and external audits based on federal and VHA mandates.
4. The system must comply with VA Directive 6300 Records and Information Management and with VHA Records Control Schedule (RCS) 10-1, in general and specifically with Electronic Final Version of Health Record: Destroy/Delete 75 years after last episode of patient care, or longer (if specified).

## **Performance**

1. Provide an Infobutton Query Responder on all platforms with a response time of less than .5 seconds.

2. The system shall recognize, report, and retransmit data lost, with less than 0-1% chance of incomplete patient records.
3. Provide patient data (for data within the system) transactions (e.g., capture, search, request for data) within .5 seconds.
4. Mouse or key-based UI controls, e.g., menus, checkboxes shall provide instantaneous responsiveness (<90ms).
5. Part-screen refreshes after user action shall complete within a pro-rated interval between 200 ms and 1200 ms times a percentage of the screen area being refreshed. For example, a component 10% of the screen area would refresh in  $(1200 - 200) * 0.10 + 200 = 300$  ms.

## Reliability

1. Provide system reliability:
  - Threshold = 99.9%
  - Objective = 99.99% system and application
2. Provide system reliability:
  - Level 1 severity =<1 failure per month
  - Level 2 severity =<2 failures per month
  - Level 3 severity =<3 failures per month

## Security

Provide management of electronic attestation of information including the retention of the signature of attestation (or certificate of authenticity) associated with incoming or outgoing information.

## Supportability

1. Provide alerts (that extend beyond system messages to external systems like mobile devices) for malfunctions, while preventing false alarms for local, regional, and national evaluations in real time.
2. Provide reports on performance metrics as specified in the VistA 4 Effectiveness and Value / Benefits Framework on a bi-weekly basis.
3. Provide national, regional, and local reports on performance metrics as specified in the VistA 4 Effectiveness and Value / Benefits Framework.
4. Provide performance metrics (from request for information to receipt of information on the screen) monitored by the system and system administrators so they know what the user experience is like without users having to call them and tell them the system is running very slow.
5. Provide the ability for VHA and IT staff to create standard and ad-hoc reports of usage, bandwidth, response time, login time, and other variables with a verification process for measuring the capabilities of the system.

6. Provide end-user training on how to generate the various system performance reports (e.g., in standard file formats such as Comma Separated Values [CSV], Portable Document Format [PDF], or Excel) depending on the user's needs.
7. Provide the ability to view system statistics (e.g., information on the specific network environment) and identify areas that are having issues or are beyond capacity, in near-real-time (to be quantified at a later time).
8. Technical Help Desk support for the application via instant message, on-line, phone, and remote desktop access support, shall be provided for users to obtain assistance 24/7.
9. The IT solution shall be designed to comply with the applicable approved Enterprise SLAs.
10. Data protection measures, such as back-up intervals and redundancy shall be consistent with systems categorized as mission critical (1hr restoration, 2hrs backup recovery). Impact of system failure must be monitored on a near real time basis.
11. Provide the ability to set thresholds and notification type (e.g., email or text alerts) when alerting the user about response time degradation and unscheduled outages.
12. Disaster Recovery Plans (DRP) and Continuity of Operations Plan (COOP) will be updated and tested semi-annually to address the VistA 4 product (see National Security and Homeland Security Presidential Directive: National Continuity Policy. NSPD-51/HSPD-20, May 9, 2007 <http://www.fas.org/irp/offdocs/nspd/nspd-51.htm>)

## Usability

1. Provide viewability/usability of VistA 4 applications on mobile devices.
2. User prompts and screen help shall be embedded into the system to guide use of the solution.

## Documentation

1. The training curriculum shall be provided in two hours or more of training time for primary users and secondary users to become proficient at using the VistA 4 application(s).
2. All training curricula, user manuals and other training tools shall be developed/updated by the VE Program Office and delivered to all levels of users 4 weeks in advance of the release of the enhancement through mediums that will best support the sharing of information to all affected staff.
3. Provide follow-up training classes tailored to VHA workflow 4 weeks after the users have begun to use the system.

## Appendix B: Acronym List and Glossary

The abbreviations and terms used in this RSD are defined in the [REDACTED]

### Glossary

Term	Meaning
3POB	Third-Party On-Boarding
Ent ID	Enterprise Identity
NPE	Non-Person Entities
oAuth	Open Authorization Standard
SDK	Software Development Kit
STS	Security Token Service
UI	User Interface
UX	User Experience

## Appendix C: Requirements Deferred to AcS 2.0 Increment 7

The following requirements were stated in previous AcS Requirements Specification Documents (RSDs) but were not delivered. They are delivered in AcS 2.0 Increment 7.

Feature ID	RSD Paragraph Number	RSD	Primary Text
468512	2.7.3.15 Provisioning shall provide a service to allow a system to retrieve user accounts by SEC ID.	AcS Increment 2	Provisioning shall provide a service to allow a system to retrieve user accounts by SEC ID.
461871	2.6.1.1.2 Security Token Service (STS) Support of JSON Web Token and Bearer Token	AcS 2.0 Increment 5	SSOi shall provide a JSON web token within the STS framework.
461872	2.6.1.1.3 Security Token Service (STS) Support of JSON Web Token and Bearer Token	AcS 2.0 Increment 5	SSOi shall be able to digitally sign and encrypt JSON web tokens.
461873	2.6.1.1.4 Security Token Service (STS) Support of JSON Web Token and Bearer Token	AcS 2.0 Increment 5	SSOi shall be able to verify digitally signed JSON web tokens and decrypt encrypted JSON web tokens.
461874	2.6.1.1.5 Security Token Service (STS) Support of JSON Web Token and Bearer Token	AcS 2.0 Increment 5	SSOi shall accept JSON Web tokens.
461875	2.6.1.1.6 Security Token Service (STS) Support of JSON Web Token and Bearer Token	AcS 2.0 Increment 5	SSOi shall accept JSON Bearer tokens.
461877	2.6.1.2.1 Expose STS Service with REST interface	AcS 2.0 Increment 5	SSOi shall expose the STS service with a REST interface.
468767	2.6.1.2.6.1 SSOi	AcS 2.0 Increment 2	SSOi shall support OAuth from the provider perspective.

Feature ID	RSD Paragraph Number	RSD	Primary Text
468768	2.6.1.2.6.2 SSOi	AcS 2.0 Increment 2	SSOi shall support OAuth enforcement from application perspective.
468769	2.6.1.2.6.3 SSOi	AcS 2.0 Increment 2	SSOi shall support mobile client registration (Internal for Mobile Applications).
468771	2.6.1.2.6.5 SSOi	AcS 2.0 Increment 2	SSOi shall support management and enforcement of OAuth policies (Internal for Mobile Applications).
468772	2.6.1.2.6.6 SSOi	AcS 2.0 Increment 2	SSOi shall support fine-grained revocation (Internal for Mobile Applications).
468773	2.6.1.2.6.7 SSOi	AcS 2.0 Increment 2	SSOi shall support limiting the number of access or refresh tokens (Internal for Mobile Applications).
468774	2.6.1.2.6.8 SSOi	AcS 2.0 Increment 2	SSOi shall support self-registration of clients (Internal for Mobile Applications).

## Template Revision History

<b>Date</b>	<b>Version</b>	<b>Description</b>	<b>Author</b>
September 2015	1.7	Updated Headings and spacing to conform with latest OIT Documentation Standards guidelines	Process Management
June 2015	1.6	Updated to conform with latest Section 508 guidelines and remediated with Common Look Office tool	Process Management
May 2015	1.5	Revised by the PMAS Process Improvement Lockdown Team	PMAS Process Improvement Lockdown Team
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 page to enhance search capabilities	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