

# **Department of Veterans Affairs**

## **Identity and Access Management Access Services 2.0 Increment 4**

### **Requirements Specification Document**



**May 2014  
Version 1.0**

## 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
5/20/2014	1.0	Completed a quality review. Embedded email approval signatures to the PDF to post on the AcS TSPR. Document version changes to 1.0 upon approval.	Bruce [REDACTED]
5/9/2014	0.3	Updated with Formal Review Feedback	AcS Analysis Team
5/2/2014	0.2	Updated with Peer Review Feedback	AcS Analysis Team
4/30/2014	0.1	Completed a tech edit review	Bruce [REDACTED]
4/28/2014	0.1	Initial Draft	AcS Analysis Team

*Place latest revisions at top of table.*

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

*Remove blank rows.*

## Artifact Rationale

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

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

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Purpose .....	1
1.2	Scope.....	2
1.3	Abbreviations and Definitions.....	2
1.4	References .....	2
<b>2</b>	<b>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	Maintenance Screen .....	5
2.6.2	Single Sign-On – Internal (SSOi) .....	7
2.6.2.1	IAM Central Login Page: Error Messages.....	7
2.6.2.2	IAM Central Login Page: SSOi Session Timeout.....	8
2.6.2.3	IAM Authenticated Landing Page and IAM Logged Off Page.....	9
2.6.2.4	IAM Standard SSOi AuthorizationTraits.....	11
2.6.2.5	STS Support of AD/Kerberos Token Exchange.....	12
2.6.3	Specialized Access Control .....	12
2.6.4	Provisioning .....	14
2.6.5	Role Engineering and Compliance Tool .....	17
2.7	Graphical User Interface (GUI) Specifications .....	25
2.8	Multi-divisional Specifications .....	25
2.9	Performance Specifications .....	25
2.10	Quality Attributes Specification .....	27
2.11	Reliability Specifications .....	27
2.12	Scope Integration .....	28
2.13	Security Specifications .....	28
2.14	System Features.....	29
2.15	Usability Specifications .....	29
<b>3</b>	<b>Applicable Standards .....</b>	<b>29</b>
<b>4</b>	<b>Interfaces.....</b>	<b>30</b>
4.1	Communications Interfaces .....	30
4.2	Hardware Interfaces .....	30
4.3	Software Interfaces .....	30
4.4	User Interfaces.....	30

<b>5</b>	<b>Legal, Copyright, and Other Notices .....</b>	<b>30</b>
<b>6</b>	<b>Purchased Components .....</b>	<b>30</b>
6.1	Defect Source (TOP 5).....	31
<b>7</b>	<b>User Class Characteristics .....</b>	<b>31</b>
<b>8</b>	<b>Estimation .....</b>	<b>31</b>
<b>9</b>	<b>Approval Signatures .....</b>	<b>33</b>
<b>Appendix A</b>	<b>Use Case Specification .....</b>	<b>34</b>
A.1.	Use Case Name .....	34
A.2.	Brief Description .....	34
A.3.	Use Case Trigger .....	34
A.4.	Use Case Context Diagram .....	34
A.5.	Use Case Actors .....	34
A.6.	Preconditions .....	34
A.6.1.	Precondition 1 .....	34
A.7.	Basic Flow of Events .....	34
A.7.1.	First Step of Basic Flow .....	34
A.8.	Alternative Flows .....	34
A.8.1.	First Alternative Flow .....	34
A.8.2.	Second Alternative Flow .....	34
A.9.	Sub Flows .....	34
A.9.1.	First Subflow .....	34
A.9.2.	Second Subflow .....	35
A.10.	Postconditions .....	35
A.10.1.	Post Condition One .....	35
A.11.	Special Specifications .....	35
A.11.1.	First Special Specification .....	35
A.12.	Extension Points .....	35
A.12.1.	Name of Extension Point .....	35
<b>Appendix B</b>	<b>IAM Standard SSOi Authentication Traits .....</b>	<b>36</b>

## List of Figures

Figure 1: AcS Maintenance Screen Mock-Up .....	7
Figure 2: IAM Authenticated Landing Page .....	10
Figure 3: IAM Logged Out Page .....	11
Figure 4: Bind a Provisioned User to a VistA Account .....	16
Figure 5: Integration of Role Engineering and Compliance Tool with AcS Services .....	17
Figure 6: Cumulative Probability (“S-curve”) Chart .....	32

## List of Tables

Table 1: Document References .....	3
Table 2: AcS Maintenance Screen Requirements .....	5
Table 3: SSOi Central Login Page Business Needs and Requirements Enhancements .....	7
Table 4: SSOi Session Timeout Business Needs and Requirements Enhancements .....	8
Table 5: SSOi Authenticated Landing Page Business Needs and Requirements Enhancements .....	9
Table 6: SSOi Standard Authorization Traits Business Needs and Requirements Enhancements .....	11
Table 7: SSOi Support of AD/Kerberos Token Exchange Business Needs and Requirements Enhancements .....	12
Table 8: Specialized Access Control Business Needs and Requirements Enhancements .....	13
Table 9: Provisioning Business Needs and Requirements Enhancements .....	14
Table 10: Resource Attribute/Metadata Management Business Needs and Requirements Enhancements .....	18
Table 11: Applicable Standards .....	29
Table 12: SSOe-SSOi User Session .....	36
Table 13: SSOe-SSOi STS – Indirect .....	40
Table 14: SSOi STS – Direct .....	47

# 1 Introduction

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

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

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

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

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

## 1.1 Purpose

The purpose of this document is to summarize the business and functional requirements that are required for the development and implementation of AcS 2.0 Increment 4.

The AcS 2.0 Increment 4 requirements described in this document are drawn from VA AcS FY15 Business Requirements Documents (BRDs). Additional AcS 2.0 Increment 4 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 document supports the development of the AcS 2.0 Increment 4 System Design Document (SDD), which provides guidance for the implementation and development of the AcS solution.

This document 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 audience for this document includes the following:

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

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

The current development partners include the following:

- The Development team responsible for implementing AcS-approved 2.0 Increment 4 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 document encompasses the AcS requirements that VA is requesting for AcS 2.0 Increment 4. The AcS requirements include the following components:

- Single Sign-On – Internal (SSOi)
- Specialized Access Control (SAC)
- Provisioning
- Role Engineering and Compliance
- Maintenance Screen

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

- Identity Proofing (IP)
- Virtual Directory
- e-Signature (eSig)
- Compliance Audit and Reporting (CAR)
- Credential Service Provider (CSP)

Requirements for Single Sign-On – External (SSOe) and AccessVA are addressed in a separate RSD.

## 1.3 Abbreviations and Definitions

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

## 1.4 References

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

**Table 1: Document References**

<b>Title</b>	<b>Date</b>	<b>Published By</b>
<a href="#">AcS FY15 BRD</a>	01/2014	OIS BPMO
<a href="#">Section 508 Standards Guide</a>	04/16/2010	General Service Administration
<a href="#">NIST Special Publication (SP) 800-63 Version 1.0.2: Electronic Authentication Guideline</a>	04/2006	National Institute of Standards and Technology (NIST)
<a href="#">VA Directive 6500: Information Security Program</a>	08/2006	VA
VA Directive 6501; VA Identity Verification In Person Proofing (IPP) Process; IAM Handbook	Last updated: 09/01/2010	VA
VA IAM Handbook 6510	TBD	VA
<a href="#">VRM IAM Scope and Vision Document</a>	10/2012	VA
<a href="#">Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, Version 2.0</a>	12/2011	Federal CIO Council
<a href="#">OMB 04-04 E-Authentication Guidance for Federal Agencies</a>	12/2003	Office of Management and Budget (OMB)
<a href="#">Sec-ID MVI iRSD</a>	9/2012	IAM Integration Analysis Team
<a href="#">AcS i3 RSD</a>	9/2012	IAM Access Service Analysis Team
<a href="#">AcS i4 RSD</a>	3/2013	IAM Access Services Analysis Team
<a href="#">AcS 2.0 Increment 2 RSD</a>	8/2013	IAM Access Services Analysis Team
<a href="#">AcS SDD</a>	12/2013	AcS Development Contractors
AcS 2.0 Increment 2 UC Model	TBD	
<a href="#">AcS 2.0 Increment 3 RSD</a>	4/2013	IAM Access Services Analysis Team
<a href="#">Role Management in IdentityIQ</a>	9/2013	SailPoint



Title	Date	Published By
<a href="#">Role Models and Methodology</a>	3/2010	SailPoint
<a href="#">Lifecycle of a Certification</a>	7/2013	SailPoint
<a href="#">SailPoint Best Practices – Certification Generation on large deployments</a>	12/2013	SailPoint
<a href="#">Delimited File Application Set-up and Configuration</a>	2/2014	SailPoint
<a href="#">Managing Extended Attributes</a>	2/2014	SailPoint
<a href="#">IAM Portal Strategy</a>	2/2013	IAM Technical Lead
<a href="#">IAM IP-MVI Integration iRSD</a>	11/2013	IAM Access Services Analysis Team

## 2 Overall Description

The scope and functionality for AcS 2.0 Increment 4 are limited to the AcS services specified in this document.

### 2.1 Accessibility Specifications

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

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

### 2.2 Business Rules Specification

The business rules specifications are identified in section 2.6.

### 2.3 Design Constraints Specification

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

### 2.4 Disaster Recovery Specification

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

### 2.5 Documentation Specifications

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

## 2.6 Functional Specifications

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

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

### 2.6.1 Maintenance Screen

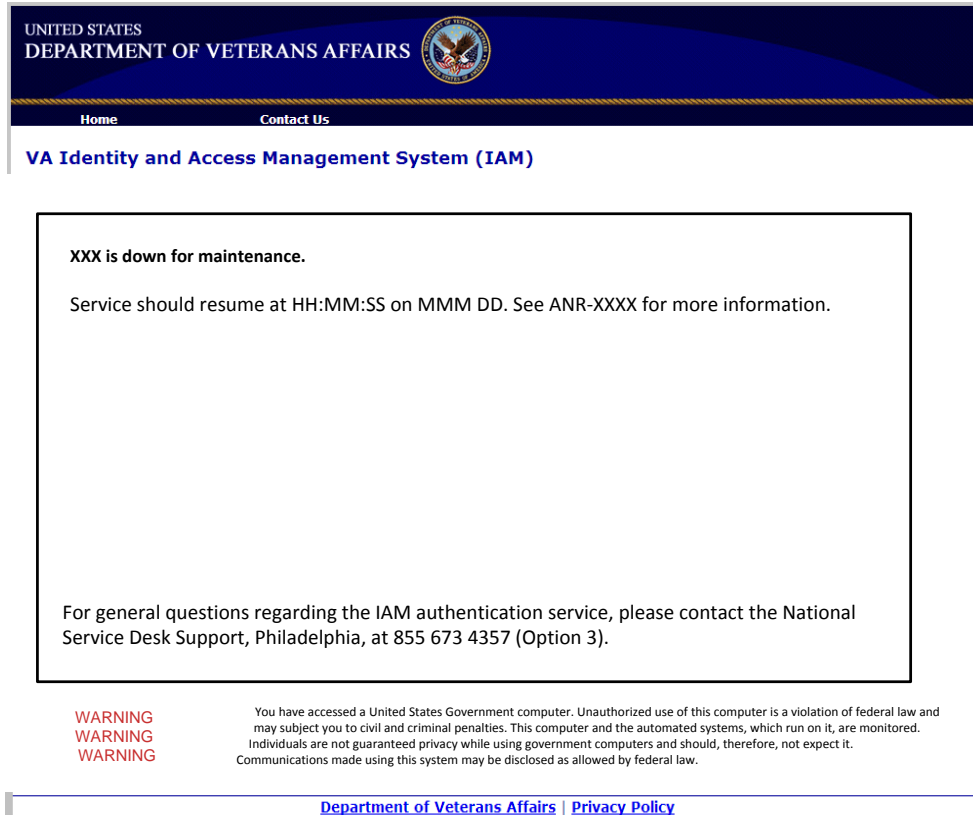
With the maturing of the various services provided by AcS, there is a need to implement a maintenance page displayed during system downtime for those services that include a user interface (e.g., SSOi, Provisioning, CAR, Role Engineering and Compliance Tool, IP and CSP). The following table identifies the requirements for this maintenance page.

**Table 2: AcS Maintenance Screen Requirements**

BRD BN	Requirement	In-Scope Requirement Clarification
1.0, 3.0, 9.0, 12.0, 22.0, 23.0	The AcS Services shall display a screen informing users when the service has been brought down due to system maintenance.	When the SSOi, Provisioning, CAR, Role Engineering and Compliance Tool, IP, or CSP Service is down for maintenance, the affected system(s) shall display a page informing the user that the site requested is down for maintenance. Refer to Figure 1 for a mock-up of the screen.
		The Maintenance Page shall display the text “XXX is down for maintenance,” where “XXX” displays the name of the down service.
		The Maintenance Page shall display the text: “Service should resume at HH:MM:SS on MMM DD. See ANR-XXXX for more information.”
		The Maintenance Page shall allow the system administrator to configure the anticipated service resumption time and the ANR number.
		The Maintenance Page shall display contact information for the National Service Desk.
		The Maintenance Page shall display the standard footer, which includes: <ul style="list-style-type: none"><li>Text: “You have accessed a United States Government computer. Unauthorized use of this computer is a violation of federal law and may subject you to civil and criminal</li></ul>

BRD BN	Requirement	In-Scope Requirement Clarification
		<p>penalties. This computer and the automated systems, which run on it, are monitored. Individuals are not guaranteed privacy while using government computes and should, therefore, not expect it. Communications made using this system may be disclosed as allowed by federal law.”</p> <ul style="list-style-type: none"> <li>• Link to the Department of Veterans Affairs web page.</li> <li>• Link to the Privacy Policy.</li> </ul>
		<p>The Maintenance page shall be Section 508 compliant.</p>
		<p>The Maintenance page shall follow all VA standards as referenced in section 2.7: Graphical User Interface (GUI) Specifications of this RSD.</p>

The requirements for the AcS maintenance screen are reflected in Figure 1 below.



**Figure 1: AcS Maintenance Screen Mock-Up**

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

### 2.6.2.1 IAM Central Login Page: Error Messages

The requirements identified in this subsection apply to the following:

- SiteMinder Integration
- CA SiteMinder SPS Integration
- IdP to SP Federation: IAM as Identity Provider

**Table 3: SSOi Central Login Page Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. Centralized Enterprise Single Sign-On – Internal (SSOi): Provide a capability to allow a user to sign on once to an application, then allow the user to access another application		
12.0	IAM Central Login Page: Error messages for SiteMinder Integration and IdP to SP Federation: IAM	When the user is not found in the IAM user data store, the IAM Central Login Page shall display the message, "Please verify your user ID and password, and try to log in again."

BRD BN	Requirement	In-Scope Requirement Clarification
	as Identity Provider	When the user enters invalid credentials during IAM SSOi authentication, the IAM Central Login Page shall display the message, "Please verify your user ID and password, and try to log in again."
		If the user fails to meet any authorization rule configured for the application in SSOi (for instance, the presence of a user in an AD Group), the following message shall be displayed by the IAM Central Login Page in cases where the user has been authenticated to the IAM user data store but fails the IAM authorization check: "You have not been authorized access to this application. Please contact your local IT support Help Desk."
		When the IAM Central Login Page encounters a server error, the IAM Central Login Page shall display the error number.

### 2.6.2.2 IAM Central Login Page: SSOi Session Timeout

The requirements identified in this subsection apply to the following:

- SiteMinder Integration
- CA SiteMinder SPS

**Table 4: SSOi Session Timeout Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. Centralized Enterprise Single Sign-On – Internal (SSOi): Provide a capability to allow a user to sign on once to an application, then allow the user to access another application		
12.0	IAM Central Login Page: Error messages for SiteMinder integration	When the SSOi user session has timed out due to inactivity, IAM SSOi shall respond to a user's attempt to interact with the integrated application by forwarding the user to the IAM Central Login Page with the target of the integrated application. The IAM Central Login Page shall display a message: "Your IAM SSO session timed out due to inactivity. Please log in again and you will be returned to your application."

### 2.6.2.3 IAM Authenticated Landing Page and IAM Logged Off Page

The requirements identified in this subsection apply to the following:

- SiteMinder Integration
- CA SiteMinder SPS

**Table 5: SSOi Authenticated Landing Page Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. Centralized Enterprise Single Sign-On – Internal (SSOi): Provide a capability to allow a user to sign on once to an application, then allow the user to access another application		
12.0	IAM Central Login Page: IAM Authenticated Landing Page: for SiteMinder Integration	Application logout may be configured to not log the user out SSOi. In these cases, after application logout, the user shall be redirected to the IAM Authenticated Landing Page. Refer to Figure 2 below.
		The IAM Authenticated Landing Page shall have the same header and footer Government warning and Help Desk information as the IAM Central Logon Page.
		The IAM Authenticated Landing Page shall contain the following text: “You have been logged out of [URL of referring application].”
		The IAM Authenticated Landing Page shall contain the following text: “You can navigate to another application protected by IAM SSOi without logging in. If you are done, you can log out of IAM SSOi by clicking the button below.”
		The IAM Authenticated Landing Page shall contain a logout button.
		If the user clicks on the Logout button on the IAM Authenticated Landing Page, the user shall be logged out of the SSOi session, and the user shall be taken to the IAM Logged Out Page. Refer to Figure 3 below.

BRD BN	Requirement	In-Scope Requirement Clarification
	IAM Central Login Page: IAM Logged Out Page	<p>The IAM Logged Out Page shall contain the following text:</p> <p>“You are logged out of IAM Single Sign-On – Internal (SSOi). If you navigate to an applicaton, you will be asked to log in again.”</p> <p>The IAM Logged Out Page shall have the same header and footer Government warning and Help Desk information as the IAM Central Logon Page.</p>

UNITED STATES  
DEPARTMENT OF VETERANS AFFAIRS

Home Contact Us

**VA Identity and Access Management System (IAM)**

**You are logged in to IAM Single Sign On Internal (SSOi)**

You have been logged out of [URL of referring application]

You can navigate to another application protected by IAM SSOi without logging in.

If you are done, you can log out of IAM SSOi by clicking the button below

**Logout**

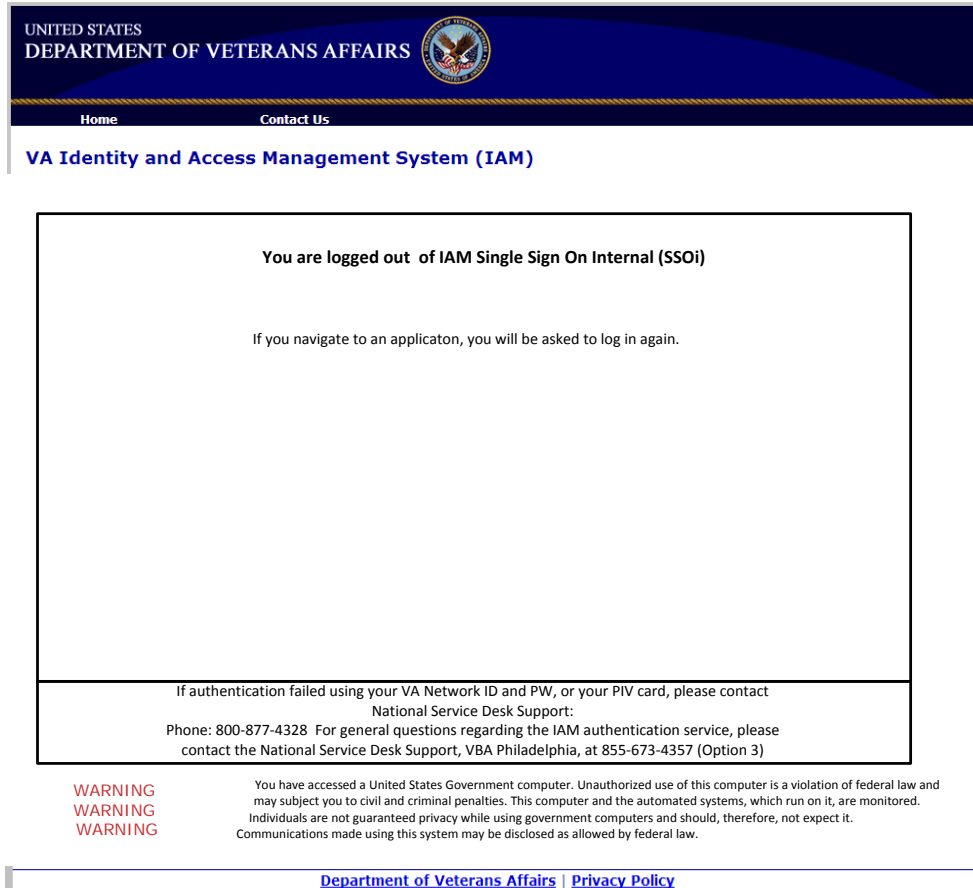
If authentication failed using your VA Network ID and PW, or your PIV card, please contact  
National Service Desk Support:  
Phone: 800-877-4328 For general questions regarding the IAM authentication service, please  
contact the National Service Desk Support, VBA Philadelphia, at 855-673-4357 (Option 3)

**WARNING**  
**WARNING**  
**WARNING**

You have accessed a United States Government computer. Unauthorized use of this computer is a violation of federal law and may subject you to civil and criminal penalties. This computer and the automated systems, which run on it, are monitored. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. Communications made using this system may be disclosed as allowed by federal law.

Department of Veterans Affairs | Privacy Policy

**Figure 2: IAM Authenticated Landing Page**



**Figure 3: IAM Logged Out Page**

#### 2.6.2.4 IAM Standard SSOi Authorization Traits

**Table 6: SSOi Standard Authorization Traits Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. Centralized Enterprise Single Sign-On – Internal (SSOi): Provide a capability to allow a user to sign on once to an application, then allow the user to access another application		
12.0	IAM Standard SSOi Authentication Traits	Provide a standard set of SSOi authentication traits for SSOi user sessions and STS tokens Refer to <a href="#">Appendix B</a>



### 2.6.2.5 STS Support of AD/Kerberos Token Exchange

**Table 7: SSOi Support of AD/Kerberos Token Exchange Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
BRD BN12. Centralized Enterprise Single Sign-On – Internal (SSOi): Provide a capability to allow a user to sign on once to an application, then allow the user to access another application		
12.0	STS support of AD/Kerberos token exchange	The STS Service shall support the receipt of an AD/Kerberos token as the basis for the creation of an STS token.

### 2.6.3 Specialized Access Control

The Specialized Access Control (SAC) service provides fine-grained and attribute-based access control for protected VA applications. SAC enhances information security by providing the ability to make fine-grained access control decisions based on predefined policies and authorization attributes (user, resource, transaction, contextual etc.). This capability relieves the need for customized coding within individual applications to perform these functions.

SAC provides the capability to make access control decisions when a user attempts to access protected information within VA applications. Once an access control decision is made, the user is either permitted or denied access to the requested resource.

SAC is considered a single system and is made up of several components that provide specific functionality, which is explained in the following:

- **Policy Enforcement Point (PEP):** The PEP intercepts a user's access request to an application and forwards it to the decision point, which produces an access control decision. Once a decision is made, the PEP receives the decision from the Policy Decision Point (PDP) and enforces it on the application. The PEP can alternatively reside on the consuming application's side and it would delegate to the PDP when it requires an access control decision.
- **Policy Decision Point (PDP):** The PDP receives access control requests from the PEP and, in turn, requests the attributes and policies necessary to make access control decisions. Once attributes and policies are obtained, the PDP evaluates them to make an access control decision, which is sent to the PEP. The PDP returns one of the following decisions: **Permit**, **Deny**, **Indeterminate**, or **Not Applicable**.
- **Policy Administration Point (PAP):** The PAP is used to create and manage policies, which are stored in internal or external policy stores.
- **Policy Information Point (PIP):** A PIP is a store that holds authorization attributes, and is consulted by the PDP during policy evaluation.
- **Context Handler:** The Context Handler mediates traffic between the SAC components. It is eXtensible Access Control Markup Language (XACML) functionality that converts decision requests in the native request format into an XACML-recognized format, and

converts authorization decisions in the XACML-recognized format to the recipient's native response format.

SAC leverages the following services as a part of fulfilling its activities:

- Virtual Directory Service (VDS): IAM AcS VDS serves as a virtual PIP by integrating with a variety of authoritative attribute stores. It provides the PDP authorization attributes pertaining to an access control request. **Note:** VDS may be integrated with any data store(s) required by consuming applications as they are onboarded.
- Policy Service (PS): The PS retrieves access control policies from a variety of policy stores that are internal or external to the SAC service. It receives requests from the PDP for an access policy pertaining to an access control request made by a user. The PS then searches for and returns the applicable policy to the PDP for evaluation.
- Integrates with the Compliance Audit and Reporting (CAR) service to support expanded compliance audit and reporting capabilities. Information regarding compliance audit and reporting features, functionality, reports, and user interfaces is provided within the CAR-related subsections of this document.

Currently, the SAC service provides the following capabilities:

- Integrates with the NwHIN/eHealth based access control artifacts to provide fine-grained access control to protect Veterans' medical information while making it accessible to those who need it. When an external partner attempts to retrieve clinical information from VA over NwHIN/eHealth, SAC is consulted for access Control Decisions. SAC is provided authorization attributes such as requestor organization identifier, patient identifier, and patient preferences for data sharing. The decision is made by evaluating these attributes against the appropriate access control policies, in this case, the eHealth Policy.

A new tool that provides a more robust authorization capability was acquired and implemented with AcS 2.0 Increment 2.

**Table 8: Specialized Access Control Business Needs and Requirements Enhancements**

BRD BN	Requirement	In-Scope Requirement Clarification
CR 2052	The SAC Service shall be XACML 3.0 compliant for Policy Administration Points (PAPs), Policy Information Points (PIPs), Policy Enforcement Points (PEPs), and Policy Decision Points (PDPs) to fully use policies and attributes to make fine-grained authorization decisions as a service. To support the transition to the XACML 3.0 standard, the SAC Service shall support XACML 2.0 messaging from the NwHIN/eHealth exchange PEP.	

## 2.6.4 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.

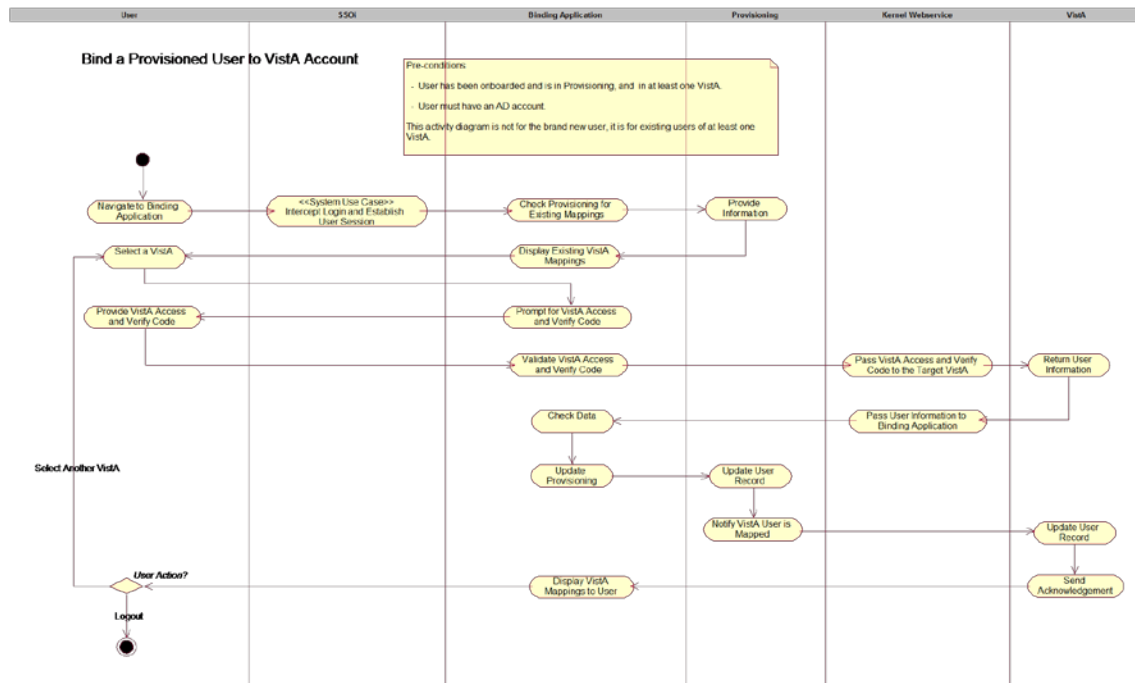
In anticipation of a service request to integrate the Provisioning service with Veterans Health Information Systems and Technology Architecture (VistA), there is a need to deploy a standards-based web service to manage the VistA New Person file. Additionally, a new IAM Binding application will facilitate the mapping of a user to the various VistA sites. A future iRSD will identify the detailed requirements pertaining to the integration between Provisioning and VistA.

**Table 9: Provisioning Business Needs and Requirements Enhancements**

<b>BRD BN</b>	<b>Requirement</b>	<b>In-Scope Requirement Clarification</b>
3.0 Digital Identity Lifecycle Management Onboarding/Offboarding: Provide a digital process of establishing and maintaining the attributes that make up an individual digital identity and support general updates to an identity such as a name change or biometric update.		
3.0	Deploy a standards-based web service to manage VistA access.	The Provisioning Service shall deploy a Service Provisioning Markup Language (SPML) web service to provisioning/deprovision users to Veterans Health Information Systems and Technology Architecture (VistA).

BRD BN	Requirement	In-Scope Requirement Clarification
		The SPML Service shall call the VistA New Person Web Service to create/enable/disable New Person records and manage key data about the person (e.g., Name, SSN) as well as network identifiers mapped to the DUZ (AD name, SEC ID) when all approvals have been recorded via the Provisioning Service.
		The SPML Service shall receive updates from the VistA New Person Web Service in the event that the New Person File is updated via a mechanism other than the Provisioning Service.
3.0	Third-Party Credential Onboarding Support	The Provisioning Service shall accept a foreign address from AccessVA during registration.
		The Provisioning Service shall collect "Postal Code" as a unique attribute, in place of "ZIP" for foreign addresses from AccessVA during registration.
		The Provisioning Service shall collect "Province/Region" as a unique attribute, in place of "State" for foreign addresses from AccessVA during registration.
		The Provisioning Service shall collect the ISO 3166-1 alpha-3 for the "Country" attribute from AccessVA during registration.
3.0	Deploy an IAM Binding Application	The IAM Binding Application shall leverage the SSOi Service for authentication.
		The IAM Binding Application shall retrieve the list of VistA instances that a user has been mapped from the Provisioning Service.
		The IAM Binding Application shall display a list of VistA instances that the user has been previously mapped.
		The IAM Binding Application shall allow a user to select an additional VistA instance to which the user should be mapped.
		The IAM Binding Application shall prevent the user from selecting a VistA instance to which the user has already been mapped.
		The IAM Binding Application shall prompt the user to enter Access/Verify codes once a new VistA instance has been selected.

BRD BN	Requirement	In-Scope Requirement Clarification
		The IAM Binding Application shall call the Remote Procedure Call (RPC) Broker to validate the Access/Verify codes and retrieve the DUZ.
		The IAM Binding Application shall display an error message to the user prompting the user to reenter Access/Verify codes in the event that the RPC Broker call fails to validate the Access/Verify codes.
		If the Access/Verify codes are valid, the IAM Binding Application shall transmit the new VistA Instance and related data for the user to the Provisioning Service.
		If the Access/Verify codes are valid, the Provisioning Service shall correlate the new VistA Instance with the user's existing Provisioning record.
		If the Access/Verify codes are valid, the IAM Binding Application will include the new VistA instance in the list of mapped instances.
		The IAM Binding Application shall prompt the user to select an additional VistA instance or exit the application.



**Figure 4: Bind a Provisioned User to a VistA Account**

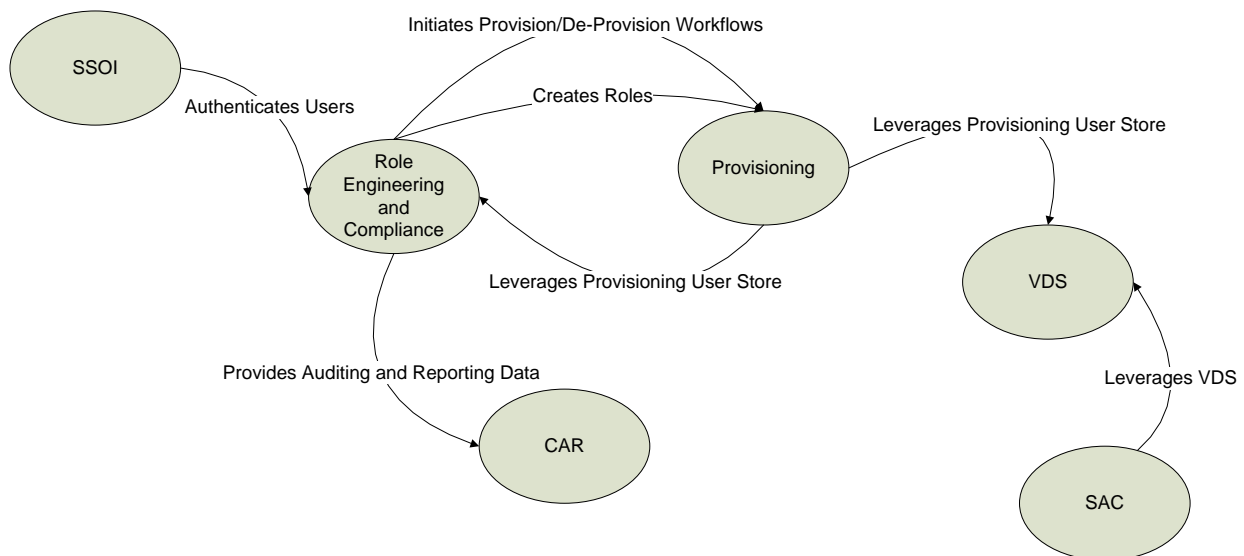
## 2.6.5 Role Engineering and Compliance Tool

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

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

VA has selected the SailPoint IdentityIQ commercial off-the-shelf (COTS) product to fulfill the business needs pertaining to Resource Attribute/Metadata Management. The elaborated requirements in this section represent the core capabilities of this tool. Unless explicitly stated, these requirements are not intended to limit the functions supported by this product.

To fulfill the business need, the Role Engineering and Compliance tool shall be integrated with the existing suite of AcS services that are depicted in Figure 5 below.



**Figure 5: Integration of Role Engineering and Compliance Tool with AcS Services**

Specifically, the Role Engineering and Compliance tool shall be directly integrated with the following services:

- **Single Sign On – Internal (SSOi):** The SSOi service is an authentication service specifically designed for controlling access for VA internal users (employees and contractors) accessing VA applications. The authentication of end user access to the Role Engineering and Compliance tool shall be managed by SSOi.
- **Compliance and Audit Reporting (CAR):** The CAR service provides the ability to proactively monitor potential compliance infractions and incidents in relation to the AcS activities and provides a single compliance auditing and reporting framework to be

leveraged across the VA enterprise. The Role Engineering and Compliance tool shall be integrated with CAR to support the generation of compliance reports, support ad hoc auditing of role mining and certifications, and support logging audit history.

- **Provisioning:** The Provisioning service provides account management for consuming applications based on their user role. To fulfill the vision of the Role Engineering and Compliance tool, the Provisioning user data store shall be used as the authoritative source for the user and their attributes. Additionally, roles defined in the Role Engineering and Compliance tool as a result of Role Mining shall be populated in the corresponding Provisioning Workflows. Entitlement changes resulting from Role Mining and/or User Certification activities shall be performed via an interface between the Role Engineering and Compliance tool and the Provisioning service to invoke the Provision User and De-Provision User workflows as needed.

Lastly, an indirect relationship exists between the Role Engineering and Compliance tool and the SAC service. Entitlement and attribute modifications resulting from Role Mining and/or User Certification activities are reflected in the Provisioning User Data Store and populated in the Virtual Directory Service (VDS). VDS is available to the SAC service when evaluating policies. The interface between Provisioning, VDS, and SAC has been implemented.

The following table identifies the elaborated requirements pertaining to this tool.

**Table 10: Resource Attribute/Metadata Management Business Needs and Requirements Enhancements**

<b>BRD BN</b>	<b>Requirement</b>	<b>In-Scope Requirement Clarification</b>
22. Resource Attribute/Metadata Management: Provide a digital process for establishing and maintaining data (such as rules for access, credential requirements, etc.) for a resource/asset being provisioned to define the access, protection, and handling controls.		
22.01	The Resource/Metadata Management service shall provide a means to support Data management for all types of user access authorizations inclusive of both Logical Access Controls and Specialized Access Controls.	The Role Engineering and Compliance tool shall interface with the Provisioning Service to add roles discovered during role mining activities.
		The Role Engineering and Compliance tool shall interface with the Provisioning Service to invoke the Provision User and Deprovision User use cases add, change, or remove user privileges resulting from the role mining and certification activities.

<b>BRD BN</b>	<b>Requirement</b>	<b>In-Scope Requirement Clarification</b>
22.02	System shall provide an easy-to-use GUI interface through which authorized administrators can view the current entitlements of their respective application(s).	The Role Engineering and Compliance tool shall consume the SSOi Service to control access for VA internal users (employees and contractors).
22.03	System shall have the ability to discover relationships between users based on similar access permissions that can logically be grouped to form a role.	The Role Engineering and Compliance tool shall identify entitlement commonalities of integrated application users and present these commonalities on the GUI.
		The Role Engineering and Compliance tool shall leverage the Provisioning User Data Store as the authoritative source for user attributes.
		The Role Engineering and Compliance tool shall allow an authorized user to create roles discovered through the systematic analysis of entitlement commonalities.
		The Role Engineering and Compliance tool shall allow a user to create a container role, which can be used to group discovered roles and entitlements.
		The Role Engineering and Compliance tool shall interface with the Provisioning Service to add roles discovered during role mining activities.
		The Provisioning Service shall deploy a service to update the Provision and Modify workflows to add roles discovered during the role mining activity.
22.04	System shall have the ability to support the cleanup of excessive or unnecessary user privileges.	The Role Engineering and Compliance tool shall interface with the Provisioning Service to invoke the Provision User and Deprovision User use cases add, change, or remove user privileges resulting from the role mining and certification activities.
		The Role Engineering and Compliance tool shall not directly provision or deprovision a user's entitlements to an integrated



BRD BN	Requirement	In-Scope Requirement Clarification
		application. Provision and deprovision actions identified within the Role Engineering and Compliance tool shall be performed via the interface with the Provisioning service.
		The Provisioning Service shall deploy a service to initiate the Provision, Modify, Deprovision workflows.
22.05	System shall have the ability to discover application roles.	The Role Engineering and Compliance tool shall leverage the Provisioning User Data Store as the authoritative source for user attributes.
22.06	System shall provide the capability to create roles manually.	The Role Engineering and Compliance tool shall interface with the Provisioning Service to add manually created roles.
		The Role Engineering and Compliance tool shall not directly provision or deprovision a user's entitlements to an integrated application. Provision and deprovision actions identified within the Role Engineering and Compliance tool shall be performed via the interface with the Provisioning service.
		The Provisioning Service shall deploy a service to update the Provision and Modify workflows to add manually created roles.
22.07	System shall provide the capability to refine and approve roles.	The Role Engineering and Compliance tool shall allow an authorized user to modify attribute filters and re-run role mining analysis.
		The Role Engineering and Compliance tool shall allow an authorized user to group entitlements into a role.
		The Role Engineering and Compliance tool shall execute an approval workflow for new and modified roles prior to publishing the roles to the Provisioning Service.

<b>BRD BN</b>	<b>Requirement</b>	<b>In-Scope Requirement Clarification</b>
		The Role Engineering and Compliance tool shall allow an authorized user to identify role approvers.
		The Role Engineering and Compliance tool shall allow an authorized user to customize the role approval workflow.
22.08	System shall provide a visual representation of roles, constraints, and hierarchies.	The Role Engineering and Compliance tool shall provide a GUI that presents the hierarchical relationship between various roles and their associated entitlements as well as role inheritance.
		The Role Engineering and Compliance tool shall display roles in a top-down, bottom-up, or grid format.
22.09	System shall support efficient sorting through extremely large volumes of user and privilege information in order to discover potential roles.	The Role Engineering and Compliance tool shall display roles in a top-down, bottom-up, or grid format.
		The Role Engineering and Compliance tool shall allow an authorized user to specify one or more applications to evaluate as well as the set of identity attributes that can be used to filter the role mining results.
		The Role Engineering and Compliance tool shall allow an authorized user to specify the minimum number of identities associated with a mined role.
		The Role Engineering and Compliance tool shall allow an authorized user to specify the minimum number of entitlements associated with a mined role.
		The Role Engineering and Compliance tool shall allow an authorized user to specify the maximum number of groups to mine.
22.10	System shall provide the capability for an administrator to re-certify privileges on a pre-defined basis.	The Role Engineering and Compliance tool shall allow an authorized user to specify the parameters of an access review.

BRD BN	Requirement	In-Scope Requirement Clarification
		The Role Engineering and Compliance tool shall allow an authorized user to specify the scheduling and frequency of an access review.
22.11	System shall provide the capability to establish and enforce a consistent set of identity compliance policies to minimize the security and privacy risk.	The Role Engineering and Compliance tool shall allow an authorized user to define risk profiles regarding number of entitlements to be evaluated during an access review.
22.12	System shall be capable of implementing policy business process rules.	The Role Engineering and Compliance tool shall allow an authorized user to define role based policies (e.g., least privilege, need to know, separation of duties) evaluated during an access review.
22.13	System shall be capable of executing and automating compliance verification.	The Role Engineering and Compliance tool shall perform an access review on-demand or at a frequency defined by an authorized user.
		The Role Engineering and Compliance tool shall send notification to role certifiers (e.g., managers, application owners) when an access review is being executed.
		The Role Engineering and Compliance tool shall send notifications to users whose access will be modified as a result of an access review when a challenge phase has been specified.
		The Role Engineering and Compliance tool shall allow an authorized user to define reminder and escalation notifications.
		The Role Engineering and Compliance tool shall use the Manager/Supervisor attribute in the Provisioning User Data Store when conducting Manager Level Role Certification.
22.14	System shall be capable of supporting the generation of compliance reports.	<p>The Role Engineering and Compliance tool shall integrate with the CAR Service for continuous updating. The reports shall include:</p> <ul style="list-style-type: none"> <li>• Policy Violations</li> </ul>

BRD BN	Requirement	In-Scope Requirement Clarification
		<ul style="list-style-type: none"> <li>• High Risk Users</li> <li>• Certification Progress</li> <li>• Certification Status</li> </ul>
22.15	System shall be capable of facilitating the cleanup of data imported via sorting and clustering.	The Role Engineering and Compliance tool shall allow certifiers to create filters to display certification results.
		The Role Engineering and Compliance tool shall allow certifiers to sort certification results.
22.16	System shall support pattern-based audits.	The Role Engineering and Compliance tool shall integrate with the CAR Service to enable ad hoc auditing of role mining and certifications.
22.17	System shall be capable of logging audit history.	The Role Engineering and Compliance tool shall store audit log locally in a format compatible with CAR.
22.19	System shall support certification campaigns to verify that granted privileges comply with business and regulatory needs, and are not over-allocated.	The Role Engineering and Compliance tool shall allow an authorized user to define risk profiles regarding number of entitlements to be evaluated during an access review.
		The Role Engineering and Compliance tool shall allow an authorized user to define role based policies (e.g., least privilege, need to know, separation of duties) evaluated during an access review.
22.20	System shall provide a dashboard that displays a graphical overview of all entries (users, resources and roles, and constraints) in a configuration along with the connections between them.	The Role Engineering and Compliance tool shall provide a dashboard that allows authorized users to personalize with drag-and-drop formatting and content selection.
		<p>The dashboard shall provide the following capabilities:</p> <ul style="list-style-type: none"> <li>• Notify users of required actions with visual alerts</li> <li>• Provide one-click entry into access request, password management and compliance activities</li> <li>• Deliver at-a-glance charts, graphs and</li> </ul>

BRD BN	Requirement	In-Scope Requirement Clarification
		reports with drill-down capabilities <ul style="list-style-type: none"> <li>• Highlight scheduled compliance events and the status of in-process tasks</li> </ul>
22.21	System shall support the import and export of configuration data.	The Role Engineering and Compliance tool shall allow certifications to be defined and performed via a scripted process.
		The Role Engineering and Compliance tool shall allow an authorized user to import an application's roles via a direct load process.
22.22	System shall be capable of being configured through various configuration data formats.	The Role Engineering and Compliance tool shall allow an authorized user to configure an application via the importation of a delimited file.
		The Role Engineering and Compliance tool shall allow an authorized user to import rules defined in an XML file.
22.23	System shall support connections to various backend data sources.	The Role Engineering and Compliance tool shall leverage connectors to interface with applications on the VA network.
22.24	System shall support various data file formats.	The Role Engineering and Compliance tool shall import delimited files and XML files and other formats as deemed necessary.
22.25	System shall support general extensions.	The Role Engineering and Compliance tool shall support definition of extended attributes as needed by consuming application integration.
		The Role Engineering and Compliance tool shall allow extended attributes to be designated as searchable.
22.26	System shall provide a job scheduling function.	The Role Engineering and Compliance tool shall allow an authorized user to specify the scheduling and frequency of an access review.
22.27	System shall be capable of preventing the creation of new roles with almost the same membership and entitlements of existing roles.	The Role Engineering and Compliance tool shall allow an authorized user to identify overlaps between roles based upon role assignment and provisioned entitlements.

BRD BN	Requirement	In-Scope Requirement Clarification
		The Role Engineering and Compliance tool shall allow an authorized user to modify the entitlements for discovered overlaps between roles.

## 2.7 Graphical User Interface (GUI) Specifications

The graphical user interface (GUI) specifications include the following:

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

## 2.8 Multi-divisional Specifications

There are no specific multi-divisional specifications for this document.

## 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.

<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. Provisioning supports 500,000 onboarding / offboarding requests per day.
- b. The provisioning repository / data store supports 10 million queries per day (300,000 from the VistA Evolution program).
- c. 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.
- d. SAC supports 325,000 transactions per day.
- e. Virtual Directory supports [VAAFI usage](#).
- f. SSOi shall support 20 million authentications per day.
- g. VDS shall support 20 million authentications by SSOi per day.
- h. The IAM Binding Application shall support 1 million authentications per day.
- i. SSOi shall be able to handle an increase of 1 million users with integration to VistA.
- j. The IAM Binding Application shall support 1 million users.
- k. VDS shall support an additional 1 million users with integration to VistA.
- l. 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.
- m. The online procedures prompted from a user interface execute under five seconds with an average of four seconds within the budgeted resource utilization constraints.
- n. The metric data indicating the performance characteristics of the system to support application monitoring is provided.
- o. The system supports 24/7/365 operations. Help desk support is provided from 7 a.m. to 7 p.m. EST.
- p. The desired system behavior is maintained at various load levels.
- q. The system response times and page load times are consistent (or better) with current system baselines and support the following:

Service	Response Times
CSP	Average response time of five seconds and a maximum response time of ten seconds
IP	Average response time of five seconds and a maximum response time of ten seconds
Provisioning	Average response time of five seconds and a maximum response time of ten seconds
SAC	Average response time of 500 milliseconds or less
CAR	Data must be returned at no more than 1 minute for every 10,000 records
e-Signature	Average response time of five seconds and a maximum response time of ten seconds

## 2.10 Quality Attributes Specification

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

- Unit testing
- Integration / functional testing
- User acceptance testing (UAT)
- Section 508 testing
- Performance testing

The AcS solution also consists of the following quality specifications:

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

## 2.11 Reliability Specifications

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

<b>Service Availability Level 4</b>	
<b>*Standards adopted from specification created by Application Structure and Integration Services (ASIS).</b>	
<b>Description</b>	Mission Critical Information
<b>Minimum Availability</b>	99.9%
<b>Maximum Downtime Per Month</b>	43 minutes
<b>Business Value</b>	Essential to fundamental business operations – outage seriously impairs functioning of business.
<b>System Response</b>	In the absence of any system superseding requirements, the system responds to user actions in three seconds or less in 90% of the attempts, and never more than 10 seconds.
<b>Operational Hours</b>	Required 24 hours a day, every day.
<b>Significant Outage</b>	More than five minutes of downtime is considered significant at any time and requires an ANR to be sent out



<b>Service Availability Level 4</b> <b>*Standards adopted from specification created by Application Structure and Integration Services (ASIS).</b>	
	to the appropriate teams.
<b>Outage Impact</b>	Interruption of service may result in severe financial, regulatory, patient safety, patient health, or other business issues.
<b>Scheduled Maintenance</b>	Maintenance, including maintenance of externally developed software incorporated into the IAM system, is scheduled during off-peak hours (evenings and weekends) or in conjunction with relevant maintenance schedules.

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

## 2.12 Scope Integration

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

## 2.13 Security Specifications

The security specifications include the following:

- AcS is deployed inside the VA firewall.
- AcS conforms to the VA security standards detailed in VA Handbook 6500 Information Security Program.
- Designated ports are opened between systems. All other ports are blocked to provide secure server-to-server communication.
- The Hypertext Transfer Protocol Secure (HTTPS) communication protocol is used for outbound and inbound traffic for external-facing applications.
- AcS communication channels are TLS/SSL-enabled and -encrypted.
- The AcS data layer is within the internal firewall zone to provide security of the data.
- AcS meets all 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 PII or sensitive information such as passwords in an encrypted or one-way hashed format and on the Secure Socket Layer (SSL) channel.

- The web servers providing access to VA applications for external users over the Internet must reside in the 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 [Continuous Readiness in Information Security Program \(CRISP\)](#).
- The system integrates with VA business applications (as determined feasible) across heterogeneous environments and platforms.

## 3 Applicable Standards

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

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

**Table 11: 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>
<a href="#">VA Directive 6500; Information Security Program</a>
VA Directive 6501; VA Identity Verification In-Person Proofing (IPP) Process
<a href="#">World Wide Web Consortium (W3C) SOAP Standard</a>
<a href="#">World Wide Web Consortium (W3C) XML Standard</a>
FICAM Roadmap and Implementation Guidance
OMB 04-04 E-Authentication Guidance for Federal Agencies
Aligns with the VA Enterprise Shared Services directive and strategy
Supports <a href="#">HSPD-12</a> specifications where applicable (i.e., Personal Identification Verification (PIV))
Follows the documentation specifications provided by the <a href="#">ProPath website</a> and VA Program Management Accountability System (PMAS)
<a href="#">6102 Handbook and the VA Web Best Practices Guide</a>
<a href="#">Approved and In-Process Devices</a>
<a href="#">Screen Resolution for Mobile Devices</a>

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

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

## **4 Interfaces**

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

### **4.1 Communications Interfaces**

The following documents provide information regarding communications interfaces:

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

### **4.2 Hardware Interfaces**

The VA AcS Solution SDD provides information regarding hardware interfaces.

### **4.3 Software Interfaces**

The VA AcS Solution SDD provides information regarding software interfaces.

### **4.4 User Interfaces**

The user interfaces are described in section 2.7 and section 2.14.

## **5 Legal, Copyright, and Other Notices**

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

## **6 Purchased Components**

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

## **6.1 Defect Source (TOP 5)**

Not applicable

## **7 User Class Characteristics**

The user community consists of the following classes:

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

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

- A technical training curriculum is developed and delivered to all levels of staff users. This may include user guidelines, in-person training, and computer-based training.
- The training curriculum states the expected task completion time for primary and secondary users.

## **8 Estimation**

The estimation information is not available at this time.

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

## Application

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

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

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

**Figure 6: Cumulative Probability (“S-curve”) Chart**

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

## 9 Approval Signatures

REVIEW DATE: <date>

SCRIBE: <name>

Signed:



Approval\_Mike\_Mims  
.msg

05/19/2014



Integrated Project Team (IPT) Chair

Date



Approval\_David\_Wulf  
f.msg

05/12/2014



, Business Sponsor, IAM BPMO

Date



Approval\_Jeff\_Podol  
ec.msg

05/09/2014



IAM Program Manager

Date



Approval\_Jerry\_Wha  
rton.msg

05/13/2014



, AcS Project Manager

Date

## **Appendix A Use Case Specification**

Not applicable

### **A.1. Use Case Name**

Not applicable

### **A.2. Brief Description**

Not applicable

### **A.3. Use Case Trigger**

Not applicable

### **A.4. Use Case Context Diagram**

Not applicable

### **A.5. Use Case Actors**

Not applicable

### **A.6. Preconditions**

Not applicable

#### **A.6.1. Precondition 1**

Not applicable

### **A.7. Basic Flow of Events**

Not applicable

#### **A.7.1. First Step of Basic Flow**

Not applicable

### **A.8. Alternative Flows**

Not applicable

#### **A.8.1. First Alternative Flow**

Not applicable

#### **A.8.2. Second Alternative Flow**

Not applicable

### **A.9. Sub Flows**

Not applicable

#### **A.9.1. First Subflow**

Not applicable

## **A.9.2. Second Subflow**

Not applicable

## **A.10. Postconditions**

Not applicable

### **A.10.1. Post Condition One**

Not applicable

## **A.11. Special Specifications**

Not applicable

### **A.11.1. First Special Specification**

Not applicable

## **A.12. Extension Points**

Not applicable

### **A.12.1. Name of Extension Point**

Not applicable



## Appendix B IAM Standard SSOi Authentication Traits

Table 12: SSOe-SSOi User Session

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
<b>Attribute Statement</b>					NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
<b>Communication</b>					
	Application/User Session Scope of Service	Name="sessionScope"		Self-Service, Business	The Scope of Service attribute is intended to bind the user's interaction with backend systems to a self-service or business type of request.  How to determine: Statically defined in Token Policy Allow application to pass in
	Transaction ID	Name="transactionId"			SourceSystem_TransactionIdNumber
	Issue/Auth Instant	Name="issueInstant"			Issue or authentication instant time (Zulu based)
<b>Authentication</b>					
	Authenticating System	Name="authnSystem"		SSOe, SSOi, Other	The authenticating system that is representing the user to the STS.
	Authentication Type	Name="authnType"		Direct, Indirect	Explains whether the authenticating system authenticated the user in a direct or indirect manner.
	Proofing Authority	Name="proofingAuth"		FICAM, DMDC, DoD-CAC, VA-PIV	The policy authority assuring the initial identity of the user.
	Assurance Level	Name="assurLevel"		LOA-1 thru 4, Proprietary, None	Assurance level as determined by NIST 800-63

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
<b>User Identity</b>					Issue identifying business user from attributes. May need to use calling application scope. Assumes app only support one.
	First Name	Name="firstName"			User's first name
	Last Name	Name="lastName"			User's last name
	SecID	Name="secId"			Unique Provisioning ID correlated with MVI
	ICN	Name="mviIcn"			The MVI unique Enterprise Identifier for each of the VA unique person records; the identifier is called Integration Control Number (ICN).
	CSID/PID	Name="corpId"			Person ID (Corporate DB)
	DODEDIPNID	Name="dodEdiPnId"			DoD EDI Person Identifier of individual (if known)
	AD samAccountN ame	Name="adSamAccountN ame"			
	AD UPN	Name="adUpn"			
		Name="adEmail"			

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	SubjectId			<pre>&lt;saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject-id"&gt; &lt;saml:AttributeValue&gt;Walter H.Brattain IV&lt;/saml:AttributeValue&gt; &lt;/saml:Attribute&gt;</pre>	<p>The Nationwide Health Information Network uses the XSPA namespace for subject-id attribute. The primary purpose of this identifier is for display and logging. This XSPA identifier should not be confused with the subject-id identifier from the XACML namespace identifier which is intended for a different purpose.</p> <p>This attribute can be built based on MVI/CSP firstName and lastName.</p>
	Subject Role	Name="urn:oasis:names:tc:xacml:2.0:subject:role"			<p>Surrogate Information: for example, Acting on behalf of. Or is this a business issues and only Acting as Surrogate is needed.</p> <p>DSLogon could have Surrogate and SurgtOnBehalfOf = EDIPI Best to extend but How? Role within own VA namespace. Apps can work in either or both namespaces.</p> <pre>&lt;Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="46255001" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT" displayName="Pharmacist"/&gt;</pre>

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Subject Organization	Name="urn:oasis:names: tc:xspa:1.0:subject:organ ization"		<saml:AttributeValue>F amily Medical Clinic</saml:AttributeVal ue>	In plain text, the organization that the user belongs to as required by HIPAA Privacy Disclosure Accounting shall be placed in the value of the <AttributeValue> element.
	Subject Organization ID	Name="urn:oasis:names: tc:xspa:1.0:subject:organ ization-id"			A unique identifier for the organization that the user is representing in performing this transaction shall be placed in the value of the <AttributeValue> element. This organization ID shall be consistent with the plain-text name of the organization provided in the User Organization Attribute. The organization ID may be an Object Identifier (OID), using the urn format (that is, "urn:oid:" appended with the OID); or it may be a URL assigned to that organization.

**Table 13: SSOe-SSOi STS – Indirect**

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
<b>SAML Identifiers</b>					
	Issuer			Name of STS; for example, sts.ssoe.va.gov	Issuer of the assertion. Default format shall be urn:oasis:names:tc:SAML:2.0:nameid-format:entity
	Subject			Subject of Statements below. For example: user@va.gov, vhamaster/vhaiswname, cn=john.doe,ou=vha,o=va,c=us	SAML defines subject as entity of assertion reference. Shall use Name Identifier Formats as specified in SAML Core 2.0 specification.  NameID one of: transient, persistent, unspecified
	Subject::SubjectConfirmation@method			method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"	For PKI direct auth: Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"
	Subject::SubjectConfirmation::SubjectConfirmationData@Recipient			Recipient="Service-Domain-Org-URI"	The Recipient attribute has been set to the value of the STS ApplieTo for the request. Using this value here ensures that the relying party or another party cannot redirect/replay this assertion to another endpoint so long as the relying party checks the attribute against its own location/identifier. The enforcement of this attribute is therefore dependent on the relying party and not the STS.

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Subject::SubjectConfirmation::SubjectConfirmationData@Address			Address="DNS Address of Requestor"	The Address attribute is set to a value that binds the token to the requestor. Using this value here helps to limit the use by another party so long as the relying party checks the attribute against its own acceptable usage scenarios. The enforcement of this attribute is therefore dependent on the relying party and not the STS.
	Conditions@NotBefore/NotOnOrAfter			15 minute duration	
	Conditions@Audience Restriction				SAML 2.0: A condition specifying the audience to which this assertion may be deemed valid. Here it is used for two reasons: 1) to clearly address the party/parties to which the requestor and issuer agreed that this assertion is valid and useable 2) as an indicator to an STS that an audience member may perform additional actions, such as requesting a derived token, with this assertion.

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Conditions@OneTime Use				SAML 2.0: A condition that indicates that a relying party should only accept this assertion once. Per the SAML spec, "a relying party should maintain a cache of the assertions it has processed containing such a condition. Whenever an assertion with this condition is processed, the cache should be checked to ensure that the same assertion has not been previously received and processed by the relying party." The enforcement of this condition is therefore dependent on the relying party and not the STS
	Advice		Optional		Possible use for sharing SSO or other SAML token.
<b>Attribute Statement</b>					NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
<b>Communication</b>					
	Application/User Session Scope of Service	Name="sessionScope"		Self-Service, Business	<p>The Scope of Service attribute is intended to bind the user's interaction with backend systems to a self-service or business type of request.</p> <p>How to determine: Statically defined in Token Policy Allow application to pass in</p>

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Transaction ID	Name="transactionId"			SourceSystem_TransactionIdNumber
	Issue/Auth Instant	Name="issueInstant"			Issue or authentication instant time (Zulu based)
<b>Authentication</b>					
	Authenticating System	Name="authnSystem"		SSOe, SSOi, Other	The authenticating system that is representing the user to the STS.
	Authentication Type	Name="authnType"		Direct, Indirect	Explains whether the authenticating system authenticated the user in a direct or indirect manner.
	Proofing Authority	Name="proofingAuth"		FICAM, DMDC, DoD-CAC, VA-PIV	The policy authority assuring the initial identity of the user.
	Assurance Level	Name="assurLevel"		LOA-1 thru 4, Proprietary, None	Assurance level as determined by NIST 800-63
<b>User Identity</b>					Issue identifying business user from attributes. May need to use calling application scope. Assumes app only support one.
	First Name	Name="firstName"			User's first name
	Last Name	Name="lastName"			User's last name
	SecID	Name="secId"			Unique Provisioning ID correlated with MVI



Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	ICN	Name="mvilcn"			The MVI unique Enterprise Identifier for each of the VA unique person records; the identifier is called Integration Control Number (ICN).
	CSID/PID	Name="corpld"			Person ID (Corporate DB)
	DODEDIPNID	Name="dodEdiPnId"			DoD EDI Person Identifier of individual (if known)
	AD samAccountName	Name="adSamAccountName"			
	AD UPN	Name="adUpn"			
	AD Email	Name="adEmail"			
	SubjectId			<pre>&lt;saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id"&gt; &lt;saml:AttributeValue&gt;Walter H.Brattain IV&lt;/saml:AttributeValue&gt; &lt;/saml:Attribute&gt;</pre>	<p>The Nationwide Health Information Network uses the XSPA namespace for subject-id attribute. The primary purpose of this identifier is for display and logging. This XSPA identifier should not be confused with the subject-id identifier from the XACML namespace identifier which is intended for a different purpose.</p> <p>This attribute can be built based on MVI/CSP firstName and lastName.</p>

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Subject Role	Name="urn:oasis:names:tc:xacml:2.0:subject:role"			<p>Surrogate Information: for example, Acting on behalf of. Or is this a business issues and only Acting as Surrogate is needed.</p> <pre>&lt;Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="46255001" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT" displayName="Pharmacist"/&gt;</pre>
	Subject Organization	Name="urn:oasis:names:tc:xspa:1.0:subject:organization"		<saml:AttributeValue>Family Medical Clinic</saml:AttributeValue>	In plain text, the organization that the user belongs to as required by HIPAA Privacy Disclosure Accounting shall be placed in the value of the <AttributeValue> element.

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Subject Organization ID	Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"			A unique identifier for the organization that the user is representing in performing this transaction shall be placed in the value of the <AttributeValue> element. This organization ID shall be consistent with the plain-text name of the organization provided in the User Organization Attribute. The organization ID may be an Object Identifier (OID), using the urn format (that is, "urn:oid:" appended with the OID); or it may be a URL assigned to that organization.

Table 14: SSOi STS – Direct

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
<b>SAML Identifiers</b>					
	Issuer			Name of STS; for example, sts.ssoe.va.gov	Issuer of the assertion. Default format shall be urn:oasis:names:tc:SAML:2.0:nameid- format:entity
	Subject			Subject of Statements below. For example: user@va.gov, vhamaster/vhaiswname, cn=john.doe,ou=vha,o=va,c= us	SAML defines subject as entity of assertion reference. Shall use Name Identifier Formats as specified in SAML Core 2.0 specification.  NameID one of: transient, persistent, upspecified
	Subject::Subject Confirmation@method			method="urn:oasis:names:tc: SAML:2.0:cm:sender- vouches"	For PKI direct auth: Method="urn:oasis:names:tc:SAML:2.0:cm: bearer"
	Subject::Subject Confirmation::SubjectConfirmationData				May use "urn:oasis:names:tc:SAML:2.0:cm:holder- of-key" in some scenarios. See FICAM SAML 2.0 specifications.
	Subject::Subject Confirmation::SubjectConfirmationData@Recipient			Recipient="Service-Domain- Org-URI"	The Recipient attribute has been set to the value of the STS ApplieTo for the request. Using this value here ensures that the relying party or another party cannot redirect/replay this assertion to another endpoint so long as the relying party checks the attribute against its own location/identifier. The enforcement of this attribute is therefore dependent on the relying party and not the STS.

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Subject::Subject Confirmation::SubjectConfirmationData@Address			Address="DNS Address of Requestor"	The Address attribute is set to a value that binds the token to the requestor. Using this value here helps to limit the use by another party so long as the relying party checks the attribute against its own acceptable usage scenarios. The enforcement of this attribute is therefore dependent on the relying party and not the STS.
	Conditions@Not Before/NotOnOr After			15 minute duration	
	Conditions@Aud ienceRestriction				SAML 2.0: A condition specifying the audience to which this assertion may be deemed valid. Here it is used for two reasons: 1) to clearly address the party/parties to which the requestor and issuer agreed that this assertion is valid and useable 2) as an indicator to an STS that an audience member may perform additional actions, such as requesting a derived token, with this assertion.

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Conditions@OneTimeUse				SAML 2.0: A condition that indicates that a relying party should only accept this assertion once. Per the SAML spec, "a relying party should maintain a cache of the assertions it has processed containing such a condition. Whenever an assertion with this condition is processed, the cache should be checked to ensure that the same assertion has not been previously received and processed by the relying party." The enforcement of this condition is therefore dependent on the relying party and not the STS
	Advice		Optional		Possible use for sharing SSO or other SAML token.
<b>Attribute Statement</b>					NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
<b>Communication</b>					
	Application/User Session Scope of Service	Name="sessionScope"		Self-Service, Business	The Scope of Service attribute is intended to bind the user's interaction with backend systems to a self-service or business type of request.  How to determine: Statically defined in Token Policy Allow application to pass in
	Transaction ID	Name="transactionId"			SourceSystem_TransactionIdNumber
	Issue/Auth Instant	Name="issueInstant"			Issue or authentication instant time (Zulu based)
<b>Authentication</b>					

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Authenticating System	Name="authnSystem"		SSOe, SSOi, Other	The authenticating system that is representing the user to the STS.
	Authentication Type	Name="authnType"		Direct, Indirect	Explains whether the authenticating system authenticated the user in a direct or indirect manner.
	Proofing Authority	Name="proofingAuth"		FICAM, DMDC, DoD-CAC, VA-PIV	The policy authority assuring the initial identity of the user.
	Assurance Level	Name="assurLevel"		LOA-1 thru 4, Proprietary, None	Assurance level as determined by NIST 800-63
<b>User Identity</b>					Issue identifying business user from attributes. May need to use calling application scope. Assumes app only support one.
	First Name	Name="firstName"			User's first name
	Last Name	Name="lastName"			User's last name
	SecID	Name="secId"			Unique Provisioning ID correlated with MVI
	ICN	Name="mviIcn"			The MVI unique Enterprise Identifier for each of the VA unique person records; the identifier is called Integration Control Number (ICN).
	CSID/PID	Name="corpId"			Person ID (Corporate DB)
	DODEDIPNID	Name="dodEdiPnId"			DoD EDI Person Identifier of individual (if known)
	AD samAccountName	Name="adSamAccountName"			

Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	AD UPN	Name="adUpn"			
	AD Email	Name="adEmail"			
	Subject Role	Name="urn:oasis: names:tc:xacml:2 .0:subject:role"			<p>Surrogate Information: for example, Acting on behalf of. Or is this a business issues and only Acting as Surrogate is needed.</p> <p>DSLogon could have Surrogate and SurgtOnBehalfOf = EDIPI</p> <pre>&lt;Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="46255001" codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT" displayName="Pharmacist"/&gt;</pre>
	Subject Organization	Name="urn:oasis: names:tc:xspa:1. 0:subject:organiz ation"		<saml:AttributeValue>Family Medical Clinic</saml:AttributeValue>	In plain text, the organization that the user belongs to as required by HIPAA Privacy Disclosure Accounting shall be placed in the value of the <AttributeValue> element.



Context	Element/ Attribute	Attribute Name	Optional / Required	Description/Example	Notes
	Subject Organization ID	Name="urn:oasis: names:tc:xspa:1. 0:subject:organiz ation-id"			A unique identifier for the organization that the user is representing in performing this transaction shall be placed in the value of the <AttributeValue> element. This organization ID shall be consistent with the plain-text name of the organization provided in the User Organization Attribute. The organization ID may be an Object Identifier (OID), using the urn format (that is, "urn:oid:" appended with the OID); or it may be a URL assigned to that organization.
<b>Authentication Statement</b>					
	AuthnStateme nt::AuthnInstan t			AuthnInstant="2014-04- 25T14:59:31Z"	This time value is encoded in UTC and follows SAML time value constraints.
	AuthnStateme nt::SessionInd ex				Specifies the index of a particular session between principle identified by the subject and the authenticating authority.
	AuthnContext:: AuthnContextC lassRef			urn:oasis:names:tc:SAML:2.0 :ac:classes:X509	A URI reference identifying an authentication context.

## Template Revision History

Date	Version	Description	Author
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