

Department of Veterans Affairs

Identity and Access Management Access Services 2.0

Requirements Specification Document Increment 2



August 2013

Version 1.1

Revision History

Date	Revision	Description	Author
05/07/13	0.1	Initial Draft	NAME REDACTED
06/15/13	0.2	Compiled Sec 2.6 and Non Functional Requirements	NAME REDACTED
6/24/13	0.3	Compiled anomalies from Peer Review	NAME REDACTED
7/10/13	0.4	Compiled anomalies from Final Review	NAME REDACTED
7/15/13	0.5	Technical Writer Edit/Added BN 1.14 and Req #12 to Section 2.6.5.1 from Final Review.	NAME REDACTED
7/29/13	1.0	Prepared document for 508 compliance and PDF conversion. Inserted email approval signatures. Changed document version number to 1.0.	NAME REDACTED
8/15/13	1.1	Changed to Increment 2 (removed "Release 2" reference). Amended Provisioning Enhancement, CSP/ IP, and eSig requirements (Section 2.6). Approved by the IAM IPT on 8/16/13	NAME REDACTED

Table of Contents

1	Introduction	1
1.1	Purpose.....	1
1.2	Scope	2
1.3	Acronyms and Definitions.....	2
1.3.1	Acronyms	3
1.3.2	Definitions	3
1.4	References.....	3
2	Overall Specifications	5
2.1	Accessibility Specifications.....	5
2.2	Business Rules Specifications	5
2.3	Design Constraints Specifications.....	5
2.4	Disaster Recovery Specifications	5
2.5	Documentation Specifications.....	5
2.6	Functional Specifications.....	5
2.6.1	Single Sign-On – Internal Service	6
2.6.1.1	Single Sign-On – Internal Service for CAC Credential	7
2.6.1.2	Single Sign-On – Internal for Mobile Applications	9
2.6.2	Provisioning – DoD Onboarding	11
2.6.3	Provisioning Service Level Enhancements.....	15
2.6.4	Specialized Access Control	22
2.6.5	CSP and IP.....	38
2.6.5.1	Decoupling CSP and IP.....	38
2.6.5.2	IP Enhancements	47
2.6.6	e-Signature	48
2.7	Graphical User Interface Specifications	51
2.8	Multi-Divisional Specifications	51
2.9	Performance Specifications.....	51
2.10	Quality Attributes Specifications	53
2.11	Reliability Specifications	53
2.12	Scope of Integration.....	54
2.13	Security Specifications	54
2.14	System Features.....	55
2.15	Usability Specifications	55
3	Applicable Standards	55

4	Interfaces	56
4.1	Communications Interfaces	56
4.2	Hardware Interfaces.....	56
4.3	Software Interfaces.....	56
4.4	User Interfaces	56
5	Purchased Components.....	56
6	User Class Characteristics	56
7	Legal, Copyright, and Other Notices	57
8	Estimation	58
Attachment A	Approval Signatures.....	59

List of Figures

Figure 2-1: AcS 2.0 Increment 2 Functional Components for SSOi.....	7
Figure 2-2: CAC User Access to VA Applications	9
Figure 2-3: Mobile Device	11
Figure 2-4: Provisioning – DoD Onboarding.....	13
Figure 2-5: Current e-Signature Service Flow	49
Figure 2-6: e-Signature Service – Name Change Flow.....	50

List of Tables

Table 1-1: Document References.....	3
Table 2-1: SSOi for CAC Business Needs and Requirements.....	7
Table 2-2: SSOi for Mobile Apps Business Needs and Requirements	9
Table 2-3: Provisioning Business Needs for DoD Onboarding.....	12
Table 2-4: Provisioning Business Needs and Requirements Enhancements.....	16
Table 2-5: SAC Business Needs and Requirements Implemented with Tool	24
Table 2-6: SAC Business Needs and Requirements To Be Migrated	34
Table 2-7: CSP/IP Business Needs and Requirements for Decoupling.....	38
Table 2-8: CSP/IP Business Needs and Requirements To Be Migrated and Tested Post Decoupling	41
Table 2-9: IP and MVI Integration Requirements To Be Migrated and Tested Post Decoupling	47
Table 2-10: IP Business Needs and Requirements Enhancements	47
Table 3-1: Applicable Standards	55
Table 8-1: Function Point Analysis Results Table.....	58

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 2.

Previous Access Services (AcS) Requirements Specification Documents (RSDs) were named by the AcS PMAS Increment (i.e., Increment 1, Increment 2, Increment 3, etc.). However, VA is shifting to an agile development and release process in which a PMAS increment may have multiple releases. The functionality delivered in a release is bundled together by the release number, and the name of this Requirements Specification Document (RSD) as AcS 2.0 Increment 2 is intended to support the PMAS agile approach.

The AcS 2.0 Increment 2 requirements described in this document are drawn from VA AcS FY14 Business Requirements Documents (BRDs). Additional AcS 2.0 Increment 2 requirements may be found in consuming application integration analysis efforts in the form of integrated 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 2 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
- VRM IAM Sub-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 the AcS-approved 2.0 Increment 2 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 2. The AcS requirements include the following components:

- Single Sign-On – Internal (SSOi)
- Provisioning
- Specialized Access Control (SAC)
- Credential Service Provider (CSP)
- Identity Proofing (IP)
- e-Signature (eSig)

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

- Compliance Audit and Reporting (CAR)

1.3 Acronyms and Definitions

The following sections provide definitions of commonly used acronyms and terms relevant to the specifications elaboration, development, and implementation of the AcS solution.

1.3.1 Acronyms

Commonly used acronyms in this document are described in the [Identity and Access Services Master Glossary](#).

1.3.2 Definitions

Commonly used terms relevant to the specification elaboration, development, and implementation of the AcS solution are described 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 Table 1-1 below, a list of references, including the document title, publication date, and publisher, is provided.

Table 1-1: Document References

Title	Date	Published By
AcS FY14 BRD	07/2012	OIS BPMD
VA VIC Integration and AcS Integration Requirement Specification Document (iRSD)	03/2012	VA AcS PD
VA Directive 6500; Information Security Program	08/2006	VA
Section 508 Standards Guide	04/16/2010	General Service Administration
CAR Requirements Packet	09/01/2011	VA
VA CSP Requirements Packet	07/25/2011	VA
e-Sig Requirements Packet distributed 20110721	07/21/2011	VA
IP Requirements Packet	07/25/2011	VA
NIST Special Publication 800-63 Version 1.0.2; Electronic Authentication Guideline	04/2006	NIST
Provisioning Business Requirements Package	07/13/2011	VA
SAC Options Discussion	12/01/2011	VetsAmerica
SAC Requirements Packet	07/25/2011	VA
Section 508 Standards Guide	04/16/2010	General Service Administration
SSOi Requirements Packet	06/08/2011	VA
VA Directive 6500; Information Security Program	08/2006	VA
VA Directive 6501; VA Identity Verification In Person Proofing (IPP) Process; IAM Handbook	Last updated 09/01/2010	VA
CAR Pilot RSD	02/23/2012	VetsAmerica
VA IAM CAR SDD	02/13/2012	VetsAmerica

Title	Date	Published By
VA IAM CAR Use Case Model	02/23/2012	VetsAmerica
VA IAM CSP RSD	11/21/2011	VetsAmerica
VA IAM VA CSP Requirements Traceability Matrix (RTM)	12/13/2011	VetsAmerica
VA IAM VA CSP Use Case Model	11/21/2011	VetsAmerica
VA IAM Infrastructure SDD	11/21/2011	VetsAmerica
VA IAM ICD	12/13/2011	VetsAmerica
VA IAM IP RSD	11/21/2011	VetsAmerica
VA IAM IP RTM	12/13/2011	VetsAmerica
VA IAM IP Use Case Model	11/21/2011	VetsAmerica
VA IAM Provisioning Use Case Model	02/09/2012	VetsAmerica
VA IAM SAC RSD	01/19/2012	VetsAmerica
VA IAM SAC Use Case Model	01/19/2012	VetsAmerica
VA IAM SAC RTM	01/19/2012	VetsAmerica
VA IAM SAC SDD	12/13/2011	VetsAmerica
VA IAM SSOi ICD	02/09/2012	VetsAmerica
VA IAM SSOi RSD	02/09/2012	VetsAmerica
VA IAM SSOi RTM	02/09/2012	VetsAmerica
VA IAM SSOi SDD	12/13/2011	VetsAmerica
VA IAM SSOi Use Case Model	02/09/2012	VetsAmerica
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)
Continuous Readiness in Information Security Program (CRISP) Integration Onboarding/Offboarding Process Flows	6/2012	CRISP Team
Master Veteran Index (MVI) Use Cases	2012	IAM Identity Services Team
SEC ID MVI Integration RSD MVI	9/2012	IAM Integration Analysis Team
AcS i3 RSD	9/2012	IAM Access Service Analysis Team
AcS i3 SDD	2/2013	HP Development Team
AcS i3 UC Model	10/2012	HP Development Team

Title	Date	Published By
AcS Master Test Plan	TBD	
AcS i4 RSD		IAM Access Services Analysis Team
AcS i4 SDD		HP Development Team
AcS i4 UC Model		HP Development Team

2 Overall Specifications

The scope and functionality for AcS 2.0 Increment 2 are limited to the access 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 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 508 Office for the purpose of being utilized within applicable projects.

2.2 Business Rules Specifications

The business rules specifications are identified in section 2.6.

2.3 Design Constraints Specifications

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

2.4 Disaster Recovery Specifications

The AcS solution is hosted by [REDACTED] and leverages the Disaster Recovery Plan and the 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 FY14 BRD and is a separate deliverable.

2.6.1 Single Sign-On – Internal Service

The Single Sign-On – Internal (SSOi) service enables the user to access configured applications within VA without requiring additional user identifiers and passwords. The Single Sign-On (SSO) requirements in this document are built upon fundamental capabilities implemented in previous AcS releases. Existing applications configured to use SSOi are Enrollment Systems (ES) and Veterans Identification Card (VIC). The requirements defined in this section are not intended to replace existing functionality supported in VA's Single Sign-On – External (SSOe) service.

VA identified the need to provide SSOi access to VA applications to authorized users through the use of mobile devices, and to provide SSOi access to VA applications to non-VA users. Applications targeted to use the new SSOi services defined below are iEHR and Identity Toolkit for Common Access Card (CAC) Authentication and Health Adaptor/Mobile Providers for Mobile Applications.

The following SSOi enhancements were identified.

In Figure 2-1 below, the AcS 2.0 Increment 2 functional components for SSOi are shown. The functions shown with black text are already deployed within the environment. The functions shown with green text are additions specifically geared to support the Department of Defense (DoD) CAC users. The functions with red text are updates to SSOi in support of the VA enhancements.

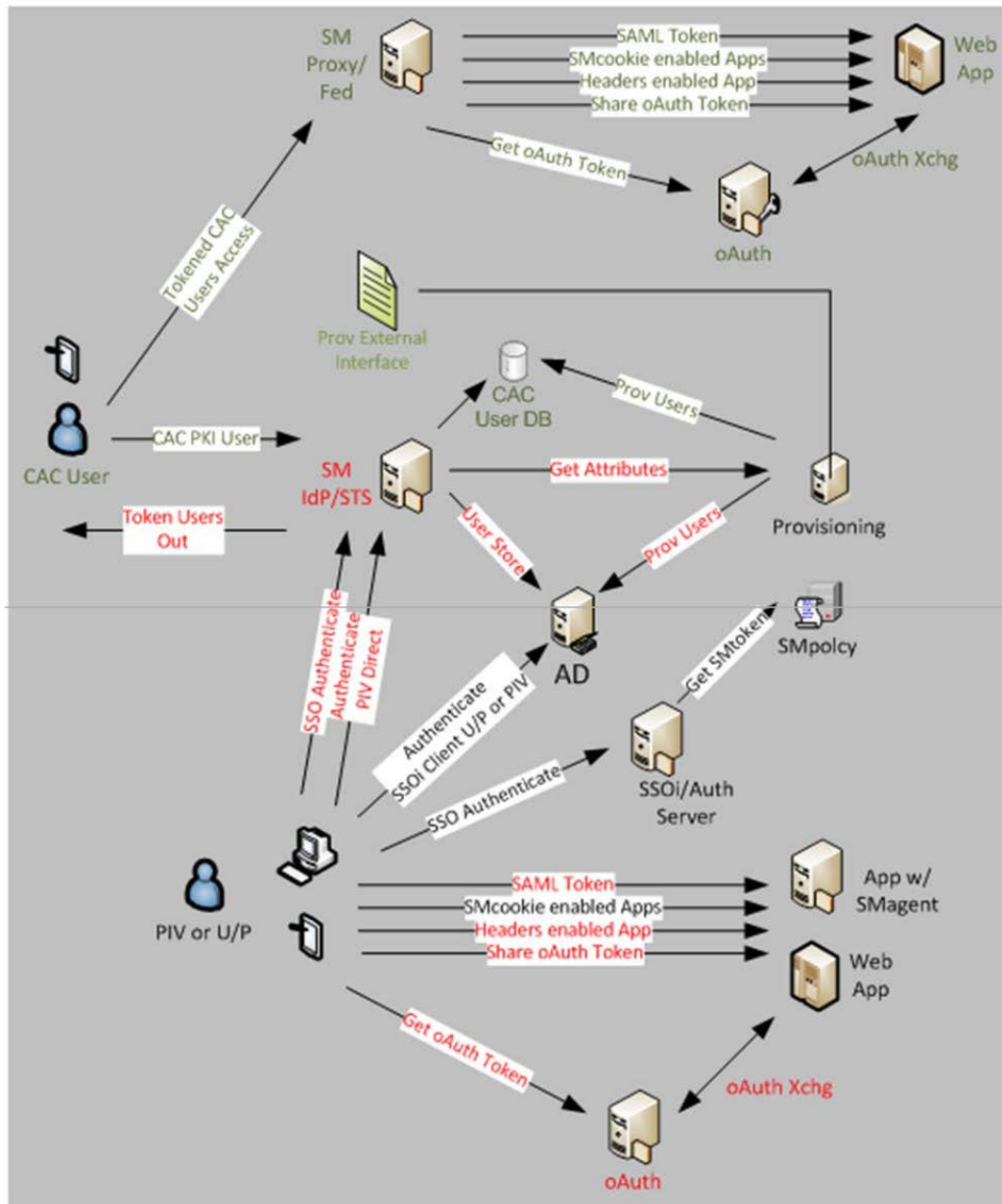


Figure 2-1: AcS 2.0 Increment 2 Functional Components for SSOi

2.6.1.1 Single Sign-On – Internal Service for CAC Credential

Table 2-1: SSOi for CAC Business Needs and Requirements

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
11.21	System shall support PIV and CAC authentication credentials.	SSOi shall provide authentication services for external access by non-VA employees to internal VA applications.	

1. SSOi shall provide proxy authentication services for external access
2. SSOi shall support a separate security realm for external access
3. SSOi shall provide an Identity Provider (IdP) and Service Provider (SP) service for CAC users
 - SSOi shall support LOA-4 user authentication with “holder-of-key” implementation
 - SSOi shall support issuance of LOA 3/4 Security Assertion Markup Language (SAML) tokens
 - SSOi shall support SAML 2.0 Web SSO post profile
 - SSOi shall support SAML 2.0 WS-Security, WS-Federation
 - SSOi shall support attribute retrieval service
 - SSOi shall issue SAML tokens for access to external services (iEHR, etc.)
4. SSOi shall support mobile application authorization for external devices and CAC users through the use of OAuth 2.0
 - SSOi shall support mobile client registration
 - SSOi shall support token query and cache
 - SSOi shall support management and enforcement of OAuth policies
 - SSOi shall support fine-grained revocation
 - SSOi shall support limiting the number of access or refresh tokens
 - SSOi shall support self-registration of clients
5. SSOi shall support SAML federation with VA PKI CSP to allow a CAC user of VAAFI to be sent into the SSOi environment
 - SSOi shall implement SAML 2.0 Service Provider interface accepting SAML tokens from VA PKI CSP
 - SSOi shall support LOA-4 token exchange with “holder of key”
 - SSOi shall support LOA-3 token exchange
 - SSOi shall support extending the SAML attributes with Provisioning data.
6. SSOi shall integrate with Provisioning data store enhancing SMsession data with provisioning attributes for CAC users.

The CAC user access to VA applications is shown in Figure 2-2 below, which is a subsection of Figure 2-1.

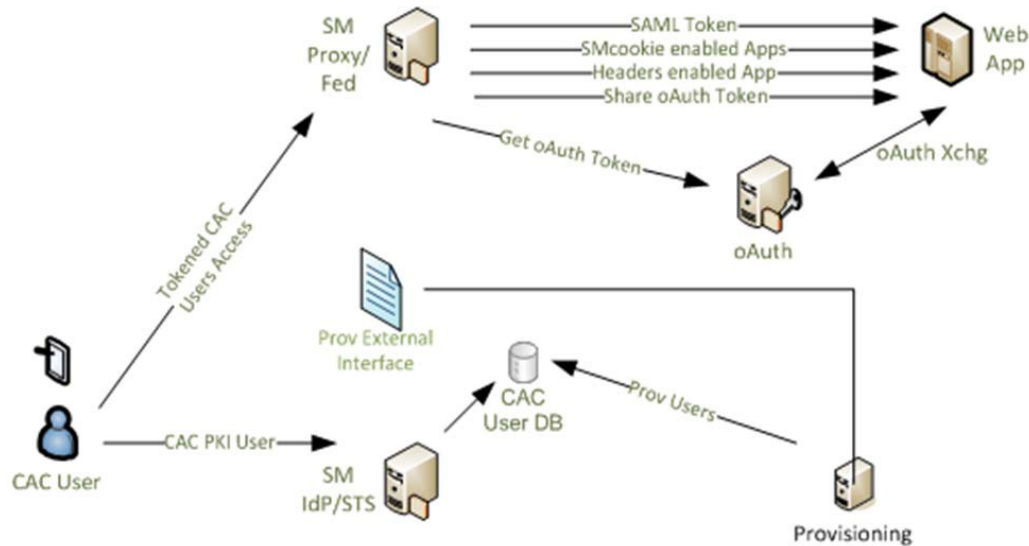


Figure 2-2: CAC User Access to VA Applications

2.6.1.2 Single Sign-On – Internal for Mobile Applications

Table 2-2: SSOi for Mobile Apps Business Needs and Requirements

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
12. 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 using the sign-on credentials.			
12.73	SSOi shall support the OAuth standard to enable SSO for mobile applications.	SSOi shall enable authorized users of VA approved Mobile Device Management (MDM) devices to access VA applications using SSOi	
6.16	System shall support multiple platforms including mobile, thin client and thick client applications.	SSOi shall enable authorized users of VA approved Mobile Device Management (MDM) devices to access VA applications using SSOi	

1. SSOi shall support a separate security realm for external access to support Mobile Applications
2. SSOi shall provide an IdP service for SSOi users
 - SSOi shall support LOA-4 user authentication
 - SSOi shall support SSO authentication by SSOi tokened user
 - SSOi shall support issuance of LOA 2/3/4 SAML tokens
 - SSOi shall support SAML 2.0 Web SSO post profile
 - SSOi shall support SAML 2.0 WS-Security, WS-Federation
 - SSOi shall support an attribute retrieval service

- SSOi shall issue SAML tokens for access to external services (iEHR, etc.)
- 3. SSOi shall provide a Secure Token Service (STS) for user session management data
 - The SSOi STS service shall Exchange user session data when presented with a valid SSO user token
 - The SSOi STS service shall be capable of authenticating web service clients using TLS client-auth
 - The SSOi STS service shall be capable of authenticating web service clients using WS-Security X509
 - The SSOi STS service response message shall support SAML format
 - The SSOi STS service response message shall support Extensible Markup Language (XML) encryption for message and attributes individually
 - The SSOi STS service response message shall support XML digital signature
 - The SSOi STS service shall support WS-Trust protocol
 - The SSOi STS service shall support WS-Policy protocol
 - The SSOi STS service shall support WS-Security
 - The SSOi STS service shall support attribute retrieval from Provisioning
 - The SSOi STS service Shall support token and attribute retrieval from Vista
- 4. SSOi shall support VA internal user LOA-4 authentication into the SSOi environment
- 5. SSOi shall support VA application integration at LOA-4
- 6. SSOi shall support “step-up” authentication allowing a LOA-2/3 authenticated users to re-authenticate at LOA-4
- 7. SSOi shall support mobile application CAC authorization through the use of oAuth 2.0
 - SSOi shall support oAuth from the provider perspective
 - SSOi shall support oAuth enforcement from application perspective
 - SSOi shall support mobile client registration
 - SSOi shall support token query and cache
 - SSOi shall support management and enforcement of oAuth policies
 - SSOi shall support fine-grained revocation
 - SSOi shall support limiting the number of access or refresh tokens
 - SSOi shall support self-registration of clients
- 8. SSOi shall support SAML federation with VAAFI
 - SSOi shall implement SAML 2.0 Identity Provider interface issuing SAML tokens to the VAAFI SP.
 - SSOi shall support SSOi SMsession authenticated users for token
 - SSOi shall support SSOi direct PKI users for token issuance
 - SSOi IdP shall support issuance of LOA-3 SAML token
 - SSOi IdP shall support issuance of LOA-4 SAML token with “holder of key”

9. SSOi shall integrate with the Provisioning data store enhancing SMsession data with provisioning attributes.

In Figure 2-3 below, the Mobile Device, as a subsection of Figure 2-1, is shown.

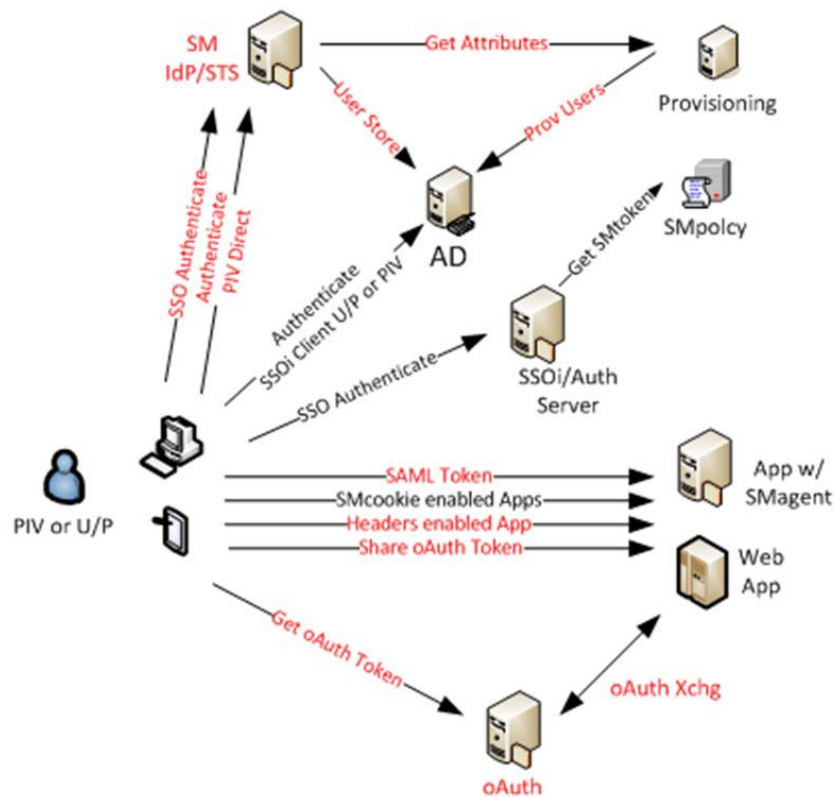


Figure 2-3: Mobile Device

2.6.2 Provisioning – DoD Onboarding

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.

Critical to the successful implementation of the Digital Identity and Privilege Management service, specifically Bind/Unbind, the DoD User Onboarding workflow enables DoD users to use the Provisioning tool and other provisioned VA systems and VA resources.

The Provisioning system integrates with the VA MVI to correlate the SEC ID to the MVI Integration Control Number (ICN) so that all identifiers for the person are known and managed by the MVI.

Table 2-3: Provisioning Business Needs for DoD Onboarding

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
4.0 Linking/Association: Provide a digital process of linking one identity record with another across multiple systems, including activation and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications.			
4.2	Develop and implement approaches and technologies enabling the linking of Third-Party credentials to the digital identity records of external users for use in application access.	Requirement Clarification provided below	

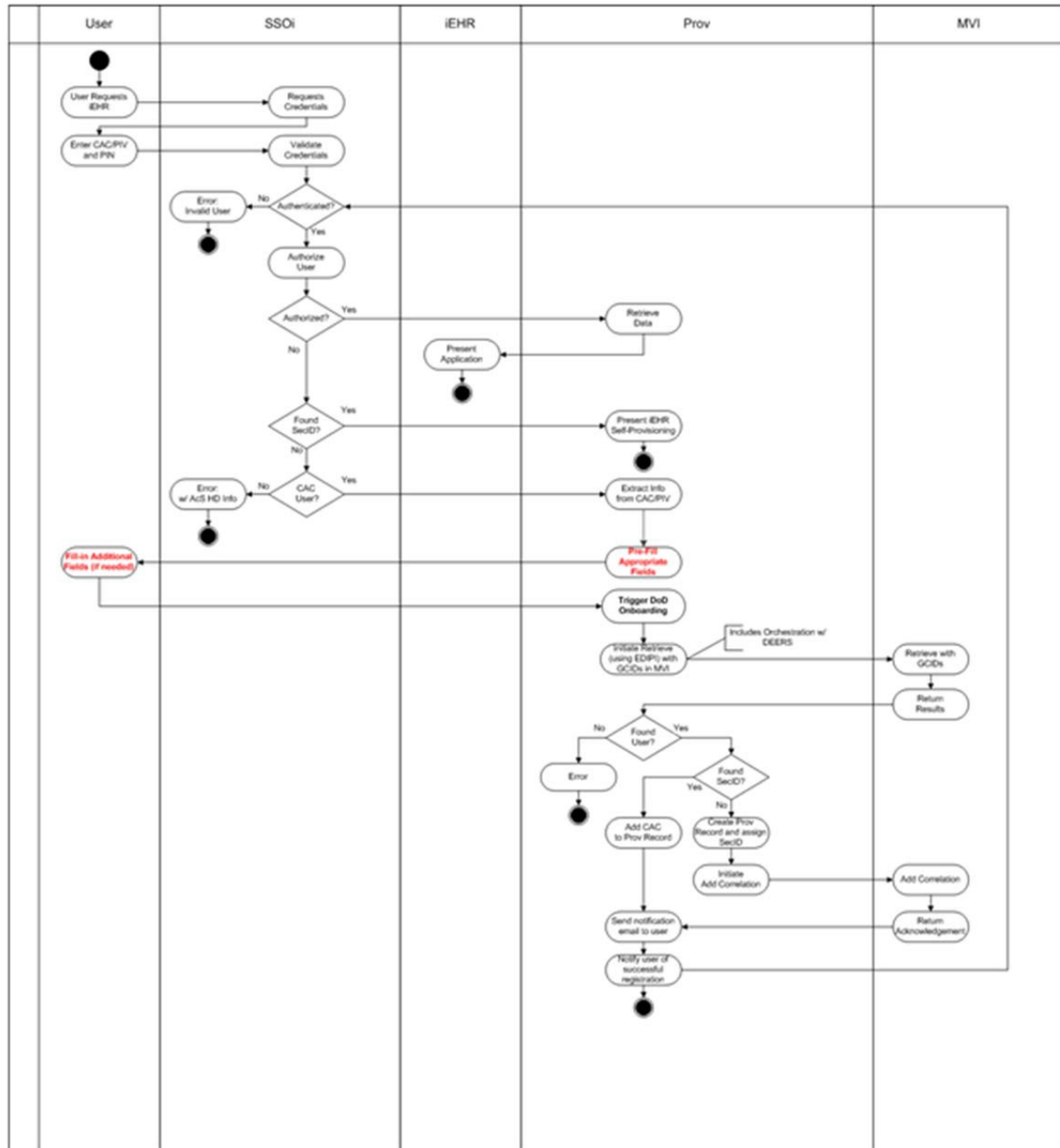


Figure 2-4: Provisioning – DoD Onboarding

The DoD Onboarding requirements include the following:

1. The Provisioning Service shall have the ability to specify authorized systems to initiate the DoD Onboarding workflow.
 - a. Provisioning shall specify SSOi as a third-party authorized system (for Increment 4).

2. SSOi shall trigger the DoD Onboarding process during authentication to iEHR (or other future DoD facing SSOi enabled applications) when the user is not authorized and no Sec ID is found (no Provisioning record exists) by redirecting the user to the Provisioning Onboard a DOD User Registration Page.
3. The Onboard a DOD User Registration Page shall extract the EDIPI from the SSOi headers and perform a Retrieve from the MVI. The Provisioning service shall be a consumer of the MVI Orchestration Service. If MVI finds the person, the retrieve shall return identity traits for that person. If the person does not exist in MVI, the Retrieve from the MVI shall call DEERS using the EDIPI to find the person. If the person is found in DEERS, MVI shall add that person to MVI and return the results to the Provisioning service for creation of a SEC ID and correlating to MVI. Detailed integration requirements are described in the [SEC Id MVI Integration RSD.pdf](#).
 - a. If the MVI search returns a person and the MVI record contains a SEC ID, then provisioning shall associate the CAC credential to the user's existing Provisioning record and shall redirect the user to the calling application (i.e., iEHR).
 - b. If the MVI search returns a person, and the MVI record does not contain a SEC ID, then the Onboard a DoD user registration page shall be displayed.
 - c. If the MVI search does not return a person, the DoD Onboarding workflow shall display an error message. **Note:** the Provisioning service shall only display the error message when the person cannot be found in both the MVI and in DEERS.
4. Provisioning shall provide an Onboard a DOD User Registration Page that contains the following fields: First Name, Middle Name, Last Name, SSN, Date of Birth (DOB), Gender, DoD Email.
 - a. The Onboard a DOD User Registration Page shall contain text explaining the first-time use of the CAC and describe the registration process purpose (to link the user's CAC to an existing VA record or link their CAC to a newly created VA record).
 - b. The Onboard a DOD User Registration Page shall be pre-populated with data available from MVI.
 - c. The Onboard a DOD User Registration Page pre-populated fields shall not be editable.
 - d. The following fields shall be required: First Name, Last Name, Gender, DoB, SSN and DoD Email.
 - e. The Middle Name field shall be included as an optional field.
 - f. The Onboard a DOD User Registration Page shall provide a submit button and a cancel button.
 - g. If the user clicks the cancel button, Provisioning shall close the SSOi session and show the logout success page.
5. If the user clicks the submit button, Provisioning shall call the Onboard a DoD User workflow to complete the following:

- i. Provisioning shall create the provisioning record using the data provided from MVI.
 - ii. Provisioning shall create and assign a SEC ID to the Provisioning record.
 - iii. Provisioning shall correlate the record with the MVI.
6. After successful DoD user registration, Provisioning shall notify the user that their CAC has been successfully processed with the following message sent to their DoD email:
 - a. The notification message shall state:

[First Name] [Last Name],

You have successfully linked your CAC to your VA record. You can now access joint DoD/VA applications and DoD enabled VA applications.

To request access to these applications please visit the VA Provisioning Service

HYPERLINK REDACTED

7. Upon completion of the DoD Onboarding workflow, Provisioning shall redirect to the calling application (i.e., iEHR).

2.6.3 Provisioning Service Level Enhancements

The Provisioning service provides portions of the 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.

Note: All the requirements that are mapped to the generic Business Need 3.0 are derived from the Provisioning Security Identifier Integration to the MVI Requirements Specification Document (RSD).

Table 2-4: Provisioning Business Needs and Requirements Enhancements

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release Release (Increment)
3.0 Digital Identity Lifecycle Management Onboard/Offboard: Provide a digital process of establishing and maintaining the attributes that make up an individual digital identity and supports general updates to an identity such as a name change or biometric update.			
3.0	The Provisioning service shall be able to support separate workflows for onboarding of Volunteers and Health Professions Trainees.		
3.0	The provisioning service shall have an authenticated onboarding graphical user interface (GUI) for Human Resources (HR), Sponsor, Contracting Officer's Technical Representative (COTR) and Contractor Lead data entry of volunteers and Health Professions Trainees.		
3.0	The Provisioning service shall be able to support separate workflows for offboarding of Volunteers and Health Professions Trainees.		
4. Linking/Association: Provide a digital process of linking one identity record with another across multiple systems, including activation and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications.			
	Develop and implement approaches and technologies enabling the linking of third-party credentials to the digital identity records of external users for use in application access.	The Provisioning Service shall make its GUI available outside of the VA intranet for supporting iEHR users.	
20.0 Provisioning: Provide an automated capability of creating user access accounts and assigning privileges or entitlements within the scope of a defined process.			
20.02	The Provisioning service shall provide the means for Provisioning Requestors (people) to initiate internal Provisioning requests for VA employees, contractors, affiliates, business partners, and clients.	The Provisioning Service shall allow a user to search for a person utilizing a VA email address and/or a DoD email address.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
3.04	Identify and utilize a unique enterprise-wide accepted identifier that will aid in identifying identities and will support the elimination of conflicting or duplicate values during all aspects of IAM administration.	<p>The Provisioning service shall provide a service to allow a system to retrieve user accounts by SEC ID or by any other account ID known the Provisioning Service.</p> <p>The Provisioning service's Get Corresponding Accounts shall be based on MVT's Get Corresponding IDs.</p> <p>The Provisioning service's Get Corresponding Accounts shall return the SEC ID and all other account IDs known to the Provisioning Service when called.</p>	
3.12	Enable automated provisioning using the attributes linked with core identity.	The Provisioning service shall include the following attributes in the information contained in the CRISP SCREENING CHECKLIST: VA Personnel Accountability System Profile, Contract Number.	
ES CR1629	The Provisioning Service shall require an Enrollment Systems (ES) approver to enter a comment when a request is rejected.	The Provisioning Service shall prompt the ES approver to enter a comment in the event that an ES approver has not enter a comment when rejecting a request	
ES CR1625	After a user has submitted a request, the Provisioning Service shall display the following text: "Task was submitted to approver, <approver name>."		
ES CR1622	For ES users, the Provisioning Service shall leverage Active Directory when mapping a user to an approver.		

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
ES CR1618	When de-provisioning an ES User, the Provisioning Service shall only require Supervisor approval.		
ES CR1617	When a user selects “Request ES Access” under the “Add/Remove Access to Others” menu, the Provisioning Service shall display the following sub-menus: <ul style="list-style-type: none"> • Request Add ES Access • Request Remove ES Access • Request Modify ES Access 		
ES CR1615	The Provisioning Service shall send one email notification to each approver listing all the roles for a user when a user has been assigned multiple roles. When an approver selects “My Work List,” the Provisioning Service shall display one item for each person awaiting approval. When an approver selects an item appearing in “My Work List,” the Provisioning Service shall display all roles requested for the person. The Provisioning Service shall allow the approver to approve, reject, or reserve each role within the item.		
ES CR1590	When provisioning an ES user, the Facility Code shall be a required attribute.		
ES CR1582	The Provisioning Service shall display an error message informing the user that a role must be selected in the event that a user clicks the Select button without checking any rolls.		
ES CR1581	The Provisioning Service shall continue to display a drop down after a user enters a search code.		
ES CR1627	The Login button shall be active on the Login Screen of the Provisioning Service. If a user presses the enter key while the Login Screen is active, the Provisioning Service shall attempt to log the user into the		

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
	Provisioning Service using the credentials entered on the screen.		
CR1728	The Provisioning Service shall be able to capture the user identity and timestamp automatically anytime a user approves or rejects a request.		
CR1729	The Provisioning service UI shall not allow a user to approve a user who has unfavorable SAC status during CRISP On-boarding.		
CR1738	The Provisioning Service shall display radio buttons to the VA Manager and Contract Lead allowing the user to select if the Employee or Contractor has returned Government Equipment, not returned Government Equipment, or did not possess any Government Equipment. The Provisioning Service shall allow the VA Manager and Contract Lead to submit or cancel once the user has selected the appropriate radio button regarding government equipment.		
CR1741	The Provisioning Service shall always display Manager Information (SEC_ID, First Name, Last Name, Email Address) automatically, without requiring a checkbox to do so, during CRISP On-boarding.		
CR1752	The Provisioning Service shall not display SEC ID to non-administrative users unless explicitly required. The Provisioning Service shall require manual entry of SEC ID.		
CR1753	The Provisioning service shall enable a contractor lead to be able to look up a user's COR and VA Project Manager during CRISP On-boarding.		
CR1754	The provisioning service shall not require a "MVI Justification" during CRISP on/off boarding.		

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
CR1757	<p>The Provisioning Service shall not display previously entered search criteria when a user launches the Search for Person Screen.</p> <p>The Provisioning Service shall not automatically select previously selected search results when a user searches using new search criteria.</p>		
CR1758	<p>The Provisioning Service shall provide a drop down list of values for the following attributes: Employment Status, Occupation Code, Department, Office Location, Cost Center, Type of Appointment, Service, Facility, Organization Field, Station Number, Duty Station Code, Facility or Assigned Duty Station, and Mail Routing Symbol.</p>		
CR1768	<p>The following set of requirements applies to the non-emergent off boarding of a Contractor.</p> <ol style="list-style-type: none"> 1. The Provisioning Service shall allow the Contract Lead to initiate off boarding of a Contractor. 2. The Provisioning Service shall require the Contract Lead to identify the date on which the Contractor's access shall be deactivated. 3. The Provisioning Service shall notify the Sponsor/COR that a Contract Lead has initiated off boarding a Contractor. 4. The Provisioning Service shall allow the Sponsor/COR to enter specific instructions for off boarding a Contractor when the Sponsor/COR acknowledges Contractor off boarding. 5. The Provisioning Service shall send a notification to the Contractor, Contract Lead, and Sponsor/COR after the Sponsor/COR acknowledgement of a Contractor off boarding. The Provisioning Service shall include any remarks entered by the Sponsor/COR on the notification as well as instructions to return Government Property. 6. The Provisioning Service shall send notification of off boarding to the systems associated with the accounts/credentials associated with the Contractor's identity known by the Provisioning Service. The 		

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
	<p>Provisioning Service shall send the notification to the external systems once the Sponsor/COR has acknowledged the off boarding request from the Contract Lead. The Provisioning Service shall include the date on which the Contractor's access shall be deactivated on the notification.</p> <p>7. The Provisioning Service shall receive notifications from external systems when the Contractor's access has been deactivated.</p> <p>8. The Provisioning Service shall notify the Sponsor/COR when external systems have provided notification of deactivation of a Contractor's access.</p> <p>9. The Provisioning Service shall allow the Sponsor/COR or the Contract Lead to indicate that the Contractor has returned all Government property. The Provisioning Service shall require the user to enter the specific property that is being returned (either in a free form text field or checkboxes).</p> <p>10. The Provisioning Service shall require the Sponsor/COR to verify the Government property returned by the Contractor in the event that the Contractor returns the property to the Contract Lead.</p> <p>11. The Provisioning Service shall allow the Sponsor/COR to identify that the Contractor has not returned Government property.</p> <p>12. The Provisioning Service shall notify the appropriate office(s) of unrecovered property.</p>		
CR1786	<p>The Provisioning Service UI task pane category "VA AcS" shall be named "VA On/Off-Boarding".</p> <p>The Provisioning Service UI task pane category "VA On/Off-Boarding" shall be reorganized On-Board User [On-Board {user type}], Off-Board User [Off-Board {user type}], Update User [Update {user type}], Reporting [CRISP Checklist, Metrics].</p>		
CR1787	<p>The Provisioning Service UI shall ensure all names in the Task Pane are fully visible by default.</p>		

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
CR1788	<p>The following set of requirements applies to CRISP Onboarding/Offboarding Metrics:</p> <ol style="list-style-type: none"> 1. The Provisioning Service shall allow a user to run a standard report or an ad hoc report. 2. The Provisioning Service shall allow a user to select one of the following standard reports: All In Process; All Completed; All. 3. The Provisioning Service shall include all persons whose on-boarding or off-boarding tasks are not completed when the user selects the “All in Process” standard report. 4. The Provisioning Service shall include all persons whose on-boarding or off-boarding tasks are completed when the user selects the “All Completed” report. 5. The Provisioning Service shall include all persons when the user selects the “All” standard report. 6. The Provisioning Service shall allow the user to select filter criteria when a user selects an ad hoc report. The Provisioning Service shall include any attributes within the Provisioning User identity record as well as any attributes on the CRISP checklist on the filter criteria. 7. The Provisioning Service shall automatically filter reporting results (both standard and ad hoc) for non-Privileged users to only include identity records that the non-Privileged user is authorized to access. 		

2.6.4 Specialized Access Control

The Specialized Access Control (SAC) service provides fine-grained, 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 user attributes. 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.

- 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 either a directory or a database that holds user attributes.
- 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.

The additional components of SAC that are not in the XACML model are described below:

- Attribute Service (AS): The AS retrieves user attributes from a PIP or a variety of authoritative identity stores, which are in the form of directories or databases. It receives requests from the PDP for user attributes pertaining to an access control request. The AS then searches for and returns the applicable attributes to the PDP for evaluation. It can be used to perform the XACML Context Handler function "as a service," which is sometimes needed for efficiency and performance. **Note:** SAC may be integrated with any data store required by a consuming application to make an authorization decision. For example, SAC uses user data from the Nationwide Health Information Network (NwHIN) data store to make an authorization decision to allow or deny access. Future identity data stores will be identified as consuming applications of SAC 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. It can be used to perform the XACML Context Handler function "as a service," which is sometimes needed for efficiency and performance.

Currently, the SAC service provides the following capabilities:

- Integrates with the NwHIN to provide fine-grained access control to protect Veterans' medical information while making it accessible to those who need it. When an end user of a VA application attempts to access a resource protected by SAC, the request is intercepted and evaluated to make a decision. The decision is made by evaluating the attributes of the user accessing the application, the application itself, and the context of the request against the appropriate access control policy.
- 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.

The current SAC solution, which is based entirely on the IBM DataPower XI50, does not provide a PAP or an out-of-the-box AS, and has limited capabilities for interacting with Policy Information Points (PIPs). The SAC service is required to be XACML 2.0 compliant for Policy Administration Points (PAPs), 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. A new tool that provides a more robust authorization capability was acquired. The following requirements are fulfilled upon the implementation of the new tool.

Note: The policies in the existing PDP are also implemented in the new tool.

Table 2-5: SAC Business Needs and Requirements Implemented with Tool

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release Release (Increment)
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.			
14.02	The SAC service shall provide the ability for a SAC System Administrator to indicate (add) client opt-in/opt-out and other client data restriction preferences on behalf of a client.	The SAC service Policy Administration Point (PAP) shall provide the ability to indicate (add) client opt-in/opt-out and other client data restriction preferences on behalf of a client.	
14.06	The SAC service shall save the opt-in/opt-out and other client data restriction preferences entered by a SAC System Administrator or provided by the client.	The SAC service shall provide the ability to save the business policy or rule entered by the SAC System Administrator.	
14.07	The SAC service shall provide the ability for a SAC System Administrator to modify the opt-in/opt-out and other client data restriction preferences entered by a SAC System Administrator or provided by the client.	The SAC service Policy Administration Point (PAP) shall provide the ability to modify the opt-in/opt-out and other client data restriction preferences provided by the client.	
14.08	The SAC service shall provide the ability for a SAC System Administrator to review the established client data restriction preferences.	The SAC service Policy Administration Point (PAP) shall provide the ability to perform a review action on the business policies or rules using the client data restriction preferences entered into the business application data store.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
14.09	The SAC service shall provide the ability for a SAC System Administrator to filter the established client data restrictions by attributes.	The SAC service Policy Administration Point (PAP) shall provide the ability to perform a filter action on the business policies or rules using the client data restriction preferences entered into the business application data store.	
14.10	The SAC service shall provide the ability for a SAC System Administrator to revoke (remove) the opt-in/opt-out and other client data restriction preferences entered by a SAC System Administrator or provided by the client without deleting the original record from the data store.	The SAC service Policy Administration Point (PAP) shall provide the ability to revoke (remove) opt-in/opt-out and other client data restriction preferences defined through the business policies and rules without deleting the original policy record from the Policy Administration Point (PAP) data store.	
14.11	The SAC service shall store all records of all opt-in/opt-out and other client data restriction preference requests even if they were declined by the policy approving authority.	The SAC service will maintain a log of all access requests and responses even if they were declined by the policy approving authority.	
		The SAC service will maintain a log of all access opt-in/opt-out and other client data restriction preference requests and responses even if they were declined by the policy approving authority.	
14.12	The SAC service shall provide the ability to manage Data Restriction attributes.	The SAC service Policy Administration Point (PAP) shall provide the ability to select a set of attributes (from registered business data sources) to be used in the process of translating the existing business policies to SAC policy records.	
		The SAC service will provide support for multiple policy information points to perform a read operation on the business data stored within the business application data store.	
		The SAC service will provide support for multiple policy information points to perform a read operation on the opt-in/opt-out and other client data restriction preferences data entered within the business application data	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
		store.	
14.13	The SAC service shall provide the ability for a SAC System Administrator to enter (add) data restriction attributes.	The SAC service Policy Administration Point (PAP) shall provide the ability to add data restriction attributes (from the business application data stores) to the business policies or rules.	
14.14	The SAC service shall save the data restriction attributes entered by a SAC System Administrator.	The SAC service shall provide the ability to save the entered business policy or rule.	
14.15	The SAC service shall provide the ability for a SAC System Administrator to modify the data restriction attributes entered.	The SAC service Policy Administration Point (PAP) shall provide the ability to modify the business policies or rules utilizing the data restriction attributes entered into the business application data store.	
14.16	The SAC service shall provide the ability for a SAC System Administrator to revoke (remove) the data restriction attributes entered without deleting the original record from the data store.	The SAC service Policy Administration Point (PAP) shall provide the ability to revoke (remove) the business policies or rules utilizing the data restriction attributes entered into the business application data store without deleting the original policy record from the Policy Administration Point (PAP) data store.	
14.17	The SAC service shall provide the ability for a SAC System Administrator to review the established data restrictions.	The SAC service Policy Administration Point (PAP) shall provide the ability to review the business policies or rules utilizing the data restriction attributes entered into the business application data store.	
14.18	The SAC service shall provide the ability for a SAC System Administrator to filter the established data restrictions by attributes.	The SAC service Policy Administration Point (PAP) shall provide the ability to filter business policies or rules utilizing the data restriction attributes entered into the business application data store	
14.21	The SAC service shall provide the ability for a SAC System Administrator to assign a User Security Attribute value to data.	The SAC service shall provide the ability to make use of the user identify attribute value(s) to establish new or update existing business policies.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
14.39	The SAC service shall provide the ability to specify scheduled periods of system un-availability.	See Section 2.11 Reliability Specification for details on operational support specifications and procedures.	
14.45	The SAC service shall have the capability to request and retrieve access control policies and user attributes.	The SAC service Policy Information Point (PIP) shall support accessing distributed policy repository and policy.	
14.46	The SAC service shall verify that the transaction is in an approved format, each mandatory field is provided, each field has a value that is within the approved schema for that transaction, and protections are intact.	The SAC service shall validate the transition from business policy to XACML policy against appropriate schema and business rules.	
		Each Policy Decision Point (PDP), Policy Administration Point (PAP), Policy Information Point (PIP), Policy Enforcement Point (PEP) component shall validate each request/response based on appropriate schemas and business rules.	
14.47	The SAC service shall have the capability to customize and apply additional workflow controls used to enforce constraints and obligations contained in the authorization decision.	The SAC service Policy Decision Point (PDP) shall have the capability to customize and apply constraint rules to reduce the access capabilities of the users.	
		The SAC service Policy Decision Point (PDP) shall have the capability to customize and apply obligation rules to enhance the expected actions of the users.	
14.48	The SAC service shall use exceptions for emergency and temporary access authorization based on established policies.	The SAC service Policy Administration Point (PAP) shall support business rules around emergency and temporary access.	
		The SAC service Policy Decision Point (PDP) shall be able to operate in an emergency access context.	
14.49	The SAC service shall provide an Attribute Service which will obtain user attributes from an external Policy Information Point.	The SAC service Policy Information Point (PIP) shall pull the information from the Attribute Service (Virtual Directory, VAP).	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
14.50	The Attribute Service shall have access to approved and authoritative attribute stores/directories for users.	The SAC service Policy Information Point (PIP) shall have access to approved and authoritative attribute stores/directories for users.	
14.51	The Attribute Service shall have ability to receive requests from the Policy Decision Point for user attributes.	The SAC service Policy Information Point (PIP) shall have ability to receive requests from the Policy Decision Point (PDP) for user attributes.	
14.52	The Attribute Service shall have ability to provide user attributes to the Policy Decision Point.	The SAC service Policy Information Point (PIP) shall have ability to provide user attributes to the Policy Decision Point.	
14.53	The Attribute Service shall not make attributes available in response to improperly formed messages.	The SAC service Policy Information Point (PIP) shall not make attributes available in response to improperly formed messages.	
14.54	If there is a need to store attributes locally, the SAC service shall ensure data is current by synchronizing local data automatically or periodically with the external authoritative source.	If there is a need to store policy or attributes locally, the SAC service shall ensure data is current by synchronizing local data automatically or periodically with the external authoritative source.	
14.55	The SAC service shall have the ability to provide adequate information to CAR service in order for CAR to create reports.	The SAC service Policy Administration Point (PAP) shall be able to audit user access and change events to policies.	
		The SAC service Policy Decision Point (PDP) shall be able to audit access control decisions, policy retrievals and policy information requests.	
		The SAC service shall integrate with CAR for continuous updating	
		The SAC service shall store audit log locally in a format compatible with CAR.	
14.56	The SAC service shall satisfy security and privacy policies for passing information (requests, decisions, attributes).	The SAC service shall satisfy HIPAA HL7, VA, and NIST guidelines for privacy, confidentiality and data integrity.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
14.57	The SAC service shall perform the security checks necessary to verify that transactions have the requisite protections.	The SAC service shall be capable of supporting a secure protocol to protect the transactions.	
14.58	The SAC service shall ensure that the data-in-transit and data-at-rest are protected using appropriate mechanisms.	The SAC service shall be capable of supporting protection of the data-in-transit and data-at-rest.	
14.59	The SAC service shall enforce separation of duties through business rules.	The SAC service Policy Administration Point (PAP) shall support mutually exclusive roles to enforce separation of duties.	
14.60	The SAC service shall verify that the content of the transaction has not been subjected to modification by an unauthorized source.	The SAC service Policy Administration Point (PAP) shall provide data integrity protection mechanisms for policy deployment.	
15 Policy Administration: Provide a digital process of creating, disseminating, modifying, managing, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection in a standard policy exchange format.			
15.01	Provide centralized control, management, and visibility to security policy across the enterprise via a user-friendly graphical interface.	The SAC user interface shall provide centralized control, management, and visibility to the security policies in graphical form using VA design standards, processes and methodologies.	
15.03	Provide ability to apply incremental updates to policy and configuration data simultaneously across all distributed decision/enforcement points.	The SAC service shall provide tools to support simultaneous updates to enterprise-wide Policy Decision Points (PDPs).	
		The SAC service shall provide tools to support simultaneous updates to enterprise-wide Policy Enforcement Points (PEPs).	
15.04	The Policy Administration Point shall utilize authoritative policy stores that serve as repositories for access control policies.	The SAC service Policy Administration Point (PAP) shall interface with authoritative policy stores by connecting to and receiving related components from policies stores.	
15.05	The Policy Administration Point shall allow Privileged User the capability to add/modify	The SAC user-interface shall support policy maintenance; including adding, modifying and deleting.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
	authorization policies.	The SAC user-interface shall support the creation of Privileged User accounts.	
15.10	Logical Access Control Services shall be provided that enable Policy Administration for enforcement of Separation of Duties Access Controls.	The SAC Service shall provide the ability to define and enforce roles to support the Separation of Duty Access Control decisions.	
15.11	Logical Access Control Services shall be provided that enable Policy Administration for enforcement of Least Privilege Access Controls.	The SAC Service shall provide the ability to define and enforce roles to support the Least Privilege Access Control decisions.	
16 Policy Decision: Provide a capability that serves as an access control authorization authority for evaluating access control policies based on a variety of inputs.			
16.05	The Policy Decision Point shall have the capability to send access control decisions to the Policy Enforcement Point.		
16.06	The Policy Decision Point shall have the capability to obtain user attributes from the Attribute Service.	The SAC service Policy Decision Point (PDP) shall interface with authoritative attribute stores by connecting to and receiving related components from attribute stores.	
16.07	The Policy Decision Point shall have the capability to obtain decision attributes from a Policy Information Point.	The SAC service Policy Decision Point (PDP) shall interface with the Policy Information Point (PIP) by connecting to and receiving related components from the Policy Information Point (PIP).	
16.08	The Policy Decision Point shall have the capability to obtain authorization policies from a Policy Store.	The SAC service Policy Decision Point (PDP) shall interface with authoritative policy stores by connecting to and receiving related components from policies stores.	
16.09	Logical Access Control Services shall be provided that enables a Policy Decision capability that serves as an access control authorization authority for Course Grain Access Controls as required by consuming applications.	Logical Access Control Services shall be provided that enables an authorized Policy Decision capability for Coarse Grain Access Control as required by consuming applications.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
16.10	Logical Access Control Services shall be provided that enables a Policy Decision capability that serves as an access control authorization authority for Role-based Access Controls as required by consuming applications.	Logical Access Control Services shall be provided that enables an authorized Policy Decision capability for Role Based Access Control as required by consuming applications.	
16.13	Logical Access Control Services shall be provided that enables a Policy Decision capability that serves as an access control authorization authority for enforcement of Separation of Duties Access Controls.	The SAC Service shall provide the ability to define and enforce roles to support the Separation of Duty Access Control decisions.	
16.14	Logical Access Control Services shall be provided that enables a Policy Decision capability that serves as an access control authorization authority for enforcement of Least Privilege Access Controls.	The SAC Service shall provide the ability to define and enforce roles to support the Least Privilege Access Control decisions.	
17 Policy Enforcement: Provide a capability that restricts access to specific systems or content in accordance with policy decisions that are made.			
17.01	The SAC service shall provide a Policy Enforcement Point (PEP) to enforce access control decisions.	The SAC service shall support the consuming application with a Policy Enforcement Point (PEP).	
17.02	The SAC service shall interface with Identity services as required to facilitate the SAC processes.	The SAC service shall be capable of interfacing with the MVI, Provisioning, Virtual Directory and other authoritative data sources as needed to receive required data to perform policy enforcement.	
17.11	If Client Preferences exist, the SAC service shall prevent end-user access to the resource requested based on the stored Client Preferences.	The SAC service shall not allow access if the Client Preferences do define access restriction.	
17.12	The SAC service shall manage system and data access based on Data Restriction attributes.	The SAC service shall obtain data restrictions from other services/applications and input to the Policy Information Point (PIP).	
17.13	In the absence of Data Restrictions, the SAC service shall allow end-user access to the resource requested.	The SAC service shall allow access if the Data Restrictions do not define access restriction.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
17.14	If Data Restrictions exist, the SAC service shall prevent end-user access to the resource requested.	The SAC service shall not allow access if the Data Restrictions do define access restriction.	
17.15	The SAC service shall manage system and data access based on User Security attributes.	The SAC service shall obtain User Security attribute value(s) from other services/applications and input to the Policy Information Point (PIP).	
17.16	In the absence of User Security attributes, the SAC service shall allow end-user access to the resource requested.	The SAC service shall allow access if the User Security attribute value(s) do not define access restriction.	
17.17	If User Security attributes exist, the SAC service shall prevent end-user access to the resource requested.	The SAC service shall not allow access if the User Security attribute value(s) do define access restriction.	
17.18	The SAC service shall manage system and data access based on Contextual Constraints.	The SAC service shall obtain Contextual Constraints from other services/applications and input to the Policy Information Point (PIP).	
17.19	In the absence of Contextual Constraints, the SAC service shall allow end-user access to the resource requested.	The SAC service shall allow access if the Contextual Constraints do not define access restriction.	
17.20	If Contextual Constraints exist, the SAC service shall prevent end-user access to the resource requested.	The SAC service shall not allow access if the Contextual Constraints do define access restriction.	
17.21	The SAC service shall manage system and data access based on Application Function attributes.	The SAC service shall obtain Application Function attribute value(s) from other services/applications and input to the Policy Information Point (PIP).	
17.22	In the absence of Application Function attributes, the SAC service shall allow end-user access to the resource requested.	The SAC service shall allow access if the Application Function attribute value(s) do not define access restriction.	
17.23	If Application Function attributes exist, the SAC service shall prevent end-user access to the resource requested.	The SAC service shall not allow access if the Application Function attribute value(s) do define access restriction.	
17.26	The SAC service shall communicate the presence of access restrictions to legacy and external applications to prevent end-user access to resources.	The SAC service shall notify the legacy and external application of the presence of access restrictions.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
17.27	The SAC service shall communicate the presence of data restrictions to legacy and external applications to prevent end-user access to resources.	The SAC service shall notify the legacy and external application of the presence of data restrictions.	
17.28	The SAC service shall communicate the presence of system resource restrictions to legacy and external applications to prevent end-user access to resources.	The SAC service shall notify the legacy and external application of the presence of system resource restrictions.	
17.29	The Policy Enforcement Point shall have the capability to intercept access requests from an authenticated requestor of a requesting application.	Prior to permitting or denying access to a request, the Policy Enforcement Point (PEP) shall intercept requests and obtain a decision from the Policy Decision Point (PDP).	
17.30	The Policy Enforcement Point shall have the capability to forward access requests to the Policy Decision Point.	To obtain the decision from the Policy Decision Point (PDP), the Policy Enforcement Point (PEP) shall forward the access request to the Policy Decision Point (PDP).	
17.31	The Policy Enforcement Point shall have the capability to receive access control decisions from the Policy Decision Point.	To obtain the decision from the Policy Decision Point (PDP), the Policy Enforcement Point (PEP) shall receive the access decision from the Policy Decision Point (PDP).	
17.32	Logical Access Control Services shall be provided that enables a run time Policy Decision Enforcement capability for Course Grain Access Controls as required by consuming applications.	The Policy Decision Point (PDP) shall communicate with the Policy Enforcement Point (PEP) to enable run time Policy Decision Enforcement capability for Coarse Grain Access Controls as required by consuming applications.	
17.33	Logical Access Control Services shall be provided that enables a run time Policy Decision Enforcement capability for Role-based Access Controls as required by consuming applications.	The Policy Decision Point (PDP) shall communicate with the Policy Enforcement Point (PEP) to enable run time Policy Decision Enforcement capability for Role-based Access Controls as required by consuming applications.	
17.36	Logical Access Control Services shall be provided that enables a run time Policy Decision Enforcement capability related to Separation of Duties Access Controls.	The Policy Decision Point (PDP) shall communicate with the Policy Enforcement Point (PEP) to enable run time Policy Decision Enforcement capability related to Separation of Duties Access Controls.	

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
17.37	Logical Access Control Services shall be provided that enables a run time Policy Decision Enforcement capability related to Least Privilege Access Controls.	The Policy Decision Point (PDP) shall communicate with the Policy Enforcement Point (PEP) to enable run time Policy Decision Enforcement capability related to Least Privilege Access Controls.	
17.39	The Policy Enforcement Point (PEP) shall have the capability to enforce access control decisions including any obligations contained in the access decision.	The SAC service Policy Enforcement Point (PEP) shall have the capability to enforce access control decisions.	

In Table 2-6, the requirements implemented in Increment 1 and 2 are identified. These requirements are migrated to the new tool and included in the regression testing of the SAC service functionality.

Table 2-6: SAC Business Needs and Requirements To Be Migrated

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
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.			
14.01	The SAC service shall provide an Attribute Service (AS) which will obtain user attributes from multiple data stores such as databases and LDAP directories.	The SAC service Policy Information Point (PIP) shall use an Attribute Service to obtain the user attributes.	Increment 1
14.03	The SAC service shall interface with other services/applications to allow a client to indicate (add) their opt-in/opt-out and other client data restriction preferences.	<p>The SAC service shall obtain client preferences from other services/applications and input to the Policy Information Point (PIP). For example, SAC service shall provide the ability to make authorization decisions based on the following attribute categories:</p> <ul style="list-style-type: none"> • Client Preference • Data Restriction • User Security • Contextual Constraints • Application Function 	Increment 1

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
14.04	The SAC service shall interface with other services/applications to allow a client to indicate (add) their client data restriction preferences for individuals.	<p>The SAC service shall obtain client preferences from other services/applications and input to the Policy Information Point (PIP).</p> <p>For example, the SAC service shall provide the ability to make authorization decisions based on the following attribute categories:</p> <ul style="list-style-type: none"> • Client Preference • Data Restriction • User Security • Contextual Constraints • Application Function 	Increment 1
14.05	The SAC service shall interface with other services/applications to allow a client to indicate (add) their client data restriction preferences for groups.	The SAC service shall obtain client preferences from other services/applications and input to the Policy Information Point (PIP) which will indicate data restriction for groups.	Increment 1
15 Policy Administration: Provide a digital process of creating, disseminating, modifying, managing, and maintaining hierarchical rule sets to control digital resource management, utilization, and protection in a standard policy exchange format.			
15.02	Provide synchronized access management services that allow for centralized policy control and distributed policy decision-making/enforcement.	The SAC service shall provide an enterprise wide view of policies.	Increment 2
15.06	Logical Access Control Services shall be provided that enable Policy Administration for Coarse Grain Access Controls as required by consuming applications.	The SAC Service shall provide the ability to manage, define, and enforce policy at the Coarse Grain level.	Increment 2
15.07	Logical Access Control Services shall be provided that enable Policy Administration for Role-based Access Controls as required by consuming applications.	The SAC Service shall provide the ability to manage, define, and enforce policy at the Role-based level.	Increment 2
15.08	Logical Access Control Services shall be provided that enable Policy Administration for Attribute Based Access Controls as required by consuming applications.	The SAC Service shall provide the ability to manage, define, and enforce policy at the Attribute-based level.	Increment 2

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
15.09	Logical Access Control Services shall be provided that enable Policy Administration for Application Specific Functionality Controls as required by consuming applications.	Logical Access Control Services shall be provided that enables an authorized Policy Administration capability for Application Specific Functionality Controls as required by consuming applications. Functionality controls to include security and privacy.	Increment 2
16 Policy Decision: Provide a capability that serves as an access control authorization authority for evaluating access control policies based on a variety of inputs.			
16.01	The SAC service shall have a policy decision point with the ability to make access control decisions.		Increment 1
16.02	The Policy Decision Point shall utilize user attributes and policies to determine authorization decisions.		Increment 1
16.03	The Policy Decision Point shall provide the following access decision responses: Permit, Deny, Indeterminate, or Not Applicable to the Policy Enforcement Point.	The SAC service Policy Decision Point (PDP) shall provide the following access decision responses to the SAC service Policy Enforcement Point (PEP): Permit, Deny, Indeterminate, or Not Applicable.	Increment 1
16.04	The Policy Decision Point shall have the capability to receive access control requests from the Policy Enforcement Point.		Increment 1
16.11	Logical Access Control Services shall be provided that enables a Policy Decision capability that serves as an access control authorization authority for Attribute Based Access Controls as required by consuming applications.	Logical Access Control Services shall be provided that enables an authorized Policy Decision capability for Attribute Based Access Control as required by consuming applications.	Increment 1
16.12	Logical Access Control Services shall be provided that enables a Policy Decision capability that serves as an access control authorization authority for Application Specific Functionality Controls as required by consuming applications.	Logical Access Control Services shall be provided that enables an authorized Policy Decision capability for Application Specific Functionality Controls as required by consuming applications. Functionality controls to include security and privacy.	Increment 1
17 Policy Enforcement: Provide a capability that restricts access to specific systems or content in accordance with policy decisions that are made.			

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
17.03	The SAC service shall interface with Authentication services as required to facilitate the SAC processes.	The SAC service shall obtain authenticated identities that participate in access control decisions.	Increment 2
17.04	The SAC service shall interface with the Provisioning service as required to facilitate the SAC processes.	The SAC service shall obtain authorizations that participate in access control decisions.	Increment 2
17.05	The SAC service shall interface with SSO services as required to facilitate the SAC processes.	The SAC service shall obtain authenticated identities that participate in access control decisions.	Increment 2
17.06	The SAC service shall determine if content restrictions exist for each user session within a subscribing application.	The SAC service Policy Decision Point (PDP) shall use policy rules to include content restrictions on protected objects.	Increment 1
17.07	In the absence of access restrictions, the SAC service shall allow end-user access to the resource requested.	If the policy rules do not define access restriction, the SAC service shall allow access.	Increment 1
17.08	If access restrictions exist, the SAC service shall prevent end-user access to the resource requested.	If the policy rules do define access restriction, the SAC service shall not allow access.	Increment 1
17.09	The SAC service shall manage system and data access based on approved Client Preference attributes.	The SAC service shall obtain client preferences from other services/applications and input to the Policy Information Point (PIP).	Increment 1
17.10	In the absence of Client Preferences, the SAC service shall allow end-user access to the resource requested.	If the Client Preferences do not define access restriction, the SAC service shall allow access.	Increment 1
17.24	The SAC service shall interface with legacy and other external applications as required to facilitate the SAC processes.		Increment 1
17.25	The SAC service shall communicate the absence of access restrictions to legacy and external applications to allow end-user access to resources.	In the absence of access restrictions, the SAC services will notify the legacy and external application of the absence of access restrictions.	Increment 1
17.34	Logical Access Control Services shall be provided that enables a run time Policy Decision Enforcement capability for Attribute Based Access Controls as required by consuming applications.	The Policy Decision Point (PDP) shall communicate with the Policy Enforcement Point (PEP) to enable run time Policy Decision Enforcement capability for Attribute Based Access Controls as required by consuming applications.	Increment 1

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
17.35	Logical Access Control Services shall be provided that enables a run time Policy Decision Enforcement capability for Application Specific Functionality Controls as required by consuming applications.	The Policy Decision Point (PDP) shall communicate with the Policy Enforcement Point (PEP) to enable run time Policy Decision Enforcement capability for Application Specific Functionality Controls as required by consuming applications.	Increment 1

2.6.5 CSP and IP

2.6.5.1 Decoupling CSP and IP

As currently deployed, the CSP and IP systems are tightly coupled, using the same person file for both CSP and IP. This tight coupling made integrations with VA's VIC system, MVI, and AcS Provisioning challenging, because use cases for integrating person information with CSP, IP, and other systems differ. The VA architects determined that to best support current and future integration efforts, CSP and IP must be decoupled.

The AcS Increment 4 RSD contains general requirements for decoupling CSP and IP, and these were deferred by the AcS development team. This document contains elaborated requirements for CSP and IP decoupling.

In Table 2-7, CSP and IP enhancements were identified for the decoupling of the CSP and IP services.

Table 2-7: CSP/IP Business Needs and Requirements for Decoupling

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
1.0 Identity Proofing: Provide a digital process that vets and verifies the information (e.g., identity history, credentials, documents) that is used to establish the identity of a system entity, initiate a chain of trust in establishing a digital identity, and bind it to an individual.			
8.0 Credential Issuance: Provide a digital process by which possession of a credential is securely passed to an entity.			
1.13	The In-person Identity Proofing service shall provide a means for the VA staff to query whether the applicant has an existing proofing record.	Requirement Clarification provided below	Increment 5
1.14	In the case an applicant has an existing proofing record, the In-person Identity Proofing service shall provide a means for the VA staff to validate any credentials issued.	Requirement Clarification provided below	Increment 5
1.21	The Identity Proofing Services data store shall interface with internal and external enterprise data stores and applications to maintain records and share data necessary to enable other IAM initiatives in the most efficient, collaborative, and data-secure manner.	Requirement Clarification provided below	Increment 5

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
1.30	The Identity Proofing Service shall pass the required data points collected from all subscribing online applications/services to the MVI.	Requirement Clarification provided below	Increment 5
1.43	The Identity Proofing Service shall interface with the VA Credentialing Service to make available to it the record of each individual's proofing status.	Requirement Clarification provided below	Increment 5
1.48	The Identity Proofing Service shall assure that the results of the In-Person Proofing are recorded and associated with the correct (existing) credential record.	Requirement Clarification provided below	Increment 5
8.02	The Credential Service shall receive Credential request from ID Proofing Service.	Requirement Clarification provided below	Increment 5
8.11	The Credential Service shall validate proofing with ID Proofing Service.	Requirement Clarification provided below	Increment 5
8.13	The Credential Service shall receive a response from the ID Proofing Service of the individual's ID Proofing Status.	Requirement Clarification provided below	Increment 5
8.19	The Credential Service shall generate a Credential after receiving a positive response from the ID Proofing Service.	Requirement Clarification provided below	Increment 5
8.20	The Credential Service shall return a rejection of Credential after receiving a negative response from ID Proofing Service.	Requirement Clarification provided below	Increment 5
8.26	The Credential Service shall receive a Credential upgrade request from the ID Proofing Service.		
8.28	The Credential Service shall receive a request to upgrade to a Level 2 Credential from the ID Proofing Service.	Requirement Clarification provided below	Increment 5

1. The VA CSP system and the VA IP system shall be decoupled.
2. The VA CSP and VA IP systems shall function as two separate services.
3. The VA CSP system and VA IP systems shall have their own person records which will not be shared with one another.
4. The VA CSP and VA IP system records shall be linked by an identifier.
5. The VA CSP system shall maintain a reference to the associated proofing records using the IP IEN.
6. The VA IP system shall maintain the existing source ID with the MVI that was created during the coupling of the VA CSP and VA IP systems, additionally, if a new source ID

is assigned, that must be coordinated with MVI in order for records to be updated accordingly.

7. The current VA CSP/IP system records shall remain in the decoupled VA IP system in order to keep the MVI correlations intact.
8. The VA CSP system shall be a consuming application of the VA IP system.
9. The VA CSP system shall allow users requesting a VA CSP to be proofed for the appropriate level of assurance.
10. The VA IP system shall provide a Retrieve Proofing Record Web Service.
11. The Retrieve Proofing Record Web Service shall return the following information:
 - IP IEN
 - First Name
 - Last Name
 - DOB
 - Phone
 - Address
 - City
 - State
 - Postal Code
 - Country
 - User ID
 - VA Affiliation
 - Assurance Level
 - Proof Date
 - Comment
 - Proof Location
 - Proof Status
 - Proof Origin
12. The IP service shall be able to provide the CSP credential information associated to the In-Person Proofing Record
13. When requested, the IP Service shall be able to Identity Proof a person to **upgrade** their VA CSP credential. **Note:** Veterans with a LOA2 credential are eligible for a VIC Card.
14. When requested, the IP Service shall be able to proof a person to be issued a VA CSP. **Note:** Veterans with a LOA2 credential are eligible for a VIC Card.

In Table 2-8, the requirements that are identified were implemented in AcS Increment 3 and 4 for the VHIC deployment in the summer of 2013. These requirements represent the delivered functionality of the integration between the VA IP system and VHIC.

The CSP and IP requirements include the following:

1. Shall require migration to the new IP service post decoupling
2. Shall be included in regression testing of the VIC AcS service functionality

Table 2-8: CSP/IP Business Needs and Requirements To Be Migrated and Tested Post Decoupling

Req #	Requirement	In-Scope Requirement Clarification	Development Release (Increment)	Requirement Location
1	The Identity Proofing service shall not capture or require an email address when completing the In-Person Proofing process.	Remove the email field from Identity Proofing Screen 1 (User Profile) Required fields: First Name, Last Name, DOB, Street Address, City, State, Country, Postal Code, Affiliation Optional fields: Phone Number VIC has no requirement for the Veteran to provide an email address during the VIC Card issuance process. VIC accepts that the Email field will be removed from the Proofing screen, and is aware that the CSP credential will become disabled. The Proofing record will still be accessible if a VIC card needs to be re-issued.	Increment 3 VIC 4.0	VIC AcS iRSD
2	The Identity Proofing service shall not capture or require a User ID to complete the Identity Proofing process.	Remove the User ID field from Proofing Screen 1 (User Profile) The user can complete In-Person Proofing without a User ID. Required fields: First Name, Last Name, Street Address, DOB, City, State, Country, Postal Code, Affiliation Optional fields: Phone Number “User ID” should not appear on the screen as field. VIC accepts that the User ID field will be removed and is aware that the CSP credential will be become disabled. The Proofing record will still be accessible if a VIC card needs to be re-issued.	Increment 3 VIC 4.0	VIC AcS iRSD

Req #	Requirement	In-Scope Requirement Clarification	Development Release (Increment)	Requirement Location
3	The Identity Proofing Service shall receive the Identity, Address, Affiliation and Proofing Location data from VIC, parse it, and use the data for pre-population according to the UI screen requirements.	<p>The VIC System shall set the Affiliation field to “Veteran” and pass it to the Identity Proofing System.</p> <p>VIC will pass the following information:</p> <ul style="list-style-type: none"> • First Name • Last Name • DOB • Street Address • City • State • Postal Code • Country • Affiliation • Proofing Location <p>Note: This information will be obtained by the VIC System from MVI and Enrollment Services (ES) and will be passed to the Identity Proofing Service</p>	Increment 3 VIC 4.0	VIC AcS iRSD
4	<p>The Identity Proofing Screen 1 (User Profile) shall contain the following fields:</p> <ul style="list-style-type: none"> • First Name • Last Name • Phone Number • Date of Birth • Street Address • City • State • Country • Postal Code • Proofing Location • VA Affiliation 	<p>Required fields: First Name, Last Name, DOB, Street Address, City, State, Country, Postal Code, Proofing Location, VA Affiliation</p> <p>Optional fields: Phone Number</p> <p>“User ID” should not appear on the screen as field.</p> <p>Default identity and address information from MVI & ES is populated. The Proofing Clerk will not be allowed to overwrite information from MVI & ES</p> <p>Proofing Location will be populated and will come from the VIC system.</p>	Increment 3 VIC 4.0	VIC AcS iRSD
5	The Identity Proofing Screen 2 (Address Verification) shall contain the following fields:	Required fields: Address Validation Type, Postmark Date, Street Address, City, State, Country, and Postal Code, ‘N/A’ check box (when	Increment 3 VIC 4.0	VIC AcS iRSD

Req #	Requirement	In-Scope Requirement Clarification	Development Release (Increment)	Requirement Location
	<ul style="list-style-type: none"> Address Validation Type Postmark Date Street Address City State Country Postal Code 	<p>applicable)</p> <p>There are no optional fields.</p> <p>The Address Validation Type and Postmark Date fields will not be pre-populated. The VIC Clerk will complete the Address Validation Type and Postmark date fields.</p> <p>VIC retrieves the address information from Enrollment Services (ES) and sends it to IP in the request. IP pre-populates the address information received from VIC on the screen. The proofing system shall prevent the user from overwriting the address information pre-populated on Screen 2.</p>		
6	<p>The Identity Proofing Screen 3 (Primary Identification) shall contain the following fields:</p> <ul style="list-style-type: none"> ID Type Country of Issuance State of Issuance Identification Number Expiration Date Information Provided/Verified By 	<p>Required fields: ID Type, Country of Issuance, State of Issuance, Identification Number, Expiration Date, Information Provided/Verified By, 'N/A' check box (when applicable)</p> <p>There are no optional fields on this screen.</p>	Increment 3 VIC 4.0	VIC AcS iRSD
7	<p>The Identity Proofing Screen 4 (Secondary Identification) shall contain the following fields:</p> <ul style="list-style-type: none"> ID Type Country of Issuance State of Issuance Identification Number Expiration Date Information Provided/Verified By 	<p>Required fields: ID Type, Country of Issuance, State of Issuance, Identification Number, Expiration Date, Information Provided/Verified By, 'N/A' check box (when applicable)</p> <p>There are no optional fields on this screen.</p>	Increment 3 VIC 4.0	VIC AcS iRSD
8	The Identity Proofing Screen 5 (Submit Proof) shall not contain any fields.	There are no required or optional fields on this screen.	Increment 3 VIC 4.0	VIC AcS iRSD

Req #	Requirement	In-Scope Requirement Clarification	Development Release (Increment)	Requirement Location
9	The Identity Proofing service shall return the system User to the VIC system upon completion of the Identity Proofing process and will pass identified traits.	Traits Passed: <ul style="list-style-type: none"> • CSPID • Assurance level • Proof Status • Comment • Proof Date • Timestamp 	Increment 3 VIC 4.0	VIC AcS iRSD
10	The VIC System shall retrieve the Level 2 Proofing record from the Identity Proofing Service	The Identity Proofing service will receive a web service call from VIC requesting a Level 2 record. The Identity Proofing service will return the Proofing record with the following data: <ul style="list-style-type: none"> • CSPID • Assurance level • Proof Status • Comment • Proof Date • Timestamp 	Increment 3 VIC 4.0	VIC AcS iRSD
11	The Identify Proofing service “Cancel” button will alert the Proofer that canceling the Identity Proofing process will cause a loss of all data and shall be prompted again if they want to cancel the process.	“Yes” and “No” will be options. If the Proofer decides to cancel, all data is lost, and the Proofer is returned to the VIC search screen. If the Proofer opts out and selects “No,” they return to the screen that they were on and will be able to proceed with the Proofing event without losing any data.	Increment 3 VIC 4.0	VIC AcS iRSD
12	The Identity Proofing service shall correlate the existing person records to the MVI prior to full integration with the MVI.	Requirements : <ol style="list-style-type: none"> 1. The IP System technical team shall provide a copy of all IP Person records to IdS for development of the CSP/IP correlation within the MVI. The outcome of this process shall be the assignment of a new or existing Integration Control Number (ICN) to each of the records enumerated. 2. The IP System application Person records sent for correlation/enumeration shall 	Increment 4 VIC 4.1	VIC AcS iRSD

Req #	Requirement	In-Scope Requirement Clarification	Development Release (Increment)	Requirement Location
		<p>include the following traits:</p> <ul style="list-style-type: none"> • Last Name • First Name • Middle Name (if available) • SSN • Date of Birth • Gender • LOA • Fully Qualified Source ID: <ul style="list-style-type: none"> ○ Assigning Authority – Value to be determined during design phase ○ Assigning Location – Value to be determined during design phase ○ Identifier Type – Value to be determined during design phase ○ Internal Entry Number – This should be the unique DB identifier for the person record in CSP/IP 		
13	The Identity Proofing service shall use the cached ICN sent from the VIC system and use it to retrieve a record in the MVI.	The ICN shall be included when retrieving a record from the MVI. The CSP/IP system shall not collect or store the ICN. Note: The ICN will be passed to CSP/IP by the VIC system.	Increment 4 VIC 4.1	VIC AcS iRSD
14	The Identity Proofing service shall have the capability of receiving a fully qualified identifier from the integrating application for use in the transaction.	<p>Qualified Identifier: An ICN, EDIPI, or Source ID.</p> <p>Integrating Applications: MVI, VIC</p> <p>The Source ID consists of the following: (1) Assigning Authority (2) Assigning Location (3) Identifier Type (4) Internal Entry Number</p>	Increment 4 VIC 4.1	VIC AcS iRSD
15	The Identity Proofing web service shall be protected by DataPower WS Proxy.	The IP web service is used by VIC and VIC is the initial consumer. However this is a general requirement for the IP web services.	Increment 4 VIC 4.1	VIC AcS iRSD
16	The VIC user shall be able to Retrieve and Add a proofing record.	(See the IP use cases in the IP RSD.)	Increment 3 VIC 4.0	VIC AcS iRSD

Req #	Requirement	In-Scope Requirement Clarification	Development Release (Increment)	Requirement Location
17	<p>The IP Web service will return one of the following conditions:</p> <ol style="list-style-type: none"> 1. Applicant has an existing L2 (or above) proofing record. <p>The VIC application will record that a proofing record exists and flag the card request to indicate that proofing has already taken place.</p> <ol style="list-style-type: none"> 2. If the Applicant has no proofing record, or has a proofing record with a status of L1, Identity Proofed Pending, or Failed – Pending, the VIC user shall proof the VIC Card Applicant according to VA Directive 6501—VA Identity Verification In-Person Proofing (IPP) Process. 		Increment 3 VIC 4.0	VIC AcS iRSD
18	The VA IP system shall not be permitted to store the ICN with the person record.		Increment 4 VIC 4.1	VIC AcS iRSD

In Table 2-9, the requirements identified for the VA IP and MVI integration were implemented in AcS Increment 3 and 4 for the VHIC deployment in the summer of 2013. These requirements represent the delivered functionality of the integration between the VA IP system and MVI.

The VA IP and MVI integration requirements include the following:

1. Shall require migration to the new IP service post decoupling
2. Shall be included in regression testing of the IP and MVI service functionality

Table 2-9: IP and MVI Integration Requirements To Be Migrated and Tested Post Decoupling

Req #	Requirement	In-Scope Requirement Clarification	Development Release (Increment)	Requirement Location
1	The Identity Proofing Service shall perform a Retrieve Person w/ Get Corresponding IDs.	Reference the following documents: <ul style="list-style-type: none"> MVI Use Case – “Retrieve Person w/Get Corresponding ID” 	Increment 4 VIC 4.1	CSP/IP MVI iRSD
2	The Identity Proofing Service shall perform a MVI Add Person/Add Correlation.	Reference the following documents: <ul style="list-style-type: none"> MVI Use Case – “Add Person/Add Correlation” 	Increment 4 VIC 4.1	CSP/IP MVI iRSD
3	The Identity Proofing Service shall perform a MVI Update Person.	Reference the following documents: <ul style="list-style-type: none"> MVI Use Case – “Update Person” 	Increment 4 VIC 4.1	CSP/IP MVI iRSD

2.6.5.2 IP Enhancements

In Table 2-10, the requirements that are not related to the decoupling of the VA CSP and VA IP systems and were not delivered in previous increments are shown. These requirements are enhancements to the current VA IP service, allowing for improved functionality.

Table 2-10: IP Business Needs and Requirements Enhancements

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
1.0 Identity Proofing: Provide a digital process that vets and verifies the information (e.g., identity history, credentials, documents) that is used to establish the identity of a system entity, initiate a chain of trust in establishing a digital identity, and bind it to an individual.			
	The VA IP system shall remove the Identification type selected as Primary ID from the Secondary ID type options.	If a driver’s license was selected as a Primary ID type, the driver’s license should not be available to be selected as a Secondary ID type.	Increment 5
	The VA IP system shall populate the Proofing Location field from a VA authoritative source.	During Identity Proofing, the Proofing Location information needs to subscribe to a data source in order to be updated automatically – SDS file.	Increment 5

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
	The VA IP system shall be able to select "N/A" (Not Applicable) as an option in the 'State of Issuance' dropdown list.	Certain Identification types are not issued by States (i.e. Birth Certificate)	Increment 5
	The VA IP system shall have the capability of receiving a fully qualified identifier from the integrating application for use in the transaction.	Qualified Identifier: EDIPI	Increment 5
	The VA IP system shall have the capability of receiving a fully qualified identifier from the integrating application for use in the transaction.	Qualified Identifier: Source ID	Increment 5

2.6.6 e-Signature

The requirements for the e-Signature (electronic signature) service were defined in the AcS Increment 2 RSD. As currently deployed, a risk (change request #1457) was presented during the integration of the Veteran Authorization and Preferences Interface Improvements (VAP ii) application with the e-Signature service in support of the eHealth Exchange (formerly known as NwHIN)) authorization flow, which allows a Veteran to create or update the NwHIN sharing authorization.

In Figure 2-5 below, the high-level flow in the current e-Signature service implementation is shown. The risk occurs when a name change happens in the context of the e-Signature service. There are several required parameters when a consuming application calls the e-Signature service:

1. **File:** PDF or Word document to be signed
2. **UserID:** Unique identifier for the user
3. **Name:** Full name of the user
4. **Filename:** Name of the file

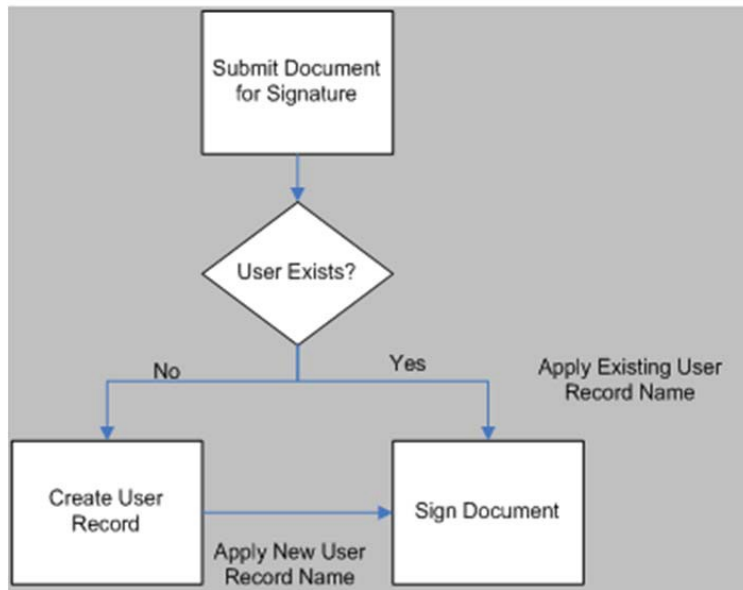


Figure 2-5: Current e-Signature Service Flow

In the current implementation, the e-Signature service upon initial use creates a record (including a key pair and certificate) using the data provided by the consuming application. The name is included in the signature field as a part of the visible signature. If the name changes, but the userID passed matches a record in the e-Signature service data store, the name displayed in the visible signature differs from the name provided in the transaction and the actual user's name.

In Figure 2-6 below, the high-level flow of the implementation based on the requirements to support name changes is shown.

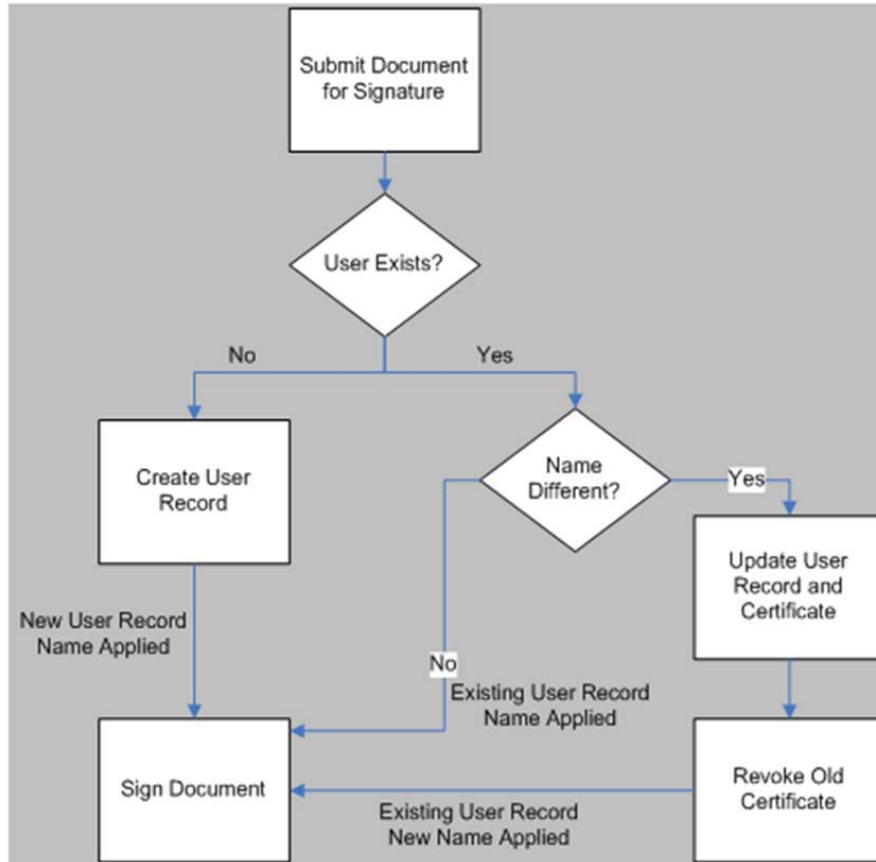


Figure 2-6: e-Signature Service – Name Change Flow

BRD BN	Requirement	In-Scope Requirement Clarification	Development Release (Increment)
BN13.1	The e-Signature service shall accept a request to apply an e-Signature.	Requirement Clarification Below	

Requirements:

1. The e-Signature service shall require userID to be equal to CSID + “_” + userID.
Note: The CSID and the userID are obtained from the VAAFI header.
2. The e-Signature service shall check whether the userID already exists in the e-Signature data store:
 - a) The e-Signature service shall compare the name on the existing user record in the e-Signature data store to the name passed for the current transaction, if the userID exists in the e-Signature data store:
 - i. The e-Signature service will use the existing record (certificate and key pair) to sign the document if the name matches.

- ii. The e-Signature service will update the existing record and certificate in the e-Signature data store with the name from the current transaction if the names do not match.
- iii. The e-Signature service will revoke the old certificate in the e-Signature data store if names do not match.
- b) The e-Signature service shall create a new user record (existing functionality) if the userID does not exist in the e-Signature data store.
- c) The e-Signature service shall maintain a history (archive) of revoked certificates for document validation.

Note: There may be an impact on the e-Signature User Licensing by adjusting the userID format as reformatting the userID causes any existing e-Signature users to be issued new certificates. Because VAP ii is the only consumer using the e-Signature service, the impact is minimal.

2.7 Graphical User Interface Specifications

- 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 are 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.

How many users does the current system support?
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"> 700,000 employees 350,000 contractors 22,000,000 Veterans
How many users does the new system (or system modification) support?
The new system is scalable to accommodate an internal and external user base of approximately 29 million.
What is the predicted annual growth in the number of system users?

The new system supports at least 10M 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 iEHR).
- 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](#).

Note: VAAFI is the only identified user of the Virtual Directory, supporting the IAM Portal Strategy.

- f. 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.
- g. The online procedures prompted from a user interface execute under five seconds with an average of four seconds within the budgeted resource utilization constraints.
- h. Metric data indicating the performance characteristics of the system to support application monitoring is provided.
- i. The system supports 24/7/365 operations.
- j. The desired system behavior is maintained at various load levels.
- k. 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

Service	Response Times
	time of ten seconds

2.10 Quality Attributes Specifications

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)
- 508 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](#).
- An implementation plan is developed for the access services.

2.11 Reliability Specifications

The AcS solution is hosted within the [REDACTED] environment as required by VA. [REDACTED] 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 [REDACTED]

***Standards adopted from specification created by Application Structure & Integration Services (ASIS).**

Service Availability Level 4

Description	Mission Critical Information
Minimum Availability	99.9%
Maximum Downtime Per Month	43 minutes
Business Value	Essential to fundamental business operations – outage seriously impairs functioning of business.
System Response	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.
Operational Hours	Required 24 hours a day, every day.
Significant Outage	More than five minutes of downtime is considered significant at any time and requires an ANR to be sent out

Outage Impact

to the appropriate teams.

Interruption of service may result in severe financial, regulatory, patient safety, patient health, or other business issues.

Scheduled Maintenance

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 of Integration

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

2.13 Security Specifications

- 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 the 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 3-1: Applicable Standards

NIST Special Publication 800-63 Version 1.0.2; Electronic Authentication Guideline
OASIS XACML 2.0
Section 508 Standards Guide
VA Directive 6500; Information Security Program
VA Directive 6501; VA Identity Verification In-Person Proofing (IPP) Process
World Wide Web Consortium (W3C) SOAP Standard
World Wide Web Consortium (W3C) XML Standard
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 HSPD-12 specifications where applicable (i.e., Personal Identification Verification (PIV))
Follows the documentation specifications provided by the ProPath website and VA Project Management Accountability System (PMAS)

XACML 2.0 is the standard leveraged by the SAC service. XACML provides the following capabilities:

- XACML 2.0 is an Organization for Advancement of Structured Information (OASIS Standards) 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 sections.

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 Purchased Components

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

6 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.

7 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).

8 Estimation

Table 8-1: Function Point Analysis Results Table

Function Point Analysis Results Table						
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:						

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

Attachment A Approval Signatures

This section is used to document the approval of the Requirements Specification Document during the Formal Review. The review should be ideally conducted face to face where signatures can be obtained 'live' during the review however the following forms of approval are acceptable:

1. Physical signatures obtained face to face or via fax
2. Digital signatures tied cryptographically to the signer
3. /es/ in the signature block provided that a separate digitally signed e-mail indicating the signer's approval is provided and kept with the document

The Chair of the governing IPT, Business Sponsor, IT Program Manager, and the Project Manager are required to sign. Please annotate signature blocks accordingly.

REVIEW DATE: <date>

SCRIBE: <name>

SIGNATURE(S) REDACTED

