**Department of Veterans Affairs**

**My Health*e*Vet (MHV)**

**Integration with**

**Identity and Access Management Services**

**AccessVA, SSOe, AMS, SAC and MVI**

**MHV Federated Credentials to Production**

**MHV Pilot Support of Delegation**

**Integration Requirements Specification Document**

**

**April 2016**

**Version 1.4**

Revision History

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 5/11/16 | 1.4 | Updates from Formal Review  and corrected signatories on IAM side | Ken Bowers |
| 4/18/16 | Del update 5.0 | Added section SAC-AMS. For Formal Review. | Ken Bowers |
| 4/14/16 | Del update 4.0 | Inputs from MHV review, added appendix with paths to applications | Ken Bowers |
| 3/17/16 | Del update 3.1 | Updates from 3/16 Delegation Call discussion | Ken Bowers |
| 3/15 | Del update 3.0 | Inputs from tech leads | Ken Bowers |
| 3/14/2016 | Del update 02.4 | Re-organized with Delegation sections. Updated existing material on Federated credential to reflect move to production added Delegation Pilot. Updates from tech review, discussion of Delegation interactions. | Ken Bowers |
| 7/17/2015 | 1.3 | Completed a tech edit review. Posted the PDF on the AcS TSPR and AcS Phase 2 TSPR. | Bruce Taylor |
| 7/15/2015 | 1.2 | Updated document with Rational Requirements Composer Feature tags to uniquely identify the traceable AcS requirements. | David Hazelbaker |
| 6/02/2015 | 1.1 | Updated BPMO signatory from Wulf to Neal | Ken Bowers |
| 5/14/2015 | 1.1 | Updates in response to Formal Review anomaly | Ken Bowers |
| 4/27/2015 | 1.1 | Updated timeout and logoff | Ken Bowers, Andrew Allen |
| 4/17/2015 | 1.1 | Changes made to focus the iRSD on the MHV Pilot | Ken Bowers |
| 4/6/2015 | 1.1 | Update based upon comments from Peer Review. Updated latest flow diagrams | Ken Bowers, Linda Reimonenq |
| 2/23/2015 | 1.1 | Update to latest PS traits, add information about CSPs and requirements that IAM should direct MHV user’s registration with Norton and connect.gov at LOA 2. Updated To be flow to align with BUC discussions  Clarified landing page when SSOe timeout happens | Andrew Allen, Ken Bowers |
| 1/22/2015 | 1.1 | Restructure for MHV 12.12 to account for   * MHV IEN in PS headers * MHV CSP selector pop up “widget” * MHV no longer checking internally stored hash * MHV new SSO flow * MHV account update passed on IAM traits flow * MHV new user registration based on IAM traits | Ken Bowers |
| 8/22/2014 | 1.0 | Completed a tech edit review. Reformatted to coincide with iRSD template v1.3. Embedded the email approval signatures in the PDF to be posted on the AcS TSPR. | Bruce Taylor |

*Place latest revisions at top of table. Remove blank rows.*

Table of Contents

[1.0 Introduction 1](#_Toc450738362)

[1.1 Purpose 1](#_Toc450738363)

[1.2 Scope 1](#_Toc450738364)

[1.3 References 3](#_Toc450738365)

[1.3.1 Requirements, Design, and Service Description Documentation 3](#_Toc450738366)

[1.3.2 Business Policy Documentation 4](#_Toc450738367)

[1.3.3 Abbreviations and Definitions 4](#_Toc450738368)

[2.0 Functional Requirements 4](#_Toc450738369)

[2.1 Functional Requirements for MHV – User Handling 4](#_Toc450738370)

[2.1.1 Assumptions 4](#_Toc450738371)

[2.1.2 AccessVA Enablement for MHV 4](#_Toc450738372)

[2.1.2.1 Users Starting on MHV 5](#_Toc450738373)

[2.1.2.2 Users Starting in AccessVA 6](#_Toc450738374)

[2.1.3 SSOe to MHV within the VA Firewall – Application Junction 6](#_Toc450738375)

[2.1.3.1 Portal Strategy Traits 7](#_Toc450738376)

[2.1.3.2 CSP Data Only 7](#_Toc450738377)

[2.1.4 MHV map SSOe user to MHV Account 8](#_Toc450738378)

[2.1.4.1 CSP handling 8](#_Toc450738379)

[2.1.4.2 MHV Handling of MHV IEN from SSOe 8](#_Toc450738380)

[2.1.4.3 MHV Check for Existing MHV Accounts to Correlate 8](#_Toc450738381)

[2.1.4.4 Register SSOe user for new MHV account 9](#_Toc450738382)

[2.1.4.5 As-Is and To-Be Flows for SSOe user and MHV account 9](#_Toc450738383)

[2.1.5 Perform Logoff and Timeout 16](#_Toc450738384)

[2.2 Functional Requirements for MHV – Delegation 16](#_Toc450738385)

[2.2.1 Prerequisites and assumptions 17](#_Toc450738386)

[2.2.2 Identify Delegators – Call AMS service 17](#_Toc450738387)

[2.2.3 Manage Business Authorization Policies 17](#_Toc450738388)

[2.2.4 Enforce Authorization Decision Call IAM SAC 19](#_Toc450738389)

[2.2.5 Identify Delegator’s MHV Account: Call MVI 20](#_Toc450738390)

[2.2.6 User switches between MHV accounts 21](#_Toc450738391)

[2.2.7 MHV Audits Delegator data access 21](#_Toc450738392)

[2.2.8 MHV shall audit call to AMS service 21](#_Toc450738393)

[2.2.9 Delegation flow 21](#_Toc450738394)

[2.3 Functional Requirements for IAM - User 22](#_Toc450738395)

[2.3.1 CSP Selection Options for MHV Users 22](#_Toc450738396)

[2.3.2 AccessVA Account Registration Redirects 23](#_Toc450738397)

[2.3.3 Search for Person (Unattended) for MHV 23](#_Toc450738398)

[2.3.4 Retrieve Person (Returning Corresponding IDs) for MHV 23](#_Toc450738399)

[2.3.5 Get Corresponding IDs for MHV 23](#_Toc450738400)

[2.3.6 Add Person (Add Correlation) for MHV 23](#_Toc450738401)

[2.3.7 Unlink Correlation from ICN for MHV 23](#_Toc450738402)

[2.4 Functional Requirements for IAM – Delegate Views Delegator Data 24](#_Toc450738403)

[2.4.1 Support Retrieve Authorizations call 24](#_Toc450738404)

[2.4.2 Authorize Delegate to view Delegator’s data 24](#_Toc450738405)

[2.4.3 SAC-AMS Integration to provide ACI for VAHP and VHA PR 24](#_Toc450738406)

[2.4.4 Support call to getCorrespondingIds for Delegator data 25](#_Toc450738407)

[3.0 Other Specifications 25](#_Toc450738408)

[3.1 Design Constraints Specifications 25](#_Toc450738409)

[3.2 Disaster Recovery Specifications 26](#_Toc450738410)

[3.3 Performance Specifications 26](#_Toc450738411)

[3.3.1.1 Federated Credential –National Release 26](#_Toc450738412)

[3.3.1.2 Delegation Pilot 26](#_Toc450738413)

[3.4 Quality Attributes Specifications 26](#_Toc450738414)

[3.5 Reliability Specifications 27](#_Toc450738415)

[3.6 Security Specifications 28](#_Toc450738416)

[Attachment A: Approval Signatures 29](#_Toc450738417)

[Appendix A: User Paths to MHV and VDT 31](#_Toc450738418)

[3.7 User paths to MHV 31](#_Toc450738419)

[3.7.1 Production As-Is Paths to MHV SSOe session 31](#_Toc450738420)

[3.7.2 Federated Credential Pilot Paths 33](#_Toc450738421)

[3.7.3 Federated Credential To Be Paths to MHV SSOe session 34](#_Toc450738422)

[3.8 User Paths to Veteran Delegation Tool 35](#_Toc450738423)

[3.8.1 Paths to VDT Delegation Pilot 35](#_Toc450738424)

[3.8.2 Paths to VDT Production 36](#_Toc450738425)

List of Figures

[Figure 1: MHV Authenticate External User – User Starts on MHV 5](#_Toc424908988)

[Figure 2: MHV SSO As-Is Activity Diagram 11](#_Toc424908989)

[Figure 3: MHV SSO Pilot Release Activity Diagram 11](#_Toc424908990)

[Figure 4: MHV SSO Connect Page with Registration Activity Diagram 12](#_Toc424908991)

[Figure 5: MHV SSO Confirm Account Found by MHV Activity Diagram 13](#_Toc424908992)

[Figure 6: MHV SSO To-Be National Release Activity Diagram 14](#_Toc424908993)

List of Tables

[Table 1: IAM Reliability Specifications 27](#_Toc450726736)

# Introduction

## Purpose

The purpose of this integration Requirements Specification Document (iRSD) is to provide the requirements that the My Health***e***Vet (MHV) Development team needs to implement to integrate MHV with Identity and Access Management (IAM) services, in accordance with the IAM service request: SR-370. This iRSD reflects changes in IAM to simplify the Single Sign On (SSO) flow into MHV and changes in MHV to allow for the login to MHV to correlate existing MHV accounts and MHV account registration from traits provided by IAM.

In addition, this iRSD reflects changes for a Production Pilot of MHV flows to allow a delegate to view the MHV account of the person who granted the delegate access, in accordance with the IAM service request: SR-451.

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

* IAM Identity Services (IdS) mandate memorandum (VAIQ #7011145). All applications within VA are mandated by the memo to comply with IAM requirements to ensure that references to the identities of Veterans and their beneficiaries are accurate.
* IAM Access Services (AcS) functionality within VA is mandated by VAIQ #7060071 (<http://vaww.iam.va.gov/IAM_Business_PMO.asp>).

The target audiences for this iRSD include the following:

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

**Note**: This iRSD does not contain the detailed requirements for the changes needed in the MHV system to integrate with IAM services. The MHV team should use this iRSD as a guide for writing the detailed system and, if applicable, user interface design specifications. The MHV team should include both IAM business and technical representatives as stakeholders regarding the MHV design documents. The [Quality Attributes Specifications](#_Quality_Attributes_Specifications) section provides more information about the integration process.

## Scope

This iRSD provides the high-level requirements for updates to the MHV integration with IAM services to address two MHV features:

* MHV use of Federated Credential move from Pilot to Full Production for SSOe user access to MHV
* MHV Pilot of Delegation

**MHV Use of Federated Credential – Pilot to Full Production**

The MHV user will leverage a Single Sign-On – External (SSOe)-enabled Credential Service Provider (CSP), commonly referred to as a “Federated Credential” or “Sign-In Partner.” The flow through AccessVA may be through the AccessVA web page, or through the AccessVA pop-up CSP selector (sometimes referred to as a “widget”).

This iRSD provides requirements for the transition between the following:

* An “As-Is” Pilot Release state. Federated Credential Pilot users go to an alternate MHV SSOe Pilot URL.
  + At the pilot URL users login via the IAM widget using federated credentials. Pilot users leverage Norton Symantec and Connect.gov credentials such as Verizon and ID.me.
  + At the pilot URL, new MHV SSOe logic identifies a user’s MHV account based on a check of the MHV IEN provided by IAM.
  + To ensure uninterrupted production operations, DS Logon serves regular non-pilot users only, and the AccessVA web page will only offer DS Logon to for access to MHV
* A “To-Be” Full production state. All SSOe users go through the flow piloted in the “As-Is” state
  + In the national release, DS Logon users will be routed through the new MHV SSOe logic and the “As Is” MHV flow will be removed.
  + The AccessVA web page and widget will show the full set of federated credentials for MHV.
    - MHV acceptance of the all federated credentials may be implemented across several releases

**MHV Pilot of Delegation**

MHV will enter a production Pilot to support Delegation. Delegations are managed in IAM’s Authorization management Service (AMS). The key flow in MHV is: Delegate logs in to MHV and navigates to view the data of a delegator (a person such as a Veteran or MHV Account Holder who has granted access to the Delegate user).

In order to execute this flow, the delegate must log into MHV with an SSOe session. The Delegation Pilot does not depend on MHV’s full implementation of the federated credential integration.

This iRSD provides requirements for the MHV Delegation Pilot:

* No “As-Is” flow is shown as there is no current implementation of Delegation MHV
* The “To-Be” is the MHV Delegation Pilot flow. Delegation Pilot users go to an alternate Delegation MHV Pilot URL. At that URL, MHV provides the ability for them to navigate to view the Delegator’s information.

**Services**

The MHV integration with IAM calls the following IAM services:

* AccessVA:
  + Third-Party Credential Onboarding (3POB)
* SSOe
* MVI:
  + Get Corresponding Identifiers (IDs) service
  + Currently, the MVI integration touch point for SSOe with the Department of Defense Self-Service Logon (DS Logon) already relies on the MVI Get Corresponding IDs service. For MHV to start leveraging the Portal Strategy, MHV will call the MVI Get Corresponding IDs service to first check whether the ICN or EDIPI is available.
  + Search Unattended service
  + The “To-Be” state includes the possibility of SSOe sessions that only have traits from a Credential Service Providers (CSP) and no IAM Portal Strategy traits. In those cases, MHV will call the MVI Search (Unattended) service with the CSP’s traits in the VA Authentication Federation Infrastructure (VAAFI) header, and request that the correlated identifier be included in the information returned from MVI.
* IAM Authorization Management Service (AMS)
  + Retrieve Authorizations
* IAM Special Access Control (SAC)
  + Authorization Request

## References

### Requirements, Design, and Service Description Documentation

The applicable IAM requirements, design, and service description documents include the following:

* [Enterprise-Level IdM Requirements (ENTRs)](http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/Enterprise_id_management_bis_reqs_2014.pdf)
* [VA Enterprise Identity and Access Management (IAM) Services (VAIQ #7011145)](http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/VAIQ%207011145%20Memo_Roger_Baker.pdf)
* [Designation of Identity and Access Management Business Sponsor (VAIQ #7060071)](http://vaww.iam.va.gov/IAM_Business_PMO.asp)
* [MVI Use Cases](http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1385&Type=Parked&From=GlobalGroup)
* [AcS Use Cases and Models](http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1653&Type=Active#Documentation)
* [MVI Service Description Document](http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/MVI_Service_Description.pdf)
* [AcS Application Integration Guide – External](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/AcS%20Application%20Integration%20Guide%20-%20External.pdf)
* IAM Portal Strategy
* [SSOe VAAFI AccessVA 2.0 Increment 3 Requirements Specification Document (RSD)](http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1653&Type=Active)
* [VA IAM AcS Integration Patterns](http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1653&Type=Active)
* [IAM](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/VAAFI_Application_Integration_Guide.pdf) VAAFI Application [Integration](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/VAAFI_Application_Integration_Guide.pdf) Guide
* AcS Common Business Rules Document - page and doc links: <http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1803> <http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services_Phase_2/AcS_Common_Business_Rules_Document.pdf>

### Business Policy Documentation

The applicable IAM business policy documents include the following:

* [VA Directive 6500 Information Security Program](http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=374&FType=2)
* [Section 508 Standards Guide](http://www.section508.gov/section-508-standards-guide)

### Abbreviations and Definitions

The abbreviations and terms used in this document are defined in the [Identity and Access Services Master Glossary](http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/Identity_and_Access_Services_Master_Glossary.pdf).

# Functional Requirements

## Functional Requirements for MHV – User Handling

### Assumptions

The MHV integration with IAM services is based on the following assumption:

1. The MHV user will use an SSOe-enabled CSP.

### AccessVA Enablement for MHV

AccessVA provides users with a simplified logon experience with VA resources and web applications. The purpose of AccessVA is to centralize user access and allow for easy logon to VA web applications in a secure method without the need to remember multiple user names and passwords.

SSOe (also known as VAAFI) provides e-authentication services through a trusted network of VA applications, VA business partners, and CSPs. It is the responsibility of SSOe to authenticate the user and route that user to the targeted VA application or portal. SSOe also supports the Portal Strategy, which establishes requirements to each portal implementation that would allow portlets and/or portal based applications to be deployed under any portal that is compliant with the portal integration pattern.

The following requirements allow MHV to use the AccessVA portal. By using the AccessVA portal, MHV will benefit from the IAM Portal Strategy and third-party onboarding. These processes are owned by IAM and do not require additional steps from MHV, but may require additional actions to be completed by the MHV user to complete VA registration.

MHV users will need to obtain a credential from one of the trusted CSPs. See [section 2.3.2](#_AccessVA_Account_Registration) for AccessVA requirements for sending MHV users to CSP proofing flows.

In Figure 1 below, the activity flow diagram depicts the process of a user starting on MHV prior to login and using AccessVA and SSOe to access MHV.



Figure : IAM SSOe flow example – User Starts on MHV

Note: There are multiple possible paths for users to arrive at MHV with an SSOe session. See Appendix A: User Paths to MHV and VDT for illustrations of possible paths in pilots and in production.

#### Users Starting on MHV

The new navigation path for users starting on MHV is shown in the diagram above.

1. MHV shall display an option that directs users to AccessVA.
2. AccessVA shall display the AccessVA Authentication Pop Up CSP selector widget
3. MHV user selects the desired CSP login button.
4. AccessVA shall redirect the user to the desired CSP
5. MHV user shall log in to the CSP.
6. MHV shall redirect the user to MHV and MHV will process the SSOe session according the requirements in section “MHV Login and Account creation.”
7. MHV users who were required to complete third-party on-boarding shall be directed to the MHV splash page upon successful completion of on-boarding.

**Note**: When a CSP account is used for the first time to access a VA resource, the CSP account will need to go through the third-party onboarding account to associate the CSP account with the user's VA identity. After the successful or unsuccessful completion of the third-party onboarding process, the user will be automatically logged out. A user interface (UI) screen will display and indicate a successful or unsuccessful result and an “OK” button. When the user clicks the “OK” button, the user will be redirected to the MHV splash page.

#### Users Starting in AccessVA

Users will also be able to start on the AccessVA web page

1. On the AccessVA page, the user picks MHV as the destination.
2. Access VA displays the unauthenticated AccessVA homepage with MHV pre-selected as the selected destination.
   1. In the Pilot, only DS Logon will be displayed
   2. In full production, all CSPs that offer LOA2 or higher will be displayed.

Additional steps in this flow are identical to those identified in [section 2.1.2.1](#_Users_starting_on).

### SSOe to MHV within the VA Firewall – Application Junction

The SSOe to MHV application junction allows authenticated SSOe session users to pass to the application across a mutually authenticated Transport Layer Security (TLS) channel (where both client and server are required to authenticate), provided the session user passes the access control and authorization checks.

**Assumptions**:

* User has been previously authenticated and is a valid SSOe session user.
* MHV has specified the access controls to be configured to allow for CSP user access at LOA 2 or higher (Credential Agnostic: All VA IAM accepted credentials at LOA2 or higher will be available to MHV users).
  + For Pilot users, the following CSPs are or will shortly be available at LOA 2 or higher at the time of document creation for
    - VA PIV
    - DOD CAC
    - Norton Symantec
    - Connect.Gov
  + During the Pilot, regular non-Pilot users will only have DS Logon available. Note that once the user goes to the DS Logon authentication page, they have the option of entering a username and password or a CAC card.
  + Once the MHV Federated Credential flows move to National Release, all LOA 2 CSPs will be available to the general population. MHV acceptance of credentials may roll out over several releases
* As new CSPs are accepted by AccessVA, those CSPs will be automatically available to MHV users at the relevant LOA.

#### Portal Strategy Traits

**Integration Requirements**:

1. MHV shall process the authentication traits defined in the Secure Hypertext Transfer Protocol (HTTP) headers.

**Note:** Refer to the AcS Common Business Rules Document for the list of Portal Strategy traits.

1. MHV shall process the SSOe session according the requirements in section “MHV map SSOe user to MHV Account.”

**Note**: Refer to section 6.5 of the [AcS VAAFI Application Integration Guide](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/VAAFI_Application_Integration_Guide.pdf) for trait format information.

#### CSP Data Only

In some scenarios, SSOe returns CSP data only. MHV is expected to provide or not provide access based only on the data passed through SSOe by the CSP from the user’s login to that CSP. The “CSP data only” scenario can occur when IAM VAAFI is running, but an IAM service involved in providing Portal Strategy data (Provisioning, Virtual Directory, and or/MVI) is unavailable.

Refer to the AcS Common Business Rules Document for more information about the data provided by each CSP.

When users arrive at MHV with CSP-only traits, MHV will need to determine the VA identity of the user.

If the CSP is DS Logon, MHV submits an EDIPI to the MVI Get Corresponding IDs call to obtain the correlated identifiers. Note that if the user has a VA record but MVI does not yet have that user’s EDIPI, this call will return “not found.”

For a CSP other than DS Logon, MHV will call the MVI Search (Unattended) service with the CSP traits in the VAAFI headers, and request that the correlated identifier be included in the information returned from MVI.

**Note:** MHV already calls MVI’s Search (Unattended) in other flows.

**Requirements for CSP-only**:

1. MHV shall check to determine whether there is a VA identity known of the user
   1. If the EDIPI is in the VAAFI headers, MHV shall call the MVI Get Corresponding IDs service with the EDIPI.
   2. If the EDI PI is not in the VAAFI headers, MHV shall have the capability to search MVI for person identity records using the approved search criteria. To accomplish this, MHV shall send a query to the MVI’s Search for Person (Unattended) function. MHV shall request that the correlated identifier list be included in the information returned from MVI. The MHV request to MVI shall contain traits in the VAAFI header obtained from the credential.
2. MHV shall process the results of the query to MVI
   1. If no matching record is found, MHV shall inform the user they cannot continue into MHV.
   2. If a matching record is found, MHV shall process the SSOe session according the requirements in section “MHV Login and Account creation.”

### MHV map SSOe user to MHV Account

The requirements for MHV to map the SSOe user to an MHV account depend on the following preconditions:

* The user has signed in to create a VAAFI SSOe session and navigated to MHV, per the requirements in [section 2.1.2](#_AccessVA_Enablement_for).
* MHV has checked for the presence of Portal Strategy traits, and if the traits are CSP-only, it has identified the user’s VA identity per the requirements in [section 2.1.3](#_SSOe_to_MHV).

#### CSP handling

In moving from Federated Credential Pilot to full production, MHV shall remove the special handling of DS Logon:

* For all CSPs, MHV shall execute the flow below.

#### MHV Handling of MHV IEN from SSOe

If one or more MHV IENs are present in data from IAM:

1. MHV shall check for the presence of multiple MHV IENs in the correlated identifiers. If there are multiple IENs, MHV shall display an error to the user.
2. If there is one MHV IEN, MHV shall check to see whether MHV has the account marked as inactive. If MHV has the account marked as inactive, MHV shall send an Unlink Correlation from ICN message to MVI and display an error to the user.
3. If there is one MHV IEN and MHV has the account marked as active, MHV shall display the logged in page to the user.
   1. MHV will check on the age of the treating facility list for the user. If it needs to be refreshed, MHV will call getCorrespondingIds to do so.

#### MHV Check for Existing MHV Accounts to Correlate

If no MHV IEN is present in the data from IAM, MHV shall perform processes to identify an existing MHV account that the user owns that can be updated and correlated with MVI. The processes will include two steps:

* An MHV system check to prevent the user from going through registration and then encountering an error because they are attempting to create a duplicate MHV account
* The opportunity for a user to identify their existing MHV account by entering their MHV username and password

1. MHV will perform internal checks for data matches between the SSOe data and an existing MHV account
   1. MHV will perform the checks
      1. Exact match on the combination of First Name, Last Name, Date of Birth and SSN.
      2. Match on ICN
2. If a match is found, MHV will take the user to the *SSOe User Confirm Account Found by MHV* flow and display the prompt the user for MHV username and password
   1. If the user successfully enters the MHV username and password
      1. MHV will update its user data to match the traits in the VAAFI headers
      2. MHV will send an Add Person (Add Correlation) message to MVI, correlating the MHV account with the ICN receive in the VAAFI headers
3. If a match is not found in step 1, MHV will take the user to the *SSOe User Connect Page with Registration* Flow and offer the user the option of creating a new account, or entering an MHV username and password to update an existing account. If the user chooses to update an existing account
   1. MHV will prompt the user for MHV username and password
   2. If the user successfully enters the MHV username and password
      1. MHV will update its user data to match the traits in the VAAFI headers
      2. MHV will send an Add Person (Add Correlation) message to MVI correlating the MHV account with the ICN receive in the VAAFI headers

#### Register SSOe user for new MHV account

If the user’s SSOe data passes the system checks described in the previous section, and the user indicates they want to register for a brand new account, the following occurs:

1. MHV shall bring the user to the MHV registration page with VAAFI header data for their traits pre-filled
2. The user shall not be able to change the prefilled traits except contact information (phone/address/email). Note: these changes will reside in MHV only and not be propagated to other VA systems.
3. When the user saves the Registration page, MHV will send an Add Person (Add Correlation) message to MVI correlating the MHV account with the ICN receive in the VAAFI headers

#### As-Is and To-Be Flows for SSOe user and MHV account

The following As-Is, Pilot, and To-Be activity flow diagrams show the process at each stage after the user has signed in to create a VAAFI SSOe session and navigated to MHV.

* As-Is Production *Map SSOe user to MHV Account*
  + Applies only to DS Logon
* As-Is Pilot *Map SSOe user to MHV Account*
  + MHV Federated Credential Pilot flow
  + Applies to all other CSPs
* *SSOe User Connect Page with Registration* Flow
  + As-Is – displayed only in MHV Federated Credential Pilot
  + To-Be – displayed to all users, no logic change to flow compared to As-Is
* *SSOe User Confirm Account Found by MHV* Flow
  + As-Is – displayed only in MHV Federated Credential Pilot
  + To-Be – displayed to all users, no logic change to flow compared to As-Is
* To-Be Production *Map SSOe user to MHV Account*
  + Drops special handling of DS Logon
  + All credentials follow flow below DS Logon special handling that is expressed in “As-Is Pilot Map SSOe user to MHV Account”

**Note**:It is recommended that the following diagrams be viewed in Microsoft Word at a 300% zoom level.



Figure : As-Is Production Map SSOe User to MHV Account



Figure : As-Is Pilot Map SSOe User to MHV Account



Figure : As-Is and To-Be SSOe User Connect Page with Registration Activity Diagram



Figure : As-Is and To-be SSOe User Confirm Account Found by MHV Activity Diagram



Figure : To-Be Map SSOe User to MHV Account (credential agnostic)

### Perform Logoff and Timeout

**User Initiated Logoff**:

The following is the logoff behavior when the user initiates a logoff from MHV (e.g., clicks a logoff button on the MHV page).

1. MHV shall terminate its local application session.
2. MHV shall request that SSOe terminate the SSOe session.
3. SSOe shall terminate the SSOe session.
4. SSOe shall redirect the MHV user to the MHV splash page.

**Timeout Policy**

1. MHV shall be in compliance with the VA 6500 timeout policy.

**Idle/Session Timeout Scenario 1: Both SSOe and MHV have timed out**

One timeout scenario is that the user has not been active in MHV or any other SSOe application. This leads to a state where both the SSOe and MHV sessions have timed out.

1. MHV shall terminate its local session when the MHV session timeout has occurred.
2. If the user clicks a link in MHV after the SSOe session has timed out, SSOe shall redirect the MHV user to a MHV hosted timeout error page.
3. MHV shall host a timeout error page notifying the user that their session has expired and they will need to log in again.

**Idle/Session Timeout Scenario 2: MHV has timed out but SSOe session is still active**

A second timeout scenario is that the user has not been active in MHV, but has been active in other SSOe-protected systems. This leads to a state where the MHV session has timed out but the SSOe session has not

1. MHV shall terminate its local session when the session timeout has occurred.
2. If the user clicks a link in MHV while the SSOe session is still active, SSOe shall direct the user to the link the user selected
3. MHV shall establish a new MHV session for the SSOe user and display the page.

## Functional Requirements for MHV – Delegation

In the MHV Delegation flow there are three major phases of the flow where IAM comes into play:

* Identify Delegators: Identify the user’s current active Delegators (persons such as Veterans or MHV account holder who have delegated to user) so MHV can present links to view the Delegator’s information to the user
* Check User’s Access Rights: When the user navigates to view a Delegator’s data, check with IAM SAC to ensure they have authorization to do so at that moment
* Identify Delegator’s MHV Account: Map the Delegator’s information from IAM to their MHV account – in order to do this, MHV will need to call MVI to get the Delegator’s MHV IEN

### Prerequisites and assumptions

In order for a user to act as a Delegate in MHV and view a Delegator’s data, the following prerequisites must be met:

* The MHV user must have an SSOe LOA 2 user session
* The MHV user session must have full Portal Strategy traits
* The user must have an active delegation from the Delegator that applies to MHV access (VA Healthcare Proxy or VHA Personal Representative). This delegation must be set up in the IAM Authorization Management System (AMS) system, commonly known as “IAM Delegation.”

There following assumptions apply to the MHV Delegation Pilot

* Pilot users go to a special URL for the MHV Delegation Pilot
* The user has an active MHV Premium account
* The Delegator has an active MHV Premium account
* The initial Pilot implementation will be restricted to VAHP with Full Access.

### Identify Delegators – Call AMS service

Before MHV can display a link for a user to view a Delegator’s data, MHV will need to determine whether the user has any active Delegators. In order to do so, MHV will need to call the AMS Service “Retrieve Authorizations”

**Requirements**

1. MHV shall call the AMS Service “Retrieve Authorizations”
   1. MHV shall submit the Sec ID of the user
2. MHV shall filter the response for Active Delegators
   1. MHV shall filter on Status for “Active” to identify active delegations.
   2. MHV shall filter Authorization Type for VA Healthcare Proxy (VAHP) or VHA Personal Representative (VHA PR)

**Note:** the identifier returned for the Delegator may be ICN or SecID, depending on the AMS flow used to create the delegation. If the Delegator directly created the delegation through the IAM Veteran Delegation Tool, the Delegator’s SecID is associated with the delegation. If a staff user created the delegation, the Delegator’s ICN is associated with the delegation

1. MHV shall continue the business process to present the user the capability of navigating to view Delegators who have an active VAHP or VHA PR delegations to the user

### Manage Business Authorization Policies

The task to manage the business authorization policies includes the creation of business data sharing policies by security and privacy groups, governance entities and consuming application business groups. Additionally, these entities define/identify the associated authorization decision information (ADI) attributes (across categories such as, subject, resource, action, environment etc.) that will eventually be referenced by the XACML-codified versions of the business data sharing policies.

1. MHV will make access decisions based on the following business authorization policy/policies:

**VA Healthcare Proxy**

* A person may have full access to available Electronic health information from the MHV Patient Portal for any person for which he or she is an active VA Healthcare Proxy with full access designated on the VAHP form.
* A person may have read/print/download access available Electronic health information from the MHV Patient Portal for any person for which he or she is an active VA Healthcare Proxy with read/print/download access designated on the VAHP form.

**Note**: the read/print/download access will not be utilized in the initial Pilot implementation but will be added at some point.

**VHA Personal Representative**

* A person may have full access to available Electronic health information from the MHV Patient Portal for any person for which he or she is an active VHA Personal Representative.

1. MHV shall rely on the following attributes (identifiers, description, data type, category, and possible values) to be used in the authorization policy decisions. Note: formal definition of these attributes shall be delivered in the Integration Control Document (ICD) during implementation.

* User’s Identifier (SecID)
* Delegator’s Identifier (ICN or Sec ID)
* Delegation Type to be consulted (VAHP or VHA Personal Representative)
* Permission Preference of VAHP Delegation to be consulted
* Status of Delegation to be consulted (Active)

1. MHV and IAM agree on the sources from which to obtain authorization attributes.

* The XACML request from the MHV PEP shall contain
  + User’s Identifier
  + Delegator’s Identifier
  + Delegation Type
  + (If applicable) Permission Preference
* SAC shall consult the AMS to retrieve the following information about authorization at time of policy evaluation
  + Status of Delegation

### Enforce Authorization Decision Call IAM SAC

MHV will need to call IAM SAC to confirm that the user is authorized to view that Delegator’s data.

**Requirements**

1. In response to a user’s attempt to access protected data about a Delegator through MHV, the MHV Policy Enforcement Point (PEP) shall consult IAM SAC to verify if the access can be granted. MHV shall consult IAM SAC the first time a user navigates to the Delegator’s data within an SSOe user sessions.
2. The MHV PEP shall generate the XACML 3.0 authorization decision request containing the following attributes:

**Note:** formal definition of these attributes shall be delivered in a Service Description Document or an Integration Control Document (ICD) during implementation.

* 1. Authorization decision based on VA Healthcare Proxy Delegation

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute Category** | **Attribute Name** | **Value** | **Source for MHV PEP** |
| Subject | User’s Identifier | SecID | SSOe user session |
| Subject | Delegation Type | VAHP | AMS Retrieve Authorizations |
| Resource | Delegator’s Identifier | ICN or Sec ID | AMS Retrieve Authorizations |
| Action | Permission Preference of VAHP Delegation to be consulted | For full: ReadWrite  For r/p/d: Read | AMS Retrieve Authorizations |

* 1. Authorization decision based on VHA Personal Representative

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute Category** | **Attribute Name** | **Value** | **Source for MHV PEP** |
| Subject | User’s Identifier | SecID | SSOe user session |
| Subject | Delegation Type | VHA PR | AMS Retrieve Authorizations |
| Resource | Delegator’s Identifier | ICN or SecID | AMS Retrieve Authorizations |
| Action | Permission Preference of VHA PR to be consulted | Any value |  |

1. The MHV PEP shall send this decision request to the SAC PDP via the DataPower proxy.
2. The SAC PDP shall process the decision based on MHV authorization policies return an XACML 3.0 authorization decision response to the MHV PEP. The response can include:
   1. Permit
   2. Deny
   3. Indeterminate
   4. Not applicable
3. The MHV PEP will enforce authorization decisions returned by the SAC PDP. Enforcement can be the following:
4. Permit access to the Delegator’s data
   1. Deny access (in the case of SAC returning Deny, Indeterminate or Not Applicable)
5. The user will continue with the MHV business workflow.

### Identify Delegator’s MHV Account: Call MVI

In order to identify the MHV account associated with a Delegator, MHV needs to call MVI getCorrespondingIds.

**Assumption**

MHV has previously called SAC PDP to determine that the user has access to the Delegator’s data.

**Requirements**

MHV needs to call MVI to obtain Delegator’s MHV IEN

1. MHV shall call MVI getCorrespondingIds in order to obtain the MHV IEN for the Delegator
   1. MHV shall submit the Delegator’s ICN or SecID returned from IAM AMS

MHV then needs to check the Delegator’s correlated identifiers for an MHV IEN.

1. If there are multiple Delegator IENs, MHV shall display an error to the user.
2. If there is one Delegator MHV IEN, MHV shall check to see whether MHV has the account marked as inactive. If MHV has the account marked as inactive, MHV shall send an Unlink Correlation from ICN message to MVI and display an error to the user.
3. If there is one MHV IEN and MHV has the account marked as active, MHV shall display the initial display of the Delegator’s data to the user.
   1. MHV will check on the age of the treating facility list for the Delegator. If it needs to be refreshed, MHV will call getCorrespondingIds to do so.
4. If there are no MHV IENs MHV shall display an error message.

### User switches between MHV accounts

**User-initiated switch of MHV Accounts**

Assumption: when a Delegate user has access to both their own MHV account and a Delegator’s MHV account, MHV will present the user the opportunity to navigate between their own account and a Delegator’s account.

At the time of the switch, MHV may change its own internal user session to reflect the MHV account the user is viewing. MHV should not break the SSOe session during these switches.

**Requirements**

1. When an MHV Delegate user switches between MHV accounts, MHV shall leave the SSOe session active.

### MHV Audits Delegator data access

**Requirements**

* 1. MHV shall maintain audit trail of all access by user to Delegator’s data
  2. MHV shall audit calls to SAC PDP and policy enforcement decision

### MHV shall audit call to AMS service

**Requirements**

* 1. MHV shall audit calls to the AMS service

### Delegation flow



## Functional Requirements for IAM - User

The IAM functional requirements for the MHV integration are identified in this section.

### CSP Selection Options for MHV Users

IAM shall offer two user interface paths for selecting a CSP to use for entering MHV

1. **[FEATURE 556044]** AccessVA shall make its pop up CSP selector available to MHV. During the Pilot, DS Logon will not be offered on the CSP selector.
2. **[FEATURE 556045]** The AccessVA web site will continue to offer a path to MHV. During the Pilot, only DS Login will be offered on the AccessVA web site.
3. In Full Production, all CSPs that support LOA 2 or higher accounts shall be displayed for MHV in AccessVA and on the pop up CSP selector

### AccessVA Account Registration Redirects

Some CSPs allow for registration at various LOAs. MHV only requires the LOA-2 credentials from these CSPs. MHV wants to ensure their users are directed to register at LOA 2 and not asked to register at higher, more difficult LOAs.

1. **[FEATURE 556047]** AccessVA shall redirect users who are attempting to access MHV to a Norton Symantec page that offers Norton Symantec account creation with an LOA-2 online proofing flow.
2. **[FEATURE 556048]** AccessVA shall redirect users who are attempting to access MHV to a Connect.gov flow that will offer users account creation with an LOA-2 online proofing flow for Connect.gov credentials.

### Search for Person (Unattended) for MHV

**Note**:MVI already supports Search for Person (Unattended) calls from MHV in other contexts.

**Requirements**:

1. MVI shall support Search for Person (Unattended) requests from MHV.

### Retrieve Person (Returning Corresponding IDs) for MHV

**Note**:MVI shall support Retrieve Person (Returning Corresponding IDs) calls from MHV in other contexts.

**Requirements**:

1. MVI shall support Retrieve Person (Returning Corresponding IDs) requests from MHV.

### Get Corresponding IDs for MHV

**Note**:MVI already supports Get Corresponding IDs calls from MHV.

**Requirements**:

1. MVI shall support Get Corresponding IDs requests from MHV.

### Add Person (Add Correlation) for MHV

**Note**:MVI already supports Add Person (Add Correlation) calls from MHV.

**Requirements**:

1. MVI shall support Add Person (Add Correlation) requests from MHV.

### Unlink Correlation from ICN for MHV

**Note**:MVI already supports Unlink Correlation from ICN calls from MHV.

**Requirements**:

1. MVI shall support Unlink Correlation from ICN requests from MHV.

## Functional Requirements for IAM – Delegate Views Delegator Data

### Support Retrieve Authorizations call

**Requirement**

1. AMS shall support Retrieve Authorizations calls from MHV.

### Authorize Delegate to view Delegator’s data

Note: see 2.2.3 Manage Business Authorization Policies in this document for definition of attributes related to policy decisions and sources of attributes (MHV PEP or ACS).

**Requirement**

1. MHV authorization business policies/rules applicable to delegation shall be converted to XACML 3.0 policies and stored in SAC.
2. The SAC PDP shall receive a XACML 3.0 authorization request from the MHV PEP
3. The SAC PDP shall select the applicable policy based on the attributes specified in the request from the MHV PEP (known as “target attributes”).
4. The SAC PDP shall evaluate the policy.
5. As a part of the policy evaluation, the PDP shall obtain Access Control Information (ACI) by calling the AMS service.

Note: see “SAC-AMS integration to provide ACI for VAHP and VHA PR” section for details

1. The SAC PDP shall generate the XACML authorization decision response containing:
2. Disposition (permit/deny)
3. The SAC PDP shall return an XACML 3.0 authorization decision response to the MHV PEP.

### SAC-AMS Integration to provide ACI for VAHP and VHA PR

This section has internal IAM requirements to ensure SAC can obtain Access Control Information from AMS in order to perform an authorization of access based on VAHP and VHA PR delegation types.

**Requirements**

1. SAC shall call AMS to Retrieve any existing authorizations
2. SAC shall submit the following data
   1. Data to retrieve an active VA Healthcare Proxy Delegation between the user and Delegator with specified permission

|  |  |
| --- | --- |
| **Data** | **Value** |
| User’s Identifier | SecID |
| Delegation Type | VAHP |
| Delegator’s Identifier | ICN or Sec ID |
| Permission Preference of VAHP Delegation to be consulted | For full: ReadWrite  For r/p/d: Read |
| Delegation Status | Active |

* 1. Data to retrieve an VHA Personal Representative between the user and the Delegator

|  |  |
| --- | --- |
| **Data** | **Value** |
| User’s Identifier | SecID |
| Delegation Type | VAHP |
| Delegator’s Identifier | ICN or Sec ID |
| Delegation Status | Active |

1. AMS shall return any delegation that meets the submitted criteria
2. SAC shall incorporate the data returned from AMS in the policy evaluation.

### Support call to getCorrespondingIds for Delegator data

**Note**:MVI already supports Get Corresponding IDs calls from MHV.

**Requirements**:

1. MVI shall support Get Corresponding IDs requests from MHV.

# Other Specifications

## Design Constraints Specifications

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

* MVI Service Description Document
* AcS Application Integration Guide – External
* AcS Interface Control Documents

## Disaster Recovery Specifications

There are no disaster recovery specifications for the MHV integration with IAM services. The IdS disaster recovery specifications include the following:

* The disaster recovery specifications are detailed in the Person Service Identity Management (PSIM) Continuity of Operations (COOP) Plan, Master Patient Index (MPI) COOP Plan, and Austin Information Technology Center (AITC) Master Disaster Recovery Plan. These documents are protected and stored securely in the VA Security Management and Reporting Tool (SMART) system.

The AcS disaster recovery specifications include the following:

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

## Performance Specifications

#### Federated Credential –National Release

MHV estimates the following:

* 80,000 – 100,000 user logins daily
* Number of users: 2.9 million registered users
* Number of concurrent users: 3500 concurrent users
* Volume: monthly average volume of 43 thousand new users
* Estimated growth rate: 20% annual growth estimated of new users
* Standard hours of operation: 24/7 maintenance /upgrades usually conducted on Saturday at 10 p.m. ET
* Peak usage times: 9 a.m. – 4p.m. CT

#### Delegation Pilot

MHV estimates the following:

The Pilot will start with a handful of users. It may be increased to several hundred.

## Quality Attributes Specifications

MHV shall be required to conform to all IAM design and coding standards.

The IAM and MHV Integration teams comply with the quality specifications set forth by the VA IAM Project Management Plan, Section 5 Quality Management Approach. IAM and MHV participate in the following activities to ensure the quality of the system:

* Acceptance and baseline of the iRSD
* Change control
* Unit testing
* Integration/functional testing
* User acceptance testing

The following quality processes are followed:

1. Stakeholder Review and Oversight

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

1. Requirements Management Traceability

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

1. Change Control

The baselined version of this iRSD is stored in IBM Rational Team Concert (RTC). Changes to this iRSD shall be accomplished by creating an IAM work item (WI) and shall follow standard Program Management Accountability System (PMAS) approval processes.

1. Integration Testing

The integration testing for the MHV-IAM integration shall be accomplished via connection to the MVI Stage 1A test environment and AcS software quality assurance (SQA) test environment.

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

## Reliability Specifications

The IAM reliability specifications are identified in the following table.

**Table** **1: IAM Reliability** **Specifications**

| **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 |
| **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 Automated Notification Report (ANR) to be sent out to the appropriate teams |
| **Outage Impact** | Interruption of service may result in severe financial, regulatory, patient safety, patient health, or other business issues |
| **Scheduled Maintenance** | Scheduled maintenance must provide continuity of service availability with minimal interruption |

## Security Specifications

To be IAM compliant, MHV needs to meet the following requirements:

1. MHV shall conform to the VA security standards detailed in VA Handbook 6500 Information Security Program.
2. MHV shall follow VAAFI standards when interacting with MVI, Veteran Health Identification Card (VHIC), Identity Proofing (IP), Electronic Signature (ESig), and Provisioning (Prov). VAAFI is the security framework between these IAM services and MHV.
3. Before invoking calls, MHV shall register with the IAM Development team in accordance with the guidance from the standard process for IAM integration via the AcS Application Integration Guide – External document.

# Attachment A: Approval Signatures

Signed: Kathleen Frisbee Date

Co-Director, Connected Health

Signed: Theresa Hancock Date

MHV V/CHIO Director

Signed: John Brekke Date

MHV PD Program Manager

                                                                                                                                   <mm/dd/yyyy>

Signed: Sara Temlitz                                                                                                        Date

Data Quality Business Product Manager

                                                                                                                                   <mm/dd/yyyy>

Signed: Jeff Podolec                                                                                                       Date

IT Program Manager

                                                                                                                                   <mm/dd/yyyy>

Signed: Jerry Wharton                                                                                                   Date

AcS Program Manager

                                                                                                                                   <mm/dd/yyyy>

Signed: Tamara Neal                                                                                                       Date

Business Sponsor, IAM Business Program Management Office

                                                                                                                                   <mm/dd/yyyy>

Signed: Shelby Bell                                                                                                          Date

ICAM Business Sponsor

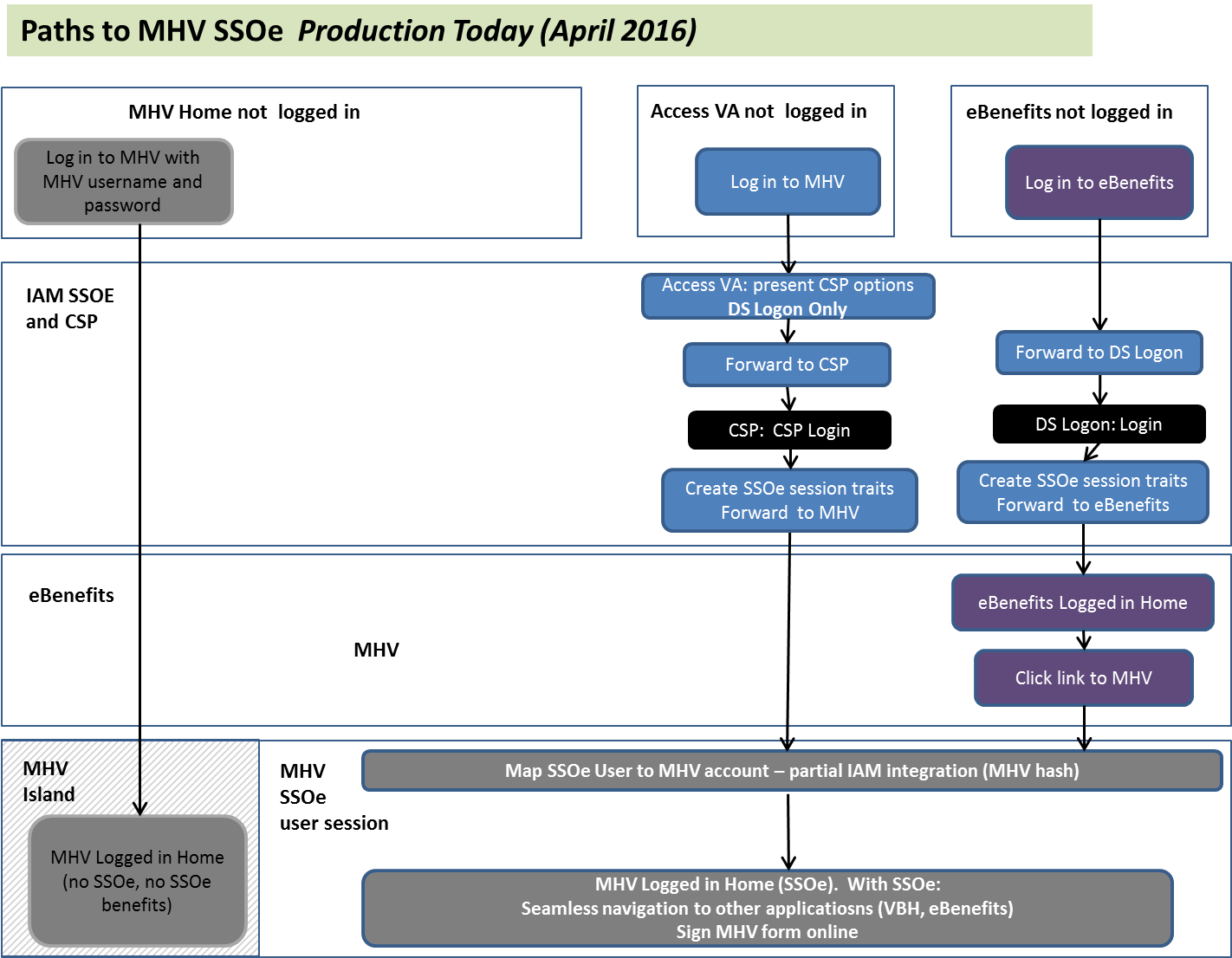
# Appendix A: User Paths to MHV and VDT

This appendix provides additional context for the above requirements.

## User paths to MHV

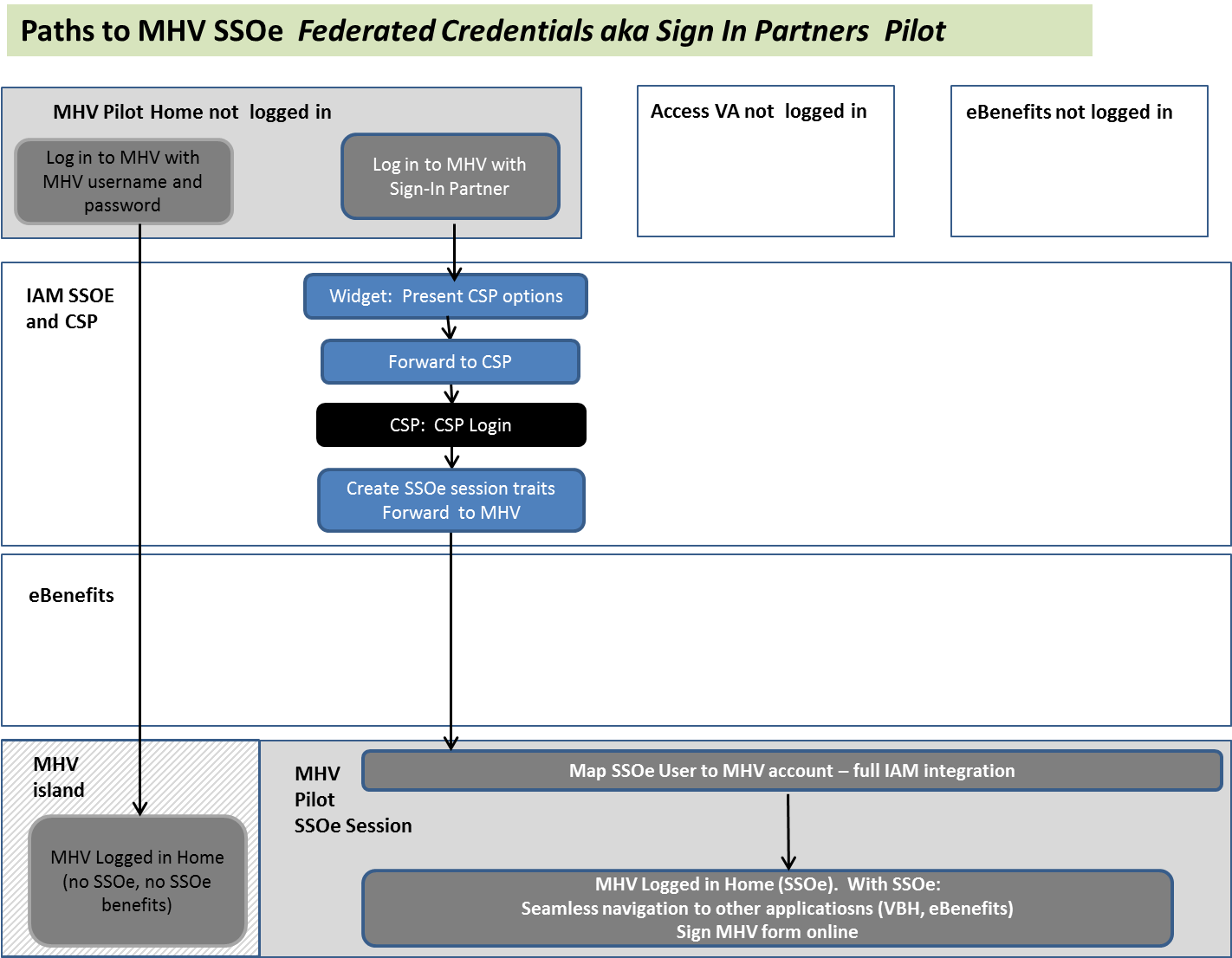
### Production As-Is Paths to MHV SSOe session

In the As-Is production state during Federated Credential Pilot, there are two paths to SSOe sessions, both restricted to DS Logon. MHV legacy username and password are good for MHV only, does not provide benefits of an SSOe session.



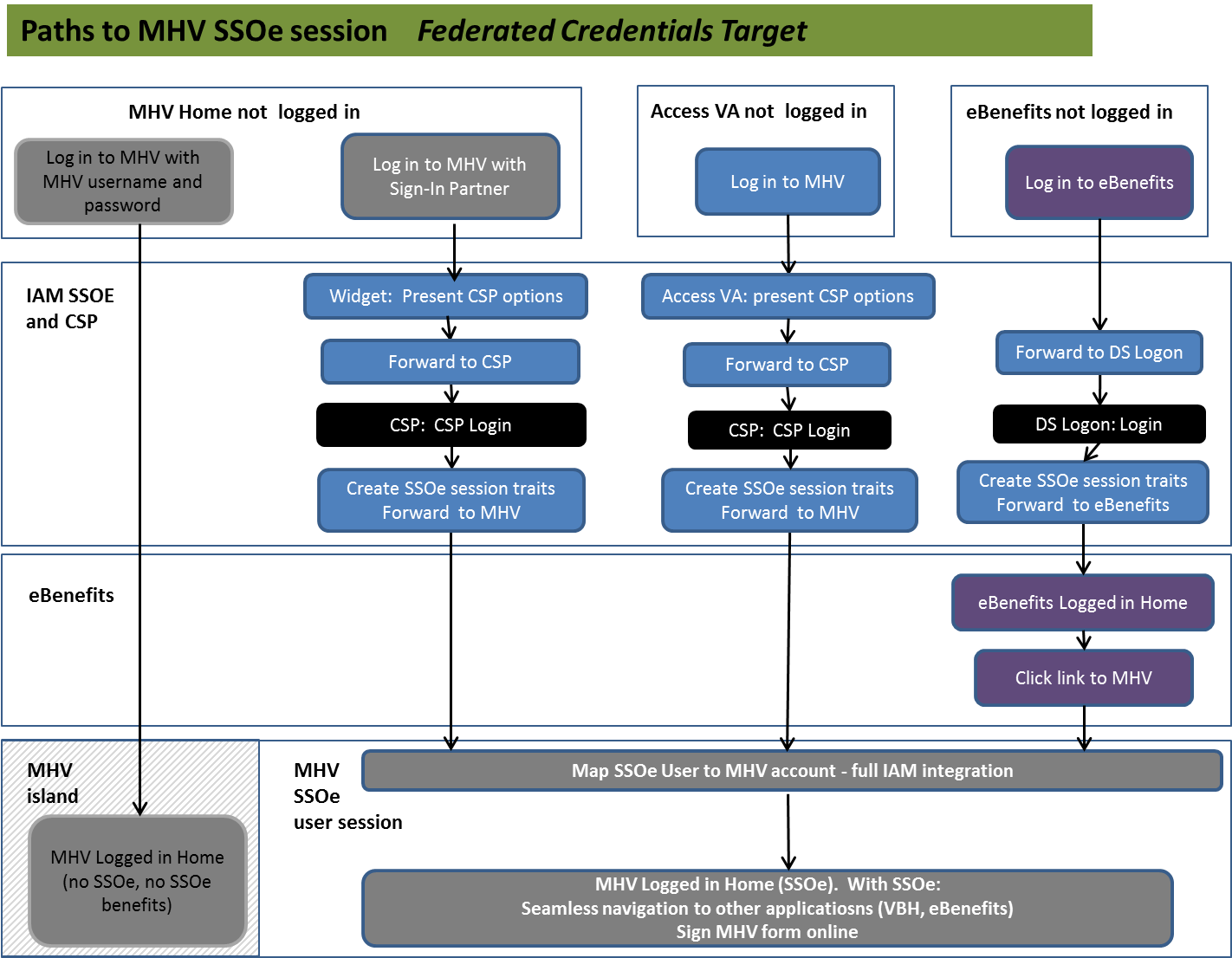
### Federated Credential Pilot Paths

From a special Pilot URL, MHV users can pick from a range of credentials.



### Federated Credential To Be Paths to MHV SSOe session

Below are the primary paths, but others are possible. Once a user has an IAM SSOe session they may navigate in various ways (not just through eBenefits) before navigating to MHV. From the perspective of MHV’s “Map SSOe User to MHV Account” activity, the particular path the user took has no impact. The user has arrived at a MHV with an IAM SSOe session, and MHV needs to determine the user’s MHV account based on the SSOe data provided by IAM.



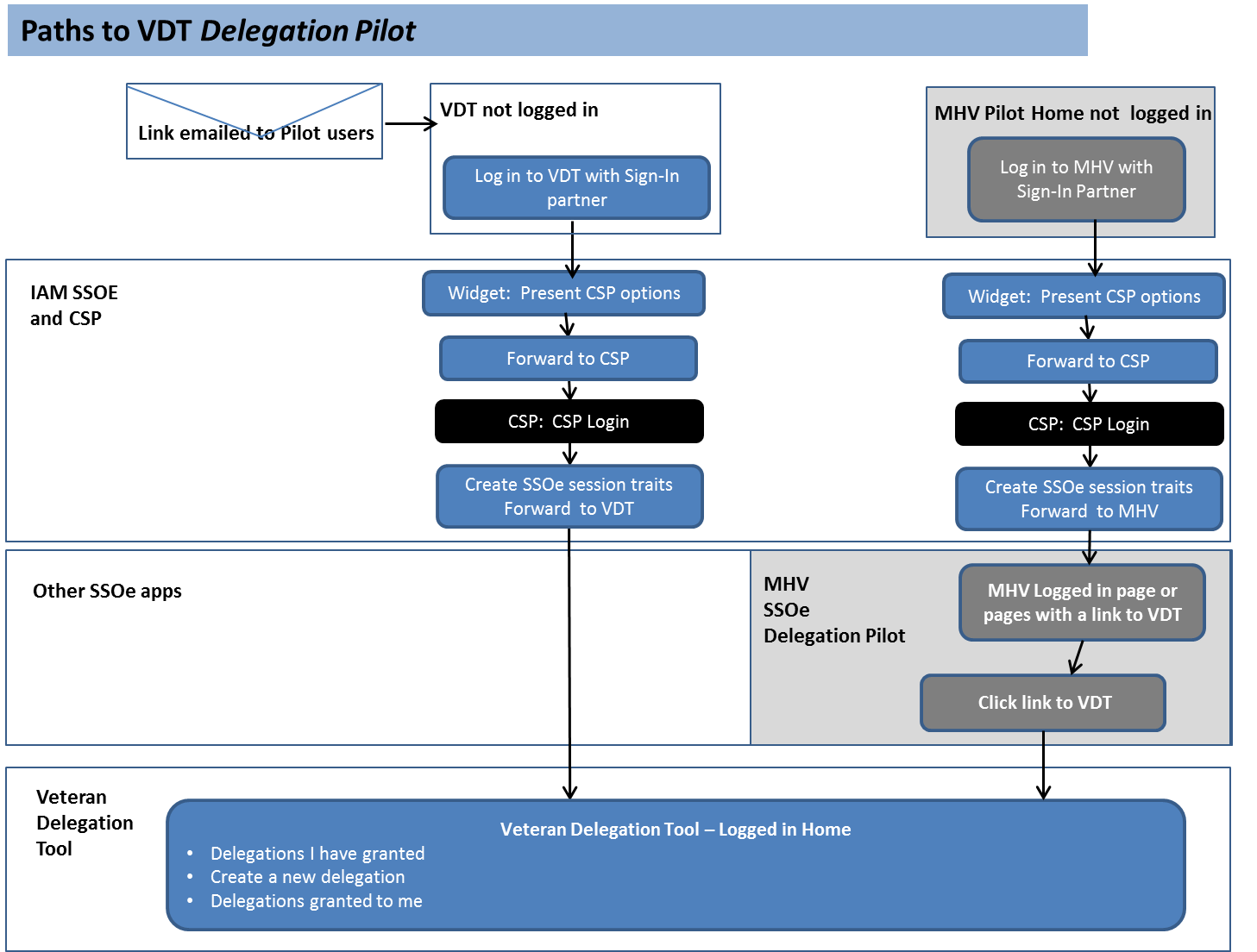
## User Paths to Veteran Delegation Tool

For reference, the flows below show Pilot and To Be paths for users to get to the Veteran Delegation Tool (VDT), the IAM user interface where veterans and other external users can manage their delegations. There are no requirements in this iRSD related to these flows.

### Paths to VDT Delegation Pilot

In order to meet the goals of a limited Pilot of overall Delegation functionality, a link to VDT will be provided to Pilot participants. IAM does not plan to put a link to VDT on AccessVA during the Pilot.

An optional additional path would be to provide a link to VDT on MHV Pilot pages – that is also included in this illustration.



### Paths to VDT Production

Veteran Delegation Tool would appear on AccessVA. In addition, MHV and other applications could provide links to VDT.

