VA Enterprise Design Patterns:

3. Interoperability and Data Sharing

3.3 Utilizing Enterprise Identities

Office of Technology Strategies (TS)
Architecture, Strategy, and Design (ASD)
Office of Information and Technology (OI&T)

Version 1.0

Date Issued: November 2015

THIS PAGE INTENTIONALLY LEFT BLANK FOR PRINTING PURPOSES

APPROVAL COORDINATION

TIMOTHY L MCGRAIL 111224

Digitally signed by TIMOTHY L MCGRAIL 111224
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=tim.mcgrail@va.gov, cn=TIMOTHY L MCGRAIL 111224
Date: 2015.11.10 13:50:35 -05'00'

Date:

Tim McGrail
Senior Program Analyst
ASD Technology Strategies

PAUL A. TIBBITS 116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=paul.tibbits@va.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2015.11.10 18:11:28 -05'00'

Date:

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Organization	Notes
0.1	6/4/15	ASD TS	Initial Draft
0.2	7/22/15	ASD TS	Revised draft to incorporate stakeholder input submitted before and during the Stakeholder Kickoff.
0.3	8/3/15	ASD TS	Based on input from IAM collaboration meetings, made the following changes: • Removed the words "for Veterans" from the title of the document. • Revised the Problem Statement and Business Case • Revised the Current Capabilities section • Added content to the Future Capabilities section
0.4	8/17/15	ASD TS	• Incorporated feedback from IAM and HC IdM • Incorporated feedback from vendors • Moved part of Section 2.1 and list of common terms to the appendices
0.5	8/31/15	ASD TS	• Added identity theft/fraud reporting to the list of issues addressed by the DP • Added identity theft/fraud content to Section 2 and Section 3 • Developed use cases
0.6	9/16/15	ASD TS	• Incorporated input from key stakeholders • Changed content on identity theft indicator to specify that MVI POCs cannot change it • Removed Add Veteran Claimant use case
0.7	9/22/15	ASD TS	• Formatting and consistency edits

REVISION HISTORY APPROVALS

Version	Date	Approver	Role
0.1	7/16/15	Nicholas Bogden	Utilizing Enterprise Identities for Veterans Enterprise Design Pattern Lead
0.2	7/30/15	Nicholas Bogden	Utilizing Enterprise Identities for Veterans Enterprise Design Pattern Lead
0.3	8/12/15	Nicholas Bogden	Utilizing Enterprise Identities Enterprise Design Pattern Lead
0.4	8/24/15	Nicholas Bogden	Utilizing Enterprise Identities Enterprise Design Pattern Lead
0.5	9/10/15	Nicholas Bogden	Utilizing Enterprise Identities Enterprise Design Pattern Lead

0.7	9/28/15	Nicholas Bogden	Utilizing Enterprise Identities Enterprise Design Pattern Lead
1.0	November 2015	Tim McGail	ASD TS Design Pattern Final Review

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 BUSINESS NEED 1
1.2 APPROACH 2

2 CURRENT CAPABILITIES AND LIMITATIONS 2

2.1 THE IAM PROGRAM AND MVI 2
2.2 ENTERPRISE IDENTITY (EI) CHALLENGES 3
2.2.1 Lack of Common Nomenclature for VA Identity Management 3
2.2.2 Lack of Adequate Governance to Enforce Requirements 4
2.2.3 Poor Data Quality Management 4
2.2.4 VA Identity Fraud Policies Fail to Address or Leverage MVI 5

3 FUTURE CAPABILITIES 7

3.1 COMMON NOMENCLATURE FOR VA IDENTITY MANAGEMENT 7
3.2 IDENTITY SERVICES INTEGRATION PROJECT REQUIREMENTS 8
3.3 CORE ENTERPRISE REQUIREMENTS FOR IDENTITY DATA QUALITY 8
3.3.1 Essential Data Quality Roles and Responsibilities 9
3.3.2 Leverage Existing Data Quality Resources 10
3.4 REPORTING FRAUD THROUGH MVI 10
3.4.1 Identity Fraud Reporting Procedure 11
3.4.2 Using MVI for Other Aspects of Identity Fraud Handling 11
3.5 SUMMARY OF SOLUTIONS 12
3.6 ALIGNMENT TO THE TECHNICAL REFERENCE MODEL (TRM) 12

4 USE CASES 14

4.1 NEW SYSTEM OR CONSUMING APPLICATION THAT LEVERAGES EIS 14
4.1.1 Purpose 14
4.1.2 Assumptions 14
4.1.3 Use Case Description 14
4.1.4 Use Case Context Diagram 15
4.2 REPORTING SUSPECTED IDENTITY FRAUD 15
4.2.1 Purpose 15
4.2.2 Assumptions 16
4.2.3 Use Case Description 16
4.2.4 Use Case Context Diagram 17

APPENDIX A. DOCUMENT SCOPE 18

A.1 SCOPE 18
A.2 INTENDED AUDIENCE 18
A.3 DOCUMENT DEVELOPMENT AND MAINTENANCE 19

APPENDIX B. MVI CHARACTERISTICS AND CAPABILITIES 20

B.1 STRUCTURE AND CONTENT OF MVI IDENTITY RECORDS 20
B.1.1 MVI Identity Records *20*
B.1.2 MVI Corresponding Identifiers *24*
B.1.3 MVI Integration Patterns *26*
B.2 ENTERPRISE CAPABILITIES AND SERVICES SUPPORTED BY MVI 27
B.2.1 Identity and Access Management *27*
B.2.2 Sharing Information with Non-VA Partners *27*
B.2.3 Maintaining Consistent Identity Records Across the Enterprise *27*
B.2.4 Record Locator Service *28*

APPENDIX C. DEFINITIONS 29

C.1 ENTERPRISE DEFINITIONS FOR KEY IDENTITY MANAGEMENT TERMS 29
C.2 KEY TERMS AND DEFINITIONS 33

APPENDIX D. ACRONYMS 34

APPENDIX E. REFERENCES, STANDARDS, AND POLICIES 36

FIGURES

Figure 1: Correlation between a Person's Primary View and their Records in Other Systems.... 21
Figure 2: Sample Veterans Health Identification Card (VHIC) 25

TABLES

Table 1: Traits in an MVI Identity Record 21
Table 2: Corresponding IDs in MVI Records 25
Table 3: Enterprise Definitions for Key Identity Management Terms..... 29
Table 4: Key Terms and Definitions 33
Table 5: Acronyms..... 34

1 INTRODUCTION

1.1 Business Need

Until recently, the Department of Veterans Affairs (VA) lacked a shared, enterprise-wide system or standard for representing individual people in the real world. Organizational units at the line of business (LOB)[1] level (or lower) used their own separate ways to identify, track, and refer to the people they served. VA had no reliable basis for sharing information about or coordinating service delivery to individual people without shared Enterprise Identities (EIs) to use as a common reference point for those people.

To address that capability gap (and persistent access management issues), VA launched the Identity and Access Management (IAM) program in 2010. All present and future VA systems and applications that use and/or retain Veteran data are required to integrate with the Master Veterans Index (MVI), VA's designated authoritative data source (ADS) for identity data. All VA LOBs, offices, programs, and project teams now have the EIs they need to address systemic service delivery problems and support new, innovative capabilities and service offerings.

VA has realized significant improvements in the data management and service delivery capabilities since instituting the IAM program. IAM contends with multiple problems on how some VA applications[2] consume identity services, and they include:

1. **Disagreement over Definitions.** Different LOBs have different working definitions for common terms, stalling efforts to develop enterprise policies, standards, and best practices.
2. **Lack of Adequate Governance.** Executives and project managers within VA organizations are ignoring requirements to integrate with MVI because existing governance structures do not enforce those requirements.
3. **Poor Data Quality.** Some consuming applications do not have sufficient quality control measures to ensure correctness and accuracy in their own identity data, which impacts correlation to MVI EIs.
4. **Deficient Enterprise Identity Fraud Handling.** MVI has identity theft/fraud notification capabilities, but VA's incident response policies and processes do not address or leverage them.

[1] VA LOBs include the Veterans Health Administration (VHA), the Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA).
[2] "Applications" in this context refers to major applications, systems, and services.

These issues significantly hamper VA's efforts to leverage EIs in pursuit of its strategic goals, including the implementation of other planned Enterprise Shared Services (ESS) and the transition to a service-oriented VA Enterprise Architecture (VA EA).

1.2 Approach

The goals of this Enterprise Design Pattern are to:

- Help the IAM program in efforts to continuously improve existing services, deploy new capabilities, and promote productive adoption and use of enterprise identity services.
- Define terminology associated with managing and using Veteran records.
- Increase rates of compliance with requirements to integrate with MVI and use EIs.
- Establish core roles and responsibilities for identity data stewardship and quality assurance in consuming applications.
- Outline basic requirements to use MVI for reporting suspected or confirmed incidents of identity fraud.

This Enterprise Design Pattern supports the strategic goals of integrating Veteran data, building and maintaining the VA EA, and providing Veterans with more transparent access to their own records. Elements of this Enterprise Design Pattern may be applied to upcoming VA ESS, including future ADS designated under the Enterprise Information Management (EIM) policy.[3]

2 CURRENT CAPABILITIES AND LIMITATIONS

2.1 The IAM Program and MVI

OI&T established VA's IAM program in 2010 as part of a strategic effort to address the Department's persistent security and service delivery problems. Since VA has records on more than 22 million Veterans, beneficiaries, and others, building a new EI ADS would have been prohibitively difficult and costly. OI&T instead selected an existing identity data store that closely resembled the desired final product – the Veterans Health Administration Master Patient Index (VHA MPI) – and adapted it into VA's ADS for identity data.

The resulting MVI, while an enterprise resource, is still owned and managed by the VHA Data Quality Healthcare Identity Management (HC IdM) Program. HC IdM is responsible for:

- Integrity of identity data within MVI.

[3] Refer to *VA Memorandum: VA Identity Management Policy* (VAIQ 7011145) http://vaww.iam.va.gov/docs/IdentityManagementPolicyMemo.pdf

- Identity management guidance, requirements, policies, and site support to MVI field points of contact (POCs).
- Support for identity data sharing efforts with external partners.
- Establishing the business and technical requirements levied on each MVI consuming application within VA.

MVI's equipment, software, and related services are operated by the Identity Services (IdS) team. The IdS Integrated Technical Team (ITT) is responsible for helping VA system and application owners establish and maintain integration with MVI (i.e., become consuming applications). IdS and HC IdM are distinct and separate from IAM, although the latter depends on MVI to support its authentication, authorization, and access control functions.

For a complete description of MVI identity records, including Primary View (PV) identity traits and corresponding identifiers, refer to Section B.1.

2.2 Enterprise Identity (EI) Challenges

MVI and its related services provide the means for VA LOBs, programs, and projects to adopt and leverage EIs in their own systems and processes. With EIs, these organizations can deploy new solutions and capabilities previously unavailable. Some parts of VA are taking advantage of the opportunity presented by EIs while others struggle to comply with mandates to use EIs, use EIs incorrectly, or both.

The IAM program faces recurring issues from some of its consuming applications that interfere with full adoption and effective use of VA identity services. These issues are:

- Lack of common nomenclature related to Veteran identity/records management.
- Lack of awareness about requirements to use identity services.
- Inadequate data quality management preventing identity correlation.
- Enterprise identity fraud handling policies do not address or leverage MVI capabilities.

2.2.1 Lack of Common Nomenclature for VA Identity Management

The VA LOBs each have their own lexicon of terms related to managing Veteran identities and Veteran data. LOBs may, for example:

- Interpret/use the same word differently.
- Use different words to describe the same concept or activity.
- Commonly use terms that have no equivalent in other LOBs.

The differences are significant enough that they preclude the kind of cooperation necessary for data sharing or correct use of the identity management system. Without commonly accepted enterprise-wide terms for identity and data management, it is prohibitively difficult to develop (let alone implement) policies around usage of the VA identity management system. Any

attempt to do so would be thwarted by lack of consensus on the meaning or usage of key terms.

2.2.2 Lack of Adequate Governance to Enforce Requirements

The VA Identity Management Policy mandates all VA systems and applications that use and/or retain Veteran identity data to integrate with MVI. Existing systems were required to establish integration by October 2012. Some of these systems were not designed to support a service oriented architecture (SOA) model: both they and MVI required extensive (and sometimes costly) modifications and additions to integrate with each other.

To mitigate this problem, VA established a Project Management Accountability System (PMAS) requirement for projects to address MVI integration before their Milestone 2 review. In principle, all projects thereafter would address MVI integration at an early stage and at minimal levels of difficulty and expense. In practice, many project teams fail to include MVI integration capability before their Milestone 2 review because executives and team leads are unaware of integration requirements. Modifying their project to comply at such a late stage is costly and time-consuming. This lack of awareness and resulting cost persists despite extensive ProPath specifications and regular outreach/awareness efforts conducted by IAM.

The issue has been mitigated to some degree by a March 2015 requirement for New Product projects to address MVI integration before the Milestone 0 review. Project teams are required to submit a Business Requirements Document (BRD) to the IAM Service Governance Manager for evaluation.[4]

The issue persists in enhancement projects, which begin at Milestone 1. Non-compliant enhancement projects are not caught until the Milestone 2 review and consequently implement expensive late-stage corrective measures. As of July 2015, the PMAS Milestone 1 review specifically addresses IAM services and MVI integration. This change may increase compliance with MVI integration requirements.

2.2.3 Poor Data Quality Management

VHA still uses MVI as a patient index for managing electronic health records (EHR). Errors in MVI records – including accidental duplication or merging of identities – present a significant patient safety risk.HC IdM maintains a quality standard for MVI data that far exceeds the requirements of a typical enterprise identity management system. HC IdM has very well-

[4] Refer to the first use case for this Enterprise Design Pattern (in Section 4,1) for a description of this process.

defined and mature processes for ensuring data quality, to include verifying input, correcting mistakes, and change control.

Non-VHA consuming applications may not have (or not enforce) similar quality standards for the identity data they retain. They lack adequate means to prevent, proactively detect, or correct problems. For example:

- Mistyped/transposed characters introduced during data entry
- Inconsistent formatting makeing data difficult to read and interpret correctly
- Erroneous merging or duplication of identity records

As a consequence, their identity records suffer from frequent and persistent data quality issues. These issues do not typically compromise MVI records, mostly due to the strict constraints HC IdM places on write access to the system.[5] They do however interfere with correlation between consuming applications' records and their "mates" in MVI, due to mismatches between identity traits in the respective systems' identity records.

The most frequent and visible consequence of such correlation failures is that they prevent Veterans from accessing their data through self-service applications. MVI identity records are the basis for VA single sign-on (SSO) credentials and a Veteran's critical path to accessing his/her correlated data through applications and Web services. If a Veteran's target record is not appropriately correlated to his/her EI, the critical path to that record is broken. In effect, data quality issues compromise VA's ability to offer transparent data access and on-demand service to Veterans and beneficiaries through self-service applications.

2.2.4 VA Identity Fraud Policies Fail to Address or Leverage MVI

The MVI PV contains an "Identity Theft" field used to flag EIs involved in suspected or confirmed identity theft. By default, the Identity Theft field is set to "No." Flagging the record by changing the value to "Yes" indicates an individual's identity information has been stolen and has been or may be used to impersonate them. VHA uses the indicator as part of its identity theft/fraud handling processes – it is visible in VistA applications used by clinicians and other Veteran-facing staff.[6]

---

[5] HC IdM has full access to MVI person records. Veterans and beneficiaries can update some of their identity traits through self-service applications. Beyond that, internal VA users in certain roles (e.g., hospital registration staff, benefits counselors) have access to a limited set of MVI write operations through some major consuming applications, based on business need.

[6] For a description of VHA's identity theft reporting and handling requirements, refer to *VHA Directive 1906: Data Quality Requirements for Healthcare Identity Management and Master Veteran Index Functions* section 16:

HC IdM flags EIs when it receives an identity fraud notification from:

- The VA Office of the Inspector General (OIG), when it opens an identity fraud indication concerning a particular person or persons.
- An MVI POC for either a VHA facility or non-VHA consuming application.

If HC IdM receives a notification from the later source, it passes the notification on to the OIG. In either circumstance, HC IdM flags the affected EI(s) using the Identity Theft indicator. The flag itself is not visible to the majority of non-VHA consuming applications, but it does affect those applications by triggering special MVI technical controls:

MVI technical controls that segregate it with the following special restrictions:

- Write access denied for all users other than those in HC IdM.
- The EI cannot be located using identity trait-based queries (i.e., a combination of first or last name, Date of Birth (DOB) and Social Security Number (SSN). It can still be retrieved with corresponding identifiers.
- External user SSO/self-service logon credentials associated with the identity record are disabled.

Segregating an EI with these controls interferes with some legitimate access and operations, but also protects it from tampering while it is involved in an OIG investigation. When the OIG concludes its investigation, it notifies HC IdM, which sets the Identity Theft indicator back to "No" and restores normal access to the EI.

Most identity fraud notifications sent to HC IdM come from either the OIG or VHA facilities. Occasionally, an MVI POC for a non-VHA consuming application will notify HC IdM using the issue reporting function of the IdM Toolkit. Through MVI, VA has (inadvertently) acquired a partial enterprise capability to report and respond to individual cases of identity fraud.

MVI is not consistently used for identity fraud handling outside of VHA. It is unclear whether any consumers with MVI POCs (not all consuming applications have them) mandate reporting through the IdM toolkit. Most non-VHA consuming applications do not register the status of the Identity Theft indicator. VA's incident response policies, which were last updated years before the advent of MVI, do not deal with handling individual identity theft cases at all.[7]

"Patient Records Involved in Medical Identity Theft."
(http://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=2880)

[7] See *VA Handbook 6500.2: Management of Security and Privacy Incidents*.

VA has the technical capability to improve safeguards against identity theft and identity fraud, but that capability will remain underutilized until VA makes a concerted effort to leverage it.

3 FUTURE CAPABILITIES

VA's efforts towards enterprise-wide identity management services have focused primarily on the technological capabilities necessary to support those services. VA has not devoted the same level of effort, attention, and resources to the governance aspects of identity management. As a consequence, some parts of VA misuse, underuse, or fail to use the identity management services that VA has provided.

The capabilities described in this Enterprise Design Pattern partly address this overarching governance issue by:

- Defining a common enterprise vocabulary around identity management and designating a governance mechanism for defining future ambiguous or contested terms.
- Building new identity services requirements and compliance checkpoints into the Enterprise Technical Architecture Compliance Criteria (ETA CC).
- Establishing a baseline set of roles, responsibilities, and core processes for identity data quality management.
- Outlining requirements to use MVI/the IdM Toolkit for reporting suspected or confirmed incidents of identity fraud, as captured in BRD for future IAM releases.

In the long term, VA's approach to governance includes MVI and its capabilities as a mandated ESS, and an essential pillar of the VA EA. This requires providing IAM and HC IdM with the authority and resources for the services they provide. Doing so will allow VA to build the governance framework it needs to fully leverage its existing technologies and enable future ones, like cloud services in accordance with the VA EA. Only with well-defined policies and business rules can VA achieve the strategic goals that motivated creating an enterprise identity management system in the first place.

3.1 Common Nomenclature for VA Identity Management

The *IAM Services Master Glossary*[8] will serve as the authoritative source of definitions and business usage for terms related to identity management. IAM and HC IdM will coordinate on periodic reviews of and revisions to the *Glossary*.

[8] Available at http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/Identity_and_Access_Services_Master_Glossary.pdf

This Enterprise Design Pattern lists and defines (in Section C.1) key identity management terms that are:

- Commonly used, but not defined in the current version (1.5) of the *IAM Services Master Glossary*.
- Defined in the *IAM Services Master Glossary*, but in need of updates or revisions.

3.2 Identity Services Integration Project Requirements

The June 2015 introduction of PMAS Milestone 1 requirements to use IAM services will reduce the occurrence of non-compliance with MVI integration mandates. IAM, HC IdM and the PMAS Business Office will undertake additional measures to further improve levels of compliance.

HC IdM will select Business Subject Matter Experts (SMEs) to participate in PMAS Milestone 0 and Milestone 1 reviews. At those early stages of the PMAS process, they are able to drive cost-effective approaches and corrective actions (as necessary) for all types of projects that use identity data. HC IdM will also educate other members of the PMAS Working Group on the following topics:

- Which projects are required to use IAM services (i.e., integrate with MVI).
- The IAM governance process for New Product and Enhancement projects.
- Appling MVI integration patterns.
- How to detect a non-compliant project.

The PMAS Business Office will coordinate with HC IdM to ensure that the ETA CC checklist includes one or more references to VA identity services. Project leads are required to review the ETA CC checklist at Milestone 0 of a New Product project. This will serve to alert project teams to the need for MVI integration early in the development process, to plan their project schedules and activities accordingly.

3.3 Core Enterprise Requirements for Identity Data Quality

Correlation failures due to poor data quality have a significant downstream impact, disrupting capabilities and functions that depend on the identity management system. Millions of legacy (i.e., pre-MVI) Veteran records across VA – in consuming applications and elsewhere – have data quality issues that prevent correlation. Ex post facto data quality measures to correct these records are of limited utility, since many do not contain sufficient information to attribute them with certainty to a single individual. For VA, the most critical area of focus is proactive enterprise-wide policies, standards, and business rules to better manage the records it creates going forward.

It will take time for VA to develop appropriate enterprise standards and business rules for identity data quality, along with related training and other resources.[9] In the interim, VA will begin addressing recurring quality issues by:

- Defining roles and responsibilities for data quality in consumer organizations.
- Leveraging existing VA data quality resources, programs, and SMEs.

3.3.1 Essential Data Quality Roles and Responsibilities

The roles and responsibilities outlined below apply to VA consumers – i.e., VA organizations that own and use consuming applications – with respect to consuming applications that retain Veteran data. These roles may overlap or apply to more than one consuming application (for example, to all the consuming applications owned by a particular office).

Business Owners are business sponsors and project/program managers of a consuming application. Their responsibilities include:

- Formally designate Data Stewards for the consuming application and provide them with the support and resources they need for data quality maintenance and improvement.
- Formally designate at least one candidate to serve as the MVI POC for the consuming application, or make the Data Stewards responsible for doing so.[10]
- Ensure that the consuming application is properly integrated with VA identity management services by engaging in the IAM governance process when it is developed or enhanced.
- Implement any enterprise, LOB/organization-specific, and application-specific administrative and technical controls for data quality. These include controls specified by IAM or HC IdM.
- Ensure data quality incidents are promptly reported to the consuming application's Data Steward and MVI POC.
- With input from Data Stewards, invest in monitoring and continuous improvement of the consuming application's data quality assurance capabilities.

Data Stewards are VA personnel responsible for maintaining and/or operating the consuming application's data store, such as database administrators. Their responsibilities include:

- Correct known data quality issues, whether they are isolated or recurring/systemic in the consuming application, as directed by the Business Owner and/or HC IdM.

---

[9] Enterprise business rules for consistent formatting and quality in identity data may be addressed in a future Enterprise Design Pattern document.

[10] HC IdM ultimately designates MVI POCs, but requires input and cooperation from Business Owners and/or Data Stewards to do so.

- Perform regular data quality audits and take appropriate action on findings from data quality audits, which may include:
    - Providing an analysis and summary of findings to the Business Owner.
    - Investigating any potential issues discovered during the audit, and taking corrective action.
    - Developing recommendations for future data quality enhancements and improvements to submit to the Business Owner.
- Develop and support enforcement of access rules for identity data in consuming application, with input and approval from the Business Owner.
- If requested/directed by the Business Owner, formally designate at least one MVI POC to serve as a liaison with HC IdM.

MVI POCs are designated individuals who serve as a consumer and/or consuming application's liaison to HC IdM. They are authorized to use the HC IdM Toolkit. Their responsibilities include:

- Promptly reporting data quality incidents to HC IdM.
- Duties described in *VHA Directive 1906: Data Quality Requirements for Healthcare Identity Management and Master Veteran Index Functions* as appropriate/applicable.
- Other data quality-related monitoring, coordination, and reporting tasks as directed by HC IdM.

By formalizing these roles and responsibilities, consumers will better engage in local and enterprise-wide efforts to improve and maintain the quality of identity data. They will also facilitate improved functionality and usability for VA identity management services.

3.3.2 Leverage Existing Data Quality Resources

VHA has a mature data quality program and a variety of data quality resources for other LOBs and the VA enterprise to draw on for their own data quality efforts, for example:

- Standards and processes (e.g., VHA Directive 1906), which serve as templates and best practices for organizational data quality controls.
- Training and informational materials provided by the VHA Data Quality Program.[11]
- HC IdM SMEs and tools for data quality auditing.

3.4 Reporting Fraud through MVI

This section references the roles described in Section 3.3.1: having a designated Data Steward and MVI POC(s) with access to the IdM Toolkit is a prerequisite for the reporting processes

[11] VHA's Data Quality Program website can be found at: http://vaww.vhadataquality.va.gov/index.php?lang=en

described here. Reporting identity fraud using the IdM Toolkit is intended to supplement – not replace – current reporting policies, processes, and requirements.

3.4.1 Identity Fraud Reporting Procedure

1. Reporting to the MVI POC
    a. Any VA staff suspecting for any reason that a VA internal or external user may be a victim of identity fraud will:
        i. If not an authorized user of the IdM Toolkit, immediately notify their supervisor and/or security staff.
        ii. If an authorized user of the IdM Toolkit, immediately notify HC IdM as described in Part 3.
    b. Once alerted to possible or confirmed identity fraud, supervisors and security personnel will immediately notify the appropriate MVI POC(s) and data steward(s).
2. Reporting Security and Content Requirements
    a. Identity fraud reports not transmitted using the IdM Toolkit are communicated in writing via a VA-sanctioned secure messaging system (e.g., encrypted VA email).
    b. Identity fraud reports will have a title or heading of "IDENTITY FRAUD ALERT" and be marked Urgent, High Priority, or the equivalent.
    c. Information in the identity fraud report will include:
        i. The sender and date/time the report was sent (entered manually, if not included automatically).
        ii. The EDI-PI, MVI ICN, or a known corresponding identifier for the affected EI, and the DOB of the affected person.[12]
        iii. A summary explanation of why the reporter suspects identity fraud (e.g., the affected Veteran called and provided the initial alert).
3. Once alerted to possible or confirmed identity fraud, MVI POCs will immediately use the IdM Toolkit to send an identity theft notification by:
    a. Retrieving the EI of the affected person using the appropriate identifier.
    b. Using the issue reporting function of MVI to send an alert to HC IdM, along with a summary explanation of the reason for suspecting identity fraud.

3.4.2 Using MVI for Other Aspects of Identity Fraud Handling

Common enterprise requirements and business rules for using MVI in identity fraud handling are beyond the scope of this document, but may be addressed in future Enterprise Design Pattern increments.

[12] The DOB is intended to provide additional verification in case the identifier is mistyped.

Until VA develops such requirements and business rules, VA organizations may independently leverage MVI's Identity Theft indicator for other identity fraud handling activities. For example, the Identity Theft indicator may be used to:

- Trigger alerts to security personnel, data stewards, and other relevant POCs in VA.
- Alert Veteran-facing staff that someone may try to impersonate a particular Veteran or beneficiary using stolen identity information.
- Automatically restrict access to the records of affected individuals in the consuming application.

Implementing read access to the Identity Theft indicator is not a standard feature of any consuming application interface to MVI, and will require the assistance of HC IdM.

3.5 Summary of Solutions

The capabilities described in this section address:

- Common nomenclature for enterprise identity management terms
    - Define terms that are contested and/or ambiguous
    - Establish a governance mechanism for resolving future terminology issues
- Universal, consistent use of the IAM Governance Process during the initial PMAS Milestone tasks for both New Product and Enhancement projects
    - Include question(s) about MVI integration in the Enterprise Technical Architecture Compliance Criteria (ETA CC) Checklist used at PMAS Milestone 0
    - Ensure that an IdM Business SME participates in Milestone 0 and 1 reviews
- Defined core roles and responsibilities for identity data stewardship and quality assurance in consuming applications
- Basic requirements to use MVI/the IdM Toolkit for reporting suspected or confirmed incidents of identity fraud

3.6 Alignment to the Technical Reference Model (TRM)

This section provides examples of TRM-approved tools that consumers may use to maintain and improve data quality in consuming applications.

Tool Category	Example Approved Technology
Business Rules Engines	Drools, JBoss BRMS, Spring Web Flow
Business Process Management Engines	Appian BPM Suite, IBM Business Process Manager
Data Quality Management	AutoDelivery, DataFax, SAS Quality Control

Tool Category	Example Approved Technology
Database-Related Management Tools	Hibernate ORM, Data Access, Oracle Enterprise Manager
Master Data Management	Occupational Access System, Protégé
Security Event and Information Management	HawkEye AP, HTTPWatch, Intrust Agent

4 USE CASES

The following use cases demonstrate the application of capabilities/recommendations described in this document.

4.1 New System or Consuming Application that Leverages EIs

4.1.1 Purpose

One of the most critical and persistent issues derailing VA's attempts to leverage identity management services is lack of compliance with PMAS requirements related to those services. Project teams that fail to address MVI integration during their Milestone 0 and Milestone 1 activities scramble to course-correct later in the PMAS process. By not engaging with IAM early on, they may also miss opportunities to leverage the full capabilities of VA identity services in their projects.

This document describes a scenario in which a group of project leads engage with IAM early in the development of a new consuming application. When they add a new capability to their application years later, they engage with IAM again to determine whether they need to make any modifications to their MVI integration solution. Their attention to MVI integration requirements helps them adhere to the established schedule and budget for their project.

4.1.2 Assumptions

- The project in question launches during or after 2015.
- The ETA CC Checklist contains questions about IAM services and/or IAM integration.

4.1.3 Use Case Description

A VA program is designing a new appointment scheduling system. Multiple processes in this system require Veteran identity information. The Project Manager and Business Analyst for the project review the ETA CC Checklist. One of the items on the checklist specifies that project teams working on products that use Veteran identity data submit an IAM Service Request during the requirements definition phase of the project. The IAM Service Request process is described in ProPath *Project Initiation (PRI)* Process Activity 4: Evaluate Enterprise Shared Services.

1. The Project Manager creates and submits an IAM Service Request Package (SRP), following the guidance available in the IAM Service Request Submission User Guide. The IAM SRP includes the following project artifacts:
    a. IAM Service Request
    b. BRD
    c. Business Flow Diagrams
2. The IAM Service Governance Manager receives and evaluates the SRP todetermine the need for VA identity management services. The Manager will:

    a. Work with the Project Manager to schedule a meeting with the IAM Governance Review Intake Team (GRIT), the Business Sponsor, and other members of the primary project team.
    b. Prepares and obtains necessary signatures on a Memorandum of Understanding (MOU) defining the services and actions required of all parties.
3. The IAM GRIT team meets with the Business Sponsor, who presents the business requirements and business flow diagrams from the IAM SRP. The GRIT Team collectively determines to approve or disapprove IAM Service Request.
    a. If the IAM Service Request is disapproved, it is returned to the Project Manager with the Meeting Agenda and Minutes explaining the decision. Depending on the reason for disapproval, he may have to revise and resubmit the IAM SRP.
    b. If the IAM Service Request is approved, the IAM Governance Manager is notified to create and monitor the appropriate change requests.
4. Upon approval of the Service Request, the IAM GRIT team and IAM Governance Manager:
    a. Create Change Requests associated with the specifications contained in the approved IAM Service Request and IAM SRP.
    b. Designate an IAM Project Team and IAM Project Manager to complete the Change Request.
5. The IAM Project Manager and IAM Project Team assist the primary project team in implementing the change request. The IAM SRP and Change Request inform the development of the Project Charter.
6. When the Business Sponsor initiates an Enhancement project to add new functionality to the appointment scheduling system, the Project Manager submits an updated IAM Service Request package for review. The output of the subsequent review will inform the updated Project Charter.

4.1.4 Use Case Context Diagram

- [SWIM LANE PROCESS DIAGRAM DEPICTING USE CASE 4.1]

4.2 Reporting Suspected Identity Fraud

4.2.1 Purpose

In many cases, HC IdM sets the “Identity Theft” indicator in an MVI record to “Yes” in response to an alert from the OIG that they are investigating a case of identity fraud. Less frequently, the first identity fraud alert sent to HC IdM (or the OIG) comes from an alert MVI POC. This use case is an example of the latter situation, and demonstrates:

- How non-VHA users of consuming applications can provide VA with initial notice of suspected or confirmed identity fraud.
- Existing and notional technical security controls triggered by a change in the Identity Theft indicator:
    - EI segregation in MVI (existing)

    - Notifications to designated roles/parties through a secure channel (notional)
- Resolution of an identity fraud incident.

4.2.2 Assumptions

- The user does not have write access to MVI through a consuming application: he needs to use the IdM Toolkit.
- Setting the Identity Theft email triggers notifications (through a secure channel) to designated roles/parties.
- The user's organization has some established internal processes for reporting and responding to identity fraud, but they are not influenced by or dependent on MVI and not included here.[13]

4.2.3 Use Case Description

1. A Veterans Benefits Administration (VBA) Call Center Operator receives a call from a Veteran who claims that someone has opened multiple lines of credit in her name. She believes that her identity has been stolen and is concerned that the thief may try to use her VA benefits or gain access to her medical records. The Operator obtains the Veteran's EDI-PI (the Member ID printed on her VHIC card) and DOB.
2. The Operator uses the IdM Toolkit to:
    a. Retrieve the Veteran's EI using her EDI-PI and DOB
    b. Notify HC IdM of the reported identity fraud via the IdM Toolkit's reporting function
3. HC IdM Quality Auditor receives and reviews the issue report. He then sets the Identity Theft indicator in the specified record from "No" to "Yes."
4. MVI executes preprogrammed automated workflows in response to the change in the Veteran's Identity Theft status:
    a. Generates a log of the change, including when it was made and which user made it (the Quality Auditor).
    b. Sends a notification to designated POCs in HC IdM, OIG, and other VA organizations, containing:
        i. Relevant identifiers for the affected Veteran record (e.g., EDI-PI, MVI ICN)
        ii. Alert that the Identity Theft indicator has been set for the record.
    c. Engages additional security controls for the Veteran's record that will remain in effect until the Identity Theft indicator is reset:
        i. Restricts write access to the record so that only HC IdM users are authorized to modify it.
        ii. Disables external user SSO/self-service login using credentials associated with the identity record.

[13] Enterprise-wide business rules for processing and responding to the MVI Identity Theft indicator may be addressed in a future Enterprise Design Pattern.

iii. Hides the record from identity trait queries – it can only be retrieved using identifier-based queries.

5. OIG opens an identity fraud investigation based on the alert from MVI. Investigative activities may include:
    a. Contacting appropriate law enforcement agencies.
    b. Following up with the affected Veteran.
    c. Following up with the Call Center Operator who provided the initial alert.
    d. Issuing alerts and instructions to internal VA organizations.
    e. Coordinating with the Social Security Administration (SSA).
6. After a period of two months, OIG concludes the investigation and instructs HC IdM to:
    a. Change the Veteran's SSN
    b. Reset the Identity Theft indicator on her record.
7. As instructed, HC IdM enters a new SSN for the Veteran and sets the Identity Theft indicator on her record to "No." As a result, the additional security controls applied in step 3(c) are removed.
8. MVI publishes the updated SSN to some consuming applications and makes it available for others to retrieve as needed.[14]

4.2.4 Use Case Context Diagram

- [SMARTART PROCESS CHART DEPICTING USE CASE 4.3]

[14] The mechanism used to update a given consuming application depends on how it is integrated with MVI. Refer to Section B.1.3: MVI Integration Patterns for further details.

Appendix A. DOCUMENT SCOPE

A.1 Scope

This Enterprise Design Pattern addresses persistent issues related to VA's identity services and the ADS for identity data supporting those services. This document addresses the following goals:

- Enhance existing VA enterprise identity management system (MVI) to augment enterprise identity management capabilities across LOBs.
- Promote adoption of, and innovation with, EIs at the LOB and project team level.
- Engage Data Stewardship, Governance Boards, and LOBs in the data definition and development of enterprise business rules for EIs and identity traits.
- Develop enterprise requirements and standards for reporting suspected or confirmed incidents of identity fraud.

The following concepts are outside the scope of this design document:

- IAM and HC IdM processes and operations for managing, using, and sharing data in the VA enterprise identity management system (MVI).
- Enterprise administrative controls, technical controls, and business rules for responding to reported incidents of identity fraud.
- EI-supported technical security controls:
    - Authentication, Authorization, and Access (AA&A) functions related to or reliant on enterprise identities.
    - Ensuring data messaging security and authenticity.
- Technical implementation of changes to applications, services, components, and/or mechanisms to manage/publish identities from ADS in the VA EA data layer.[15]
- Infrastructure and hardware design specifications.
- Vendor-specific technologies (including database management systems).

A.2 Intended Audience

The primary audience for this document consists of VA stakeholders who are required to use the ADS for Veteran identity data in both existing and future applications, systems, services, and processes. Specifically, these stakeholders are:

- System and application owners/stewards
- System architects

[15] Technical implementation is managed by the Veteran Relationship Management Identity and Access Management Integrated Project Team and ASD Technical Integration.

- Business process architects

A.3 Document Development and Maintenance

This document was developed collaboratively with internal stakeholders from across the Department and included participation from VA OI&T, Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). Extensive input and participation was also received from VHA, VBA and the National Cemetery Administration (NCA). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Updates are coordinated with the Government lead for this document, which will also facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

Appendix B. MVI Characteristics and Capabilities

This section describes the structure and content of MVI identity records, along with the enterprise capabilities/services that MVI supports.

B.1 Structure and Content of MVI Identity Records

Each identity record in MVI contains three types of data about the person it represents:

1. The PV, considered the VA enterprise "gold copy" of a person's identity record. The PV is the best collection of traits known about an Identity among all the sites at VA where that the person has been seen.
2. Additional identity traits used for correlation with records in other systems (in combination with traits from the PV).
3. Corresponding IDs that represent the person/their identity in MVI in other systems, including the EDI-PI, MVI ICN, SecID, BIRLS file number, etc.

Identity traits are the basis for correlating (i.e., matching) a person's EI with their records in consuming applications. If the two records meet or exceed a preset "comparison score" of matching identity traits, they are considered to correlate to each other (and to belong to the same person).

In the matching algorithms used to establish correlation, some identity traits have a greater weight in comparison scoring than others. For example, matching DOBs and SSNs add more to the total comparison score than matching gender values or birth cities.

B.1.1 MVI Identity Records

Each EI in MVI has a globally unique MVI Integrated Control Number (ICN) that corresponds to the PV or "gold copy" of their identity traits. Identity traits are distinctive customer data characteristics belonging to a particular individual (e.g., first name, last name, date of birth, sex). No single identity trait is enough to uniquely identify an individual – even SSNs are not globally unique – but a combination of three or more highly specific traits will suffice. Based on this principle, MVI supports deterministic queries of EIs using a combination of an individual's first or last name, DOB, and SSN.

Identity traits enable looking up individual records and provide the basis for establishing correlations (i.e., matches) between an individual's EI and their records in MVI consuming applications. Figure 1 below illustrates correlation and how it links a Veteran's records – including unique identifiers – to his or her EI.

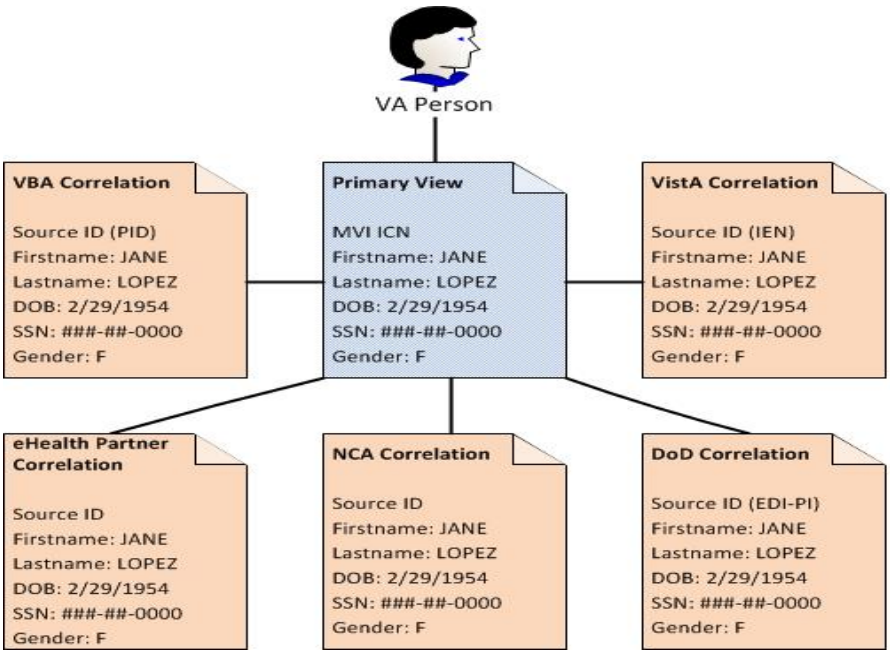

Figure 1: Correlation between a Person's Primary View and their Records in Other Systems

Correlation ties an individual's VA records to the common reference point of his/her EI, and provides the necessary foundation for capabilities like data sharing and single sign-on (SSO). For a complete description of the content of MVI identity records and a more detailed explanation of correlation, refer to Appendix B: MVI Characteristics and Capabilities.

Table 1 below lists the full set of identity traits (both PV and correlation) included in an MVI record.[16] Most of the possible contents of the MVI identity trait fields are listed in the "comments" column. The "Trait Type" column indicates whether a particular trait is included in the PV or for correlation only.

Table 1: Traits in an MVI Identity Record

Identity Trait/Attribute	Data Type	Comments	Service Reference	Trait Type
Source ID	String	150 max	Person	Primary View

[16] The table is based on the identity traits detailed in HC IdM's *MVI Service Description Document* (Version 3.3).

Identity Trait/Attribute	Data Type	Comments	Service Reference	Trait Type
ID Type	Value	National Identifier (NI) Patient Identifier (PI) Employee Identifier (EI) Patient Number (PN)	MVI Source ID Types	Primary View
Assigning Authority	String	Dynamic List	Person	Primary View
Assigning Facility	Value		Assigning Facility	Primary View
IDStatus	Value	A-Active D-Deprecated from a Duplicate M-Deprecated from a Mismatch U-Deprecated from an Unlink H-Deprecated from a Local Merge PCE-Pending Cat Edit correlations	Person	Primary View
LastName	String	Max 25	Persons	Primary View
FirstName	String	Max 25	Persons	Primary View
MiddleName	String	Max 25	Persons	Primary View
SSN	Numeric	9	Persons	Primary View
SSN Verification	Value	0 – New Record 1 – In Process 2 – Invalid per SSA 3 – Re-Send to SSA 4 – Verified	Persons	Primary View
Pseudo SSN Reason	Value	R – Refused to Provide S – SSN Unknown N – No SSN assigned	Persons	Primary View
Prefix	String	10	Persons	Primary View
Suffix	String	10	Persons	Primary View
Mother's Maiden Name (MMN)	String	2-35	Persons	Primary View

Identity Trait/Attribute	Data Type	Comments	Service Reference	Trait Type
Place of Birth City (POBC)	String	2-20	Persons	Primary View
Place of Birth State (POBS)	Value	FIPS Code	State	Primary View
Gender	Value	Male, Female	Persons	Primary View
Date of Birth (DOB)	Date	Date	Persons	Primary View
Multiple Birth Indicator (MBI)	Value	N, Null, Y	Persons	Primary View
Identity Theft	Value	0 – No 1 – Yes Null	Persons	Primary View
Alias	String	Multiples	Alias	Primary View
Date of Death	Date	Date		Primary View
Address **Line 1** **Line 2** **Line 3** **City** **State**	 String String String String Value	 3-35 3-30 3-30 3-28 From State File		Primary View
Phone Number	String	Max 4-23		Primary View
Ethnicity	Value	0000-0 – Declined to Answer 2135-2 – Hispanic or Latino 2186-5 – Not Hispanic or Latino 9999-4 – Unknown by Patient	Persons	Correlation
Race	Value	1002-5 – American Indian or Alaska Native 2054-5 – Black, or African American 2028-9 – Asian 2076-8 – Native Hawaiian or Other Pacific Islander 2106-3 – White 2131-1 – Other Race	Persons	Correlation

Identity Trait/Attribute	Data Type	Comments	Service Reference	Trait Type
Bad Address Indicator (BAI)	Value	1 – Undeliverable 2 – Homeless 3 – Other 4 – Address not found	Persons	Correlation
Marital Status	Value	D – Divorced M – Married N – Never Married S – Separated W – Widow/Widower U – Unknown		Correlation
Religious Preference	Value	1-83[17]		Correlation

B.1.2 MVI Corresponding Identifiers

Many MVI consuming applications use unique identifiers to refer to individual people and serve as a primary key to their records. The MVI ICN is the primary key for person records in MVI itself, while identifiers from other systems are foreign keys to an EI's correlated records in consuming applications. The ID numbers on a Veteran Health Identification Card (VHIC), shown in Figure 2 below, are examples of corresponding identifiers.

[17] The 83 available values in the "Religious Preference" field correspond to either a particular religious affiliation or an alternative response, for example, "Other," "Unknown/No Preference," and "Asked but declined to answer."

Figure 2: Sample Veterans Health Identification Card (VHIC)

The ten-digit Member ID corresponds to the cardholder's Department of Defense (DoD) Electronic Data Interchange Person Identifier (EDI-PI). The EDI-PI is a 10-digit code created for DoD affiliates and assigned by the Defense Enrollment Eligibility Reporting System (DEERS). The Plan ID is a unique identifier assigned by VHA. Other Corresponding IDs include the Person Identifier (PID) assigned by the VA Corporate Database and the Internal Entry Number (IEN) assigned by My Health*e*Vet (MHV).

Queries that employ corresponding identifiers are the preferred method for consuming applications to locate and retrieve individual EIs. A complete list of corresponding identifiers used in VA consuming applications and DEERS are shown in Table 2 below.[18]

Table 2: Corresponding IDs in MVI Records

ID	Description
DoD EDI-PI	DoD Electronic Data Interchange Person Identifier (EDI-PI), a 10-digit code created for DoD affiliates and assigned by the Defense Enrollment Eligibility Reporting System (DEERS)
SecID	Security Identifier (SecID) assigned by the IAM Provisioning service

[18] Refer to the *MVI Service Description Document* for a complete list.

ID	Description
PID	Person Identifier (PID) assigned by the Corporate Database
BIRLS File Number	File Number assigned by the Beneficiary Identification Records Locator System (BIRLS)
MHV IEN	Internal Entry Number (IEN) assigned by My Health*e*Vet (MHV)
VHA Correlated Systems ID	Patient identifier assigned by VistA
PIV ID	Identifier associated with an individual's VA-issued Personal Identity Verification (PIV) card, if they have one

B.1.3 MVI Integration Patterns

IdS ITT offers a set of customizable integration patterns that enable consuming applications to meet HC IdM's requirements in a manner appropriate to their particular technical and business characteristics. The following summary descriptions are drawn from the *MVI Service Description Document*. [19]

- **Enterprise:** The primary pattern selected for integrating with the MVI. In this pattern, the system or application subscribes to identity trait updates "pushed" from MVI. Enterprise Integration supports person related data sharing across the enterprise so that an LOB can utilize information collected within another LOB. The Enterprise Integration pattern allows disparate systems within an organization to retrieve information from other enterprise systems/external partners and/or to share information with other enterprise systems/external partners.
- **Aggregate:** Similar to Enterprise Pattern, except there is no business need to receive identity trait updates from MVI. In this pattern, the system or application "pulls" information from MVI as needed. This model is mostly employed for User Interface or Call Center applications.
- **Decentralized:** A system integrated with this pattern only supports management of its internal assets for a confined business process. The business process supported/managed within the integrated system is a continuation of a business process started in another system that is correlated to the MVI. There are two types of Decentralized business patterns: Pure and Hybrid.

[19] Found at http://tspr.vista.med.va.gov/warboard/ProjectDocs%5CMVI%5CMVI_Service_Description.pdf.

- **Decentralized Pure:** There is no business need for this integrated system to retrieve or to share information with other lines of business.
- **Decentralized Hybrid:** There IS a business need for this integrated system to retrieve information from other LOBs as a continuation to the business process.

- **Repository:** Systems integrated with the Repository pattern store business events for informational use by other business processes.

B.2 Enterprise Capabilities and Services Supported by MVI

B.2.1 Identity and Access Management

The specifics of how EIs are used for purposes of AA&A are beyond the scope of this document. For purposes of this document, security-related identity management functions are relevant in that some of them depend upon correlations between MVI and consumer records. Identity-based SSO only functions as intended if the user's identity in the ADS correlates to all of his/her records in other VA systems.

B.2.2 Sharing Information with Non-VA Partners

Some of MVI's identity service consumers belong to non-VA organizations, for example, contractors (e.g., IBM), federal and healthcare partner organizations (e.g., the Centers for Disease Control), and DoD. For the purposes of this document, the most noteworthy sharing partner is DoD. As shown in Table 2, one of the Corresponding IDs associated with each ICN is an EDI-PI, the identifier used in DoD DEERS. If an individual is enrolled in DEERS but not in MVI, DEERS can create an MVI record for that individual: the reverse also applies.

The integration between MVI and DEERS allows MVI to cross-reference an individual's VA identity with his or her DoD identity. Separating Servicemembers and Veterans do not have to provide copies of DoD records when they submit claims or applications (as they did in the past) to prove eligibility for benefits. They only have to provide their EDI-PI, which MVI uses to cross-reference their VA record with their DoD DEERS record.

B.2.3 Maintaining Consistent Identity Records Across the Enterprise

The MVI Identity Service (Ids) broadcasts identity trait updates to dozens of systems of interest (i.e., subscribers) to which the person identity record is correlated. For example, when a change to a Veteran's legal name is entered in MVI, that update is automatically reflected in systems that use the Enterprise integration pattern. Service consumers that use the Aggregate pattern retrieve individuals' identity traits from MVI on an as-needed basis.

In practical terms – regardless of the integration pattern used – MVI supports a "write once, write everywhere" capability for updating Veteran identity information in VA data stores. It eliminates the need for redundant, time-consuming, error-prone manual data entry on individual systems that contain Veteran identity information.

B.2.4 Record Locator Service

MVI maintains a record locator service that can be used to find all records belonging to a particular identity in service consumers. Service consumers integrated with the Enterprise and Decentralized Hybrid patterns may (depending on business need) use the MVI ICN as an index to locally retained Veteran records.

Appendix C. Definitions

This Appendix contains two sets of definitions:

- Key identity management terms and definitions that are being incorporated into the next version of the *IAM Services Master Glossary*, as per Section 3.1.
- Terms that are not related to identity management, but are specific to and used in this document.

C.1 Enterprise Definitions for Key Identity Management Terms

The terms and definitions included in Table 3 below will be incorporated into the next version of the *IAM Services Master Glossary*.

Table 3: Enterprise Definitions for Key Identity Management Terms

Key Term	Definition
Accuracy	The degree to which a data value, or set of values, correctly represents the attributes of the real-world object or event. To be correct, a data value must be the right value and must be represented in a consistent and unambiguous form.
Catastrophic Edit	Includes changes to an individual's records that result in the record being changed to that of another person, caused by, but not limited to, edits to patient identity (e.g., name, SSN, date of birth, gender) and/or erroneous merging of two or more distinct identity records into a single record within a system.
Consistency	The degree to which a set of data is equivalent in redundant or distributed databases, e.g., between MVI and the data stores of its consuming applications.
Consumer	Refers collectively to the business owners, data stewards, and internal users of a consuming application.
Consuming Application	An application, system, or service that consumes (i.e., integrates with or uses) VA shared services and/or authoritative data sources.
Correlation	A link or association between an individual's person record in MVI and that individual's records in consuming applications. Correlations are established on the basis of matches between sets of identity traits contained in each record.

Key Term	Definition
Correlation Failure	Occurs when an individual's EI and their records in a consuming application cannot be correlated automatically (typically due to data quality issues). Either: • The EI cannot be correlated with *any* record in the target consuming application; or • The EI is correlated with the *wrong person's* record in the target application.
Corresponding ID *or* Corresponding Identifier	A unique identifier in a person's MVI EI representing that person in an MVI consuming application (e.g., DEERS, BIRLS, or CORP). Those identifiers "correspond" to the person's MVI ICN. Corresponding IDs are the preferred basis for MVI database queries by its service consumers (through the FindCandidate operation). *See also* ID *or* Identifier.
Enterprise Identity (EI)	From the perspective of VA identity management, EIs are: • Provided on a one-to-one basis – one real-world person, one identity. • Logical representations of individual Veterans, dependents, beneficiaries, users and surrogates – VA's persons of interest. EI records contain: • VA's enterprise unique identifier (Integration Control Number) assigned and maintained by the Master Veteran Index (MVI). • A "Primary View" or "gold copy" of a person's identity traits. • Corresponding identifiers in other systems. • Additional traits used for matching (i.e., correlating) and locating records across systems.
Enumeration	Enumeration refers to assigning an MVI ICN to a person record, and occurs when a person record is first populated in MVI.

Key Term	Definition
ID Domain	A set of person IDs among which there is to be one unique person ID value per person or entity represented. For example, a hospital Admission, Discharge & Transfer computer system (which may serve multiple hospitals within a region or healthcare network) creates IDs for people as they are entered into the system. The set of IDs it manages is an ID Domain. An ID Domain has a Domain Name which uniquely identifies it from other ID Domains. People can have an ID from many ID Domains. Therefore, a person ID value has meaning for identification only if the correct ID Domain qualifies the ID value. For example, an MVI ICN can only be assigned by MVI, and only has a valid association with a specific individual within the MVI domain. Multiple systems can "reside" in an ID Domain if they utilize/reference person IDs from the same ID Domain. For example, a lab system and a billing system can use the same medical record numbers to identify people. Each system can be said to "reside" in the same ID Domain.
ID *or* Identifier	Identifiers are a sequence of characters (numbers, letters, and/or punctuation marks) assigned to a person by an ID Domain and subsequently used to represent and refer to that person within the ID Domain. Within each ID domain, each identifier assigned to a person is globally unique and specific to that person. Examples of system-delimited ID domains and their identifiers include: • MVI - Integrated Control Number • VA Corporate Database – PID • BIRLS – File Number • DEERS – EDI-PI *See also* Corresponding ID *or* Corresponding Identifier.

Key Term	Definition
Identity Trait	Identity traits are distinctive customer data characteristics belonging to a particular individual, e.g., first name, last name, date of birth, sex, Social Security Number. No single identity trait is globally unique, but in combination these traits constitute personally identifiable information (PII) for specific individuals. In the VA identity management system, identity traits serve to: • Associate a real-world Veteran, family member, or other person with his/her VA enterprise identity (EI) record. • Correlate an individual's EI record with his/her records in EI consuming applications.
Mis-selection	Mis-selection occurs when a user attempts to access or retrieve an identity record belonging to one individual and accidentally accesses or retrieves a record belonging to a different individual. If the user continues his/her task before realizing the mistake, he/she may make a catastrophic edit.
Traceability	The extent to which data are well documented, verifiable and easily attributed to a source.
Validity	The degree to which the data conform to defined business rules.
Veteran	According to 38 U.S.C. § 101(2); 38 C.F.R. § 3.1(d): (d) "Veteran" means a person who served in the active military, naval, or air service and who was discharged or released under conditions other than dishonorable. (1) For compensation and dependency and indemnity compensation the term "Veteran" includes a person who died in active service and whose death was not due to willful misconduct. (2) For death pension the term "Veteran" includes a person who died in active service under conditions which preclude payment of service-connected death benefits, provided such person had completed at least 2 years honorable military, naval or air service, as certified by the Secretary concerned.

C.2 Key Terms and Definitions

Table 4: Key Terms and Definitions

Key Term	Definition
Enhancement Project	A type of project in PMAS that is focused on upgrading or modifying an existing product, rather than developing a new product. These projects start at Milestone 1 of the PMAS process.
Enterprise Shared Service (ESS)	A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions. http://vaww.ea.oit.va.gov/enterprise-shared-services-service-oriented-architecture/
MVI Integration Enterprise Design Patterns (Integration Patterns)	A set of customizable configuration options for consumer systems, applications, and services to integrate with MVI. The pattern and customization options for a particular consumer are selected by HC IdM, based on the consumer's business and technical characteristics.
New Product Project	A type of project in PMAS that is focused on developing a new system, application, or service. These projects start at Milestone 0 of the PMAS process.
Service	A mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description.
Service Oriented Architecture (SOA)	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.

Appendix D. ACRONYMS

The following table, Table 5, provides a list of acronyms that are applicable to and used within this document.

Table 5: Acronyms

Acronym	Description
AA&A	Authentication, Authorization, and Access
ASD	Architecture, Strategy and Design
BIRLS	Beneficiary Identification Records Locator System
BRD	Business Requirements Document
DEERS	Defense Enrollment Eligibility Reporting System
DoD	Department of Defense
EA	Enterprise Architecture
EDI-PI	Electronic Data Interchange Person Identifier
EHR	Electronic Health Record
eMI	Enterprise Messaging Infrastructure
ESS	Enterprise Shared Services
ETA	Enterprise Technical Architecture
ETA CC	Enterprise Technical Architecture Compliance Criteria
ETSP	Enterprise Technology Strategic Plan
HC IdM	Data Quality Healthcare Identity Management
HL7	Health Level Seven International
IAM	Identity and Access Management
IAM GRIT	IAM Governance Review Intake Team
IAM SRP	IAM Service Request Package
IPT	Integrated Project Team
IT	Information Technology
LOB	Line of Business
MHV	My Health*e*Vet
MHV IEN	My Health*e*Vet Internal Entry Number
MOU	Memorandum of Understanding
MPI	Master Patient Index
MVI	Master Veteran Index
NCA	National Cemetery Administration
OIG	Office of the Inspector General
OIS	Office of Information Security
OI&T	Office of Information and Technology

Acronym	Description
PHI	Protected Health Information
PID	Person Identifier
PII	Personally Identifiable Information
PMAS	Project Management Accountability System
POC	Point of Contact
PV	Primary View
SDD	System Design Document
SDE	Service Delivery and Engineering
SecID	Security Identifier
SOA	Service-Oriented Architecture
SSA	Social Security Administration
SSO	Single Sign-On
TMS	VA Learning University Talent Management System
TRM	Technical Reference Model
VBA	Veteran Benefits Association
VHA	Veteran Health Administration
VHIC	Veteran Health Identification Card
VistA	Veterans Health Information Systems and Technology Architecture

Appendix E. References, Standards, and Policies

This Enterprise Design Pattern is aligned to the following VA OI&T references and standards applicable to all new applications being developed in VA, and are aligned to the VA ETA:

#	Issuing Agency	Applicable Reference/ Standard	Purpose
1	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in VA, which applies to all applications that leverage ESS.
2	VRM IAM	VONAPP Direct Connect Benefits from MVI Release: Identity and Access Management (IAM) Identity Services (IdS) Increment 12 Release http://vaww.iam.va.gov/pressreleases/VONAPP_MVI_Increment12_FINAL.pdf	Announces the release of IAM IdS Increment 12 and new capabilities/services provided in that release, including integration with DEERS in order to provide identity verification.
3	VA OI&T	VA Memorandum: VA Identity Management Policy (VAIQ 7011145) http://vaww.iam.va.gov/docs/IdentityManagementPolicyMemo.pdf	• Establishes the Master Veterans Index (MVI) as the authoritative source for identity traits of Veterans and all other persons of interest to VA • Mandates a unique identifier for all Veterans and requires that all VA applications integrate with MVI.
4	VA IAM	Identity and Access Management Portal Strategy Document (Version 2.1)	Describes the functions, capabilities, and content of records in MVI.
5	VA OI&T	VA Directive 6518: Enterprise Information Management http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=791&FType=2	Establishes official policy for the implementation of Authoritative Data Sources (ADSs) in VA.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
6	VHA	VHA Directive 1906: Data Quality Requirements for Healthcare Identity Management and Master Veteran Index Functions http://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=2880	• Establishes data quality requirements for identity records in MVI, including corrective actions for catastrophic edits and handling suspected or confirmed cases of identity theft/fraud. • Defines key VHA data quality terms. Some of these terms, and modified versions of their definitions, are included in the Enterprise Design Pattern's common enterprise nomenclature.
7	VHA HC IdM	Master Veteran Index Service Description Document (Version 3.3) http://tspr.vista.med.va.gov/warboard/ProjectDocs%5CMVI%5CMVI_Service_Description.pdf	Describes MVI services offered to consumers, available operations for using those services, and MVI integration patterns for different types of consumers.
8	VHA HC IdM	VHA Handbook 1907.5: Repair of Catastrophic Edits to Patient Identity http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=2776	Defines the term "catastrophic edit" and establishes processes, roles, and responsibilities for correcting catastrophic edits to patient identity records.
9	NIST	NIST Special Publication 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations (Appendix J) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf	Establishes controls for collecting, maintaining, and using personally identifiable information, including quality controls for identifying information.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
10	VHA HIG DQ	Understanding Dimensions of Data Quality http://vaww.vhadataquality.va.gov/index.php?option=com_phocadownload&view=category&download=194:data-quality-dimensions&id=3:data-governance&Itemid=475&lang=en	Lists and provides definitions of dimensions/characteristics used to evaluate data quality. These terms and definitions are included in the Enterprise Design Pattern's common enterprise nomenclature.
11	VA IAM	Identity and Access Management Services Master Glossary (Version 1.5) http://tspr.vista.med.va.gov/warboard/ProjectDocs/MVI/Identity_and_Access_Services_Master_Glossary.pdf	Terms and definitions used by/within the IAM program. Some of these terms and definitions are included in the Enterprise Design Pattern's common enterprise nomenclature.
12	VA	VA Memorandum: Prioritizing MyVA Customer Data Integration (CDI) Initiative (VAIQ 7628848)	• Emphasizes the criticality of an authoritative data source for identities to the MyVA initiative • Source of language used in the proposed definition of "Identity Trait"
13	VA OI&T	ProPath: Project Initiation (PRI) http://www.va.gov/PROPATH/map_library/process_PRI_ext.pdf	Process Activity 4: Evaluate Enterprise Shared Services describes the inputs, activities, and outputs of the IAM Service Request process.
14	VA OIS	VA Handbook 6500.2: Management of Security and Privacy Incidents https://vaww.portal.va.gov/sites/vbaco-iso/VA%206500%20Handbooks/VA%20Handbook%206500.2%20-%20Management%20of%20Security%20and%20Privacy%20Incidents.pdf	Documents VA policies for identity theft/fraud incident management, and privacy/data breach incidents more generally.