

OneVA Identity Services Segment Architecture Handbook

DRAFT

Pending Action	Contact
Develop Governance Appendix	Fran Parker
Develop Project Planning Appendix (including performance planning)	TBD
Update Services Standards Appendix	Denise Kitts

References:

- EDE Enterprise IdM white paper | December 2006
- Identity Management Program Concept Paper | July 2006
- Joint VA – DoD Common Service Member/Veteran Population Plan | December 2006
- Joint VA – DoD Identity Management (IdM) Framework and OneVA IdM Requirements | March 2006
- OneVA Patient/Person Identity Management white paper | October 2006
- VA / DoD Data Sharing Workgroup Update | February 2006
- VHA Person Service Identity Management web site

DRAFT

Table of Contents

1 Introduction..... 5

 1.1 Purpose..... 5

 1.2 Organization Roles & Responsibilities..... 5

 1.3 Definitions 6

 1.4 Scope 8

 1.5 Business Profile..... 14

 1.6 Identity Management Initiatives 16

 1.7 Identity Services Governance 18

 1.8 Service Oriented Architecture Governance..... 19

2 Identity Services Segment Architecture Profile 20

 2.1 IdM Services Segment Architecture Overview 20

 2.2 OneVA Identity Services Components..... 23

 2.3 Identity Data Domain Management Framework..... 33

 2.4 Impacted/Involved Systems..... 38

3 Implementation Plan 40

 3.1 VA/DoD Common Population 41

 3.2 VA/DoD IdM Data Sharing Services..... 42

 3.3 OneVA Identity Services 45

 3.4 VA LOB Integration of Identity Services 50

 3.5 Immediate Next Steps 51

A. Project and Performance Planning 52

B. Governance..... 53

C. Service Standards..... 54

Table of Figures

Figure 1.3-1 OneVA EA Segments 8

Figure 1.4-1 Baseline (Current) State of VA IdM 9

Figure 1.4-2 Target (Desired Future) State of VA IdM..... 10

Figure 1.4-3OneVA Idm Services 11

Figure 1.4-4 Service Layer Details 12

Figure 1.4-5 Person Information Management Architecture..... 13

Figure 1.4-6 Correlation and Synchronization..... 14

Figure 1.6-1 Relationship of RE & CM..... 17

Figure 2.1-1 Identity Services Architecture..... 21

Figure 2.1-3OneVA IdM Services Oriented Architecture..... 23

Figure 2.2-1 Conceptual Design for OneVA Identity Services 24

Figure 2.2-2 OneVA Identity Services 25

Figure 2.3-1 Hybrid OneVA identity data domain management framework 33

Figure 2.3-2 Conceptual OneVA Person Information Services..... 35

Figure 2.3-3 Party Information Model..... 37

Figure 3.2-1 Timeline of high level milestones 44

1 Introduction

1.1 Purpose

This document is a product of the Department of Veterans Affairs, Office of Enterprise Architecture Management (OEAM).

The purpose of this document is to clarify and articulate definition of the Department of Veterans Affairs (VA) Enterprise Identity Services Segment Architecture, explain basic concepts of identity management as they relate to the VA and discuss how existing initiatives within the VA align to these concepts. This document establishes a high-level starting point for VA's approach for developing an identity management (IdM) EA strategy and implementing an enterprise-wide identity management infrastructure.

This handbook:

- Describes enterprise identity management components and features
- Establishes a common vocabulary and semantics for identity and access management
- Identifies services related to enterprise identity management
- Discusses current enterprise identity and access management related initiatives within VA
- Recommends a high-level approach to enterprise identity management within VA

1.2 Organization Roles & Responsibilities

Defining, designing, developing and deploying OneVA Identity Services involves a number of VA organizations. These include, but are not limited to:

1.2.1 OI&T

The VA Office of Information and Technology:

- Assures sufficient resources are available
- Acquires, implements and integrates technology infrastructure for OneVA Identity Services

1.2.2 OEAM

The Office of Enterprise Architecture Management:

- Defines and manages the OneVA Identity Services Segment Architecture, including VA-wide communication.
- Governs design, development, and deployment of Identity Services
- Facilitates consolidation and integration of IdM requirements

1.2.3 EA Council

The Enterprise Architecture Council:

- Provides business governance for IdM
- Ensures appropriate stewardship for IdM processes and master data

[A more detailed description of Identity Services governance is in section 1.7.]

1.2.4 RE/CM IPT's

Registration & Eligibility and Contact Management (RE/CM) Integrated Project Teams:

- Define IdM requirements as well as document use cases, processes and CONOPS
- Establish priorities and timelines for designing, developing, deploying and integrating Identity Services
- Validate and approve designs
- Perform functional testing
- Provide subject matter expertise
- Provide stewardship for change management.

1.2.5 LOB's

VA Lines of Business (LOB's):

- Make use of OneVA Identity Services as they become available.
- Upgrade and/or replace legacy applications to take advantage of Identity Services Oriented Architecture

1.3 Definitions

Identity. According to the Oxford English Dictionary, identity is “The fact of being who or what a thing or person is.”

In the “information age,” identity is the set of characteristics and attributes, including names, biometric characteristics, relationships, roles and so forth, which serve to identify some person or some thing in a particular context. For example, the fact that a person is over 21 in the US is sufficient to identify them in the context of purchasing alcohol, while

their name, job role and employee number are required to identify them in the context of updating their personnel details in the human resources system at their place of employment. Identity attributes can manifest themselves in physical and digital forms, such as a driving license and an employer-issued smart card. It is important to recognize that identity management applies primarily to digital representation of the attributes, or more correctly, claims to possess the attributes, made by a person, or another person, which serve to identify a person or thing: digital identity.

Identity Management. *The set of processes and supporting technologies which together manage the electronic definition, storage and lifecycles of digital identities and associated policies; and the application of those identities and policies to establish trust in the exchange of electronic information between multiple parties (persons or organizations).*

Segment Architecture. The Office of Management and Budget, Federal Enterprise Architecture (FEA) Program Management Office defines segment architecture as follows:

The information technology architecture for a Line of Business (LOB) or common technology service (called a “Service Component” in the FEA Service Component Reference Model (SRM)). Segment architecture has more detail than the overall Enterprise Architecture and is typically associated with a specific program. Segment architecture ultimately described at the level where measurable results (performance improvement, cost reduction) can be achieved.

VA uses segment architectures as the vehicle for promoting and accelerating IT projects and defines two types of segment architectures:

Core Mission (Business) – focused on a Line of Business (LOB)

Business Services – focused on cross-cutting and shared IT capabilities

The business and service architecture segments currently envisioned for VA are illustrated in the figure that follows.

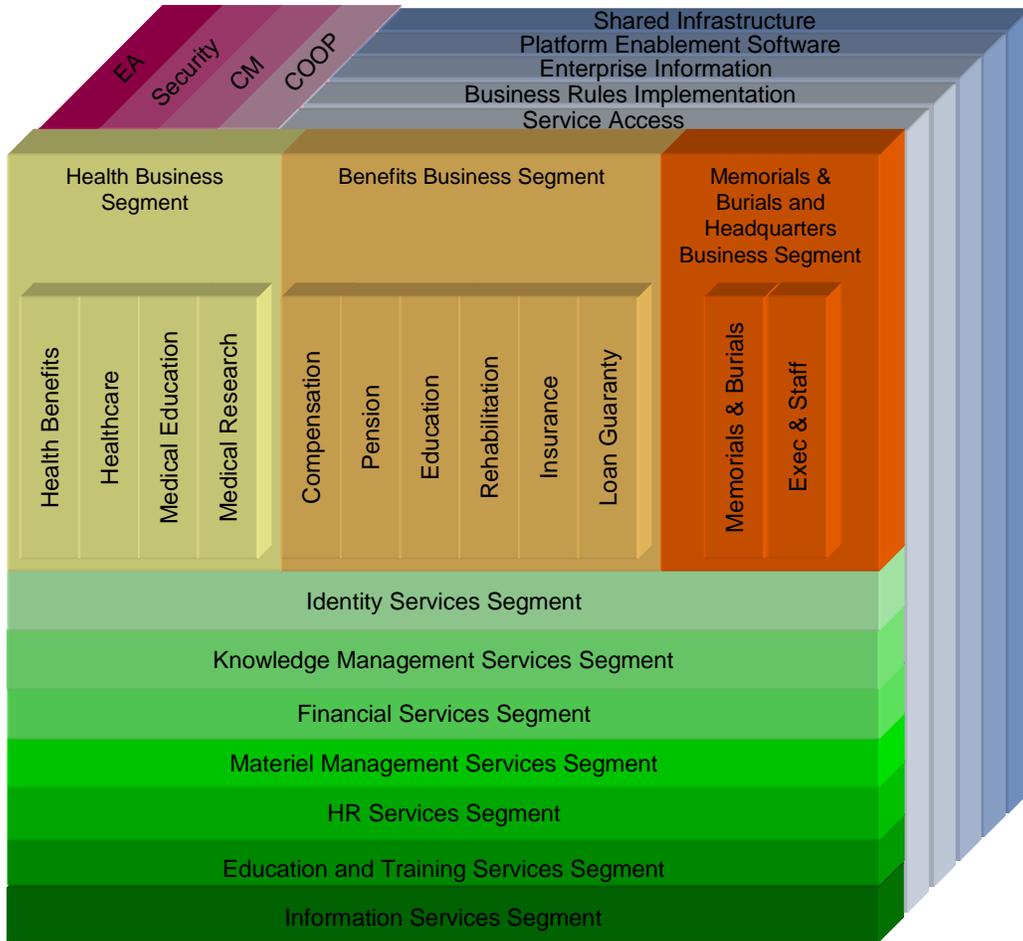


Figure 1.3-1 OneVA EA Segments

1.4 Scope

This handbook focuses specifically on the OneVA Identity Services Segment Architecture. This segment addresses the following identity management needs:

- a) Provide an enterprise identity management service/capability to support the various business lines within VA, as principally represented by the three administrations Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and the National Cemetery Administration (NCA),
- b) Uniquely identify all people about which the VA manages information: primarily veterans, but also other beneficiaries, employees, contractors, providers, etc.
- c) Facilitate information sharing.

In order to meet these needs and other identity management requirements, the department intends to implement comprehensive identity services.

Included in the broad scope of OneVA Identity Services are Self-Service Kiosks, Telephone services and directories, postal mail services, email services (internal and external), and fax services along with supporting identity management utility services such as MS Active Directory and LDAP (Lightweight Directory Access Protocol). The availability of a unique person identifier is the foundation to all processes related to persons, such as OneVA Network Registration, enhanced veteran self-service, assignment of National Provider Identifiers (NPI) and OneVA Contact Management initiatives.

The following graphics and scenarios illustrate the baseline and target states of VA Identity Services.

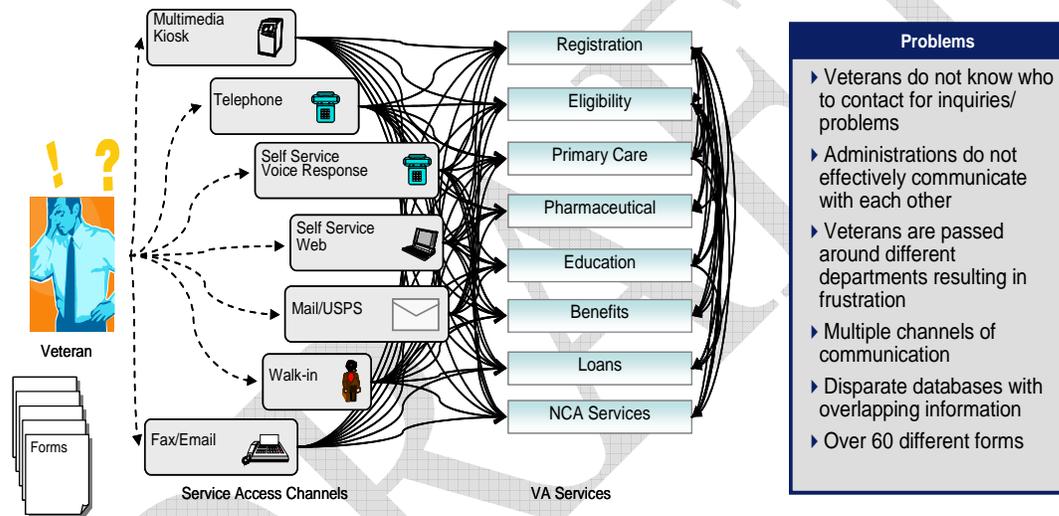


Figure 1.4-1 Baseline (Current) State of VA IdM

1.4.1 Current State Scenario

Currently, the VA has no single governing standard for identity management. The result is a proliferation of processes, security domains, and home grown authentication and authorization mechanisms across systems and applications. Whenever a Veteran approaches the VA for information, a service or support, there is a different process and interface depending upon the reason for the contact. The next time a Veteran contacts the Department for the same reason, it is likely that he will be recognized and the experience will be familiar. Unfortunately, when a Veteran contacts the VA for a different purpose, the experience probably will not be familiar. Further the Veteran will likely not be known, or if known will still have to furnish the same information previously provided; using different forms (often pages and pages) and processes. This is frustrating to the Veteran, wastes the Veteran's time and the time of VA employees, and is prone to error.

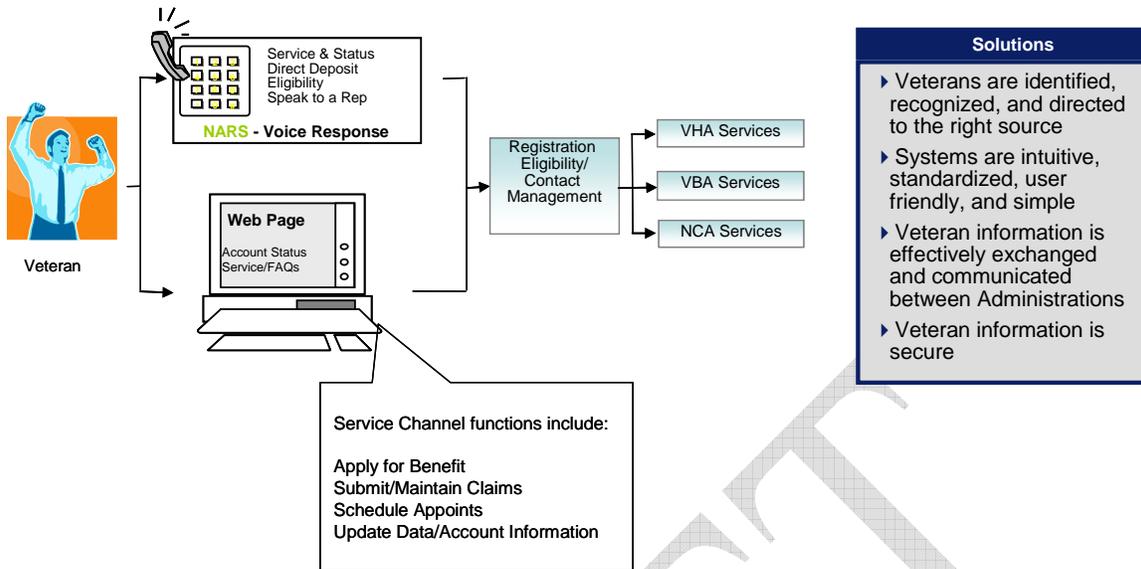


Figure 1.4-2 Target (Desired Future) State of VA IdM

1.4.2 Desired State Scenario

When “Veteran Centric” OneVA Identity Services are fully implemented, any Veteran approaching the VA for any information, service or support will use a single set of processes even though there may be multiple technologies providing interface capabilities. These processes will be supported by automated services which will be delivered via a service oriented architecture that has multiple layers (see Figure 2.1-2 OneVA IdM Services Oriented Architecture). Ultimately, the OneVA Identity Services will apply to other VA-related people such as employees and contractors as well as organizations.

A simplified, notional view of OneVA Identity Services follows:

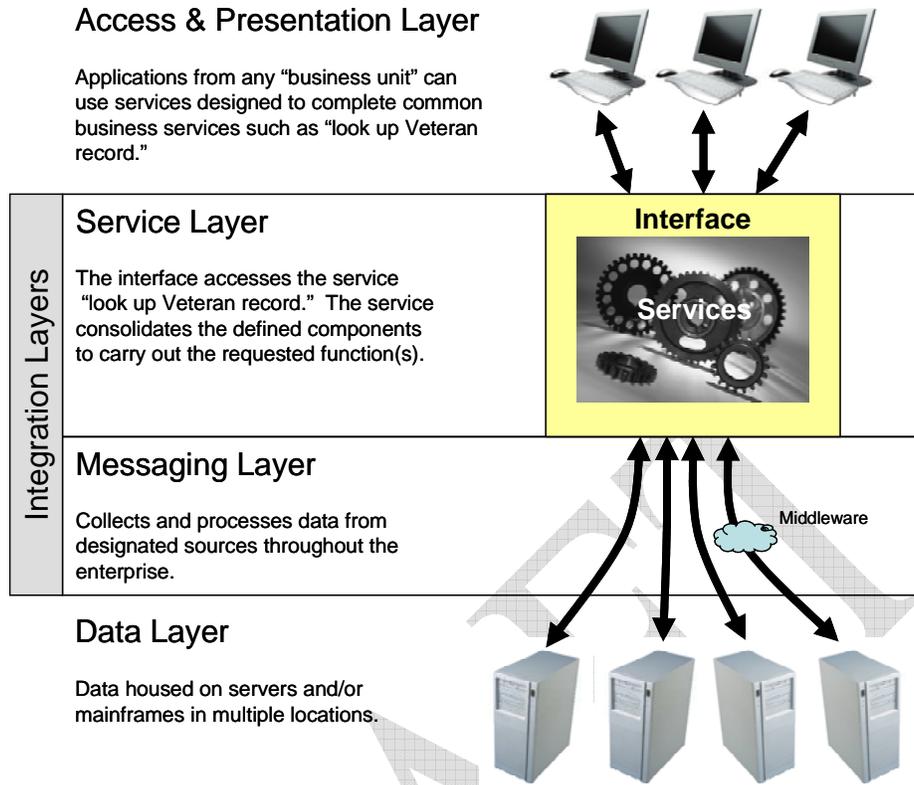


Figure 1.4-3OneVA Idm Services

Within the Service Layer, there will be business services and service components supporting business processes.

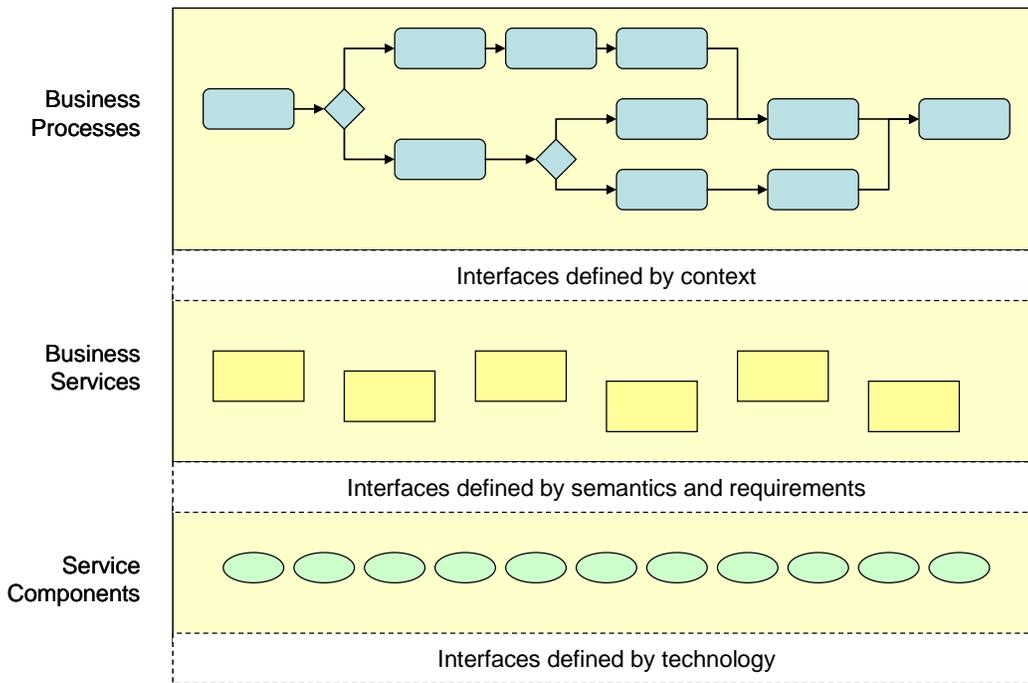


Figure 1.4-4 Service Layer Details

Specific OneVA IdM Business Services are described below in section 2.1 and illustrated in Figure 2.2-2 OneVA Identity Services.

1.4.3 Identity Management and Person Information Management

The traditional and common industry understanding of identity management involves components and features such as identification, authentication, authorization, provisioning, and single sign-on. Identity management, as it is commonly understood in the industry, revolves around the management of *access control credentials* – credentials used for authentication and authorization to resources including systems, applications, facilities, and others. For example, user names and passwords used to log into Windows, BDN, MyHealthVet and other systems and applications are a form of access control credentials.

VA OEAM also recognizes that Identity Services could and should be used by any and all business processes during which a person’s identity is necessary. At the same time OEAM realizes that some business processes and applications may never make use of OneVA Identity Services due to technological or budget constraints.

Identity Information is a subset of Person Information and therefore Identity Management must be tightly coupled with Person Information Management.

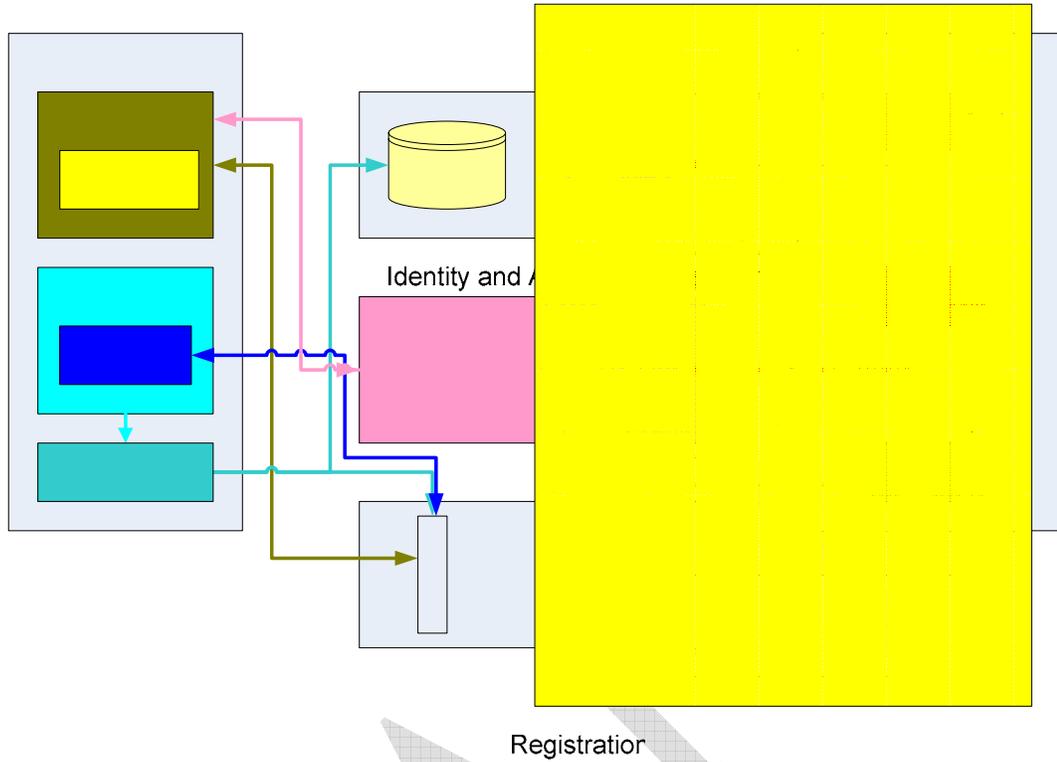


Figure 1.4-5 Person Information Management Architecture

Person information is composed of data used and stored in systems and applications for business purposes. For example, data about employees resides in HR systems and person demographics of veterans are stored in various VA systems. Managing these disparate subsets of person information across systems at the VA must focus on at least two areas:

- 1) **Data Consistency** – managing the process of keeping person data consistent across systems (data correlation and data synchronization), and
- 2) **Data Sharing** – enabling information in one system to be shared with another.

The ability to uniquely identify every person for which VA maintains information is the principle function of identity management. The VA needs to be able to provide an identifier and a credential (access control credential) that is recognized enterprise wide. In order to effectively credential every person about which the VA maintains information, the VA must be able to uniquely identify every person, necessitating the implementation of a unique identifier as well as person information management services such as person identity correlation and synchronization services.

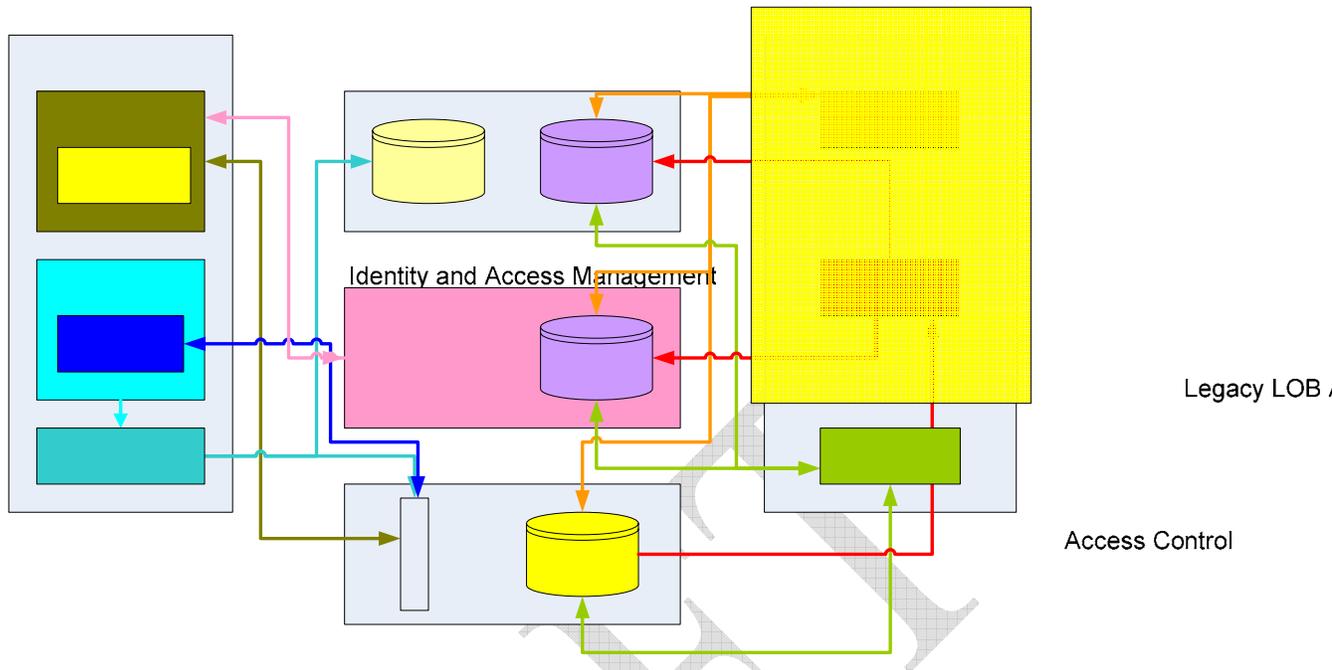


Figure 1.4-6 Correlation and Synchronization

With a unique identifier in place, all person information across all systems and applications must be “related” to this unique identifier. The unique identifier will enable the correlation of person information across systems and synchronization of selected data elements, especially person identity trait and demographic attributes. This directly addresses data sharing needs – enabling information in one system to be shared with another.

An example of the use of a unique identifier at the VA is the Veterans Health Administration’s *Master Patient Index (MPI)* system – a custom-built system developed to address the issue of aggregating and correlating veteran health records stored across VHA medical facilities.

1.5 Business Profile

In February 2006, VA published the following statements pertaining to Identity Management:

- VA is developing its OneVA identity management strategy
- VA has determined that it will establish a single unique identifier (VA ID) for use across all of its internal information systems
- This identifier will be used for veterans, other beneficiary, agents acting on behalf of veterans and beneficiaries and for other appropriate purposes
- The VA ID will conform to appropriate standards such as ASTM-E 1714

LDAP Interface

Legacy LOB A

Access Control

New LOB A

VA Enterprise

- *VA will accept the DoD EDI PI unique identifier and correlate this to the VA ID to assure a one-to-one match*
- *Through this correlation VA will be capable of both accepting data from DoD and of passing information back to DoD using the EDI PI*
- *The VA correlation capability will accept and utilize defined demographic identity traits as well as the EDI PI as appropriate*

The need to uniquely identify veterans and other beneficiaries as well as VA employees and contractors (and potentially others) is the principle reason for establishing Enterprise Identity Services that will:

- a) Facilitate the information sharing, and
- b) Enable transformation to a single unique identifier for each person the VA cares about, even when that person is associated with the VA in multiple ways. For example, a veteran can also be an employee or a contractor.

The ability to establish and maintain unique person identifiers, coupled with a single set of services to manage them, is critical for enabling VA Lines of Business (LOB) to seamlessly share inter-administration data to support business processes that increasingly cross VA Administration boundaries.

1.5.1 Improve data-sharing practices between Administrations

There is the need to seamlessly share necessary identity traits, benefit determination, demographic and treatment information, as appropriate, in order to support the business functions of the VA Administrations. Establishment of a unique identifier is the fundamental step for enabling these activities and assuring interoperability across VA Administrations and LOB's. VA needs to establish mechanisms to enable information that identify a person in one LOB to be available to other LOB's, thereby reducing redundant data collection and enabling the ability to view and/or share information as appropriate and authorized.

1.5.2 Improve data-sharing opportunities with external agencies

VA has a specific need to improve data sharing activities and opportunities with DoD, Social Security Administration (SSA), and other external agencies that will result in improved efficiencies for VA LOB's and meet their business needs. These data sharing opportunities shift and reduce the burden to provide redundant demographic information from the person (patient, beneficiary, employee, provider), to the organization.

1.5.3 Improve efficiency of current self-service applications

Through implementation of an Identity Services capability, VA will be better equipped to support all LOB's that have self-service applications, such as MyHealthVet and other forward facing applications. Identity Services are part of the solution for implementing

any self-service functionality. In addition, an Identity Services capability will support and enable the implementation of authentication and authorization activities.

1.6 Identity Management Initiatives

Certain lines of business have attempted to implement a common identity management framework across their applications, reusing common authentication and authorization components and enabling single sign-on within a security domain. Examples include Loan Guaranty applications accessed through the Veterans Information Portal (VIP), which uses Computer Associates (CA) Site Minder for authentication and authorization; MyHealthVet applications sharing the underlying BEA Portal authentication and authorization components; and other Microsoft based web applications that use Active Directory for authentication and authorization.

There are two major identity management initiatives at the VA that span the enterprise – the VA E-Authentication project and the Personal Identity Verification (PIV) project. Both projects, though independent, are implementing e-Gov identity management functionality that impacts all of VA.

The Registration and Eligibility (RE) Program also has an initiative that is directly addressing Veteran Identification, Correlation, Authentication, and Authorization. The stated goal of RE is to provide a single point of registration, and an enterprise-wide knowledge base for veteran identification. In addition, there are several more RE initiatives that address identity management indirectly. These include VA and DoD Data Sharing and Interdepartmental Data Sharing. All of these initiatives will need to be integrated as elements of the OneVA Identity Services segment architecture. Note that while not currently within scope of the RE Program, VA Identity Services will need to include registration of employees, contractors, affiliates, and partners as well as veterans (customers).

VA has also identified a need to improve service to veterans and others through improving contact management. The OneVA Contact Management (CM) Program is addressing the need for improvements in managing contacts – “touch points” – with veterans, beneficiaries, and other stakeholders. Enterprise Identity Services that provide identification, authentication, and authorization are integral to supporting enhanced contact management capabilities via the Internet and other environments which means that all of the CM identity management initiatives will need to be integrated into the OneVA Identity Services segment architecture.

The figure below shows the relationship between the Registration & Eligibility and Contact Management programs. It also illustrates the scope of the OneVA Identity Services segment architecture.

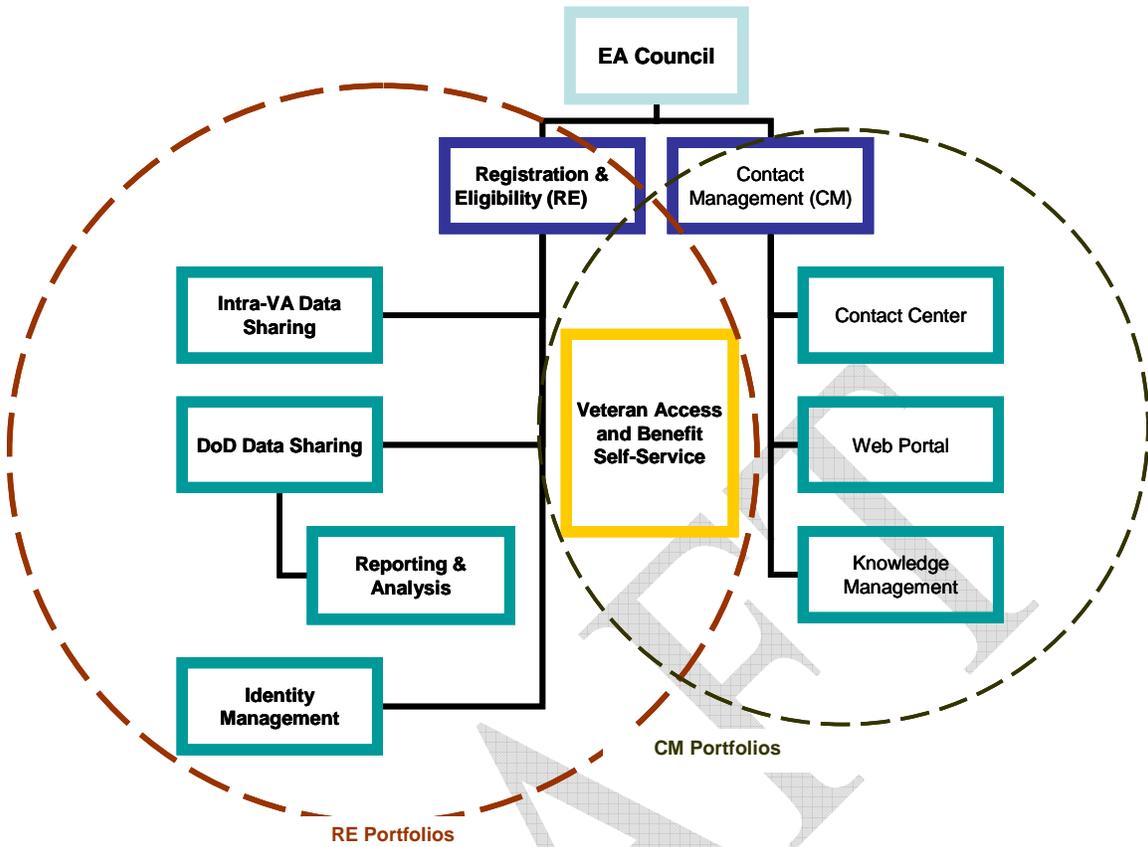


Figure 1.6-1 Relationship of RE & CM

The table below indicates the initiatives and applications that are part of OneVA Identity Management.

IdM INITIATIVE	ORGANIZATION						
	RE	CM	VHA	VBA	NCA	HR	OCIS
OneVA Registration & Eligibility	x		x	x	x		
Identity Management IPT	x		x	x	x		
VA/DoD Data Sharing IPT	x		x	x	x		
Inter-Administration Data Sharing IPT	x		x	x	x		
Self-Service IPT	x	x	x	x	x		
Inter-Agency Registration Capability	x?		x	x	x		
VHA Enrollment System Redesign	x?		x				
OneVA Contact Management		x	x	x	x		
Portal		x					
Contact Center		x					
Knowledge Management		x					
Enhanced Application for Benefit	x			x			
GSA e-Authentication			x				
Person Identity Verification (PIV)	x					x	
Common Person Identity Correlation			x				

IdM INITIATIVE	ORGANIZATION						
	RE	CM	VHA	VBA	NCA	HR	OCIS
DoD/VA CHDR			x				
CDR/CHDR Interoperability			x				
VA/DoD Health Record Export Project			x				
VA Health Information Interchange (VHIE)			x				
Health Information Exchange Gateway (HIEG)			x				
VA Health Information Model v.3 (VHIM)			x				
National Provider Identifiers (NPI)			x				
VBA Application Modernization				x			
Telecommunications Modernization Program (TMP)							x?
Public Key Infrastructure Project (http://vaww1.va.gov/proj/vapki/forpki.htm)			x				x

Table 1.6-1 VA IdM Initiatives

The EA Council has approved and prioritized the following projects that will be impacted by or will impact OneVA Identity Services:

1. Establish a VA ID
2. Consolidate the 31 DoD Interfaces
3. C&P Data Sharing Service
4. One VA Cross Administration Beneficiary consolidated data view (supports enterprise beneficiary lookup)
5. Person Level Data Sharing Service
6. E-Authentication
7. Web Inquiry/Registration
8. Other (Computable) Data Sharing Service
9. E-Signature
10. Web Application for Benefits
11. Inter-Administration Request and Resolution Workflow Tool
12. Reporting and Analysis Data Warehouse
13. Common Population Strategy Work plan
14. PEB

1.7 Identity Services Governance

The key to successfully implementing Identity Services is centralized control that enables flexibility and yet reduces complexity and variation. Centralized control requires management of service development, deployment, and access to ensure that Identity Services are consistently used across the department. Without standards, establishing centralized control is difficult to impossible. Without enforcement, standards are just words in a document. Controlling all of the moving parts (technology, application, information, business processes) of services architecture is a complex task. Governance

serves a crucial role in providing consistency, control and a measured approach to growth.

OneVA Identity Services governance is the responsibility of the **EA Council** (see Figure 1.6-1). This board provides policy guidance, advice and assistance in defining, designing and deploying Identity Services throughout the VA. It serves as the core group providing advocacy for integration of business and technology architectures across VA boundaries. The board serves as a focal point for development and coordination of VA-wide policy and guidance.

Under the guidance and management of the EA Council, **Integrated Project Teams** (IPT's) serve as transformation councils for their disciplines. They are responsible for:

- Gathering, refining and consolidating business requirements
- Performing business domain analysis and process engineering analysis
- Identifying business components, services, and process modules

OEAM serves as the technical board for Identity Services. OEAM ensures alignment of IT with business, following industry and enterprise standards, and technically ensures that exposed services match the requirements for evolution and reusability as defined in the general guidelines for the enterprise service development. OEAM's SOA technical board members will be well versed in emerging industry trends, state-of-the-art technologies, and standardization efforts. They are responsible for framing the technical enterprise architecture blueprints (the master IT plan for the enterprise), identifying niche architecture patterns, and promoting reusability principles. They work closely with the SOA COE and EA Council to ensure the following SOA governance guidelines are addressed.

1.8 Service Oriented Architecture Governance

In order to effectively and efficiently deliver Identity Services it is necessary to establish and maintain an effective and efficient architecture for all VA services. A Service Oriented Architecture (SOA) **Center of Excellence (COE)** will need to be established within **VA OI&T**. The VA, with hundreds of developers functionally and geographically dispersed, needs a common development approach to maintain consistency and interoperability among services. Developers in far-flung business units need to know what services exist and the policy of reuse of services needs enforcement to make it a reality. A SOA COE that provides guidance to developers in designing, developing and deploying service-oriented architecture technologies can make that happen.

The SOA COE communicates to developers through face-to-face meetings and publishes "blueprints" for designing services. The main idea is to encourage the use of common guidelines so service development practices remains consistent. The SOA COE:

- Controls SOA "roadmap"
- Supports large and complex projects

- Keeps SOA-based implementation aligned with the business requirements
- Maintains authority over technical artifacts such as architecture blueprints, enterprise templates, and design assets

The following are SOA governance guidelines that enable such architecture.

- **Business Process Definition:** Because business services and service components directly support instances of business processes it will be necessary to define the processes thoroughly and accurately. Typically, this will be done under management and control of the IPT's by a joint business-IT group. EA Council and OEAM will help determine which should be standardized across VA.
- **Architectural Compliance:** Just a builder has to follow the architectural plans and codes for a house, so do services need to need to reflect the standards of the On-VA enterprise architecture "blueprint." OEAM and the EA Council will review all proposals for service design to ensure architecture compliance. They will also identify proposals that duplicate resources and enforce reuse.
- **Service Management:** A "repository" of services is necessary to help both service developers and business consumers know what services exist and what they do. This will encourage reuse and will help business analysts know what capabilities are available.
- **Data Management:** The data that services act upon can come from multiple sources whose context may not be known by the services. Further, the data may be combined and used in multiple ways. Reducing data chaos and ensuring service data quality requires a data architecture that makes the context of data (metadata) explicit so that services use data and translate data consistently.
- **Security and Compliance:** Because services are not stand-alone applications, they can interact with each other and be accessed by users in unexpected ways. Security policies and provisioning must address the mix-and-match nature of services.
- **Performance Management:** Because service use is ad hoc, composite applications and performance load will be unpredictable. Policies and principles must be implemented to manage priorities and performance levels under severe usage.

(Additional information may be found in Appendix B, "Governance.")

2 Identity Services Segment Architecture Profile

2.1 IdM Services Segment Architecture Overview

This is a cross cutting services segment that impacts and supports all veteran-facing activities and business processes and all automated enabling business applications. A variety of factors, on both the supply and demand side of the market, exert a powerful influence on the department's Identity Services segment architecture. The ongoing supplier consolidation and the associated shift away from a best-of-breed approach and towards integrated identity management suites have resulted in the decision to deliver

identity management capabilities as shared services that can be exploited by business function and information services. Effective control of identity services will require policies which define identity-specific requirements of each interaction, such as how a consumer of a business function service must be authenticated or their rights to access particular information. And, because those identity services depend on identity data, the disparate repositories which contain them must be reconciled and unified.

OneVA Identity Services will be a set of horizontal, resource-agnostic capabilities, as shown in Figure 2.1-1.

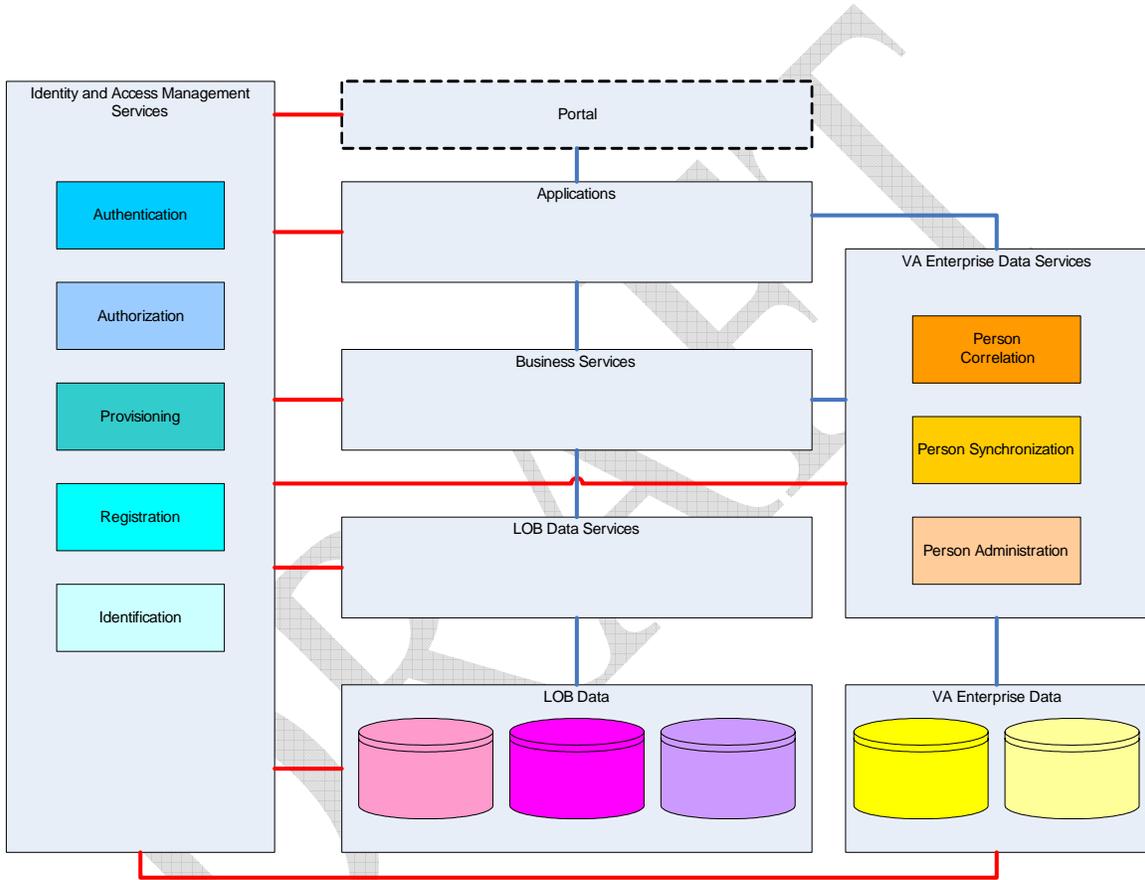


Figure 2.1-1 Identity Services Architecture

OneVA Identity Services Segment Architecture will adhere to 7 core tenets:

- Identity-centric – Identity Services will necessarily reflect an architectural approach which is identity-centric – this will provide the most consistency and flexibility. Identity Services must be generic and all-encompassing – they cannot reflect a single business process or application

- Roles as first class identity assets - party roles must be modeled at the intersection of identities, entitlements, and organizational structures and managed as part of the broader identity management lifecycle
- Role-specific authentication – authentication mechanisms must reflect the levels of risk and the granularity of the resources associated with that risk, without over-burdening the individual, and should apply to both parties in an interaction
- Integrated identity data silos –identity data integration approaches that combine the benefits of meta-directory and virtual-directory technologies, allied with tooling to assist with data reconciliation
- Federated – as a transition tactic, when integration is not yet possible and feasible, a federated approach may be used for mediation of relationships at the heart of identity management, which in turn depends on managing and brokering the trust that underpins those relationships
- Shared identity services – identity management capabilities must be delivered as distributed infrastructure services, which are defined according to clear contracts which are enforced through policies
- Policy-based and service-oriented – there is a need to authorize access to business functions and information at the level of each service using policy-based approaches to the definition and enforcement of access control requirements

The Identity Services segment architecture has a number of characteristics which are essential if it is to provide an identity management foundation for the long term which is capable of supporting the broad array of business requirements in an incremental fashion.

- It is based on a clear separation of identity management concerns, with identity management capabilities delivered as a set of distributed infrastructure services, underpinned by a services repository and ultimately an integrated identity data repository.
- Resources access these services through policy-based mediation, which also serves to control the monitoring and audit functions required to mitigate risk, and enforce compliance, and demonstrate auditable logs.
- Identity data is managed throughout its lifecycle, from core data maintenance through to provisioning and de-provisioning, by a set of processes implemented using automated workflow and process management technologies, to increase efficiency, enforce consistency, and facilitate integration of identity management and business processes.
- Open standard protocols and data formats bridge the gaps between the layers to facilitate interoperability between the architectural components and the broader IT infrastructure.

A critical aspect of the Identity Services segment architecture is that it is based on a clear separation of identity management concerns. This means that identity and access services

– authentication, access control, logging and audit, federation – need to be delivered as shared infrastructure services, governed by a unified policy management layer and underpinned by a federated identity data repository. It also means that these shared identity services should make use of other infrastructure services, such as workflow management, and must be usable by the broader application and IT infrastructure. At the same time the identity and access services, particularly authentication and access control, must be autonomous – to allow entitlements, for example, to be varied in accordance with available authentication facilities.

Each layer should present a common interface to all services that depend on the functionality of that layer, and open standard protocols and data formats are non-negotiable for those common interfaces to facilitate interoperability. The figure below depicts a potential OneVA IdM services oriented architecture (SOA).

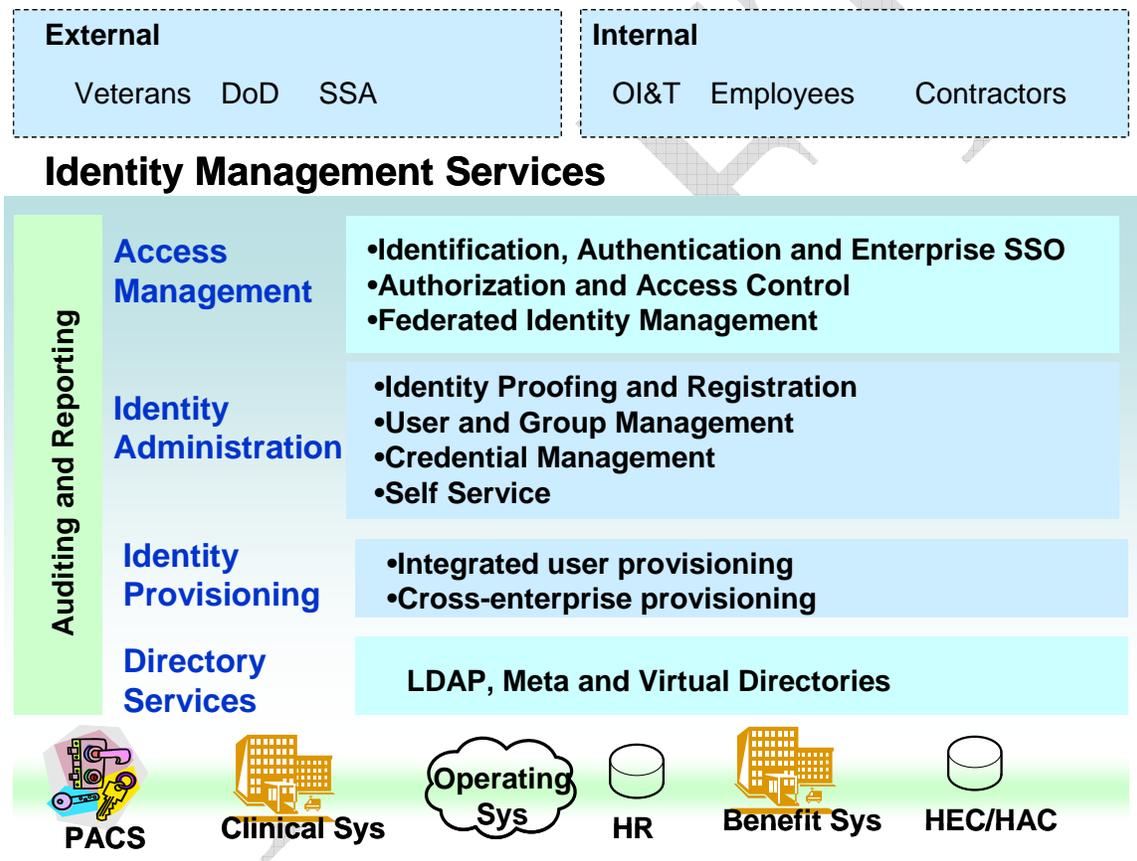


Figure 2.1-2OneVA IdM Services Oriented Architecture

2.2 OneVA Identity Services Components

The following figure illustrates a conceptual design for the OneVA identity services.

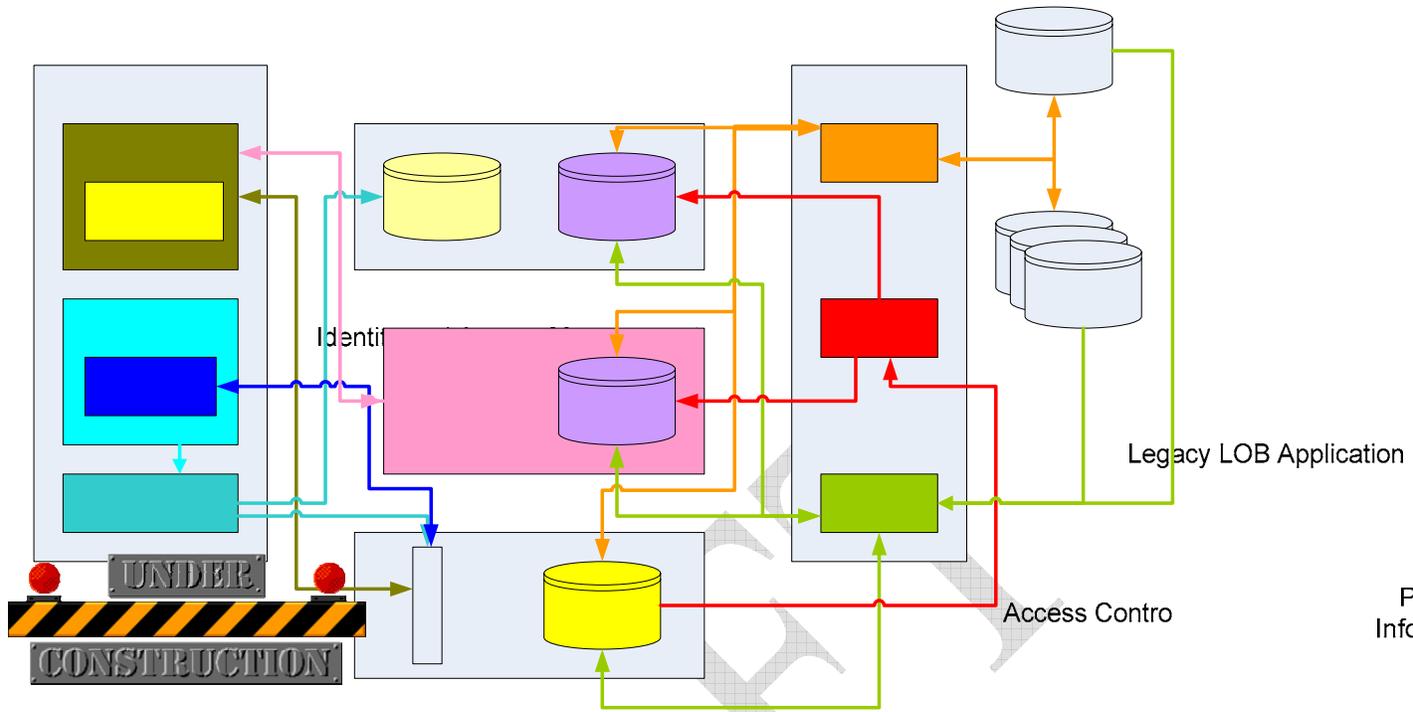


Figure 2.2-1 Conceptual Design for OneVA Identity Services

Registrator

New LOB Application

A typical workflow for OneVA Identity Services is illustrated in the graphic that follows.

Provisioning

VA Enterprise Data

LDAP Interface

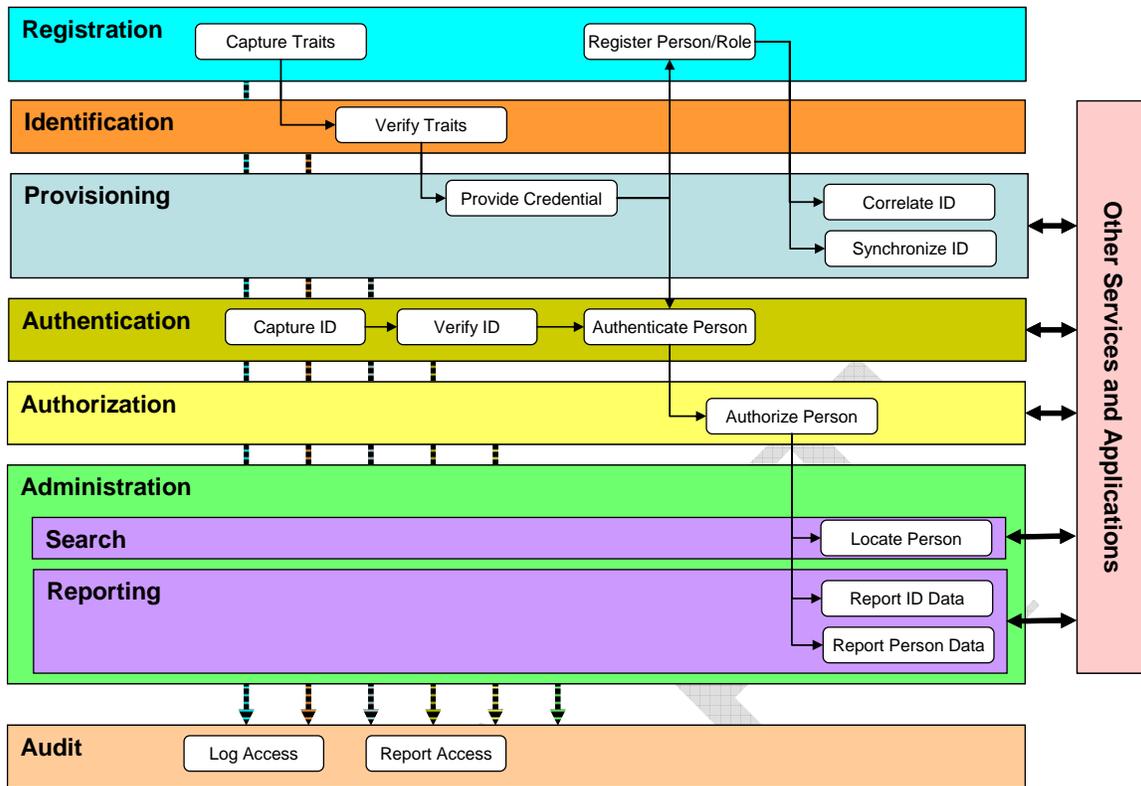


Figure 2.2-2 OneVA Identity Services

Important basic identity management services and therefore basic components of the identity and access management environment are, for example, identification and authentication, access control, authorization, audit, provisioning and registration services. Included are the infrastructures for establishing and managing such services such as registration, provisioning, security management and configuration, services for assigning rights, duties, functions, roles, etc., as well as time stamping. The table below provides an overview of IdM service requirements.

Requirement	Description	Service
<ul style="list-style-type: none"> Enterprise-wide distributed authentication Single Sign-on 	<ul style="list-style-type: none"> Strong authentication for all users and systems/persistent sessions Fewer logons with a goal of achieving single sign-on to all VA applications 	<ul style="list-style-type: none"> Identification and authentication
<ul style="list-style-type: none"> Enterprise-wide distributed authorizations 	<ul style="list-style-type: none"> Enterprise-wide hierarchical security policies, business oriented least privilege and need-to-know access, business partner access, centralized user profiles, policy based access control 	<ul style="list-style-type: none"> Access control and authorization
<ul style="list-style-type: none"> RBAC and role engineering 	<ul style="list-style-type: none"> Structural roles and functional roles, Rule-based access control, constraints 	

Requirement	Description	Service
<ul style="list-style-type: none"> •Emergency access •Federated authorizations •Distributed/local access control 		
<ul style="list-style-type: none"> •Enterprise-wide information system audit 	<ul style="list-style-type: none"> •Centralized auditing, processing, and reporting 	<ul style="list-style-type: none"> •Accountability
<ul style="list-style-type: none"> •Monitoring security function 		
<ul style="list-style-type: none"> •Application audit 		
<ul style="list-style-type: none"> •Centralized user and system administrative and security management •Federated Identity Management 	<ul style="list-style-type: none"> •Enterprise-wide administrative and security management information bases/operation centers 	<ul style="list-style-type: none"> •Identity Administration
<ul style="list-style-type: none"> •Administrative Identifiers 	<ul style="list-style-type: none"> •Enterprise-wide person identifiers 	
<ul style="list-style-type: none"> •Identity proofing and user credentials •Trusted identity credentials •User Self-Service 	<ul style="list-style-type: none"> •Registration 	
<ul style="list-style-type: none"> Creation, modification, deletion, suspension, restoration of a defined set of accounts or attributes 	<ul style="list-style-type: none"> •Centralized management of accounts and attributes •Cross-enterprise provisioning 	<ul style="list-style-type: none"> Identity Provisioning
<ul style="list-style-type: none"> Enterprise-wide administrative and security management information bases. 	<ul style="list-style-type: none"> •LDAP, Meta and Virtual Directories 	<ul style="list-style-type: none"> •Directory Services

Table 2.2-1 High Level IdM Requirements

Authentication and authorization define that users must be authenticated once, logically centrally, with centralized authorization and security management information bases supporting distributed access control decision function architectures. The uniform enterprise-wide fine-grained access control decisions must be maintainable without requiring time consuming and costly modification to individual application systems. The validation of permissions and roles must be validated in a centralized way across the enterprise. Sign-on and access to network resources must be available from any workstation across co-operating security domains. Security policies must be capable of

dynamic implementation, revocation or suspension of user permissions and accounts as determined by proper authority. People must be authenticated and authorized in a security domain supporting custom and personalized capabilities as well as individual privacy decisions (as permitted by policy). Based on flexible access decision rules, user authorizations to multiple systems must be managed, negotiated, and decided without the need to modify individual system account information.

The distributed authentication and authorization infrastructure must provide support for hierarchical security policies, implementation, control, and security management, replacing hard-coded policies with flexible network-based ones and providing ability to support multiple security policies. In that context, a common, reusable, distributed model for authentication/authorization services, accommodating policies not in legacy/COTS system originally, has to be provided.

Registration includes credentialing, provisioning, and supporting services.

2.2.1 Identification and Authentication

2.2.1.1 Description

Identification

The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items. SOURCE: FIPS 201

The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. SOURCE: SP 800-47

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources and information system. SOURCE: SP 800-53; FIPS 200

Identification and authentication are closely linked yet separate, individual processes. *Identification* is simply a subject's claim of who it is (which may or may not be true). When we log on to a system, we type in our user identifier to "identify" ourselves. *Authentication* is proof that the subject is who it claims to be. Once we identify ourselves, the system asks us to input some form of proof, such as a password, a number generated on a hand-held token device, or our fingerprint. Authentication, when used in conjunction with the user's account name, provides that user access to the protected resource.

Authenticated subjects include people, processes and devices. Accessed entities include physical facilities (buildings, rooms), networks, computers, and applications. To be

effective, an authentication mechanism must uniquely identify a subject, and it must be resistant to forgery.

VA will leverage the capabilities of OneVA Person Identity Verification (PIV) based user identity certificates to provide an authentication and single sign on capability that will become VA's primary logon service for employees and contractors. During the initial logon process, users will authenticate themselves to a network Security Server by proving possession of the secret key portion of their PKI certificate. Information available to the Security Server will be used to complete the NT network logon and to authenticate users to applications.

Similarly, VA will leverage the capabilities of the Federal e-authentication program to provide identity assertions for veterans.

2.2.1.2 Key Benefits

Authentication is the foundation for most security services including access control, auditing, digital signatures, non-repudiation, and single sign-on. Therefore, it is arguably the single most important security service. Authentication services support VA's architecture goal of supporting distributed information systems. Authentication services:

- Reduce costs by centralizing authentication services formerly distributed to each application,
- Simplify the user's logon experience,
- Provide services essential to centralized auditing,
- Simplify VA's security management environment,
- Provide the capability to create suspend or delete user access across the enterprise,
- Future-proof the enterprise to change.
- Support document signing/cosigning.

Using a host-based identification and authentication mechanism with accounts on each system, a user may acquire numerous passwords each of which must be remembered. Logon becomes a distracting annoyance that tempts many users to either write down passwords where they can be compromised or else select weak passwords. "Authentication as a service" tends to eliminate these weaknesses while providing better overall security management.

Single Sign-on (SSO) SSO is about providing a single identity to the user for identification purposes. It allows a user to access all allowed systems with the look and feel of a single "master key", greatly simplifying the user experience. SSO is an inherent capability of an SOA-based authentication service.

2.2.2 Authorization

2.2.2.1 Description

Authorization

Access privileges granted to a user, program, or process. SOURCE: CNSSI 4009

Access control

The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). SOURCE: FIPS 201

Access control and authorization services ensure that people, computer systems, and software applications can use only those resources (e.g., files, directories, computers, networks) that they are authorized to use and then only for approved purposes. Access controls protect against unauthorized use, disclosure, modification, and destruction of resources and unauthorized issuing of system commands. Authorization control is that portion of access control specifically involved with the granting of rights. Access control and authorization mechanisms can be identity, context, role, or rule-based.

By distributing authorization/access management functions users do not need to have an account on each end system for which access is requested. Users obtain authorization credentials from a network security server.

2.2.2.2 Key Benefits

- Support distributed heterogeneous application architecture with a homogeneous distributed security infrastructure leveraged across the enterprise.
- Provide a common, consistent security authorization and access control infrastructure.
- Provide mechanisms to systematically describe and enforce enterprise security policy throughout the organization for consistency, maintenance, ease of modification, and to demonstrate adherence to applicable regulation and law.
- Provide "economies of scale" where it is desired to change the approach of individually managing the configuration of each point of enforcement to one which establishes a consolidated view of the safeguards in effect throughout the enterprise.
- Provide centralized control, management, and visibility to security policy across the enterprise. This allows for additional key features such as delegated administration, centralized policy analysis, and consolidated reporting.

- Permit an organization to centrally grant, suspend, or revoke any or all ability to connect to or access enterprise resources either individually or collectively and with the capability to enforce these policies at run-time.
- Support access decisions that are sensitive to a user's credentials in addition to identity. For example, the user may have to be a licensed healthcare professional in order to access a medical record.
- Support delegation. A user might delegate access for a resource to another user (e.g., a physician might delegate access to his patient's records to a specialist).
- Support sender verification. When a user receives a signed document, he must be sure the sender was, in some sense, authorized to sign and send the document. A simple example would be a prescription, which must be signed by a doctor. A simple identity certificate is insufficient, as it does not indicate the sender's credentials (i.e., that he is a doctor).
- Provide a common/reusable model for future-proofed authorization services,
- Accommodate policies not in legacy/COTS system originally, support for multiple hierarchical security policies
- Create standard security authorization infrastructures supporting a variety of enterprise-wide end-to-end security applications.
- Replace hard coded policies with flexible network-based ones, while reducing the amount of security code maintained and developed, speed system certification,
- Provide scalable security modules incorporating agile interfaces to external systems,

2.2.3 Provisioning

2.2.3.1 Description

The process of managing attributes and accounts within the scope of a defined business process or interaction. Provisioning an account or service may involve the creation, modification, deletion, suspension, restoration of a defined set of accounts or attributes. SOURCE: OASIS SPML

Provisioning of user access control credentials refers to the creation, maintenance, correlation, synchronization and deactivation of user-objects and user-attributes, as they exist in one or more systems, directories or applications, in response to an automated or interactive business processes. Provisioning software may include one or more of the following processes: change propagation, self service workflow, consolidated user administration, delegated user administration, and federated change control. Provisioning is typically a subsystem or function of an identity management system that is particularly useful within organizations where users may be represented by multiple user objects on multiple systems.

2.2.3.2 Key Benefits

- Provide ability to provision incremental updates to policy and configuration data simultaneously across all distributed decision/enforcement points.
- Automate the process of user management (authorization, roles, authentication),

2.2.4 Audit

2.2.4.1 Description

Security Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. SOURCE: NIST SP 800-32; CNSSI-4009

Audit Trail

A record showing who has accessed an Information Technology (IT) system and what operations the user has performed during a given period. SOURCE: NIST SP 800-47

Technical Security Audit is part of the accountability control objective. The accountability control objective is stated as: “Systems that are used to process or handle classified or other sensitive information must assure individual accountability whenever either a mandatory or discretionary security policy is invoked. Furthermore, to assure accountability the capability must exist for an authorized and competent agent to assess and evaluate the accountability information by a secure means, within a reasonable amount of time and without undue difficulty.”

Accountability is the concept that individual persons or entities can be held responsible for specified actions, such as obtaining informed consent or breaching confidentiality. [National Research Council, 1991] Accountability is achieved through the implementation of a pervasive technical audit service. Audit provides a record of potential insecurities irrefutably traceable back to the originator of the action. To be effective, security audit must be on.

In distributed systems, audit is produced at multiple locations on multiple components, making review and analysis difficult. Accordingly, in such a system, it is very desirable to consolidate and forward low-level audit from various audit-producing sources to a central audit server. A distributed audit server provides capability for collecting, forwarding, processing, and reporting audit events originating from diverse sources.

Audit provides a record of potential insecurities irrefutably traceable back to the originator of the action. To be effective, security audit must be on.

A security audit trail provides a journal of security-related events collected for potential use in intrusion detection and/or security audits. Audit is a pervasive function of the healthcare system providing essential accountability features. Audit also provides assurance of the correct operation of the system's security features by monitoring user and system access to data and resources. Audit is generated as a byproduct of the security controls in place; authentication, access and authorization (privileging), and upon occurrence of specific security-relevant events (e.g., modifying a file). Audit acts as a deterrent to (unauthorized) user activities and as such users should know that their actions are being monitored (usually part of a log-on banner). Audit also provides a means to assess the degree of harm caused should a break-in occur.

An automated audit tool provides the means of identifying events at different levels of security, performing automatic profiling, reporting and alerting and a facility to store, sort and search for potential insecurities. The audit tools can reformat diverse trails to a single composite format that can then be automatically processed. Since the amount of audit produced may be considerable, a single centralized audit server is a practical way to manage workflow without affecting the response time of operational systems.

Audit records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges. Audit generating sources typically permit system administrators to specify which types of events should be audited and whether successful and/or failed attempts to perform certain actions should be logged.

2.2.4.2 Key Benefits

- Security audit provides not only end-user accountability required by law (HIPAA, Sarbanes-Oxley) but a means to assess damage done to a system by malicious action or accident.
- Security audit generated by the actions of other security services provides a check on their proper operation.
- In a distributed system, centralized audit collection and processing also provides a method to obtain near-real-time misuse detection and alerts.
- An automated audit tool provides the means of identifying events at different levels of security, performing automatic profiling, reporting and alerting
- Security audit generated by the actions of other security services provides a check on their proper operation.

2.3 Identity Data Domain Management Framework

VA has defined an **identity data domain management framework** that allows for VA and DoD to more effectively share needed information between departments and will also form the backbone for inter-departmental collaboration.

Figure 2.3-1 displays the proposed framework. This framework has been labeled a hybrid model as it combines a federation of data domains between VA and DoD and establishes a consolidated identity data domain with VA (across VA, VBA, NCA, VHA).

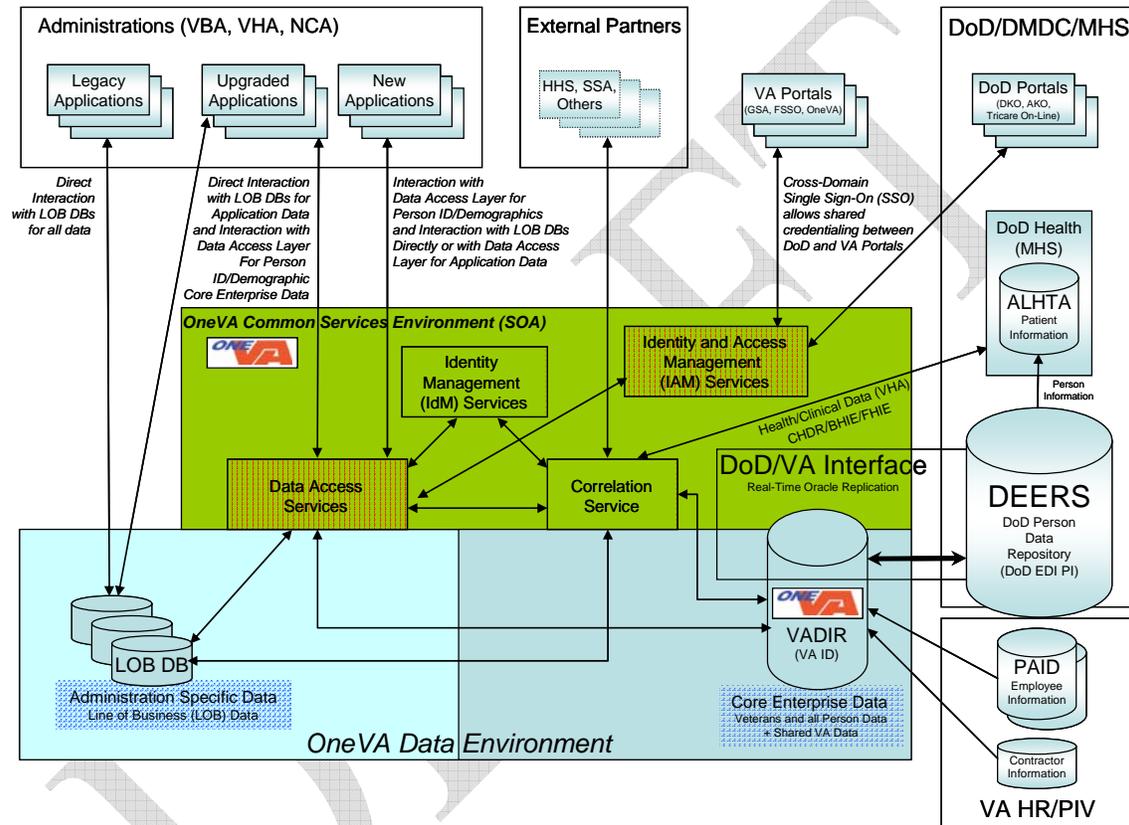


Figure 2.3-1 Hybrid OneVA identity data domain management framework

The identity data domain management framework is composed of several components:

- Unique identifiers assigned by enumeration engines
- Correlation services that associate unique identifiers
- Consolidated identity services within VA

2.3.1 Unique Identifiers Assigned by Enumeration engines

Enterprise identifiers provide identification consistency across an enterprise of systems, and most importantly allow for unambiguous representation of a person between systems. These identifiers are meant to be shared only electronically.

DoD will enumerate persons within its domain and will assign a unique enterprise identifier, called the Electronic Data Interchange Person Identifier – EDI PI. Currently the DoD EDI PI is assigned to every individual in the DMDC personnel data repository (PDR) which includes military active duty, Reserve & National Guard personnel and their dependents, retired military personnel and their dependents. From 1985 forward, it includes separated military personnel with no remaining DoD benefit eligibility

VA will enumerate persons within its domain and will assign a unique enterprise identifier, called here the VA ID. This identifier will eventually be assigned to all persons within VA, including veterans, beneficiaries and other persons (e.g. employees, contractors, etc.).

2.3.2 Correlation Services that Associate Unique Identifiers between VA and DoD

VA and DoD are implementing a plan to consolidate data interfaces. VA and DoD have agreed to use the DoD assigned EDI PI as the unique identifier on all information exchanges between VA and DoD. DoD will include the EDI PI on all transmissions to VA. VA will receive DoD's identifier and associate it with the VA identifier. The correlation service will determine if a match exists within VA for the transmitted DoD information. If a match exists, the correlation service will establish a match between identifiers, the EDI PI and the VA ID will be associated with each other. If no match exists, a VA ID will be enumerated for that individual by the correlation service.

This correlation service can be extended, as necessary, to incorporate data exchanges from other external agencies, such as Health and Human Services, Social Security Agency, etc. The correlation service would likewise establish an association between those agency's unique identifiers and the VA ID.

Finally, the correlation service will be useful in associating identifiers between internal VA systems.

2.3.3 Consolidated Identity Services within VA

The department will implement a consolidated identity service within VA. This service will assign a VA identifier to all veterans, beneficiaries, employees, etc. within VA. OneVA Identity Services will feature a central repository of all persons' identities within VA. LOB's will retain computing applications for business workload and transaction processing; however, the job of enumerating an individual, processing identity trait

updates, etc. will be delegated to VA’s consolidated identity services. LOB systems would be modified to utilize the consolidated services.

Necessary ingredients for implementing consolidated Identity Services are a set of Person Information data access services that can be executed by business processes in work-flow execution streams, or invoked by legacy application systems. These data management services must be granular enough to be atomically executable in concept, functionally independent of each other, and functionally coherent. The following is a set of potential Person Information data management services that should satisfy the business functionality requirements for Person Information for any line of business within VA. The services are closely related to the conceptual entities defined in the VA Conceptual Data Model (an extracted, high level conceptual information model for person/party information is shown in Figure 2.3-3).

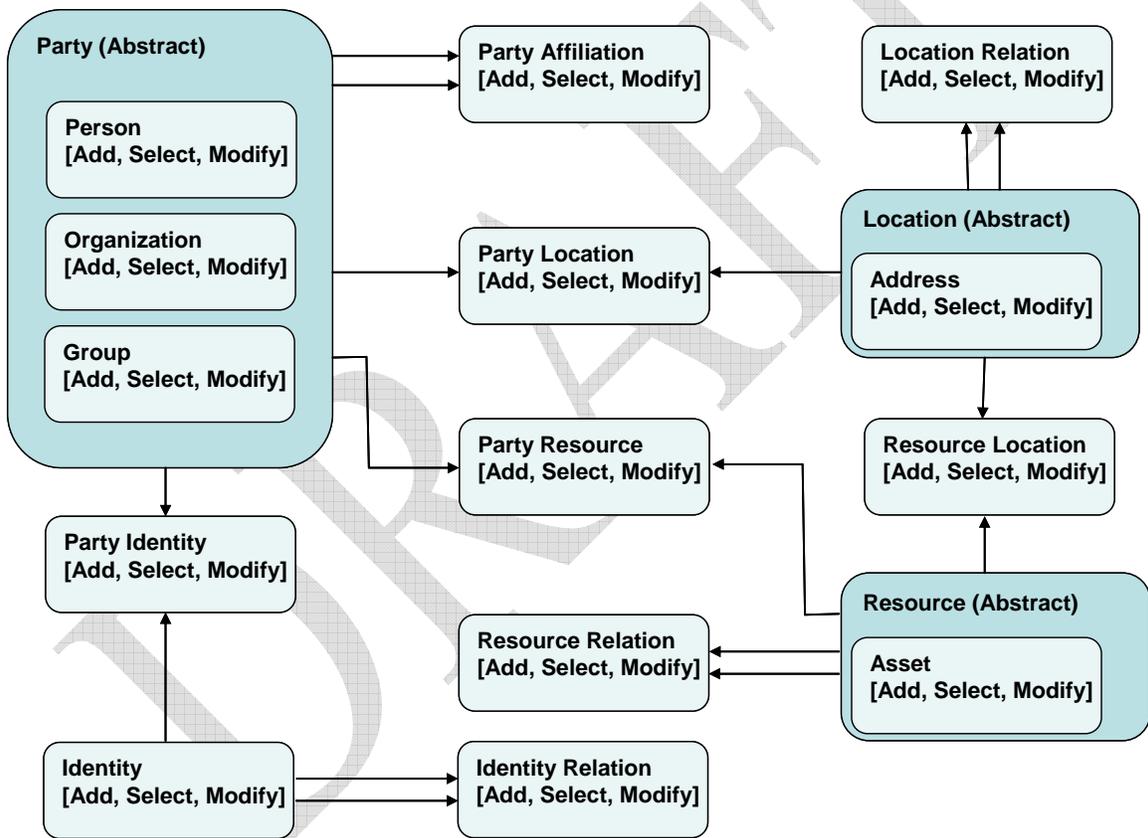


Figure 2.3-2 Conceptual OneVA Person Information Services

This set of data services provide the capabilities necessary to capture and manage Person Information needed for VA that would serve any of its LOB’s. This business-oriented data management services strategy will allow the VA to avoid building any new “stovepipe” databases for person information, and will enable synchronization of the redundant data captured in existing “stovepipe” databases.

This can only be achieved by establishing an enterprise data environment with the following characteristics:

- Single logical sources from which to get a complete view of the enterprise data objects
- Increased awareness of the profile and characteristics of the data in the enterprise
- Improved data quality across the enterprise
- Enforced data standards by using a data services layer
- Data that's clearly visible and readily accessible
- Reduced reliance on custom interfaces and proprietary formats
- Clearly identified authoritative data sources that are effectively used throughout the enterprise
- Security that's "baked into" the solution, and not an afterthought
- Data that's easily discoverable by potential consumers across the organization

Achieving this vision will require a comprehensive strategy that defines how the enterprise's data should be managed in an SOA environment. This strategy must address issues such as data governance, data modeling from an enterprise SOA perspective, data quality, security, and technology solutions such as data services.

2.3.4 Party (Person) Information Model

The figure below illustrates a common pattern in the information modeling world – one being adopted by the VA EA – the Party Information Model. This model abstracts persons, organizations, and groups into a single “party” concept that takes into consideration their common characteristics (attributes, relationships, and even behaviors). It allows persons, organizations, and groups to be treated in many ways as if they are the same kind of things, while still recognizing their unique characteristics. Figure 2.3-3 is for illustrative purposes only. The VA Conceptual Data Model contains the complete model of the concepts illustrated.

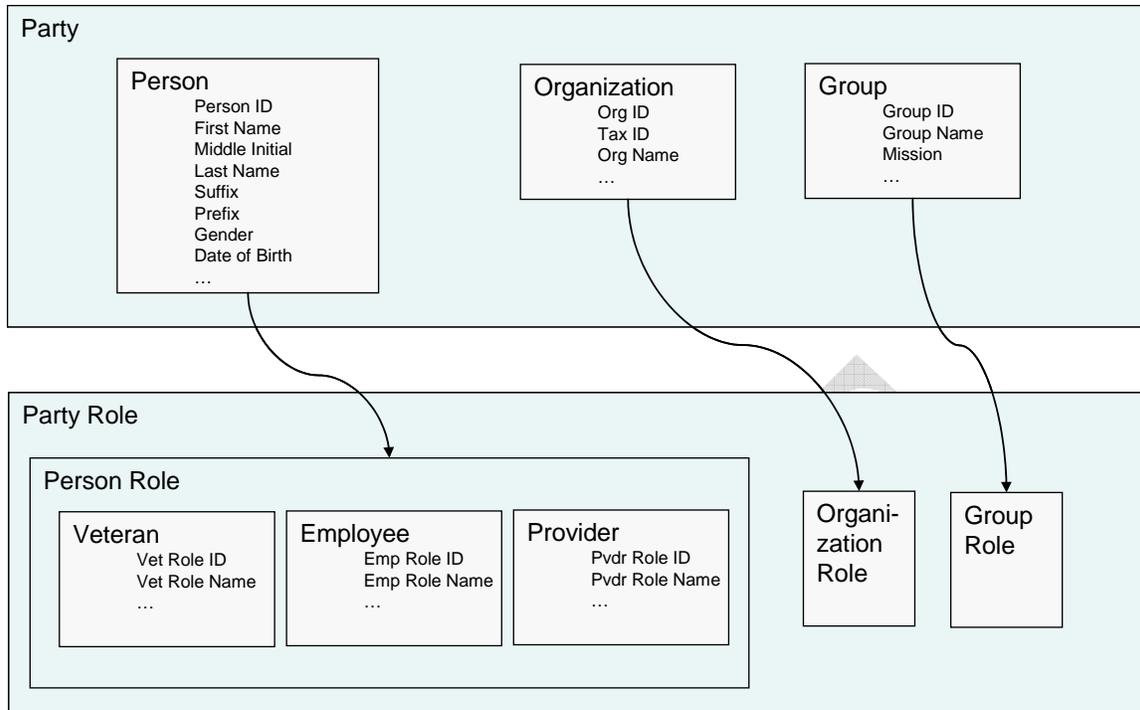


Figure 2.3-3 Party Information Model

Party role, which may be specialized as a person role, organization role, or group role, is generally defined as a particular function, responsibility, or competency of a party. For example, the individual roles of the person specialization of party (person roles) may include veteran, provider, or employee. The individual roles of the organization specialization of party (organization roles) may include health care provider organization, health record maintenance organization, health care support organization, and partner organization. The individual roles of the group specialization of party (group roles) may include, for example, family group, sample population group, or therapy group.

A party role is sometimes referred to as a party relationship role since it often associates a given person, group, or organization with another person, group, or organization (not shown in the above figure). Note that a given party can assume one or more roles at a given point in time. For instance, John has several roles: John is an employee of VA; John is the spouse of Mary; John is a patient enrolled within the Veterans Health Administration (VHA), John has a primary care specialist, and John has health care records in one or more specific VHA offices (organizations).

This model recognizes that there are characteristics that are common to a party or party specialization (such as person date of birth and gender) independent of their roles or relationships; and characteristics (such as provider credentials, contact details, and accounts) that are facts about a party in a particular role.

The matrix shown below shows the conceptual data elements for the person identity traits captured by various VA systems. The highlighted elements are those specifically identified by the RE IdM IPT.

Person Identity Data Element Cross-Reference							
Data Element Name	MPI	VADIR	BIRLS	BOSS/AMAS	Vista	PAID	VA Conceptual Data Model
Name Information							
Last Name	x	x	x	x	x	x	x
First Name	x	x	x	x	x	x	x
Middle Name	x	x	x	x	x	x	x
Name Prefix	x				x		x
Name Suffix	x	x	x		x	x	x
Name Type (e.g., legal, alias)		x		x			x
Personal Information							
Date of Birth	x	x	x		x	x	x
Date of Death	x	x	x		x		x
Death in Service			x				
Death Verification Status	x						x
Gender	x	x	x		x	x	x
Marital Status	x	x		x			x
Social Security Number	x	x	x	x	x	x	x
SSN Verification Status	x						

Table 2.3-1 Person Identity Data Element Cross Reference

2.4 Impacted/Involved Systems

OneVA Identity Services will eventually interface with practically every system in department and LOB portfolios. Some specific systems are discussed below.

2.4.1 VBA Systems

VBA has divided their portfolio into core systems (Compensation and Pension, Education, and Vocational Rehabilitation and Employment) and non-core systems (Loan Guaranty, Insurance).

Legacy system modernization is primarily focused on VBA’s core systems, including its Corporate Database (Corporate), Benefits Delivery Network (BDN) and Beneficiary Identification and Records Locator Subsystem (BIRLS). While, VBA has begun implementation of common services to access/use core information in Corporate, it has not yet standardized rules into a single service suite for identity management. The migration path for VBA’s core systems then requires rule standardization/implementation, followed by database synchronization service between VBA databases and the OneVA ID database. This would allow VBA to achieve integration without requiring comprehensive database changes (to utilize OneVA identifier instead of VBA identifier) with simultaneous cutover to the service for the

applications. These interim steps would enable VBA to change individual applications to utilize the OneVA service on a migration schedule. It may be determined after further analysis that VBA core systems could proceed to direct integration with OneVA IdM service.

Non-Core Loan Guaranty (LGY) systems are assumed to be able to begin direct integration with OneVA Identity Services. LGY's systems are consolidated into one computing platform and will have standardized/consolidated identity management rules.

2.4.2 NCA Systems

There are two major computing systems for NCA: Burial Operations Support System (BOSS) and Automated Monument Application System (AMAS). These systems are consolidated computing systems. It is assumed that NCA systems will be able to begin direct integration with OneVA Identity Services.

2.4.3 VHA Systems

Currently the VHA Identity Management Program manages over 12 million patient identities. This capability enables health care providers the ability to share patient health information (their medical record) data between any facilities that have seen the patient, including sharing data with the Department of Defense (DoD).

While VHA has implemented the MPI, it will need to implement changes to business rules to become consistent with business rules harmonization activities. Additionally, VHA will need to modify its systems in order to take advantage of OneVA Identity Services that enable better access management and data sharing. VHA will still maintain the MPI for internal use and modify their systems to utilize the OneVA Identity Services without falling out of compliance with the Universal Healthcare Identifier (ASTM E 1714)

In addition, VHA ADR (Administrative Data Repository) is the database containing traits about person for administrative (non-clinical) applications. It contains (or will contain) demographic, insurance, enrollment traits, in addition to the identity traits.

2.4.4 VA-DOD database (VADIR)

The VA/DoD Identity Repository (VADIR) is the enterprise database that contains the population of interest to the VA. It will ultimately contain the "Common DoD/VA Population" (Shared with DoD) composed of:

- Veterans,
- Beneficiaries (Future, as Required)

- Employees & Contractors, Volunteers, Associates (PIV) (Future) (*Not Shared with DoD*)
- Organizations *Health Care Providers*, Banks, Mortgage Companies, Funeral Homes, et al(As Required by LOB's) (Future) (*Not Shared with DoD*)
- Others: (*Not Shared with DoD*)

The VA Enterprise Database will contain data that correlates identities in DEERS and VADIR and maps the DoD EDI PI to VA ID/ICN. This requires enumeration with a VA ID/ICN at the time that an identity for a person is created. The Interchange Control Number (ICN) is likely to be the VA Internal ID. It is:

- Compliant with existing Health Data Standards
- Already functions as the VHA person identifier

The DoD EDI PI and VA ID/ICN are instantly correlated at time of service member accession, thus are linked for anyone new in the common population. As a result, over time, the magnitude of the identifier correlation problem rapidly decreases.

The establishment of the VA Enterprise Database is a high priority activity for both VA and DoD due to cross-servicing of populations. *In addition, DoD Health Systems must move to DoD EDI PI by DoD Directive. This effort is pre-positioned to support that effort, to the benefit of VA as well as DoD.*

The current OneVA DOD database is fed by a one-way interface from DOD. It is anticipated that this system will be modified to interoperate with OneVA Identity Services and to receive identity updates from DOD.

VADIR will continue to evolve, and it may or may not end up as the OneVA “To-Be” enterprise database for the VA.

3 Implementation Plan

This section describes a notional plan for and interim states toward implementing the OneVA Identity Services solution. This is preliminary and is expected to evolve. These states are presented sequentially, however many of them can and will be implemented concurrently. Specific schedules and dependencies will be published in project plans and transition plans. The plans will also include performance metrics and measurement approaches. (See Appendix A, “Project and Performance Planning” for more information)

The major activities/initiatives described in this handbook are:

VA/DoD Common Population

VA/DoD Data Sharing

VA IdM

- E-Auth
- PIV
- Contact Mgmt
- External federation

LOB integration (or federation)

3.1 VA/DoD Common Population

The DoD/VA Common Population Project is a multi-phased initiative that seeks to establish a common DoD/VA service member/veteran population based on a combination of the DEERS database and on trusted VA sources for veterans who are not in DEERS. When fully implemented, this common population will encompass sharing of identity, demographic and military service information between the Departments.

The DOD/VA Service Member/Veteran Common Population activities are divided into multiple phases. This document primarily addresses Phase 1, with discussion of the later phases, especially Phase 2. Note that project phases do not need to occur sequentially, so it is possible, for example, to initiate analysis/elaboration activities for Phase 2 during Phase 1. Phases for this project are as follows:

Phase 1: Identify the population of persons within VA who have military service information and provide them to DoD/DMDC. Generate DoD EDI Person Identifiers (EDI PIs) for those persons and share updated person information with VA via the existing interface with VADIR. Originally, it was planned to provide military service information to DoD at the same time as the person information, but on further study, the nature of the data within one of the primary VA data sources (VHA's VistA), in which military service information is distributed among over a hundred local VistA sites, made it necessary to add another phase for military service information.

Phase 2: Consolidate and process military service history information from trusted VA sources. Provide DoD/DMDC with detailed military service information and create an authoritative source for military service information shared with VA.

Phase 3: Create and implement a process to support incremental additions to the DoD military service population with new additions from VA and to support incremental updates to person and/or military service information when VA authoritative data changes.

Phase 4: Enhance identity correlation services between VA and DOD to allow VA and DOD to establish collaboration between identity domains. Note that the following two phases are specific to the VA side and may not be part of the Common Population activities:

Phase 5: Instantiate VA enterprise data service layer to facilitate common access methods for military service information to support LOB business processes.

Phase 6: Enhance VA legacy applications to interact with the authoritative VA person data repository and common military service population data repository (VADIR).

3.2 VA/DoD IdM Data Sharing Services

OneVA IdM integrated product team (IPT), VA OI&T and DoD are coordinating to complete the drafting of the plan to satisfy the JSP objective of a migration path to a OneVA Identity Services solution that enables seamless integration between VA and DoD and that achieves a consolidated identity domain within VA. This capability will allow veterans to access their personnel information.

Even with bulk consolidation of VA repositories with DOD establishing an EDI PI for each person, and with real time transmission of identity information through correlation services, it may nonetheless be possible that VA is presented with instances where a beneficiary claims military service status while the authoritative source of military service information does not support such claim.

In these instances the beneficiary's veteran status may be also be supported by other evidence, such as a physical DD 214. In such instances as these it will be necessary to continue transacting business with a beneficiary using the provided evidence to establish veteran status. In sample scenario VA would generate an identifier in its consolidated identity domain. A VA application/user would then search for military service information; however, supporting military service information in the framework would not be available. This scenario results in a state where there is a claim that is inconsistent with VA's DOD database contents.

A policy must be put in place between VA and DOD that would allow VA to notify DOD of the discrepancy between a veteran's claimed status and DOD documented status. This mechanism would allow VA to notify DOD that a qualified VA representative collected appropriate military service information and that further review may be required.

It is necessary to establish rules to support a collaboration mechanism that allows VA to notify DOD that a discrepancy exists between the authoritative source for military service information within VA and a trusted source (e.g. the veteran's DD214 or equivalent).

Services between VA and DOD need to be established that allow VA to request DOD to resolve missing identity entry with qualifying military service information. It may be necessary for this service to incorporate transmission of evidence supporting the request (e.g. imaged DD 214).

It would remain DOD's responsibility to establish a unique DoD identity for the individual. Should DOD establish both identity and qualifying military service information, DOD would update VA with an EDI PI and military service information in the DOD data feed to VA.

3.2.1 Timeline

The timeline presented in Figure 3.2-1 provides a high-level set of milestones for implementing the OneVA IdM solution and for enhancing collaboration between VA and DoD. The timeline also organizes the milestones by holder of primary responsibility. Those milestones mapped above the timeline are primarily responsibility of VA, while those milestones below the timeline are primarily responsibility of DoD. Where specific dates are not known, a generic timeframe is provided that represents a quarter. Additionally, two milestones are not mapped as timeframes will need to be established for these. These milestones are:

- Design/Develop Modifications to Legacy Systems to Convert to OneVA IdM
- Extend EDI PI to DoD Systems (Date TBD)

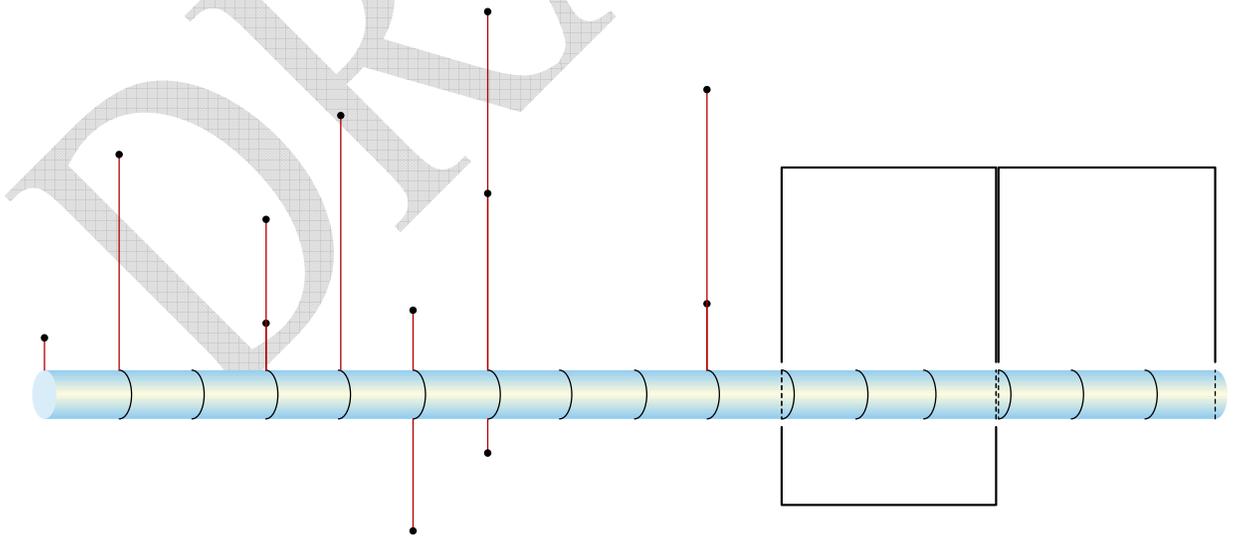


Figure 3.2-1 Timeline of high level milestones

3.2.2 Milestones

- **Complete OneVA IdM Plan Strategy (Completed: 3/2006):** VA has identified the preferred identity management framework and has worked with DoD to make adjustments to the identity management approach.
- **Start Analysis of VA Sources of Military Service Data (Start 4/2006):** VA will initiate the analysis of its multiple sources of military service information. This activity will be engaged in collaboratively with DoD. The activity will result in candidate sources for military service information from VA and assessment of the quality of that information.
- **Complete Systems Requirements Specification (SRS) (Due 6/2006):** VA will complete the definition of mid-level requirements (functional and non-functional). These will form the SRS and will then be used to identify number and type of use cases and to support engineering analysis of alternatives.
- **Complete Architectural Analysis for Identity Management (Due: 6/2006):** This activity will develop a detailed architecture for the identity management framework.
- **Define Process for Consolidating VA Military Service Data (Due 7/2006):** VA and DoD will complete definition of the process by which VA will pre-process military service information, transmit the information to DoD for enumeration and inclusion in its master repository of member military service data, and transmit back to VA (with EDI PI assigned).
- **Complete Engineering Analysis of internal VA ICN to Finalize Solution (Due 8/2006):** VA will complete the analysis of solutions to support both the correlation with DoD and the internal consolidated identity services.
- **Define Policy/Requirements for VA to Handle Exceptions (Due 8/2006):** Working with VA, DoD will develop policy that will allow VA to have exception handling process where VA can request DoD to add a person to DoD domain.
- **Complete Detailed Use Cases (9/2006):** VA will develop a set of detailed use cases that will define in detail needed systems' behaviors. This documentation will be used to define a detailed project plan that validly addresses requirements.
- **Start Consolidating VA Military Service Data (Start 9/2006):** VA will initiate transmission of pre-processed extracts to DoD. DoD will process and transmit back to VA with EDI PI. It is anticipated that this activity will be an ongoing activity.
- **Start Processing of VA Military Service in DoD (Start 9/2006):** DoD will initiate processing of supplied VA military service records. This processing will include assignment of an EDI PI (e.g. enumerating the person) and/or updating

- personnel history information within DoD personnel data repositories. Upon DoD successful processing of military service information, DoD will transmit updated record to DoD via consolidated DoD to VA feed.
- **Complete Design of Central System (Due 12/2006):** VA will complete detailed design of VA-DoD correlation and central identity management services. VA-DoD correlation service will be collaboratively designed with DoD.
 - **Complete Plan for Central-System Build-Out (Due: 12/2006):** Working with DoD, VA will develop a plan for the construction of the identity management solution. This plan will be a resourced project plan.
 - **Implement DoD to VA Identity Management Update Services (Due: Q2 FY2007):** DoD and VA will collaborate to implement identity management update services to the consolidated DoD feed to VA. These services will enable VA to maintain a fully replicated instance of DoD information within VA.
 - **Start Build-out of Central System and VA-DoD Correlation (Start Q2 FY2007):** Following development of fully resourced project plan, VA will initiate development of the identity management solution. This build out will follow a set of iterations/phases identified in the project plan. The build out of the central service will incorporate self-service and single sign-on capabilities.
 - **Develop VA Sequencing Plan for Converting Legacy Systems (Q3 FY2007):** VA will develop a sequencing plan that identifies the scope (e.g. number), order and estimated cost of the migration of the LOB systems to the new identity management solution.
 - **Design/Develop Modifications to Legacy Systems to Convert to OneVA IdM (Date TBD):** The timeframe for executing the legacy systems conversion is contingent both on the build out of the central system and the completion of the legacy systems conversion sequencing plan.
 - **Extend EDI PI to DoD Systems (Date TBD):** – DoD will extend use of the EDI PI as the unique identifier across DoD enterprise. This activity will result in DoD systems using EDI PI as unique identifier and will encompass such systems as DoD Health Systems, etc.

3.3 OneVA Identity Services

This section identifies migration phases/activities for developing internal, consolidated enterprise identity services.

Phase 1: Detailed Process Analysis. It is necessary to develop detailed process models that will reflect “to be” state of identity management business processes under OneVA IdM.

Phase 2: Harmonization of Identity Management Business Rules. There is the need to establish consistency in identity management rules across administrations and business lines. The activity of harmonizing business rules may in fact occur as part of detailed requirements/use cases. This will also apply to DoD and how matches are performed when the data are sent and also how the IdM is matched to the VA-DoD database (VADIR) to get started.

Phase 3: Detailed Requirements and Use Cases. It is necessary to develop a series of granular analysis artifacts for the final state OneVA Identity Services solution.

Phase 4: Engineering Analysis and Recommendation of Identity Services Solution. Detailed cost estimate and assessment of capability to meet documented requirements will need to be performed against potential solutions.

- An engineering analysis will be performed to identify the appropriate Identity Services solution to meet requirements in a cost-advantageous manner.
- VA will need to sequence collected use cases that will be realized in development iterations of the OneVA Identity Services.
- OneVA Identity Services will be constructed consistent with a defined iteration plan. The construction will also support interim states of OneVA Identity Services.

One likely business process that will use the OneVA Identity Services will be an enhanced “self-service” capability for service-members and veterans to securely access increasing number of VA services via the Web.

In the current situation, while a veteran can log on to a VA system and apply for a benefit, he or she has not actually been authenticated, or credentialed, and therefore there is no presumption that the person using the systems is actually the person applying for the benefit – in other words, that a user is who he or she claims to be. This limitation hampers the ability of VA to implement a fully online transaction, e.g. a person seeking benefits may start a transaction online but will complete the benefit application through other mode (in person, mail, etc.).

The following are activities that must be implemented and integrated as part of the complete set of identity services.

3.3.1 OneVA E-Authentication

E-Authentication refers specifically to an E-Gov initiative that supports the President’s Management Agenda and the Paperwork Reduction Act. This initiative, an example of *Federated Identity Management*, is intended to enable *Cross Domain Single Sign-On (CDSSO)* to participating Federal government websites through the GSA Portal.

The scope of the OneVA E-Authentication project is limited to customers; the management of VA employees and affiliates is not within its scope. This initiative

provides the standards-based authentication architecture for persons to gain access to services provided by the Federal government over the Internet. Users obtain an electronic credential from a credential service provider (CSP), such as Employee Express or Operations Research Consultants (ORC.com), and authenticate at the GSA Portal. Once authenticated at the GSA Portal, as users navigate to other participating Federal government websites, GSA will “pass” the user’s credentials to the websites using a SAML assertion. Essentially, Federal government websites agree to trust credentials that are accepted by the GSA Portal.

The OneVA E-Authentication project is building a solution using the IBM Federated Identity Management (FIM) product. At the time of this writing, the E-Authentication project team has purchased a 16 processor license of the FIM product, along with the hardware on which the FIM product will be deployed; although at this juncture, there is delay on the deliver of the hardware. The E-Authentication project team has identified 27 external facing VA applications to SAML enable, and MyHealtheVet has been selected to be the first pilot implementation. The project team estimates completion of the MyHealtheVet pilot at about January 2007, but expects a delay to the schedule due to the hardware delivery delays. Enabling E-Authentication of the other external facing VA applications will follow, likely one at a time, after the completion of the MyHealtheVet pilot. The integration of all 27 external facing VA applications is expected to complete in the three to five year range.

While the scope of the E-Authentication project is fairly limited in nature, specifically dealing with access to VA systems through a SAML based federated identity model, the technologies purchased by the VA have capabilities that extend far beyond the objectives of the project. For this initiative, the VA has purchased sufficient software and hardware that can potentially meet the VA’s enterprise need for identification, authentication and authorization. Much of the IBM FIM product functionality overlaps with PIV’s project objectives.

The architecture, design and implementation of the E-Authentication solution overlap with enterprise identity management in the areas of identification, authentication and authorization.

3.3.2 Personal Identity Verification (PIV)

PIV is a component of the Homeland Security Presidential Directive 12 (HSPD-12), which establishes a common identification standard for Federal employees and contractors. At the VA, this program is managed by the Office of Human Resources.

As of this writing, the PIV project has yet to procure a solution, but the result of its product and solution alternative analysis and selection process favored the Computer Associates (CA) product suite, which is capable of addressing many of the enterprise identity management functional requirements including authentication, authorization, identification, and provisioning requirements. The PIV team is currently developing prototypes and proof-of-concepts using existing CA licenses that the VA already own.

Current licenses will expire by March 2007, at which point current prototypes will cease and the PIV team will need to proceed with procurement of a solution, if an enterprise solution is not already available that will meet PIV requirements. The team anticipates requiring a few months to migrate to a new platform.

The PIV team is also encountering problems with ill defined interface standards as described in FIPS provided by NIST. The team is currently working closely with NIST to address the issues.

The scope of PIV is limited to VA employees and affiliates; the management of customer and partner organization representatives is not within the current scope of PIV. The focus of the PIV solution is on PIV requirements, which may or may not satisfy authentication, authorization, identification and provisioning for an enterprise identity management solution that includes partner organization representatives and customers as well. Additional processing capacity, configuration or customization may be required to service a larger user base that includes customers and partner organization representatives.

The PIV solution intends to use a combination of the VA HR PAID system and implementations of Microsoft Active Directory as an authoritative data source for employees and affiliates, but no authoritative data source is currently available for contractors.

3.3.3 Contact Management

Contact Management (CM) is a One-VA program serving all VA customers through customer-preferred channels of access. CM is about managing an enhanced veterans and beneficiary experience while encouraging constituent self-service.

CM will provide a centralized knowledge and data management systems providing for consolidated One-VA information environment used by constituents and employees alike. CM will implement the benchmarking standards for assessing and continually improving VA's customer service. CM will coordinate among the Administrations and implement consistent benchmarking standards for assessing and continually improving VA's customer service

Contact Management is a program initiative that will implement its business driven functional products with a Phase One product roll out scheduled for before September 30, 2008.

3.3.4 Federated Identity Management Services

Single sign-on capability within VA may leverage identity sharing processes described above. Data sharing between VA and DoD can be enhanced to allow VA to share assigned credentials from DoD. These certificates would be associated with valid VA identities through correlation services. This sharing would establish correlation of

identities and access certificates that would allow common access for individuals known to both systems.

VA's authentication and access control services would be modified to allow a person to present her/his credentials to gain access to VA's applications. A person may then be able to supply her/his credential once within DoD, and if already known in VA, simply launch VA self-service applications from within a DoD context. The individual's credentials would have been presented, behind the scenes, by a DoD system to VA's authentication service. There the individual would have been associated with her/his VA identifier and the corresponding credentials. Similarly, a member may provide her/his credential to authenticate within VA, and provided there is agreement between VA and DoD on credentials, could gain similar access to DoD resources with a single sign-on.

This capability would support, for example, the Army National Guard Member who has been activated and is logging on to the Army Knowledge Online (AKO) Portal and is thus a registered user of the DoD Portal applications. His record is present both in DoD and in VA, and his DoD identifier has been correlated with his VA identifier in VA's identity services. If the Guardsman wishes to connect to a VA system to apply for a VA loan, she/he will not need to login on the VA side to do this. The single sign-on service would allow secure access based on her/his credentials and is seamlessly authenticated through the shared credentials. Based on this authentication and her/his personnel records in VA, the service authorizes his access to the appropriate internal VA systems.

This should also be applied to other internal applications that require authentication such as email and could even be extended to support telephone communications.

3.3.5 E-Signature

OneVA Identity Services will also provide support for E-Signatures. On June 30, 2000, President Clinton signed into law the Electronic Signatures in Global and National Commerce Act ("E-Sign"). E-Sign promotes the use of electronic contract formation, signatures, and recordkeeping in private commerce by establishing legal equivalence between:

- Contracts written on paper and contracts in electronic form
- Pen-and-ink signatures and electronic signatures
- Other legally-required written documents (termed "records") and the same information in electronic form.

E-Sign broadly recognizes the use of electronic signatures in commercial, consumer, and business transactions affecting interstate or foreign commerce, and to transactions regulated by both Federal and state governments. Three factors are critical to E-Sign:

- Authentication -- The signature must be uniquely and verifiably associated with the person who signed it.
- Non-repudiation -- Once signed, the document or contract is legally binding.

- Data integrity -- The document or contract must not be alterable once it is signed.

3.4 VA LOB Integration of Identity Services

This section identifies migration phases/activities for developing identity services for integrating the identity management across VA line of business systems.

Not all LOB systems will require the same level of effort to achieve integration with OneVA Identity Services. For instance, VBA has a current processing environment that is transitioning to its modernized platforms and remains in a blended state (e.g. mainframe and open system based).

Generally speaking, LOB systems will be integrated with OneVA Identity Services using a combination of the steps as summarized below:

- Bulk Identity Consolidation – LOB system would send identities in bulk format to OneVA identity database. This would associate LOB identity with existing identity or create new identity.
- Cycle-based updating of Consolidated Identities – Prior to implementing services to integrate with OneVA Identity Services, LOB systems may perform cycle based bulk updating with OneVA Identity Services.
- LOB's decide about the extent of remediation of systems into OneVA Identity Services – LOB's make determination as to extent of systems to be integrated with OneVA Identity Services.
- Modify Legacy Systems (necessary with VBA as it has multiple, independent applications):
 - Standardize business rules for managing/creating/searching identities
 - Implement business rules on legacy applications
 - Change database structures
 - OneVA Identity Services provides database “synchronization” service
- Integrate OneVA Identity Services – New applications or converted applications are re-written to use OneVA Identity Services.

The table below provides a summary of the steps discussed above that need to be taken by each LOB. Check marks indicate if the LOB needs to perform the LOB change step. [Note: VBA insurance (INS) was not analyzed.]

LOB Changes	OneVA DOD DB	VBA Core	VBA LGY	NCA	VHA
Bulk identity consolidation	✓	✓	✓	✓	
Cycle-based updating of consolidated identities		✓			
Decide boundary for remediation of legacy systems (e.g. will all systems need to be modified to interact with OneVA Identity Services)		✓			
Modify legacy: Standardize/Implement business rules	✓	✓			✓
Modify legacy: Modify database structures		✓			
Modify legacy: Implement OneVA DB synchronization service		✓			
Integrate OneVA identity service	✓	✓	✓	✓	✓

3.5 Immediate Next Steps

1. Refine and formalize OneVA Identity Services Program roles, stewardship and governance

2. Consolidate and Integrate IdM Initiatives
 - Consolidate and prioritize requirements
 - Complete and approve infrastructure
 - Architecture
 - Services
 - Technology
 - Integrate and complete plans and timelines

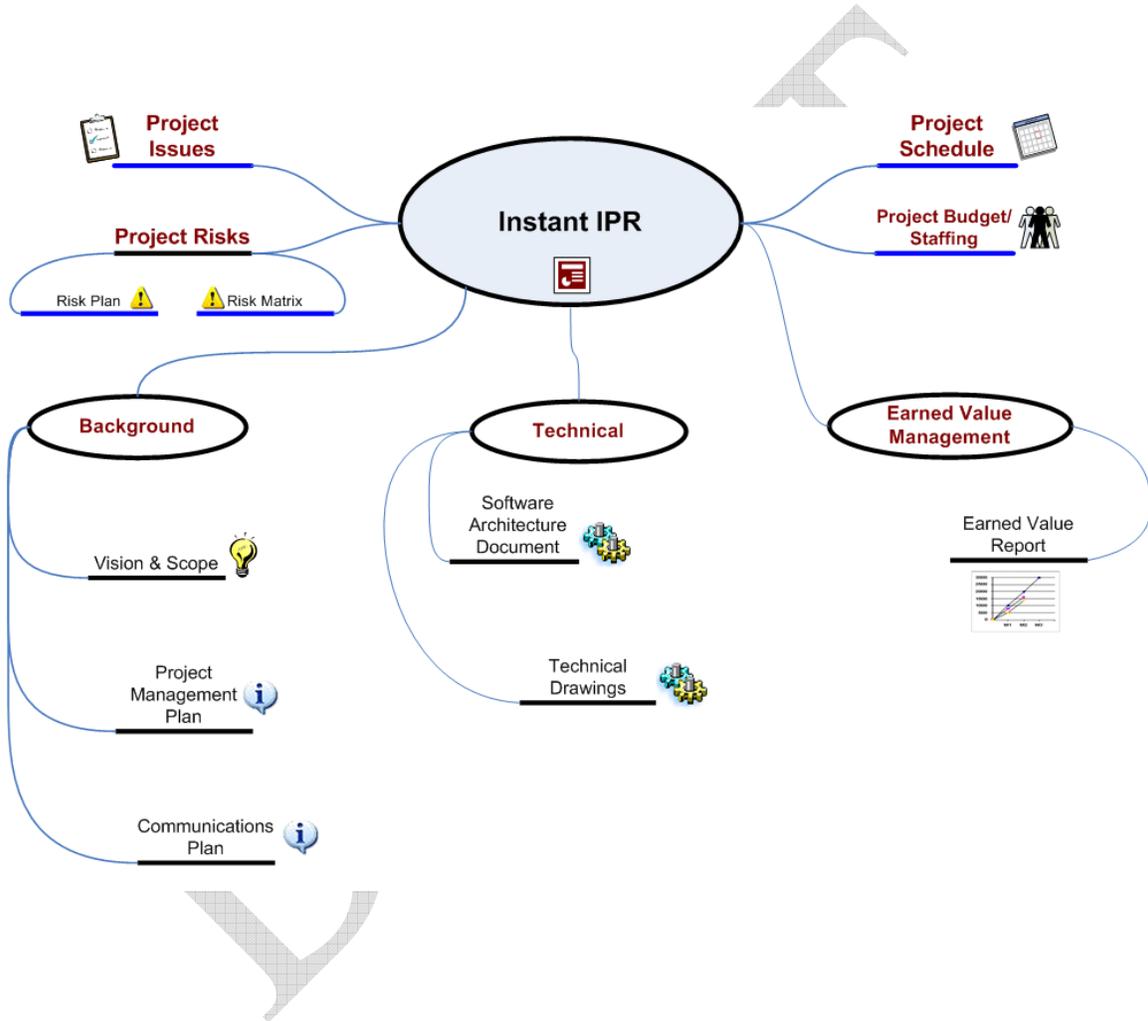
3. Design, Acquire, and Implement Technical Service Architecture

4. Design, Develop and Deploy Identity Services



A. Project and Performance Planning

The OneVA Identity Management Services project and performance planning guidance is not yet ready for publication. It is anticipated that it will address the following (adopted from VHA Person Service Identity Management Project):





B. Governance

The OneVA Identity Management governance guidance is not yet ready for publication. Governance for IdM Services will adhere to RE/CM Configuration Management Policy.

The purpose of Software Configuration Management is to establish and maintain the integrity of the products of the software project throughout the project's software life cycle.

Software Configuration Management involves identifying the configuration of the software (i.e., selected software work products and their descriptions) at given points in time, systematically controlling changes to the configuration, and maintaining the integrity and traceability of the configuration throughout the software life cycle. The work products placed under software configuration management include the software products that are delivered to the customer (e.g., the software requirements document and the code) and the items that are identified with or required to create these software products (e.g., the compiler).

A software baseline library is established containing the software baselines as they are developed. Changes to baselines and the release of software products built from the software baseline library are systematically controlled via the change control and configuration auditing functions of software configuration management.

This key process area covers the practices for performing the software configuration management function. The practices identifying specific configuration items/units are contained in the key process areas that describe the development and maintenance of each configuration item/unit.

The RE & CM contract development team will adhere to the following goals in order to implement this policy:

1. Plan software configuration management activities.
2. Identify, control, and make available selected software work products.
3. Control changes to identified software work products.
4. Inform affected groups and individuals of the status and content of software baselines.

Software Project Managers are responsible for implementing this policy.

The SID is responsible for maintaining this policy.



C. Service Standards

While there have been no standards yet developed specifically for OneVA identity management, the following is an example of service standards established for person information by the Veterans Healthcare Administration. Until and unless superseded by a specific specification for OneVA IdM, this will serve as the standard for the segment.

Common Services (CS) is a portfolio of projects that produces commonly utilized business, middleware, and infrastructure services that support Health@Vet-VistA architecture and application development.

CS provides the services necessary to support the n-tier software architecture, centralized/distributed deployment architecture and application modernization specified by the Veterans Health Administration (VHA) Enterprise Architecture and the Health@Vet Logical Model.

As motivated by e-government, One VA, and interagency information sharing initiatives, the CS team provides Health@Vet-VistA not only with software services, but with processes that promote IT modernization and effective organization evaluation and control.

Specifically, CS provides the following services and processes:

- Core business services that support person data commonly required by clinical and administrative applications (e.g., Person Service Identity Management).
- Middleware services that support interaction between n-tier software architecture levels and facilitate data transfer between systems in a centralized/distributed deployment architecture (e.g., Delivery Service).
- Infrastructure services that support common needs of individual business services (e.g., Standard Data Service).
- Migration of person administrative data from Legacy VistA to centralized database instances.
- Support of Legacy VistA operational continuity until the transition to Health@Vet-VistA is complete.
- Organizational support structures and processes that address application modernization needs.
- Project management practices that support rigorous organizational input, evaluation, and control.

The VHA website further explains: *"The Common Services collection of projects is at the heart of Health@Vet application modernization effort. Though largely transparent to end users, it provides essential infrastructure elements on which both clinical and administrative applications will be built. **It's literally the "glue" that brings the new VHA software together.***

Common Services is a unique undertaking in many ways. From the development of staff technical skills, to the discovery of detailed architectural interpretation, to the development of implementation prototypes and production software, an exciting variety of new challenges are brought to bear.

Significantly collaborative in nature, success is critically dependent not only on Common Services staff achievements but also on the participation and necessary contribution of many other groups involved in application development, architectural and technical consultation, and provisioning of supporting services such as independent testing and verification.

The Common Services program is much more than just an effort to produce software. Important objectives include active participation in the maturation of organizational structure and support services relative to Health@Vet impacts, realization of previously undiscovered pitfalls and opportunities, and proactive assistance to other development groups involved in application modernization. Common Services seeks to participate in a manner that helps maximize organizational success in the implementation of Health@Vet-VistA.

Above all, Common Services seeks to be an exemplary software development group, to pursue and achieve the highest levels of technical and architectural expertise, program and project management technique and rigor, and workplace and interpersonal professionalism."

The website also has the following description for "person information" services:

Person Service Identity Management (PSIM) will enumerate and maintain person identities of both patients and non-patients in Health@Vet-Vista.

PSIM provides the following features:

- Enumerates identities with a VA Person Identifier (VPID).
- Synchronizes identities with Vista during transition from Legacy Vista to Health@Vet-Vista.
- Maintains a history of ID changes.
- Correlates the VPID to internal and external identity domains.
- Provides duplicate prevention and resolution tools.
- Identifies and initiates identity merge and unmerge activities.
- Provides a data quality management user interface.

In legacy Vista, enumeration and duplication resolution is handled for patients only by the Master Patient Index (MPI) and has limited support for external ID correlation. Also, current MPI functionality includes records that only encompass the patient role. PSIM will enumerate from a person role-based view and aggregate redundant person records and their respective categories to a centralized and distributed view, resulting in enhanced data quality and an improved "One VA" face to beneficiaries and the public.

The complete service standards documentation is available on the VHA website:

<http://vista.med.va.gov/CommonServices/PSIM.htm>

The following is the structure of the VHA service standards and examples of the some of the documentation. Selected examples are included in this repository.

Project Software

The latest PSIM release is **PSClient 0.1**, available through the following links:

- [PSClient 0.1 Release Announcement](#)
- [PSClient 0.1 Software](#)

Project Artifacts

PSIM project management artifacts are on the [PSIM Instant IPR](#).

PSIM analyst, developer, and end user oriented artifacts are on the [PSIM TSPR](#).

PSIM Documents	Status	Date	PDF Version
Iterative Release 4 Sequence Diagrams	In Process	11.02.2004	
CS PSIM SRS IR6	In Process	07.21.2005	
PSIM Installation Guide	In Process	07.28.2004	
PSIM Master Test Plan	Approved	03.21.2006	
PSIM Detailed Test Plan IR6	Approved	03.21.2006	



 Messaging Requirements	Approved	02.03.2004	
 PSIM SAD. v1.1.1	In Process	03.10.2005	
Draft Risk List	In Process	03.18.2004	
New Person File Cleanup and Enumeration SDDs (zip file)	In Process	04.05.2005	
PSIM Use Cases (zip file)	Approved	10.19.2005	
 PSIM Use Cases for ESR APIs to Read	Approved	07.11.2005	

Project Background Information & Documentation:

- **Required by Global Group(s):** Common Services
- **Project Sponsor:** Mark Warner
- **Business Driver:** 2d - Broad-based operational enhancement that significantly improves operational efficiency.
- **Design Documents**
 1. [CS PSIM SAD IR5 v1.1.1.doc](#)
 2. [IMDO UI SAD - Draft](#)
 3. [PSIM SAD 1.6.doc](#)
- **Requirements Documents**
 1. [IMDO UI Supplemental Specifications](#)
 2. [Phase 2 SRS-based FP Estimate Workbook](#)
 3. [Phase 2 SRS-based Function Point Estimate Workbook](#)
 4. [IMDO Display Person Query Results](#)
 5. [IMDO Search for Person in ADR v1_1.doc](#)
 6. [IMDO UI Use Case Model](#)
 7. [IMDO List Exceptions in ADR](#)
 8. [IMDO Logon Logoff IMDO UI UC](#)
 9. [PS Supplementary Specification](#)
 10. [PSIM - Move Correlation UC v 1_3](#)
 11. [PSIM - Resolve Duplicate](#)
 12. [PSIM - Resolve Mismatch UC](#)
 13. [PSIM API - Person Lookup Attended](#)
 14. [PSIM API - Person Lookup Unattended](#)
 15. [PSIM Retrieve Systems of Interest Use Case.DOC](#)
 16. [PSIM- Add Patient \(MPI\) UC v1_6](#)
 17.  [PSIM- Add Person UC v1_8](#)
 18. [Retrieve Person Identity Trait History](#)
 19. [Retrieve Person Record by VPID](#)
 20. [Retrieve VPID v1_1](#)
 21. [IMDO Search for an Exception](#)
 22. [IMDO Security Administration](#)
 23. [Synchronize Message From VistA](#)
 24. [Synchronize VistA From PS Update](#)
 25. [Unverified SSN Query](#)
 26. [Update Person Correlation \(ESR\) v1_5 UC.doc](#)
 27. [Update Primary Record \(ESR\) v1_5 UC.doc](#)
- **Reviews/Testing Information**
 1. [CS PSIM Test Plan IR6 v2.3](#)
 2. [CS PSIM Test Plan IR7 v3.0](#)
 3. [Patch Checklist XU_8_397.xls](#)
 4. [Patch Review Process Checklist - XU_8_331 for release](#)
 5. [PSIM Test Eval Summary for 6.5](#)
- **Project Documents/Manuals**
 1. [IMDO Installation and User Guide](#)
 2. [PS Developer Guide.doc](#)
- **Project Management Documents**

1. [PS Project Management Plan](#)
 2. [PS Risk List](#)
 3. [PS Risk Plan](#)
 4. [PS Communication Plan](#)
 5. [PSIM Enumeration Schedule.xls](#)
 6. [PSIM Vision Scope](#)
- **Data Security Compliance**
 1. [Personal_Health_Identifier_Checklist_PS_Identity_Management.doc](#)

Linked New Service Requests

* - There are no linked new service requests for this project.

Associated Test Sites

* - There are no test sites associated with this project.

Project Status/Update Information

- **Project Status:** Active
- **Project Type:** Development
- **Date Received:** 2/3/2003
- **Most Recent Function Point Count:** 464 - SRS
- **Milestone Schedule:**

Milestone	Description	Planned Completion Date	Revised Completion Date	Actual Completion Date
-----------	-------------	-------------------------	-------------------------	------------------------