

**Identity and Access Management
Access Services 2.0 Increment 5**

**Identity Proofing
System Design Document**



Department of Veterans Affairs

March 2015

Version 1.1

Note: The revision history cycle begins once changes or enhancements are requested after the System Design Document has been baselined.

Date	Version	Description	Author
04/24/2015	1.1	Updated per anomalies	[REDACTED]
03/25/2015	1.0	Updated document to include items for increment 5 for IP	[REDACTED]

Artifact Rationale

The System Design Document (SDD) is a dual-use document that provides the conceptual design as well as the as-built design. This document will be updated as the product is built, to reflect the as-built product. Per the Project Management Accountability System (PMAS) Guide, the SDD as a conceptual design is required prior to the Milestone 1 Review. (Sections 1, 2, 3, 4, 5, 7, 9 need to be populated, as applicable.) The as-built design for each delivery must be incorporated prior to the Milestone 2 Review. (The entire document needs to be populated or updated, as applicable.)

This artifact contains information from the Department of Veterans Affairs (VA) and its contractors that are privileged, proprietary, business confidential or otherwise protected from disclosure. The information within this artifact is authorized solely for use by the individual or entity that is the intended recipient. Any additional use, dissemination, distribution, retention, or copying of this artifact, attachments, or substance is prohibited.

Table of Contents

1. Introduction	7
1.1. Purpose of the SDD.....	7
1.2. Identification	8
1.3. Scope.....	9
1.3.1. Increment 5 IP Scope.....	9
1.4. Constraining Policies, Directives and Procedures	10
1.5. User Characteristics	12
1.6. Relationship to Other Documents and Plans.....	12
1.7. Definitions, Acronyms, and Abbreviations	12
1.8. References	12
2. Background.....	13
2.1. Overview of the System.....	13
2.2. Overview of the Business Process	13
2.3. Business Benefits	17
2.4. Assumptions and Constraints.....	17
2.4.1. Design Assumptions	17
2.4.2. Design Constraints.....	17
2.4.3. Design Trade-offs	18
2.5. Overview of the Significant Requirements.....	18
2.5.1. Overview of Significant Functional Requirements	19
2.5.2. Overview of Functional Workload / Performance Requirements	26
2.5.3. Overview of Operational Requirements.....	28
2.5.4. Overview of the Technical Requirements.....	28
2.5.5. Overview of the Security or Privacy Requirements.....	29
2.5.6. Overview of System Criticality and High Availability Requirements.....	29
2.5.7. Single Sign-on Requirement.....	30
2.5.8. Requirement for Use of Enterprise Portals	30
2.5.9. Special Device Requirements.....	30
2.6. Legacy System Retirement.....	30
3. Conceptual Design	31
3.1. Conceptual Application Design	31
3.1.1. Application Context.....	31
3.1.2. High-Level Application Design	34
3.1.3. Application Locations	36
3.1.4. Application Users	37
3.2. Conceptual Data Design.....	37

3.2.1.	Project Conceptual Data Model	37
3.2.2.	Database Information	42
3.2.3.	User Interface Data Mapping	44
3.3.	Conceptual Infrastructure Design	55
3.3.1.	System Criticality and High Availability.....	55
3.3.2.	Special Technology	56
3.3.3.	Technology Locations.....	56
3.3.4.	Conceptual Infrastructure Diagram.....	58
3.3.5.	CA Identity Manager	58
3.3.6.	CA SiteMinder Policy Server/Federation Security Services (FSS)	58
3.3.7.	CA Directory	59
3.3.8.	Identity Manager Workflow DB, Oracle Database Server 11g.....	59
3.3.9.	CA Report Server	59
3.3.10.	Microsoft IIS HTTP/HTTPS Server & SiteMinder Web Agent.....	59
4.	System Architecture.....	62
4.1.	Hardware Architecture.....	62
4.2.	Software Architecture.....	67
4.3.	Network Architecture	72
4.4.	Service Oriented Architecture / ESS.....	74
4.5.	Enterprise Architecture	74
5.	Data Design	75
5.1.	DBMS Files	75
5.2.	Non-DBMS Files.....	76
5.3.	Data View.....	76
5.3.1.	IP Data Exchange with VHIC	76
5.3.2.	IP Data Exchange with CSP	77
5.3.3.	IP Data Exchange with MVI	78
6.	Detailed Design.....	80
6.1.	Hardware Detailed Design	80
6.2.	Software Detailed Design	80
6.2.1.	Conceptual Design	80
6.2.2.	Specific Requirements	88
6.3.	Network Detailed Design.....	91
6.4.	Service Oriented Architecture / ESS Detailed Design.....	91
6.4.1.	Service Description for IP	94
6.4.2.	Service Design for IP	94
6.4.3.	Retrieve Proofing Status	96
6.4.4.	SOAP Request/Response Samples.....	98

7. External System Interface Design	103
7.1. Interface Architecture	103
7.2. Interface Detailed Design	103
8. Human-Machine Interface	104
8.1. Interface Design Rules	104
8.2. Inputs.....	104
8.3. Outputs	104
8.4. Navigation Hierarchy	104
9. Security and Privacy	106
9.1. Security	106
9.1.1. Confidentiality of Sensitive Information	106
9.1.2. Privacy of Personal Information.....	106
9.1.3. Process Integrity.....	106
9.1.4. E-Sig Controls.....	107
9.2. Privacy	107
A.1. RTM	109
A.2. Packaging and Installation.....	109
A.3. Design Metrics.....	109
A.4. Acronym List and Glossary.....	109
A.5. Required Technical Documents.....	109
A.6. Attach Documents	109
A.7. IP Class Diagram.....	109

List of Tables

Table 1: System Identification.....	8
Table 2: Scope Inclusions	9
Table 3: Scope Exclusion.....	9
Table 4: Identity Proofing Business Needs and Requirements Enhancements.....	10
Table 5: Constraining Policies, Directives and Procedures	10
Table 6: Business Processes.....	14
Table 7: L2 Identity Proofing Business Process Flow.....	15
Table 8: VIC Clerk Identity Proofing Business Process Flow.....	16
Table 9 : Design Constraints.....	17
Table 10 : Functional Requirements	19
Table 11 Significant Functional Requirements - IP	19
Table 12: Service Availability Level 4.....	28
Table 13 Potential Impact Categories for Authentication Errors.....	33
Table 14: (Grouping): Application Context Description	34
Table 14 : IP Solution Application Locations.....	36
Table 15 : IP Solution Users	37
Table 16 Conceptual Data Model Description.....	38

Table 17 : Database Inventory	39
Table 18 : Database Inventory	42
Table 19: User Profile Screen Mapping.....	44
Table 20 : Address Verification Screen Mapping.....	45
Table 21 : Primary Verification Screen Mapping	45
Table 22 : Secondary Verification Screen Mapping.....	46
Table 23 : Special Technology Requirements	56
Table 24 : Hardware Appliance	62
Table 25 : Virtual Machines and Appliances.....	63
Table 26 : Pre-Production (Terremark Culpeper, VA)	63
Table 27 : Production (Terremark Culpeper, VA).....	64
Table 28 : DR (Terremark Miami, FL).....	65
Table 29 : Software Components.....	67
Table 30 : Oracle Database 11gR2	68
Table 31 : CA Directory	69
Table 32 : Web Tier – IIS Web Server	70
Table 33 : Application Tier – WebLogic Application Server.....	71
Table 34 : CA IdentityMinder.....	72
Table 35 : Operating Systems	72
Table 36 : Database File System.....	75
Table 37: VHIC-IP Data Exchange	77
Table 38: VHIC-IP User Data.....	77
Table 39: CSP-IP Data Exchange	77
Table 40: IP User Data Exchange with MVI.....	79
Table 40 : Potential Impact Categories for Authentication Errors.....	81
Table 41 : AcS 2.0 Products	84
Table 42 : Identity Proof a User.....	85
Table 43 : Create Proofing Record	87
Table 46: IP Web Service Interface Data Elements for Proof Applicant (LOA2) Request.....	94
Table 47: IP Web Service Interface Data Elements for Proof Applicant (LOA2) Response	94
Table 46 IP Web Service Interface Data Elements For Retrieve Proofing Status Request	97
Table 47 IP Web Service Interface Data Elements for Retrieve Proofing Status Response.....	98
Table 50: IP External System Interface	103

1. Introduction

The Department of Veterans Affairs (VA) currently serves Veterans, their beneficiaries, and other VA stakeholders via services across many distributed and often operationally disjoint Lines of Business (LOB). Though VA serves the stakeholders across a vast enterprise of internal and external businesses and programs, it currently lacks a single, uniform method for identifying stakeholders and applying Access Management Services to safeguard its information resources. VA also lacks the capability to harmoniously share and leverage sensitive information across its internal LOBs and external business partners. Based on this existing operating model, the Veterans Relationship Management (VRM) Program Management Office (PMO) has identified the need to establish core Access Services (AcS) to definitively and consistently identify VA stakeholders and to establish supporting processes that increase the level of security protecting the identities, information, and interests of VA stakeholders.

The enterprise-wide system as a whole is referred to as the VA AcS 2.0, which includes the applicable subcomponents. The individual subcomponents or groups are referred to as a VA AcS activity or the VA AcS activities. The VA AcS activities include the following:

Single Sign-On – Internal (SSOi)	Identity Proofing (IP)
Single Sign-On – External (SSOe)	Provisioning (PROV)
Credential Service Provider (CSP)	Specialized Access Control (SAC)
Electronic Signature (eSig)	Compliance Audit and Reporting (CAR)

Within each of the AcS activities, commercial off-the-shelf (COTS) products are used to enable the specific capabilities of the AcS 2.0 described in this document and identified by the business as referenced (where applicable) in the Business Requirements Document (BRD) and Requirements Specifications Document (RSD). The AcS 2.0's primary customers are both internal and external user communities who need logical access to VA business applications.

Identity proofing is the process of verifying a user's identity using documents or information provided during the user registration process. Identity proofing can take many forms; it may simply consist of validating a user's identity using information provided over the phone, or obtaining additional documentation such as a driver's license, social security card, birth certificate, or work visa. The focus of this activity is to provide a structured, documented, repeatable process for conducting in person proofing, validating the documentation or knowledge used to identify the person of interest, and supporting compliance for audit reporting.

1.1. Purpose of the SDD

The purpose of the System Design Document (SDD) is to describe the supporting mechanics of the IP solution. The SDD translates the requirement specifications into a document from which the developers may create the technical solution. It identifies the top-level system architecture, as well as the supporting hardware, software, communication, and interface components. This artifact is an evolving document and is a living artifact that is updated (as applicable) when modifications are incorporated and / or new capabilities are added to the solution (when appropriate).

The primary target audience is IP developers and teams who will assist in the establishment of the infrastructure, as well as the following stakeholders:

- VA, Department of Defense (DoD), business partners, and other federal agencies
- AcS 2.0 Architects
- AcS 2.0 Business Sponsors
- Developers and technical managers
- Senior management and mission owners who enforce decisions about the IT security budget
- IT security program managers, who implement the security program
- Information System Security Officers (ISSO) responsible for IT security
- IT application owners of software and/or hardware used to support AcS activities
- Information owners of data stored, processed, and transmitted by the IT applications
- Other technical support personnel and product vendors

This document provides the solution architecture and detailed design of the IP solution as well as details for understanding the specific system configurations, interfaces, workflow, Graphical User Interfaces (GUI), and data models.

1.2. Identification

The information contained herein is based on the CA Technologies (CA) COTS products to provide the core capabilities for access control services to VA stakeholders. This document explains the manner in which these COTS solutions will be deployed to provide the foundation system and software to be used by the AcS 2.0. This document applies to the following systems and software:

Table 1: System Identification

Name	Description	Abbreviation	Version	Release
VA AcS 2.0	Core set of activities to definitively and consistently identify VA stakeholders and to establish supporting processes that provide the appropriate level of security required to protect and manage the identities, information, and interests of the VA stakeholders	AcS	V 2.5.0	Release 5 (Increment 5)
Identity Proofing	Identity proofing is the process of verifying a user's identity using documents or information provided during the user registration process. The focus of this activity is to provide a structured, documented, repeatable process for conducting in person proofing, validating the documentation or knowledge used to identify the person of interest, and supporting compliance for audit reporting.	IP	V2.4.1 Build 001	N/A

1.3. Scope

This SDD focuses on the technical system design to provide the foundation for the IP solution. It provides an overview of the core capabilities, architecture, and design. It does not include default COTS product design nor does it include OOTB data definitions, tables, or models except where the design alters such elements and components. The sections below provide scope inclusion and exclusion details.

Table 2: Scope Inclusions

Includes
<ul style="list-style-type: none">• The Identity Proofing Service shall be able to collect an expiration date through year 2150 when the military identification card is presented as a proofing document.
<ul style="list-style-type: none">• IP supports MVI error codes AE (invalid payload) and AR (MVI system components down)
<ul style="list-style-type: none">• The Identity Proofing Service shall be able to collect an expiration date of INDEF (indefinite) when the military identification card is presented as a proofing document.
<ul style="list-style-type: none">• The Identity Proofing service shall require only one Primary ID in order to be In-Person Proofed
<ul style="list-style-type: none">• Provides web service based tasks and GUIs for Identity Proofer to perform the IP process for a person of interest
<ul style="list-style-type: none">• Integration with the Master Veteran Index (MVI)
<ul style="list-style-type: none">• Provide security controls consistent with NIST guidance SP-800-63 and VA 6500
<ul style="list-style-type: none">• Provide Graphical User Interfaces (GUIs) for users to obtain IP credentials and Administrators to manage the IP functionality
<ul style="list-style-type: none">• Provide Graphical User Interfaces (GUIs) for Identity Proofer to perform the ID Proofing process for the purpose of issuing L2 credentials to users
<ul style="list-style-type: none">• Provide Graphical User Interfaces (GUIs) that conform to 508 usability compliance requirements

Table 3: Scope Exclusion

Excludes
<ul style="list-style-type: none">• No Remote Identity Proofing mechanisms are provided other than Level 2 In-Person as defined in SP 800-63
<ul style="list-style-type: none">• Issuance of Level 3 or 4 credentials
<ul style="list-style-type: none">• Collection, Storage, or Transmission of Social Security Numbers or a form thereof.

1.3.1.Increment 5 IP Scope

The In-Person Proofing (IPP) process confirms the identity of an individual through review of identification documents and artifacts provided during a visit to a VA Regional Office or at any location where IPP is being conducted.

The Identity Proofing Service is being enhanced to allow the capture of new expiration date requirements when a military identification card is used as a proofing document.

Table 4: Identity Proofing Business Needs and Requirements Enhancements

BRD BN	Requirement	In-Scope Requirement Clarification
User Story: As a user, I want to be able to capture the expiration date of a military identification cardholder's proofing document as a specific date through year 2150, or indefinite.		
1.0 Identity Proofing: Provide a digital process that vets and verifies the information (e.g., identity history, credentials, documents) that is used to establish the identity of a system entity, initiate a chain of trust in establishing a digital identity, and bind it to an individual.		
1.11	Identity Proofing	[FEAT499983] The Identity Proofing Service shall be able to collect an expiration date through year 2150 when the military identification card is presented as a proofing document.
1.11	Identity Proofing	[FEAT499984] The Identity Proofing Service shall be able to collect an expiration date of "INDEF" (indefinite) when the military identification card is presented as a proofing document.

1.4. Constraining Policies, Directives and Procedures

This design complies with the following policies, directives, and procedures (as applicable). The specific requirement and sub-requirement numbers are highlighted in the individual service-specific SDDs (where appropriate).

Table 5: Constraining Policies, Directives and Procedures

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
2	VA	VA 6501 Directive	<ul style="list-style-type: none"> VA Identity Verification In-Person Proofing (IPP) Process. Defining overall Identity Proofing Methodology for VA IAM.
1	VA	VA 6300 Directive	<ul style="list-style-type: none"> Directive Records and Information Management. Defines information management framework for VA Access Services.
2	NIST	SP 800-63-2	<ul style="list-style-type: none"> Special Publication – Electronic Authentication Guideline. Defines levels of assurance in user identities presented to IT systems over open networks. Defines the data and procedural requirements for VA Access Services.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
3	NIST	FIPS-201-2	<ul style="list-style-type: none"> Federal Information Processing Standards Publication – PIV of Federal Employees and Contractors. Provides Identity Proofing, credentialing and chain of trust requirements and processes. Defines the method for secure administrative interaction and control.
4	NIST	FIPS-140-2	<ul style="list-style-type: none"> Federal Information Processing Standards Publication (FIPS) – Security Requirements for Cryptographic Modules. Defines the cryptographic standards and requirements.
5	NIST	SP 800-122	<ul style="list-style-type: none"> Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Provides technical procedures for protecting PII in information systems. Defines the information which can be used to distinguish or trace an individual's identity.
6	US Congress	Section 508 Amendment to the Rehabilitation Act of 1973	<ul style="list-style-type: none"> Section 508 Electronic and information technology requirements for Federal departments and agencies. Accessibility, development, procurement maintenance, or use of electronic and information technology. Defines the “Human-Machine Interface” accessibility requirements.
7	OMB	M-04-04	<ul style="list-style-type: none"> Memorandum to the Heads of All Department and Agencies – E-Authentication Guidance for Federal Agencies. Defines the E-Authentication requirement.
8	OMB	M-11-11	<ul style="list-style-type: none"> Requirements for Accepting Externally-Issued Identity Credentials. FICAM architecture and procedures for federal agencies.
9	GSA	FICAM	<ul style="list-style-type: none"> Federal Identity, Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance. Provides the common segment architecture and implementation guidance for federal ICAM programs.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
10	White House	NSTIC	<ul style="list-style-type: none"> National Strategy for Trusted Identities in Cyberspace (NSTIC) – Provides guidance for identity trust in cyberspace.
11	US Congress	E-Government Act of 2002	<ul style="list-style-type: none"> Federal Management and Promotion of Electronic Government Services. Defines the requirements for electronic services.

1.5. User Characteristics

The user community for the IP activities consists of internal users including VA employees, contractors and affiliates.

1.6. Relationship to Other Documents and Plans

The system design is developed based on the progressive refinement and discovery of business and functional requirements outlined and extracted from the following documents, which are located on the [AcS TSPR](#) site.

Note: The applicable standards and guidelines from the VA Handbook and NIST are identified in section 1.4 above.

1.7. Definitions, Acronyms, and Abbreviations

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

1.8. References

The document references are listed in Section 1.6 above.

2. Background

The purpose of the VA AcS Development Support task is to design, develop, implement, integrate, operationalize, and sustain an enterprise-wide VA AcS 2.0 for VA VRM. In order to coordinate AcS across several VRM work streams, multiple internal and external systems will need to be interconnected to provide access to these systems by facility, system and individual entities. The goal of AcS is to facilitate access transactions using an Enterprise Services framework. The Framework should address the user account lifecycle, from identity creation through de-provisioning of the user. To accomplish these goals, the AcS should consider highly available services in an effort to minimize unintentional disruptions for the users.

This document provides the underlying design to support the IP activities. The system design is based on a Service Oriented Architecture (SOA) approach. The solution architecture uses accepted COTS products for each of VA AcS activity and applies the leading practices as outlined by the product vendor to the extent possible. The design of the architecture supports VA's scalability, security, extensibility, and high availability requirements to provide a flexible enterprise solution.

2.1. Overview of the System

The AcS 2.0 is made up of several activities, which are necessary to provide identity and access management services to both internal VA employees / contractors and to external end users. It provides VA applications centralized authentication mechanism for internal users and federation capabilities to access external application. Authorization capabilities to provide coarse- and fine-grained application access while providing workflow for self-service account requests, approvals, and user life cycle management.

Identity proofing is the process of verifying a user's identity using documents or information provided during the user registration process. Identity proofing can take many forms; it may simply consist of validating a user's identity using information provided over the phone, or obtaining additional documentation such as a driver's license, social security card, birth certificate, or work visa. The focus of this activity is to provide a structured, documented, repeatable process for conducting in person proofing, validating the documentation or knowledge used to identify the person of interest, and supporting compliance for audit reporting.

2.2. Overview of the Business Process

A digital identity is the representation of an identity in a digital environment. Prior to establishing a digital identity, identity proofing must first occur. According to the FICAM Roadmap and Implementation Guidance, identity proofing is the process that vets and verifies the information (e.g., identity history, credentials, and documents) that is used to establish the identity. This establishes the basis for a chain of trust for the digital identity and allows for the binding of the identity to an individual.

The primary goal of the IP Service to provide an enterprise service implementation of the proofing process including the capture of data collected during the proofing event. The IP Service provides the ability to proof a user at Level of Assurance 2 as defined in National Institute of Standards and Technology Special Publication (NIST SP) 800-63.

IP also supports the CSP registration process by providing the user with a list of VA locations that provide Level 2 in-person Identity Proofing and information regarding the requirements for identity

proofing including guidance on identity document requirements. Once the user arrives at the location, they will present their documents to the Identity Proofer. The IP provides user interfaces for the Identity Proofer that guide the proofer through the ID Proofing task. Once the proofing task is successfully completed, the user will receive notification that their upgrade has completed.

Additionally, the IP supports a “VIC Clerk” mode where the Identity Proofer can provide identity proofing services for prospective VIC Card holders. The IP also provides administrative support for the IP system.

Refer to the VA AcS 2.0 Requirements Specification Document (RSD), use case, and Requirements Traceability Matrix (RTM) documents for the business process flows.

Table 6: Business Processes

Business Process ID	Business Process Name	Owner	Description
1	Level 2 User Identity Proofing	VA IAM	<p>Provides the ability to Identity Proof for Level 2 The registration and identity proofing process provides the IP with the ability to verify the true identity of the applicant. Specifically, the design includes measures to enable that:</p> <ul style="list-style-type: none"> • A person with the applicant’s claimed attributes exists, and those attributes are sufficient to uniquely identify a single person • An applicant whose token is registered is in fact the person who is entitled to the identity • An applicant cannot later repudiate the registration; therefore, if there is a dispute about a later authentication using the subscriber’s token, the subscriber cannot successfully deny he or she registered that token <p>The IP is designed to issue Level 1 and Level 2 credentials.</p>
2	VIC Clerk	VA IAM	Provides an ability for a VIC Clerk to do ID Proofing in support of the VIC business Processes.

Figure 1: Level 2 User Identity Proofing

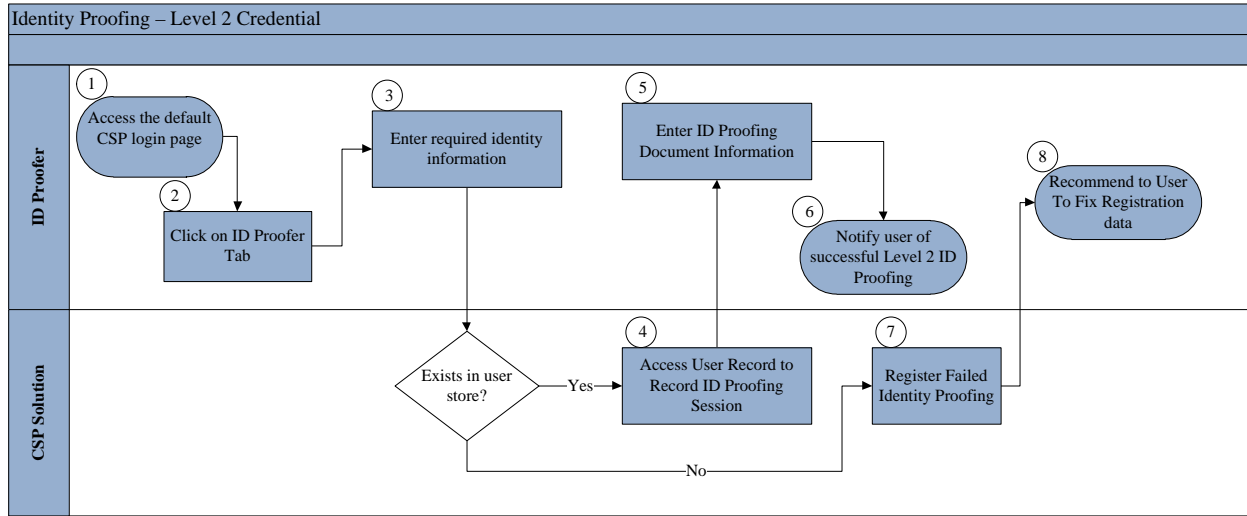


Table 7: L2 Identity Proofing Business Process Flow

Step	Description
1	Access the CSP Login page. The ID Proofer uses their credential to access the IP.
2	On this page, the ID Proofer uses the link to select the ID Proofing tab.
3	At this step, the ID Proofer fills in the data necessary for finding a unique user in the system and satisfying the requirement to prevent data fishing. The data model is minimized to require the least amount of data to support a Level 2 credential.
4	The system pulls up the unique user record to allow the ID Proofer to capture the necessary data to complete a Level 2 Identity Proofing session.
5	The ID Proofer enters the data from the ID Proofing documents.
6	The system notifies the user that the ID Proofing session has completed successfully.
7	If the user is not in the user store, the ID Proofing session fails.
8	The system notifies the user fix their data.

Figure 2: VIC Clerk

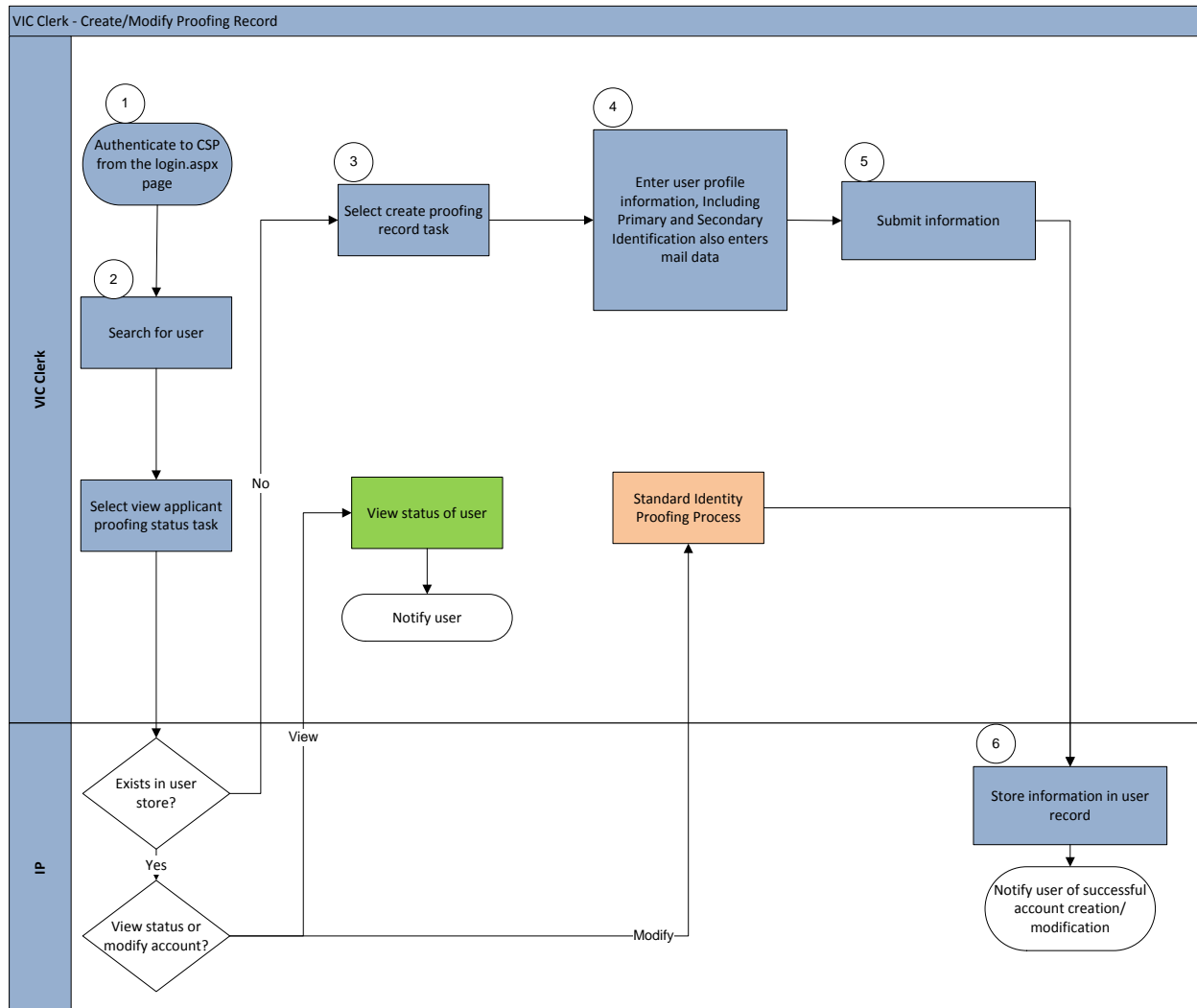


Table 8: VIC Clerk Identity Proofing Business Process Flow

Step	Description
1	Authenticate to the IP and access the Identity Proofing page
2	The VIC Clerk searches for a User, if the Clerk finds a record, the ID Proofer uses the standard ID Proofing flow
3	At this point, the VIC Clerk creates a record for the user
4	The VIC Clerks enters the user's profile information, the Primary ID information, the Secondary ID information and the mail
5	The VIC Clerk submits the record
6	At this step, the system validates the user information and stores the record for the VIC process

The preceding flows and descriptions are not intended to capture the entire IP solution, but instead are intended to provide an overview of the required business processes that have been designed into the solution and provided as described. Details of the underlying systems, processes, components, data structures, and security features are provided in later sections.

2.3. Business Benefits

Refer to Section 2.2 for business benefits and refer to the VA AcS 2015 Business Requirements Document, [BRD VA IAM Access Services 2015 4-24-14 SignatureReady.pdf](#), for additional context.

2.4. Assumptions and Constraints

This section describes the assumptions and constraints that impact the design of the IP solution.

2.4.1.Design Assumptions

This section describes the assumptions that impact the design of the IP solution.

Table 7: Design Assumptions

Component	Assumption
IP	<ul style="list-style-type: none">VA will provide trained ID Proofer to perform the proofing process. They will follow approved VA policies and processes associated with the proofing process.Identity Proofing as a service will be used for choreographing IP functionality by providing the framework to establish an identity proofing task.

2.4.2.Design Constraints

Table 9 : Design Constraints

Component	Constraints
IP	<ul style="list-style-type: none">The Identity Proofing activity supports LOA 2 In Person Identity Proofing records. This capability is not a limitation in the activity, as the activity may support higher LOA proofing records.One or more Identity Proofing records may be associated with each VA enterprise identity record, allowing versatile Identity information to be collected and used as part of user certification process.
Infrastructure	<ul style="list-style-type: none">The AcS 2.0 is designed to have 99.9% availability, and can be failed over to the Disaster Recovery site. However, this is contingent on the availability of other components outside of the AcS 2.0 such as VAAFI and Terremark, which only support 99.6% and 99.9% availability, respectively. Therefore, if the solution components support 99.9% availability, this may not be achieved due to external dependencies which may be limited to the VAAFI 99.6% figure.

2.4.3.Design Trade-offs

The following are the design trade-offs for the IP solution design:

- The user store and policy store have read-intensive operations. Based on the projected usage demands, the policy store and user store should be created in their own CA Directory Servers instances. Alternatively, if the stores are consolidated on common servers with failover topology, system's performance may degrade between the read and write transactions. Additionally, if the read intensive operations are occurring in the same place where the data is being written then it is likely that data mismatch may occur at time of the reading transaction.

2.5. Overview of the Significant Requirements

2.5.1. Overview of Significant Functional Requirements

Table 10 : Functional Requirements

Table 11 Significant Functional Requirements - IP

1. Identity Proofing (IDP) – Provide a digital process that vets and verifies the information (e.g., identity history, credentials, documents) that is used to establish the identity of a system entity; initiates chain of trust in establishing a digital identity and binding it to an individual.				High	* Remote Proofing (L2-L3) * VA CSP Upgrade of Proofing Levels (L1-L2)	FY13 4/25/2013
	1.01	The IDP service (remote) shall provide the means for each applicant requesting a FICAM Assurance Level 2 or Level 3 credential to initiate remote proofing online or via telephone.	SP800-63, Table 1 – Level 2	High		FY13 12/30/2012
	1.02	The IDP service (remote) shall retain a record of the facts of remote proofing for a minimum of 7 years, 6 months.	SP800-63, Section 7.2.2	High		FY13 12/30/2012
	1.03	The IDP service shall follow and maintain a single harmonized policy across all lines of business (for all VA users) in order to present a consolidated Veteran-centric view of benefits and services in a self-service environment.	VRM IAM Scope and Vision, Section 3.3.1	High		FY13 4/25/2013
	1.04	The IDP service shall align with internal and external business partner authentication processes including DoD to ensure the integrity of electronic data.	FICAM v2, Section 3.2.2.2	High		FY13 4/25/2013
	1.05	The IDP service shall be designed to align with related existing and planned VA systems and IAM initiatives.	FICAM v2, Section 5.2.1	High		FY13 4/25/2013
	1.06	The IDP service shall be designed to align with related existing and planned DoD systems and initiatives.	VRM IAM Scope and Vision, Section 3.3.1	High		FY13 4/25/2013
	1.07	The IDP service shall provide the means to conduct an In-person Proofing for each applicant requesting a Level 2 credential.	SP800-63, Section 7.2.1	High		FY13 4/25/2013
	1.08	The IDP service (in-person) shall be performed in an approved VA facility.	SP800-63, Section 7.2	High		FY13 4/25/2013
	1.09	The IDP service (in-person) shall be performed by VA employees trained to perform proofing, and who have access to the administrative tools to support In-person Proofing.	SP800-63, Section 7.2	High		FY13 4/25/2013

1.10	The IDP service (in-person) shall create and maintain a record of the Veteran, beneficiary, or surrogate (the "applicant") presenting forms of photo identification in compliance with Appendix B of VA Directive 6501 and the disposition of the VA staff determining that the identification (ID) provided appears valid, and that the photo matches the applicant.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.11	The IDP service (in-person) data store shall record and maintain a record of the forms of ID presented by the applicant.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.12	The IDP service (in-person) data store shall record and maintain a record of the ID number, address, and date of birth from the ID presented by the applicant.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.13	The IDP service (in-person) data store shall record and maintain a record of other data elements that the business would like to consider adding during the enrollment process, as they are defined.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.14	The IDP service (in-person) data store shall record and maintain a record of the IDP operator, date and time stamp, and other related attributes of the IDP service (in-person) transaction.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.15	The IDP service (in-person) shall provide a means for the VA staff to query whether the applicant has an existing proofing record.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.16	In the case an applicant has an existing proofing record recorded, the IDP service (in-person) shall provide a means for the VA staff to validate any credentials issued.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.17	If the forms of identification presented by the applicant do not meet the requirements in VA Directive 6500, the IDP service (in-person) shall provide a means for the VA staff to record that the proofing request was denied.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.18	The disposition of all IDP (in-person) requests, successful and unsuccessful, shall be stored and maintained for audit and historical purposes.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.19	The IDP service data store shall interface with internal and external enterprise data stores and applications to maintain in-person proofing records and share data necessary to enable other IAM initiatives in the most efficient, collaborative, and data-secure manner.	FICAM v2, Section 3.2.3	High		FY13 4/25/2013

1.20	The IDP service shall retain a record of the facts of In-person Proofing for Levels 2 and 3 for a minimum of 7 years, 6 months.	SP800-63, Section 7.2.2	High		FY13 4/25/2013
1.21	The IDP service shall retain a record of the facts of In-person Proofing for Level 4 for a minimum of 10 years, 6 months.	SP800-63, Section 7.2.2	High	Determined not to be an IAM requirement. Removed.	FY13 4/25/2013
1.22	The IDP service shall not store or maintain any PII or Personal Health Information beyond the time reasonably necessary to complete the IDP process and record the proofing event evidence.	FICAM v2, Section 6.3.1	High		FY13 4/25/2013
1.23	The IDP service data store shall interface with internal and external enterprise data stores and applications to maintain records and share data necessary to enable other IAM initiatives in the most efficient, collaborative, and data-secure manner.	FICAM v2, Section 3.2.3	High		FY13 4/25/2013
1.24	The IDP service data store shall interface with internal VA enterprise data stores and applications to maintain records and share data securely.	FICAM v2, Section 6.3.1	High		FY13 4/25/2013
1.25	The IDP service data store shall interface with external DoD data stores and applications to maintain records and share data securely.	VRM IAM Scope and Vision, Section 3.3.1	High		FY13 4/25/2013
1.26	The IDP service shall interface with all subscribing online applications/services through which an applicant is able to create a Provisioning request.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.27	The IDP service shall accept user input from all subscribing online applications/services for the purpose of determining if a record exists for the applicant in the Master Veteran Index (MVI).	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.28	The IDP service shall interface with all subscribing online applications/services to provide challenge questions for presentations to the applicant.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.29	The IDP service shall accept user input from all online applications/services for the purpose of validating the applicant's answers to challenge questions.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.30	The IDP service shall interface with the MVI to perform an unattended (online)/attended (for telephone) Person Lookup.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013

1.31	The IDP service shall pass the required data points collected from all subscribing online applications/services to the MVI.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.32	The IDP service shall accept the determination of the Person Lookup request from the MVI.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.33	The IDP service shall interface with various VA repositories to retrieve challenge questions.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.34	The IDP service shall interface with various external repositories to retrieve challenge questions.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.35	The IDP service shall evaluate the answers to challenge questions provided by the applicant.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.36	The IDP service shall evaluate the answers to challenge questions against VA repositories.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.37	The IDP service shall evaluate the answers to challenge question against external repositories.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.38	If the information presented by the applicant does not meet the requirements in VHA Directive 2007-37 Appendix A, the IDP service shall provide a means to record that the proofing request was denied.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.39	If the information presented by the applicant does meet the requirements in VHA Directive 2007-37 Appendix A, the IDP service shall provide a means to record that the proofing request was approved.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.40	The IDP service data store shall interface with internal and external enterprise data stores and applications to maintain records and share data necessary to enable other IAM initiatives in the most efficient, collaborative, and data-secure manner.	FICAM v2, Section 3.2.3	High		FY13 4/25/2013

1.41	The IDP service shall not collect, store or maintain any PII or PHI beyond the time reasonably necessary to complete the IDP process and record the proofing event evidence.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.42	The IDP service shall interface with internal VA enterprise data stores and applications to maintain records and share data securely.	FICAM v2, Section 7.1	High		FY13 4/25/2013
1.43	The IDP service shall interface with the VA Credentialing Service to make available to it the record of each individual's proofing status.	FICAM v2, Section 7.1	High		FY13 4/25/2013
1.44	The IDP service shall interface with the VA Provisioning Service to communicate as necessary any proofing status changes that affect the Provisioning Service.	FICAM v2, Section 7.1	High		FY13 4/25/2013
1.45	The IDP service shall interface with external DoD data stores and applications to maintain records and share data securely.	VRM IAM Scope and Vision, Section 1.1.1	High	Duplicate of 1.25. Removed.	FY13 4/25/2013
1.46	The IDP service shall provide the ability for a subscriber with existing Level 1 credentials to request an upgrade to Level 2 by complying with all the Identity Proofing requirements.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.47	The IDP service shall interface with all online applications/services through which an applicant is able to request a Provisioning upgrade.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.48	The IDP service shall assure that the results of the In-Person Proofing are recorded and associated with the correct (existing) credential record.	SP800-63, Section 7.2	High		FY13 4/25/2013
1.49	Upon successful completion of an upgrade request, the IDP service shall interface with the Credential Service Provider to provide the data necessary to upgrade a credential to Level 2.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.50	Upon successful completion of an upgrade request, the IDP service shall interface with the Provisioning Service to provide the data necessary to provision the user's access privileges appropriately.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.51	The IDP service (reporting feature) shall allow the definition and scheduling of standard management reports.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
1.52	The IDP service (reporting feature) shall provide the ability to establish data parameters for the generation of standard management reports.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013

	1.53	The IDP service (reporting feature) shall provide the ability to establish schedule (date) parameters for the generation of standard management reports.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.54	The IDP service (reporting feature) shall allow the customization and generation of ad-hoc and custom management reports.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.55	The IDP service (reporting feature) shall provide the ability to modify data parameters for the generation of custom/ad-hoc management reports.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.56	The IDP service (reporting feature) shall provide the ability to modify schedule (date) parameters for the generation of custom/ad-hoc management reports.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.57	The IDP service (reporting feature) shall support the storage and output of reports in a variety of formats.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.58	The IDP service (reporting feature) shall support the storage and output of reports in portable document format (PDF).	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.59	The IDP service (reporting feature) shall support the storage and output of reports in comma separated value (CSV) format.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.60	The IDP service (reporting feature) shall support the storage and output of reports in text (ASCII) format.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.61	The IDP service (reporting feature) shall provide the ability to select and configure the collection parameters of the auditable events to be captured.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.62	The IDP service (reporting feature) shall comply with the audit requirements applicable per the VA cross-cutting requirements as defined in the Office of Information Technology (OIT) Enterprise Requirement Repository.	VA Handbook 6500	High		FY13 4/25/2013
	1.63	The IDP service (reporting feature) shall interface with the Compliance, Auditing and Reporting (CAR) service to accept the identified set of auditable events required.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013

	1.64	The IDP service (reporting feature) shall provide a means to display the current set of auditable events to be stored.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.65	The IDP service (reporting feature) shall provide a means for the user to add, delete, and modify the collection parameters of auditable events.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.66	The IDP service (reporting feature) shall confirm to the user the successful addition, deletion, or modification of auditable events.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.67	The IDP service (reporting feature) shall capture each event configured as auditable.	FICAM v2, Section 8.1.4.2	High		FY13 4/25/2013
	1.68	When an IDP event occurs, the IDP reporting feature shall refer to the auditable event and configuration record to determine if the event should be captured.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.69	If the IDP service reporting feature determines the event should be captured, the event shall be stored in the IDP service reporting data store.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.70	The IDP service reporting feature shall interface with the CAR service to make available the audit event data collected and stored.	IPT Approved (2012) IDP Business Packet	High		FY13 4/25/2013
	1.71	Provide the capability to restrict the ability to create pseudonym identities and tokens as a controlled administrative over-ride function.	FICAM v2, Section 7.2	High		FY13 4/25/2013
	1.72	Provide the capability to consume identity data from credentials at FICAM Assurance Levels 2, 3, and 4 that have been created and issued external to VA.	FICAM v2, Section 3	High		FY13 4/25/2013
2. Vetting/Adjudication – Vetting will provide a digital process of examination and evaluation, including background check activities, which results in establishing verified credentials and attributes. Adjudication will provide a digital process of evaluating pertinent data in a background investigation, as well as any other available information that is relevant and reliable to determine whether a covered individual is suitable for government employment and/or eligible for particular privileges.				Medium	Vetting processes for FICAM Assurance Levels 2+	FY13 4/25/2013
	2.01	Level 2 shall encompass a primary Government Picture ID with either address of record or nationality, and financial account numbers when Remote Proofing; confirmation of address against application or internal databases, and confirmation of financial account through records checks	SP800-63, Table 1	Medium		FY13 4/25/2013

2.02	Level 3 shall encompass shall encompass a primary Government Picture ID with either address of record or nationality, and financial account numbers when Remote Proofing; confirmation of address against application or internal databases, verification of the identity document via the issuer or other databases, and confirmation of financial account through records checks(if presented)	SP800-63, Table 1	Medium		FY13 4/25/2013
2.03	Level 4 shall encompass the in person capture of a biometric and presentation of two ID documents, one of which must be a primary Government Picture ID with either address of record or nationality and the other a secondary Government ID or financial account record; confirmation of address against application or internal databases, verification of the identity document via the issuer or other databases, and confirmation of financial account through records checks(if presented)	SP800-63, Table 1	Medium	Determined to be a definition instead of a requirement.	FY13 4/25/2013
2.04	PIV shall encompass the in person capture of biometrics and presentation of two forms of identity source documents, at least one of which must be a valid State or Federal government-issued picture ID; verification of their authenticity, and preliminary and final adjudication of a background investigation at the NACI or higher level	FIPS 201-1, Section 2.2 and A.1.1.2	Medium	Determined to be a definition instead of a requirement.	FY13 4/25/2013

2.5.2. Overview of Functional Workload / Performance Requirements

The IP service for this increment shall support the following:

Operation	
Name	IP (Proofing UI)
Usage Profile (Proofing Events)	
Mean Daily volume	3500
Projected Growth	350/year
Peak Daily volume	4000
Projected Growth	400/year
Peak Hourly volume	500
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

Operation	
Name	IP (Webservice)
Usage Profile (Webservice Calls)	
Mean Daily volume	3500
Projected Growth	350/year
Peak Daily volume	4000
Projected Growth	400/year
Peak Hourly volume	500
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	10 seconds

The performance specifications are targeted for the planned consumption of AcS services for the following year; however, the performance specifications are easily scalable for future implementations. The following are the specifications as defined in the [AcS FY15 BRD](#), Section 7.2.1 Performance, Capacity, and Availability Requirements. For a detailed performance specification for each service, refer to the following subsections.

Table 11: Performance Specifications

How many users does the current system support?
<p>The IAM system supports the current and future (forecasted) user base of relying applications and systems. The system is expected to support a minimum of the following:</p> <ul style="list-style-type: none"> ▪ 700,000 contractors ▪ 350,000 employees ▪ 28 million Veterans ▪ Hundreds of internal and external VA applications
How many users does the new system (or system modification) support?
<p>The new system is scalable to accommodate an internal and external user base of approximately 29 million.</p>
What is the predicted annual growth in the number of system users?
<p>The new system supports at least 10 million users during the initial year (full production deployment of IAM suite) with at least 100% increase in numbers annually. Integration of applications on a monthly basis via IAM Governance process (process support up to 200 applications over an annual basis).</p>

The performance specifications include the following:

- The online application screens contained in the user interface render less than ten seconds with an average rendering of three seconds within the budgeted resource utilization constraints.
- The online procedures prompted from a user interface execute under five seconds with an average of four seconds within the budgeted resource utilization constraints.

- c. The metric data indicating the performance characteristics of the system to support application monitoring is provided.
- d. **User Profile:** VA Employee or Contractor on the VA Network proofing a person for a VA business process such as the issuance of a Veteran Health Identification Card (VHIC) card

2.5.3. Overview of Operational Requirements

Per Section 2.11 of the AcS 2.0 RSD, the AcS solution is hosted within the Terremark environment as required by VA. Terremark is responsible for reliability and monitoring when the AcS solution becomes operational. The tools, methods, and specifications for monitoring the reliability of the AcS solution are at the discretion of Terremark.

Table 12: Service Availability Level 4

Service Availability Level 4 *Standards adopted from specification created by Application Structure and Integration Services (ASIS)	
Description	Mission Critical Information
Minimum Availability	99.99%
Maximum Downtime Per Month	4.4 minutes
Business Value	Essential to fundamental business operations – outage seriously impairs functioning of business.
System Response	In the absence of any system superseding requirements, the system responds to user actions in three seconds or less in 90% of the attempts, and never more than 10 seconds.
Operational Hours	Required 24 hours a day, every day.
Significant Outage	More than five minutes of downtime is considered significant at any time and requires an ANR to be sent out to the appropriate teams.
Outage Impact	Interruption of service may result in severe financial, regulatory, patient safety, patient health, or other business issues.
Scheduled Maintenance	Maintenance, including maintenance of externally developed software incorporated into the IAM system, is scheduled during off-peak hours (evenings and weekends) or in conjunction with relevant maintenance schedules.

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

2.5.4. Overview of the Technical Requirements

Placeholder for RTM from RTC

2.5.5. Overview of the Security or Privacy Requirements

Per Section 2.12 of the AcS 2.0 Increment 5 RSD, the security specifications include the following:

- AcS is deployed inside the VA firewall.
- AcS conforms to the VA security standards detailed in VA Handbook 6500 Information Security Program.
- Designated ports are opened between systems. All other ports are blocked to provide secure server-to-server communication.
- The Hypertext Transfer Protocol Secure (HTTPS) communication protocol is used for outbound and inbound traffic for external-facing applications.
- AcS communication channels are TLS/Secure Sockets Layer (SSL)-enabled and -encrypted.
- The AcS data layer is within the internal firewall zone to provide security of the data.
- AcS meets all Veterans Health Administration (VHA) security, privacy, and identity management requirements and those listed in VA Handbook 6500 (Enterprise Requirements Appendix).
- AcS databases, user information stores, and information tied to individuals are secured and/or encrypted while at rest and in motion.
- Access to the administrative, management, and internal user interfaces of the authorization service is controlled through the use of SSOi.
- The system must store and transmit Personally Identifiable Information (PII) or sensitive information such as passwords in an encrypted or one-way hashed format and on the SSL channel.
- The web servers providing access to VA applications for external users over the Internet must reside in the demilitarized zone (DMZ).

2.5.6. Overview of System Criticality and High Availability Requirements

The VA AcS infrastructure supports critical business systems. The current availability requirement for mission critical systems is 99.9%. The current data centers support 99.6% availability. The Production, Preproduction, and Disaster Recovery (DR) Data Center is hosted by Terremark in Culpeper, Virginia and Miami, Florida. Terremark does not currently support an active/active geographic failover and load balancing thus failover to the DR site could take between one (1) and eight (8) hours. To mitigate the risk of not having a complete site failover, the AcS production infrastructure is intended to be scalable with limited single points of failure. The primary production platform is virtualized with a physical servers dedicated to Oracle RAC and VDS.

The DR site is contingency site that will resume data center operations in the event of a site failure. Load balancing, fault tolerance, backups and archiving, is a function of the hosting facility, Terremark and the data center operations team. Backups are described more fully in the [Production Operations Manual \(POM\)](#), but essentially are the following:

- Full backups are taken of virtual machines on a weekly basis
- Backups of virtual machines must be transported off-site at least monthly
- Backups of specific databases will be taken daily between the hours of 2 a.m. and 5 a.m. Locations of the databases will be provided in the POM.

2.5.7. Single Sign-on Requirement

CA Single Sign-On: The product must be configured to run in FIPS only mode in order to satisfy FIPS140-2 requirements. IP is currently integrated with SSOi to enable user authentication.

2.5.8. Requirement for Use of Enterprise Portals

N/A

2.5.9. Special Device Requirements

N/A

2.6. Legacy System Retirement

This section is not applicable as no legacy systems are being retired as a result of the IP solution implementation.

3. Conceptual Design

This section of the SDD provides details about the following topics:

- Conceptual Application Design
- Conceptual Data Design
- Conceptual Infrastructure Design

3.1. Conceptual Application Design

3.1.1. Application Context

This section provides context for each of the activities developed for IP.

IP is an activity that supports the Access Services Solution. Figure 2 below depicts the high-level interactions between the various activities, including interactions between AcS, with other VA applications, and to internal/external business partner applications.

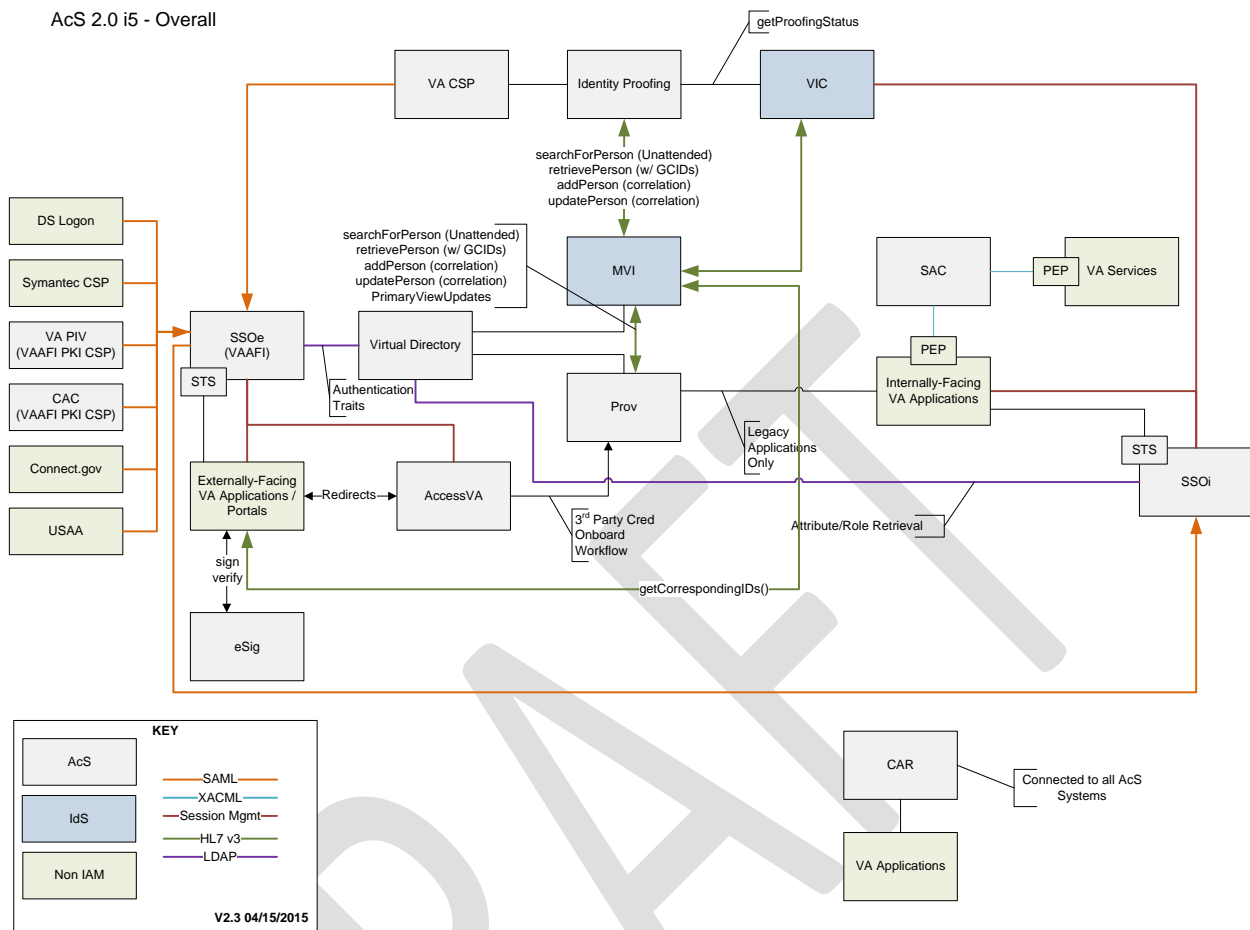


Figure 2: AcS 2.0 Overview

The IP solution activities is described in greater detail below.

An Identity Proofing service verifies proofed subject's identity (-ies) in order to establish a level of assurance of the claim that the subject is indeed who they represent themselves to be before the Identity Proofing official.

Identity proofing processes used by Government and commercial entities to establish the required level of assurance vary widely based on the target subject population, purpose of the resulting identity proofed record, etc. A common goal for each one of these identity proofing processes is to allow the enterprise to comply with legal, regulatory and due diligence requirements based on one or more of the following references FIPS 201¹, HSPD-12², OMB A-

¹ <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

² <https://www.dhs.gov/homeland-security-presidential-directive-12>

130, Appendix I³, VA Information Security Policies and Directives (e.g. VA Handbook 6500, Appendix F), NIST SP800-63⁴, and others, before the enterprise can interact with the subject, do business transactions or issue credential(s) and/or account(s) to said subject.

The identity proofing processes are based on historical and transaction information aggregated from public and proprietary data sources. Identity Proofing services can also be used as an additional interactive user authentication method for high risk transactions, such as accessing sensitive confidential or third party's personally identifiable information⁵. Identity-proofing services are classified as in-person, remote or hybrid.

The following table, as defined in OMB M04-04⁶ is referenced to the NIST SP800-63 Identity proofing processes and drives their scope and extensiveness.

Table 13 Potential Impact Categories for Authentication Errors

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod, High
Civil or criminal violations	N/A	Low	Mod	High

At the Department of VA, the Identity Proofing processes are used for establishing the validity of a claim for authorization to VA applications, resources or benefits.

The IP component capabilities allow for multitude of identity proofing processes to be defined as business needs dictate and be built to suit a specific purpose.

³ http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

⁴ <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

⁵ <http://www.gartner.com/it-glossary/identity-proofing-services>

⁶ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>

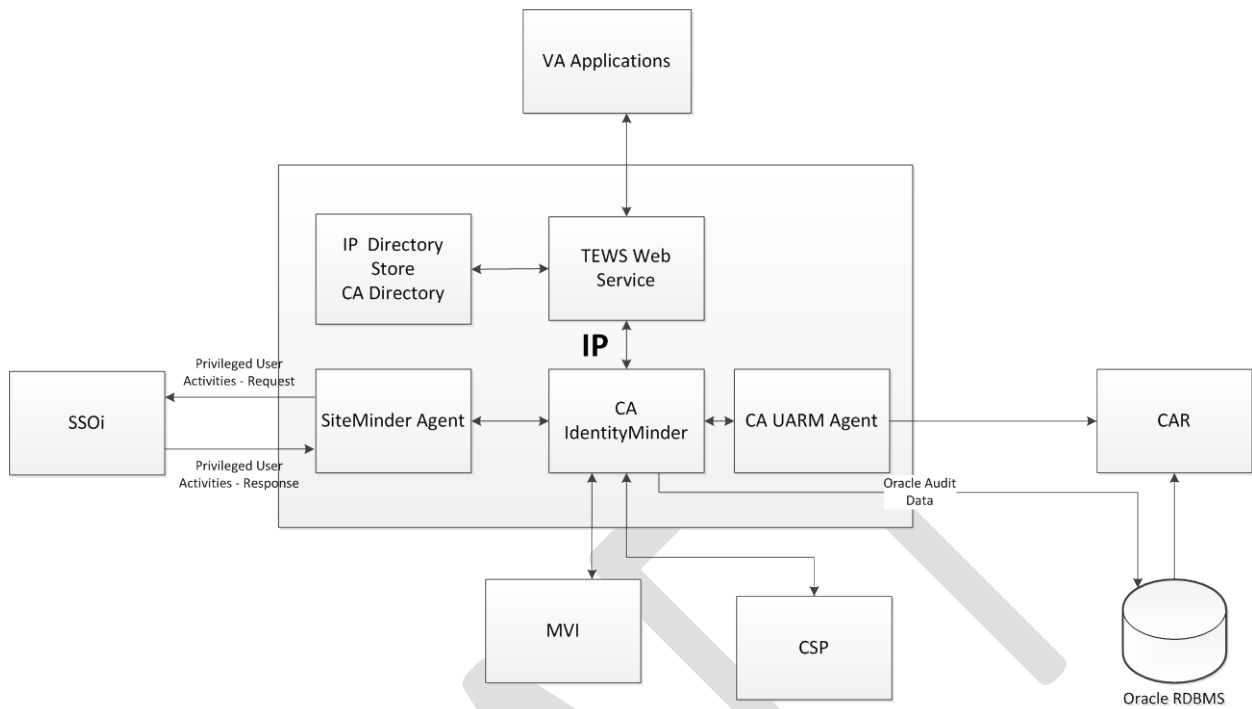


Figure 1: IP Context Diagram

ID	Interface Name	Input Messages	Output Messages	External Party
1	CSP – IP	SOAP over HTTPs	SOAP over HTTPs	Veteran
2	Business Applications –IP	SOAP over HTTPs	SOAP over HTTPs	Business Applications
3	MVI record interface-IP	SOAP over HTTP	SOAP over HTTP	MVI
4	SSOi-IP	Kerberos/SPNEGO	Kerberos/SPNEGO	SSOi
5	Provisioning-IP	LDAPS	LDAPS	Privileged IP users

Table 14: (Grouping): Application Context Description

3.1.2.High-Level Application Design

Figure 2 below provides a high-level application design for the IP and identifies the major AcS activities and/or relationships with VA applications.

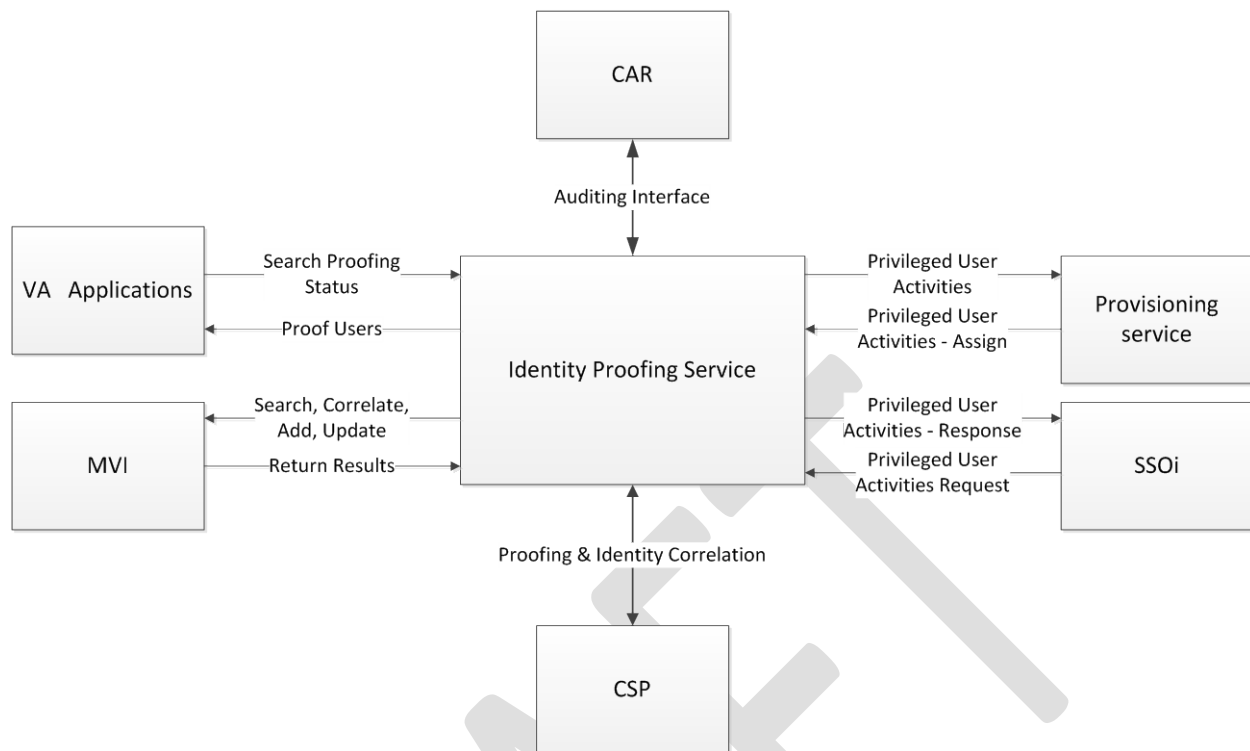


Figure 4: IP High-Level Application Design

The following table provides high-level description for each of the AcS activities. The external interfaces are interfaces for systems outside of VA and internal interfaces are interfaces for systems within VA.

Table 13: Activities in the High-Level Application Design

ID	Name	Description	Service or Legacy Code	External Interface Name	Internal Interface Name
1	CSP	CSP provides external user's credentials to VA applications that are not eligible for another VA approved credential.	Service	Self Service and Registration	VAAFI, IP, CAR
2	IP	IP facilitates evaluating and validating a user's identity to be true and unique to the degree (level) of confidence required by VA.	Service	N/A	MVI, CSP, CAR

ID	Name	Description	Service or Legacy Code	External Interface Name	Internal Interface Name
4	SSOi	SSOi provides the desktop sign-on capability to internal VA users. SSOi also provides authentication and access to VA business applications for both internal and external user populations. External credentials are brokered by the VAAFI service and are a federated partner with SSOi.	Service	Federation	AD, IP, CSP, Provisioning, SAC
5	VHIC	Application that relies on IP for Proofing Services	Service	N/A	VHIC.IP.MVI
6	MVI	Authoritative Source for Person data within the VA	Service	MVI	IAM,VHA, VBA, DoD

3.1.3.Application Locations

The following table lists the application components and their locations where they will be hosted.

Table 15 : IP Solution Application Locations

Application Component	AcS Service	Description	Location of Component
IIS Web Server	IP	Front end web server providing the administrative and self-service interface to CA IdentityMinder	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
Oracle WebLogic	IP	Application server hosting CA IdentityMinder, Provisioning Server, SiteMinder and federation.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
CA IdentityMinder	IP	CA IdentityMinder delivers a unified solution for user provisioning that manages users' identities throughout their entire lifecycle, providing them with timely, appropriate access to applications and data.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)

Application Component	AcS Service	Description	Location of Component
CA Directory	IP	LDAP directory to support CA SiteMinder, CA SSO and CA IdentityMinder backend configuration and data store.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
Oracle Database	IP	Database to support CA IdentityMinder and audit logs from different components.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
Report Server	IP	Report server for CA SiteMinder and CA IdentityMinder	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)

3.1.4.Application Users

The following table lists the user who will interact with the IP solution activities:

Table 16 : IP Solution Users

Application Component	Description	User
IP	Performs administrative functions including controlling Identity Minder related configurations and tasks and managing the proofing registration interfaces	IP Administrator
IP	Responsible for Identity Proofing users confirming identity of applicant to comply with SP 800-63 and VA 6501	Identity Proofers

3.2. Conceptual Data Design

The IP data model is designed to provide a schema that covers the data attributes necessary to meet the functional requirements, as well as provisions for the security of sensitive data types. The IP data model design leverages the default schema of the CA Directory, and provides specific extension to the default scheme to meet the specific requirements for ID proofing.

3.2.1.Project Conceptual Data Model

The conceptual data model for the IP contains known entities required to persist user and administrator information to fulfill IP Level 1 and Level 2 credentialing requirements. The following diagram represents the conceptual data design separated by the major data categories that make up the total data schema:

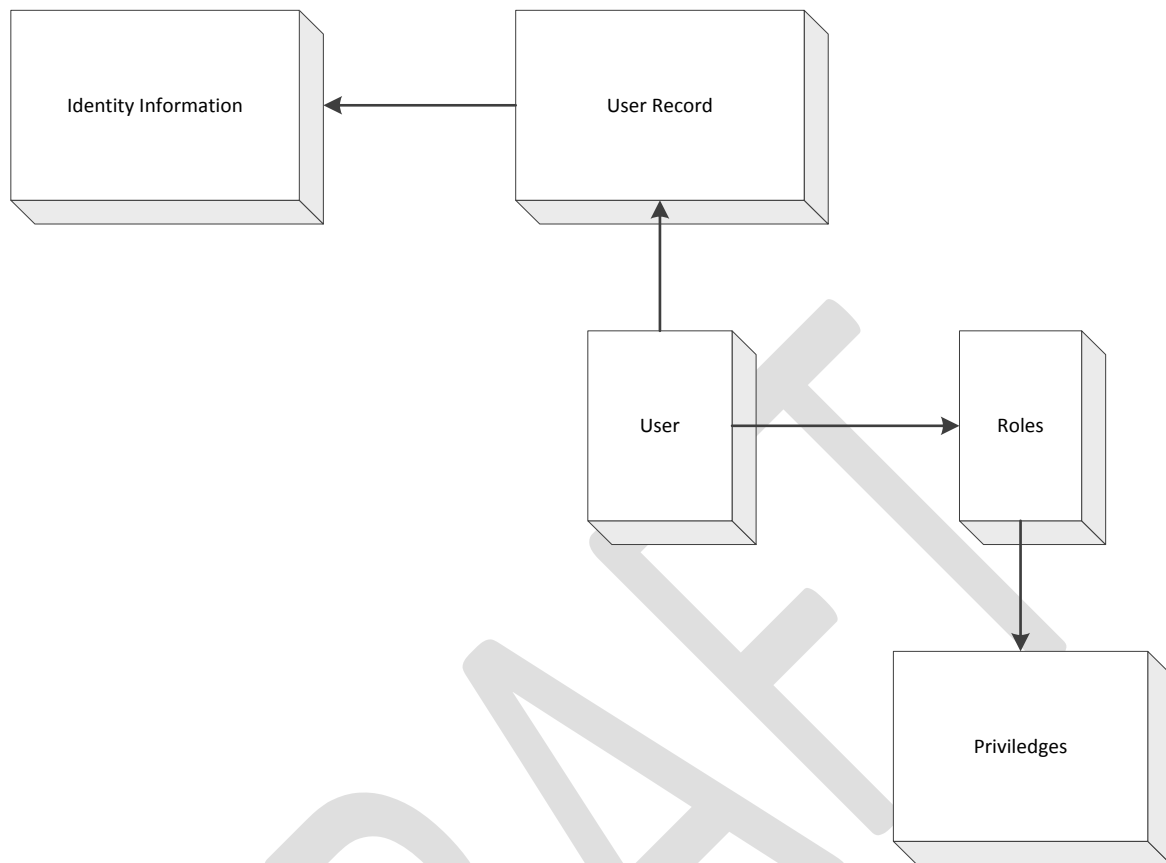


Figure 5: IP Solution Conceptual Data Model

Table 17 Conceptual Data Model Description

Identifier	Description
User	Entity that represents a user that has completed registration or has been manually added by an administrator.
User Record	Management information stored about the user.
Identity Information	Demographic and identity-specific information stored about the user.
Roles	Assignment of a Role provides a set of Privileges for specific user.
Privileges	Fine grained entitlements that grant access to specific objects with the IP.

Table 18 : Database Inventory

Ref	Object	Description	Input Relationship	Output Relationship
①	Identity (Person)	The Identity object is a set of attributes that define an identity in the VA. Identity traits are correlated and a secure identifier is assigned.	<ul style="list-style-type: none"> - One Identity 	<ul style="list-style-type: none"> - One Identity can be assigned to 0 or more Roles. - One Identity can own 0 or more Accounts. - One Identity has only one security identifier for the lifetime of the identity.
②	User (Account)	The User (Account) attributes define the login information associated with the access control for a managed resource as well as information deemed necessary to perform the business processes or data synchronization requirements.	<ul style="list-style-type: none"> - One Account is owned by 0 (means orphan account) or one Identity (the base identity to which other accounts are linked). 	<ul style="list-style-type: none"> - A user account is represented by a credential which is used for authorization and access to Services. - Account operations (add, modify, change password, suspend, restore, delete, etc.) follow one or more workflows.
③	Role	The Role attributes defines the role and the associated privileges that can be assigned to a user.	<ul style="list-style-type: none"> - One Identity can be assigned 0 or more Roles. 	<ul style="list-style-type: none"> - One Role can be members of 0 or more Provisioning Policies. - One Role can participate in 0 or more Entitlement Workflows.

Ref	Object	Description	Input Relationship	Output Relationship
④	Provisioning Policy	The Provisioning Policy object is a definition of the level of access that may be granted to a managed resource or service to particular membership(s) or Roles. The provisioning policy defines identity reconciliation and identity feed.	<ul style="list-style-type: none"> - One Role can be assigned to 0 or more Provisioning Policies. - Each Provisioning Policy may have 0 or more Roles. 	<ul style="list-style-type: none"> - One Provisioning Policy may define 1 or more Entitlements.
⑤	Entitlement	The Entitlement object is a part of the Provisioning Policy that contains the service targets and associated provisioning parameters.	<ul style="list-style-type: none"> - One Provisioning Policy may have 1 or more Entitlements. 	<ul style="list-style-type: none"> - One Entitlement can apply to 0 or more Services. It may also apply to a type of service or all services. - One Entitlement can start 0 or 1 Workflows to govern the creation or modification of accounts on an associated service.
⑥	Workflow	The Workflow object represents a business process that is associated with an action or a policy. A workflow implements the steps that are required to approve or reject a request, such as a request to provision a person with a new account.	<ul style="list-style-type: none"> - 0 or 1 Workflow can be started by 0 or more Entitlements. - 0 or more Roles can participate in workflows. - 1 or more Workflows can be started by Identity operations. - 1 or more Workflows can be started by Account operations. 	

Ref	Object	Description	Input Relationship	Output Relationship
⑦	Service	The Service object is a set of parameters that define a managed resource and associated workflows.	<ul style="list-style-type: none"> - 0 or more Services can be assigned to one or more Entitlements. - Accounts control access to services. - Services can be affected by 1 Identity Policy. - Each Service can be affected by 0 or more password policies. 	
⑧	User Policy	The User Policy contains the rules by which a user's account is created on a managed resource.		<ul style="list-style-type: none"> - One user policy can be applied to 0 or more Services.
⑨	Password Policy	The Password Policy object sets rules that passwords must meet.		<ul style="list-style-type: none"> - One password policy can be applied to 0 or more Services.

3.2.2.Database Information

Table 19 : Database Inventory

Database Name	Description	Type	Steward
CA IdentityMinder – Object Schema	Stores object definitions which are required for CA IdentityMinder. This store is for internal use only. Passwords are encrypted. The database is used by Provisioning, CSP and IP services with their corresponding instances.	Create / Replace / Interface / Modify	VRM AcS 2.0
CA IdentityMinder – Task Persistence Schema	Stores runtime tasks and in-process tasks (task sessions). Also includes Scheduler information. This store is for internal use only. The database is used by IP services with their corresponding instances.	Create / Replace / Interface / Modify	VRM AcS 2.0

Database Name	Description	Type	Steward
CA IdentityMinder – Reporting Schema	Stores snapshot data, which reflects the current state of objects in CA IdentityMinder at the time the snapshot is taken. Reports can be generated from this information to view the relationship between objects, such as users and roles. The database is used by IP services with their corresponding instances.	Create / Replace / Interface / Modify	VRM AcS 2.0
CA IdentityMinder – Task Persistence Archive Schema	Stores runtime task archives. This store is for internal use only. The database is used by IP services with their corresponding instances.	Create / Replace / Interface / Modify	VRM AcS 2.0
CA IdentityMinder – Audit Schema	Provides a historical record of operations that occur in CA IdentityMinder. The database is used by IP services with their corresponding instances.	Create / Replace / Interface / Modify	VRM AcS 2.0

Database Name	Description	Type	Steward
CA SiteMinder – Audit	Provides a historical record of operations that occur in Site Minder, and Reports are generated from of this data. The database is used by SSOi service to store its audit data.	Create / Replace / Interface / Modify	VRM AcS 2.0

3.2.3. User Interface Data Mapping

This section describes and defines the data that will be available for users of the IP solution via the user interfaces and stored / retrieved from the database, if applicable. Out-of-the-box screens are not shown.

User store schema within CA Directory is customized to store registered user record information (refer to section A below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions). The data dictionary for account and feed object attributes are covered as part of the **VAProvPerson** object class attributes (refer to Provisioning in section A).

3.2.3.1. Application Screen Interface

3.2.3.1.1. User Profile

Table 20: User Profile Screen Mapping

Graphical User Interface (GUI) Field	Field (Field in Schema that the GUI field connects to)	Comments
First Name	givenName	First Name
Last Name	sn	Last Name
Date of Birth (Age)	VADOB	Date of birth
User ID	uid	User ID
Phone Number	telephoneNumber	Business Phone
Street Address	VAPROOFEDADDRESS	Proofed Address
City	VAPROOFEDCITY	Proofed City
State	VAPROOFEDSTATE	Proofed State
Country	VAPROOFEDCOUNTRY	Proofed Country
Postal Code	VAPROOFEDPOSTALCODE	Proofed Postal Code
Email	mail	mail
Affiliation	VAAFFILIATION	VA Affiliation of User
Proofing Station	VAIPREQSOURCE	IP Source
Proofing Location	VAIDPROOFLOC	ID Proofer location

3.2.3.1.2. Address Verification

Table 21 : Address Verification Screen Mapping

Graphical User Interface (GUI) Field	Field (Field in Schema that the GUI field connects to)	Comments
Address Validation Type	VAADDRESSVALIDMETHOD	Address Validation method
Postmark Date	VAPOSTMARKDATE	Postmark Date
Street Address	VAPROOFEDADDRESS	Proofed Address
City	VAPROOFEDCITY	Proofed City
State	VAPROOFEDSTATE	Proofed State
Country	VAPROOFEDCOUNTRY	Proofed Country
Postal Code	VAPROOFEDPOSTALCODE	Proofed Postal Code

3.2.3.1.3. Primary Verification

Table 22 : Primary Verification Screen Mapping

Graphical User Interface (GUI) Field	Field (Field in Schema that the GUI field connects to)	Comments
ID Type	VASECGOVIDTYPE	Primary Government PID type
Country of Issuance	VAPRIGOVPIDCOUNTRY	Primary Government PID country
State of Issuance	VAPROOFEDSTATE	Proofed State
Identification Number	VASECGOVIDNUMBER	Primary Government PID number
Expiration Date	VASECGOVIDEXPDATE	Primary Government PID exp date
Information Provided/Verified By	VAIDPROOFER	ID Proofer name

3.2.3.1.4.

Secondary Verification

Table 23 : Secondary Verification Screen Mapping

Graphical User Interface (GUI) Field	Field (Field in Schema that the GUI field connects to)	Comments
ID Type	VASECGOVIDTYPE	Primary Government PID type
Country of Issuance	VAPRIGOVPIDCOUNTRY	Primary Government PID country
State of Issuance	VAPROOFEDSTATE	Proofed State
Identification Number	VASECGOVIDNUMBER	Primary Government PID number
Expiration Date	VASECGOVIDEXPDATE	Primary Government PID exp date
Information Provided/Verified By	VAIDPROOFER	ID Proofer name

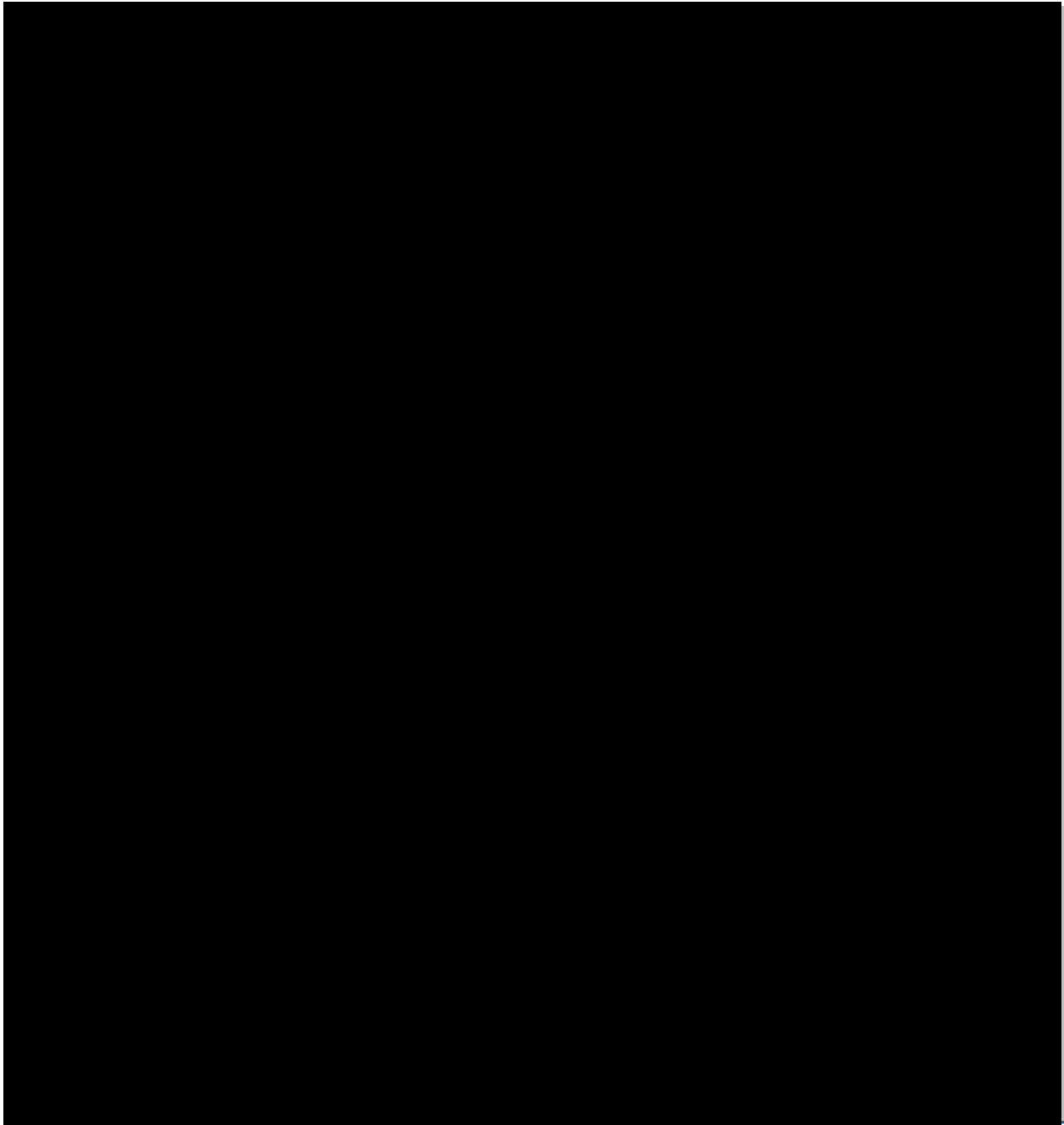
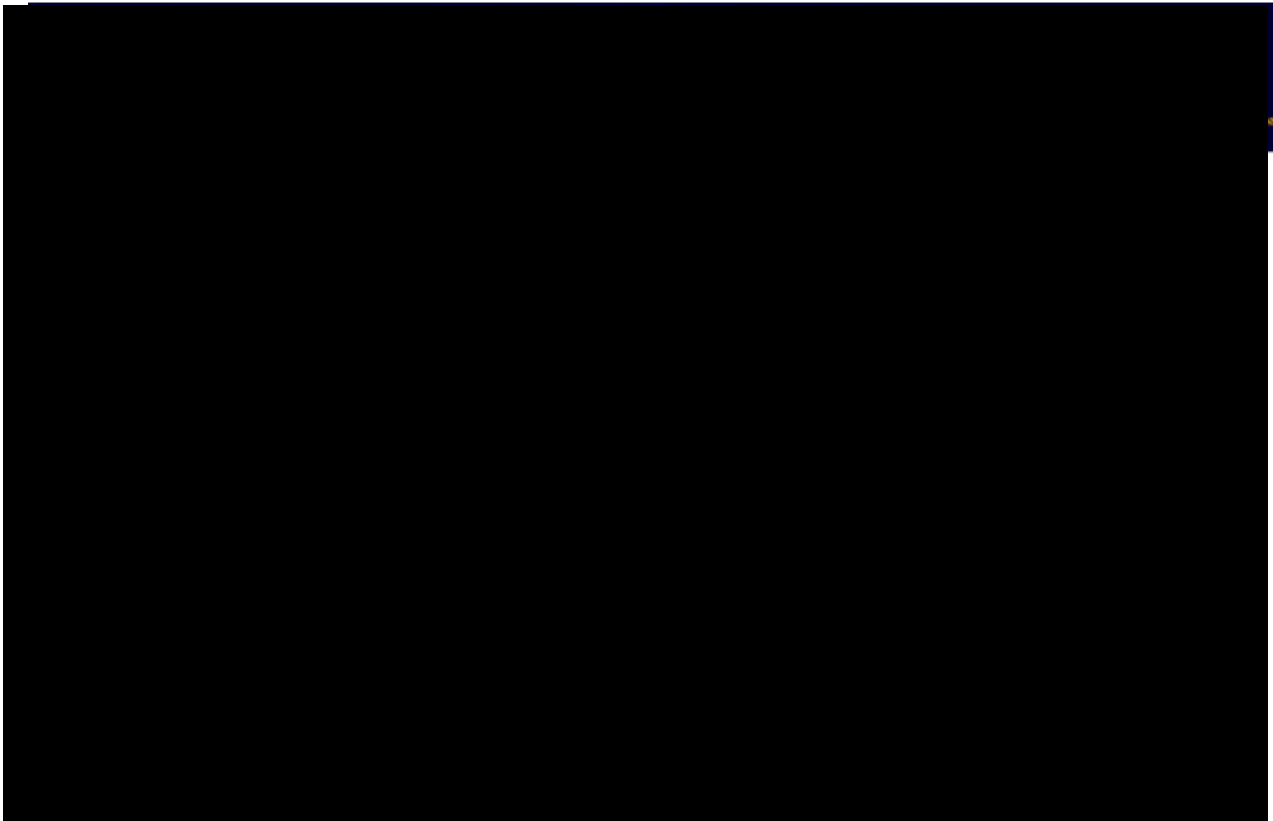


Figure 6: Identity Proof User: Step 1 User Profile

Refer to section below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.1.4.1. Step 2 Address Verification

The following screen, captures the address information of the candidate being identity proofed.



[VA Home](#) | [Privacy](#) | [FOIA](#) | [Regulations](#) | [Web Policies](#) | [No FEAR Act](#) | [Site Index](#) | [USA.gov](#) | [White House](#) | [National Resource Directory](#) | [Inspector General](#)
U.S. Department of Veterans Affairs - 810 Vermont Avenue, NW - Washington, DC 20420
Reviewed/Updated Date: May 11, 2012

Figure 7: Identity Proof User: Step 2 Address Verification

Refer to section below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.1.4.2. Step 3 Primary Identification

The following screen, captures the primary identification information of the candidate being identity proofed.

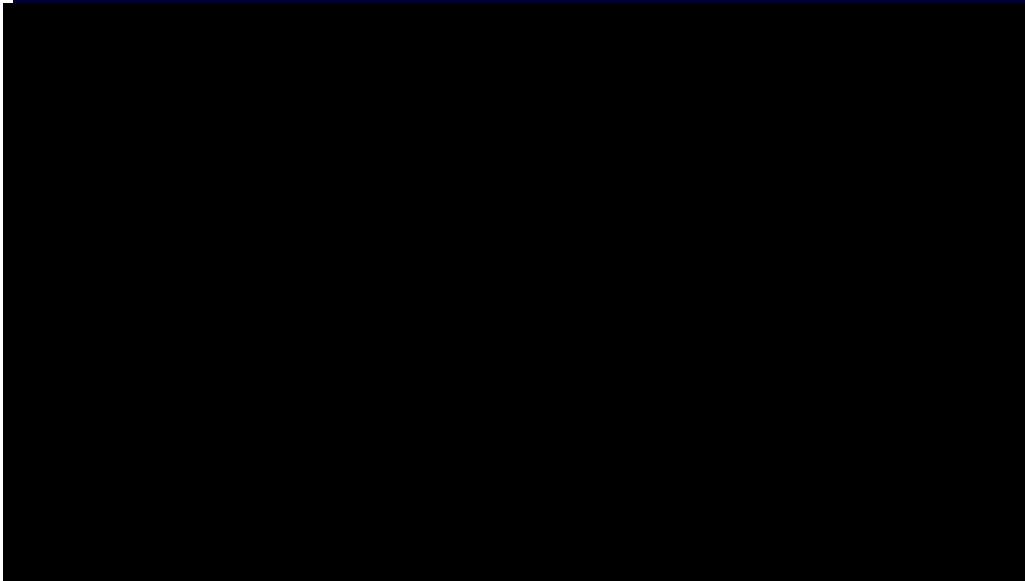


Figure 8: Identity Proof User: Step 3 Primary Verification

Refer to section below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.1.4.3. Step 4 Secondary Identification

The following screen, captures the secondary identification information of the candidate being identity proofed.

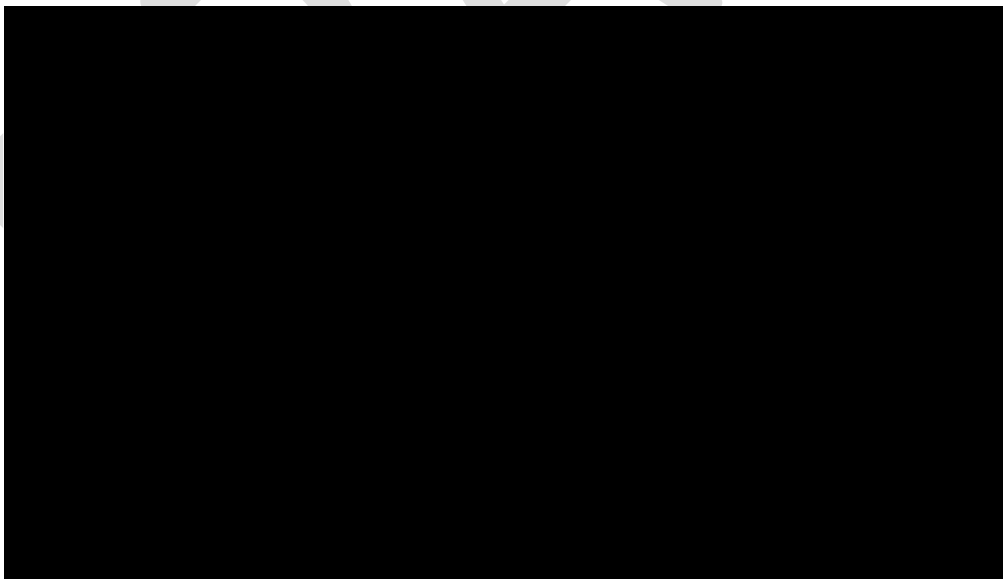


Figure 9: Identity Proof User: Step 4 Secondary Identification

Refer to section below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.1.5. Update a User

3.2.3.1.5.1. Step 1 User Profile

The following screen captures the user information when updating a user

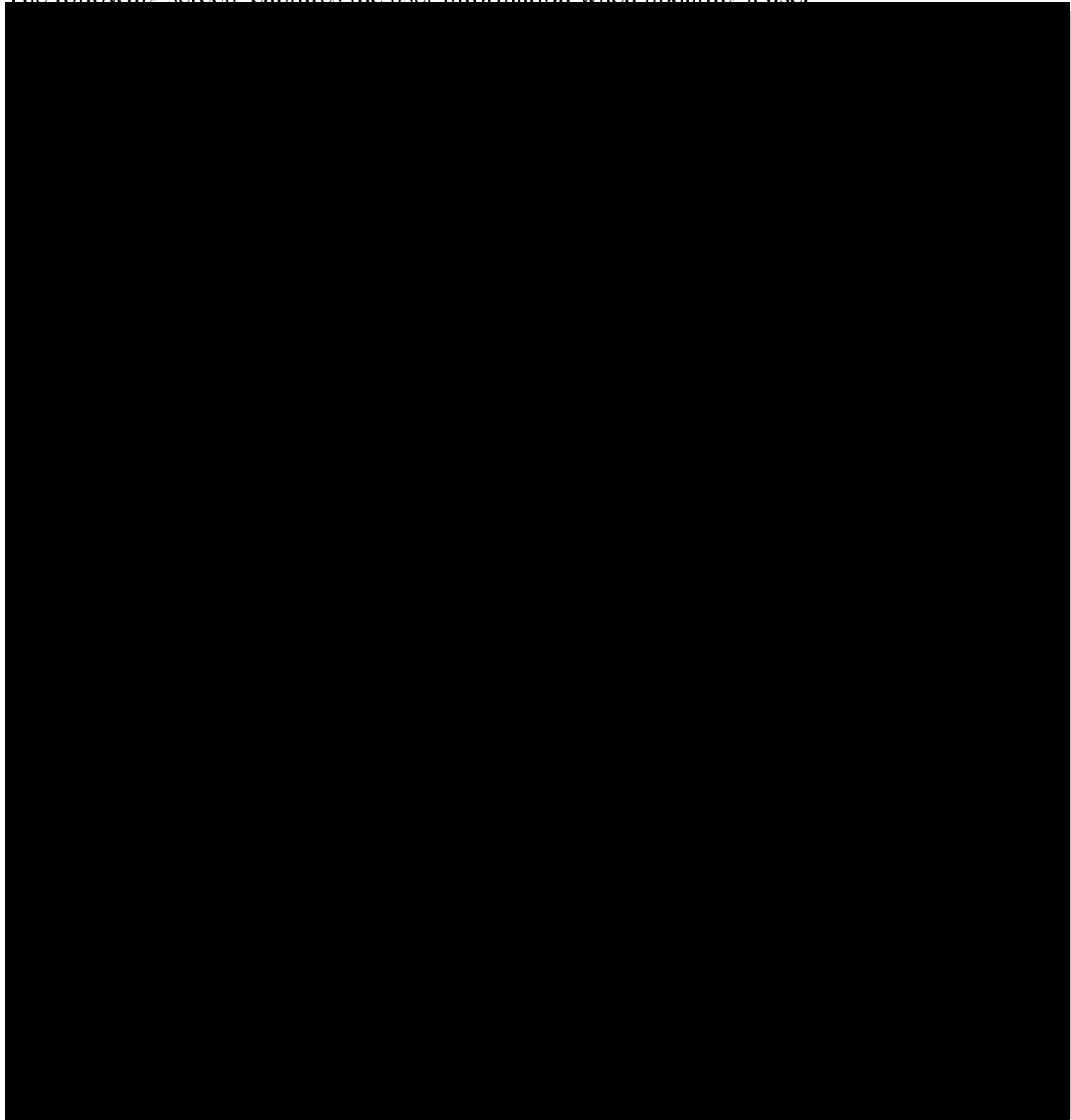


Figure 10: Update a User: Step 1 User Profile

Refer to section below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.1.5.2. Step 2 Address Verification

The following screen, captures the address information when updating a user.

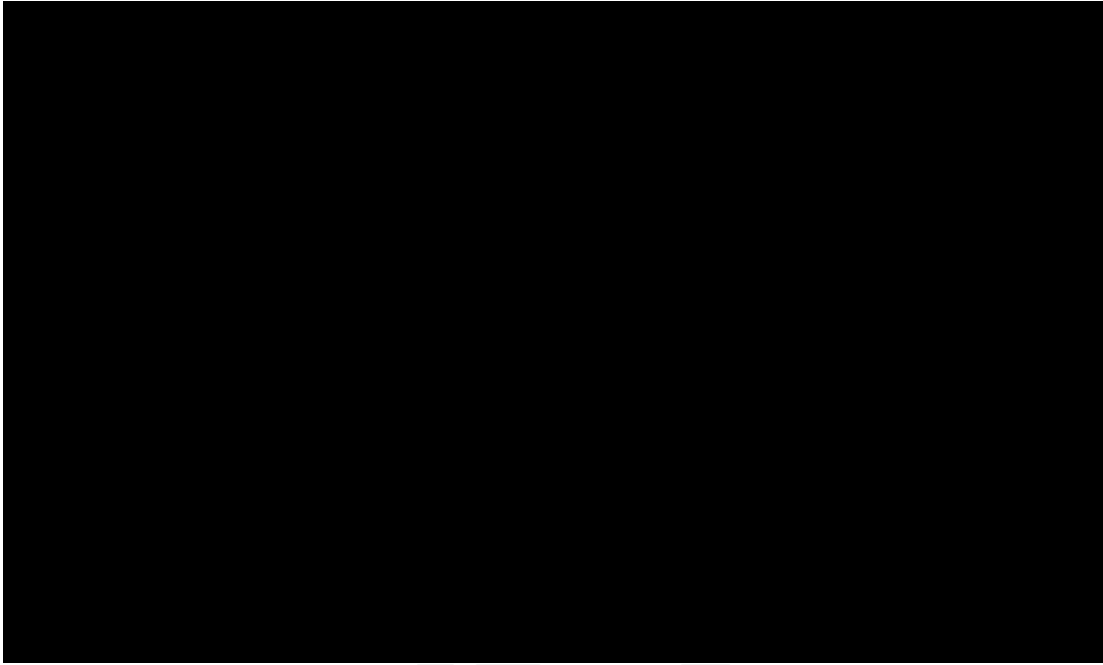


Figure 11: Update a User: Step 2 Address Verification

Refer section below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.1.5.3. Step 3 Primary Identification

The following screen, captures the primary identification information of the candidate being updated.

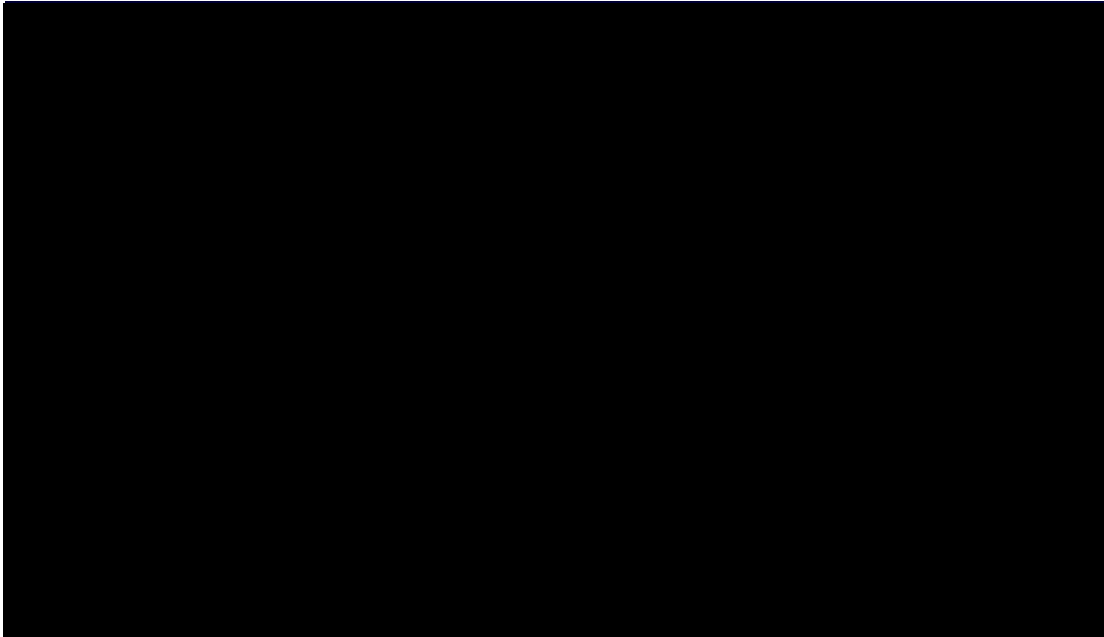


Figure 12: Update a User: Step 3 Primary Identification

Refer to section below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.1.5.4. Step 4 Secondary Identification

The following screen, captures the secondary identification information of the candidate being updated.

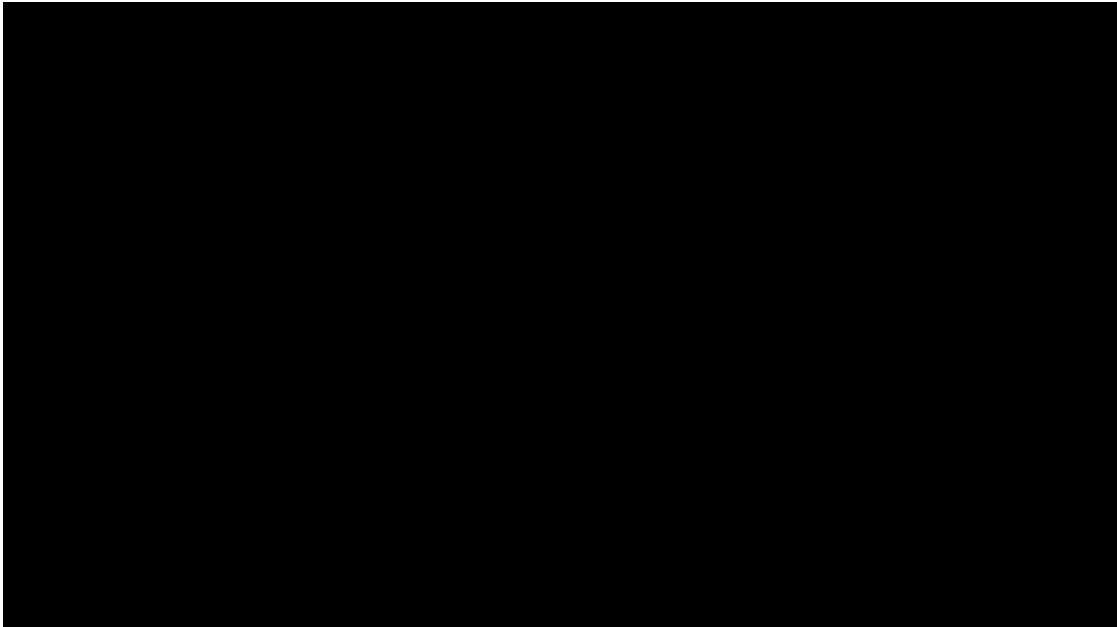


Figure 13: Update a User: Step 4 Secondary Identification

Refer to section below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.2. Application Report Interface

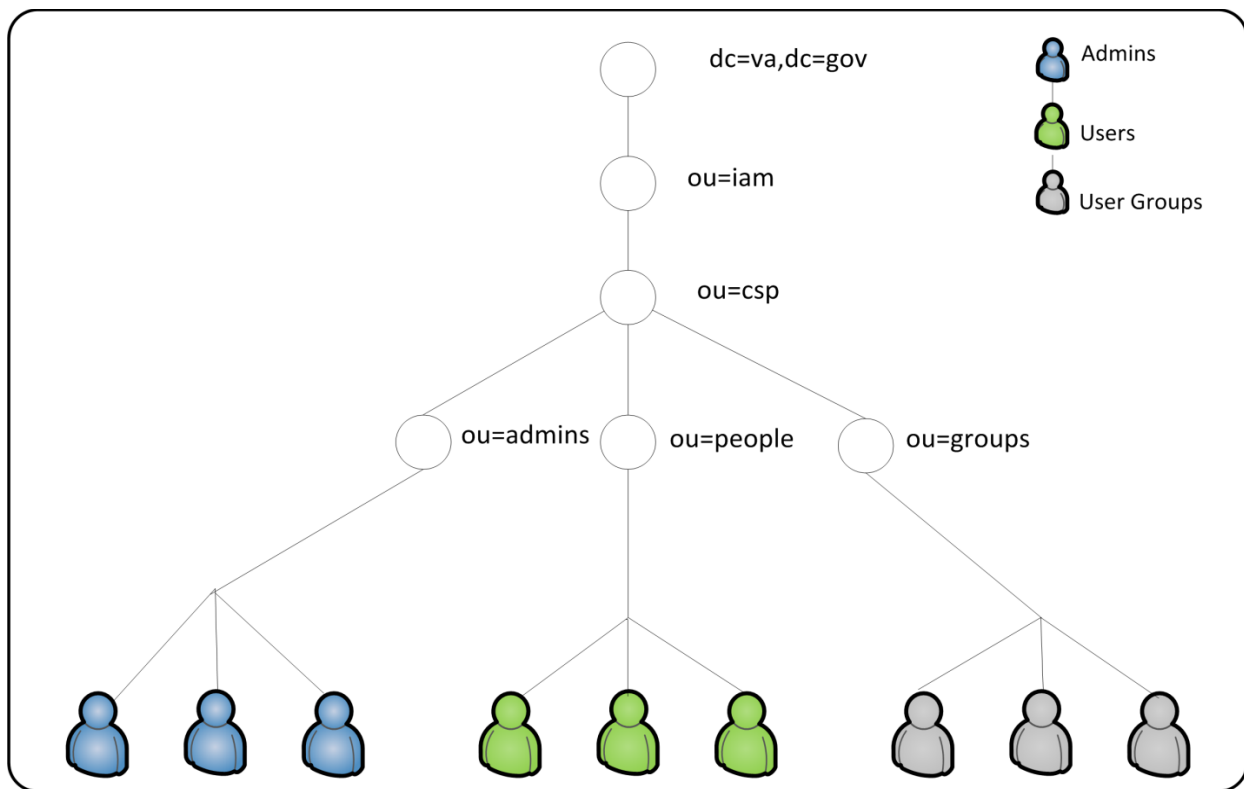
IP is integrated with the CAR solution. Please refer to the CAR SDD for further details

3.2.3.3. Unmapped Data Element

Refer to IP Data Elements below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions.

Type	Attribute Name	Description	Object Class
Identity Information	cn	FullName	inetOrg
	givenName	First Name	inetOrg
	initials	initials	inetOrg
	sn	Last Name	inetOrg
	uid	User ID	inetOrg
User Information	userPassword	Password	inetOrg
	mail	mail	inetOrg
	telephoneNumber	Business Phone	inetOrg
	c	Country	country
Access Control Attributes	VAACCESSROLES	Admin Roles Admin (IdM)	VAPerson

IP Information	VAACCESSROLESADMIN	Access Roles Admin (IdM)	VAPerson
	VAADMINROLES	Used as a constraint for IM admin roles	VAPerson
	VAADMINROLESADMIN	Admin Roles Admin (IdM)	VAPerson
	VAAFFILIATION	VA Affiliation of User	VAPerson
	VAASSURANCELEVEL	Assurance Level	VAPerson
	VADOB	Date of birth	VAPerson
	VAGENDER	Gender	VAPerson
	VAICN	Patient's ICN from MVI	VAPerson
	VAIDENTITYPOLICY	Used by identity policy synch	VAPerson
	VAIDPROOFDATE	Identity Proof Date	VAPerson
	VAIDPROOFER	ID Proofer name	VAPerson
	VAIDPROOFINGCOMMENT	ID Proofing Status Comments	VAPerson
	VAIDPROOFLOC	ID Proofer location	VAPerson
	VAPOSTMARKDATE	Postmark Date	VAPerson
	VAPRIGOVPIDCOUNTRY	Primary Government PID country	VAPerson
	VAPRIGOVPIDEXPDATE	Primary Government PID exp date	VAPerson
	VAPRIGOVPIDNUMBER	Primary Government PID number	VAPerson
	VAPRIGOVPIDSTATE	Primary Government PID status	VAPerson
	VAPRIGOVPIDTYPE	Primary Government PID type	VAPerson
	VAPRIPROFEXPDATE	Primary Profile Information Type	VAPerson
	VAPROOFEDADDRESS	Proofed Address	VAPerson
	VAPROOFEDCITY	Proofed City	VAPerson
	VAPROOFEDCOUNTRY	Proofed Country	VAPerson
	VAPROOFEDPOSTALCODE	Proofed Postal Code	VAPerson
	VAPROOFEDSTATE	Proofed State	VAPerson
	VAIPREQSOURCE	IP Source	VAPerson
	VAREGDATE	Credential Registration Date	VAPerson
	VASECGOVIDCOUNTRY	Secondary Government ID country	VAPerson
	VASECGOVIDEXPDATE	Primary Government PID exp date	VAPerson
	VASECGOVIDNUMBER	Primary Government PID number	VAPerson
	VASECGOVIDSTATE	Primary Government PID status	VAPerson
	VASECGOVIDTYPE	Primary Government PID type	VAPerson
	VASECPROFEXPDATE	Primary Profile Information Type	VAPerson
	VAADDRESSVALIDMETHOD	Address Validation method	VAPerson



3.3. Conceptual Infrastructure Design

The section provides a conceptual design of the infrastructure needed for the core capabilities of the IP. The section focuses on the primary environments and locations where the IP Services are installed. The information is provided as preliminary design and is elaborated in later detailed design section. The IP system architecture structure is designed to be flexible and scalable to support emerging/future VA requirements, such as MVI Registration, and Remote Proofing. Based on emerging requirements, the system architecture may need to support a variety of business flow scenarios through the use of the CA Identity Manager component.

The IP system is the aggregate of a number of components that interact to form the basic structure of the IP application. By coordinating the components, IP provides a secure interface for users to self-register, perform ID proofing activities, authenticate and provide SAML assertions to VAAFI for federated access to VA systems, and for administrators to monitor and manage the IP application and users. The following set of products forms the basis for the system architecture.

3.3.1. System Criticality and High Availability

The VA AcS infrastructure supports critical business systems. The current availability requirement for mission critical systems is 99.9%. The current data centers support 99.6% availability. The Production, Preproduction, and Disaster Recovery (DR) Data Center is hosted by Terremark in Culpeper, Virginia and Miami, Florida. Terremark does not currently support an active/active geographic failover and load balancing thus failover to the DR site could take

between one (1) and eight (8) hours. To mitigate the risk of not having a complete site failover, the AcS production infrastructure is intended to be scalable with limited single points of failure. The primary production platform is virtualized with a physical servers dedicated to Oracle RAC and VDS.

The DR site is contingency site that will resume data center operations in the event of a site failure. Load balancing, fault tolerance, backups and archiving, is a function of the hosting facility, Terremark and the data center operations team. Backups are described more fully in the [Production Operations Manual \(POM\)](#), but essentially are the following:

- Full backups are taken of virtual machines on a weekly basis
- Backups of virtual machines must be transported off-site at least monthly
- Backups of specific databases will be taken daily between the hours of 2 a.m. and 5 a.m. Locations of the databases will be provided in the POM

3.3.2.Special Technology

Table 24 : Special Technology Requirements

Special Technology	Description	Notional Location	TRM Status
WebSphere DataPower XI52	DataPower provides the needed WebService capabilities to VAAFI and to AcS.	All	Yes

3.3.3.Technology Locations

The high-level conceptual infrastructure diagram for the VA IP infrastructure is shown in Figure 14 below. The diagram also depicts the communication between the Terremark data centers in Culpeper, Virginia and Miami, Florida. The VA AcS infrastructure environment is set up at the Terremark data center in Culpeper, Virginia. The alternate site or disaster recovery site for VA AcS operations is the Terremark data center in Miami, Florida.

Being Developed

Figure 14: IP Production Environments

Development Environment (DEV) AITC – Austin, TX

- This environment is utilized by the Development team for initial development of service enhancements, integrations with consuming applications, defect resolution, and unit testing.
- This is a loosely controlled environment for the AcS developers to use. The development team implements and maintains the COTS products, COTS patches, and code.
- System administrators maintain the operating systems and operating system patches.
- Code and configuration is stored in Subversion source control and exported as a build when moving to the next environment.
- The initial setup instructions are fine-tuned; the migration instructions are provided to migrate the code and configuration to the subsequent environments.

Software Quality Assurance (SQA) AITC – Austin, TX

- This environment is utilized by the Development team for integration testing, load, configuration, and quality tests.
- System Administrators install, configure, and operate applications as testing is performed.
- This is a tightly controlled environment and closely resembles the Production architecture. Issues with performance or the setup instructions are performed between Developers and the Administrators responsible for the environment.
- The setup instructions are fine-tuned.

Pre-Production – Terremark Culpeper, VA

- The User Acceptance Test (UAT) for the AcS is performed in this environment.
- This is where performance testing occurs.
- System Administrators install, configure, and operate applications per the fine-tuned setup instructions and provide support as testing is performed.
- Any remaining issues with performance or the setup instructions are worked out with the System Administrators.
- The setup instructions are finalized.
- This is a tightly controlled environment and is as close to identical as possible to the Production environment.

Production – Terremark Culpeper, VA

- The finalized setup instructions are installed.
- The environment is closely monitored.

Production Disaster Recovery (DR) – Terremark Miami, FL

- This site provides hot failover capability so that services and data are maintained in the event of a failure in Production.
- This environment is identical to the Production environment.
- Once the change to Production is verified, the change is implemented in the DR environment.
- The DR environment is in the Terremark Miami, FL data center. The environment is configured with an Active-Passive topology.
- The identity services components like CA IdentityMinder, CA SiteMinder, Provisioning Manager, CA report server, CA UARM would be configured to be on software load balanced on their local site.
- There will be a directory and database synchronized across a private OC-12 connection between both sites. Multiple instances of CA Directory are deployed locally at Terremark Culpeper, VA and remotely at Terremark Miami, FL data centers in a multi-write replication mode. Multi-write replication is a mechanism for replicating updates to a number of instances to maintain that the user stores are synchronized for internal and external users.

- Oracle Data Guard is utilized for database replication from the Production data center at Terremark Culpeper, VA to the disaster recovery data center at Terremark Miami, FL sending the archive logs at an incremental time span asynchronously down to as low as 1 second.

3.3.4. Conceptual Infrastructure Diagram

This section depicts the IP with many of its internal and external connections exposed. Each sub-system of the infrastructure will be described in the next sections of this document. In each section, these connections will be described and an internal breakdown of the components will also be shown.

3.3.4.1. Location of Environments and External Interfaces

Being Developed

Figure 15: Conceptual Networks and Environments

The high-level conceptual infrastructure diagram for the VA IP infrastructure is shown in Figure 16 below. The diagram also depicts the communication between the Terremark data centers in Culpeper, Virginia and Miami, Florida. The VA IP infrastructure environment is set up at the Terremark data center in Culpeper, Virginia. The alternate site or disaster recovery site for IP is the Terremark data center in Miami, Florida.

3.3.4.2. Conceptual Production String Diagram

The following diagram, provides a logical view of the IP components.

- When the military identification card is presented as a proofing document, collect an expiration date through the year 2150.

Being Developed

3.3.5. CA Identity Manager

The CA Identity Manager is an integrated identity administration solution that serves as the foundation for CSP. Identity Manager provides:

- Creation of ID Management tasks that map to specific functional requirements.
- Workflow capabilities and a host of connectors to provision and de-provision users to backend repositories such as Microsoft Active Directory.
- Access to scripts for designing the workflow processes.

3.3.6. CA SiteMinder Policy Server/Federation Security Services (FSS)

The CA SiteMinder product provides web-based access control to the IP solution. It works directly with the IDM and CA Directory to authenticate users, establish authorization decisions based on role membership, and enforcement of password policies.

The CA FSS, the IP federation engine component, is a web application that uses HTTPS protocol to administer and manage server settings and the configuration of entities and partnerships.

The CA SiteMinder and FSS services provide:

- IP Site Protection through policy based access control
- Support for IDM security model
- SAML Assertion Generator.
- Configuration Services.
- SAML and Local Authentication Schemes.
- UserID/Password & PKI Authentication Schemes
- Single-Sign-On

3.3.7.CA Directory

The CA Directory is the LDAP repository where all user information is stored. The two main standards for directories are LDAP/Secure LDAP and X.500. CA Directory fully applies X.500 and LDAP standards to provide a distributed and reliable directory service. CA Directory uses LDAP support to access LDAP-only directories, and the X.500 distributed directory model for distribution. Communication to the CA Directory is via Secure LDAP for IP.

3.3.8.Identity Manager Workflow DB, Oracle Database Server 11g

The CA Identity Manager Workflow controls tasks through workflow processes. These processes enable CA Identity Manager to complete certain tasks and store auditing and workflow for CA Identity Manager.

3.3.9.CA Report Server

The Report Server (also known as CA Business Intelligence) generates status and ad-hoc reports, using data stored in the Oracle database.

3.3.10. Microsoft IIS HTTP/HTTPS Server & SiteMinder Web Agent

The IIS web server allows secured access to the User Interface (UI) and associated transactions with the application server. The SiteMinder web agent sits on the IIS web server as an ISAPI filter and acts as a policy enforcement point for the SiteMinder system.

The IP application is designed around the functionality and features of the products listed above. Conceptually the IDM provides the Identity Management engine for the entire application. The functional requirements are broken down into specific “tasks” and configured within IDM to match the appropriate use cases. For example Level 1 registration makes use of a “user registration” task in identity manager. That task is then configured to produce a user interface presented through the IIS web server in the form of JSPs to allow the end-user to input the necessary registration information. When an environment is created within IDM, it is tied to SiteMinder site protection. Certain tasks can be configured to be “protected” and require a user to authenticate in order to access the functionality. The “tasks” required to perform the IP functions are created within one IDM environment. Within that environment, the IDM defines which attributes within the scheme will be used for specific tasks. The tasks are tied to roles which are then tied to user records such that SiteMinder can perform authorization when those functions are requested. The SiteMinder web agent that resides on the IIS web server acts as the policy enforcement point when a user attempts to access the IP application. If there is a policy created to protect a specific function with IP application, the web agent invokes the SiteMinder policies associated with that protected resource and performs the authentication and authorization functions. Once successfully authenticated and authorized the user is presented with the IP application function requested.

The Identity Proofing component of the IP is designed in much the same fashion as any other “task” except the task is configured as a “user management” tasks allowing only privileged users to access this functionality to perform the ID Proofing functions.

The IP application is also designed to be an identity provider to the VAAFI SSOe system. This is accomplished through the use of the SiteMinder Federation services. The IP is designed to receive authentication requests from VAAFI when a user attempts to access a protected business application. The user is redirected to the IP federation login to authenticate. Once authenticated the SAML assertion is created and the user is redirected back to VAAFI and ultimately to the business application. This process is designed to be seamless to the user. Additionally, once the user is authenticated in this manner, they will have single-sign-on to other business applications under the same security domain.

The IP application is designed to produce highly detailed logging and auditing information. The CA IDM and SM products are configured to process logging with each transaction. The logging can be pushed to log files and then stored in the log database where the report server can generate valuable audit and management reports.

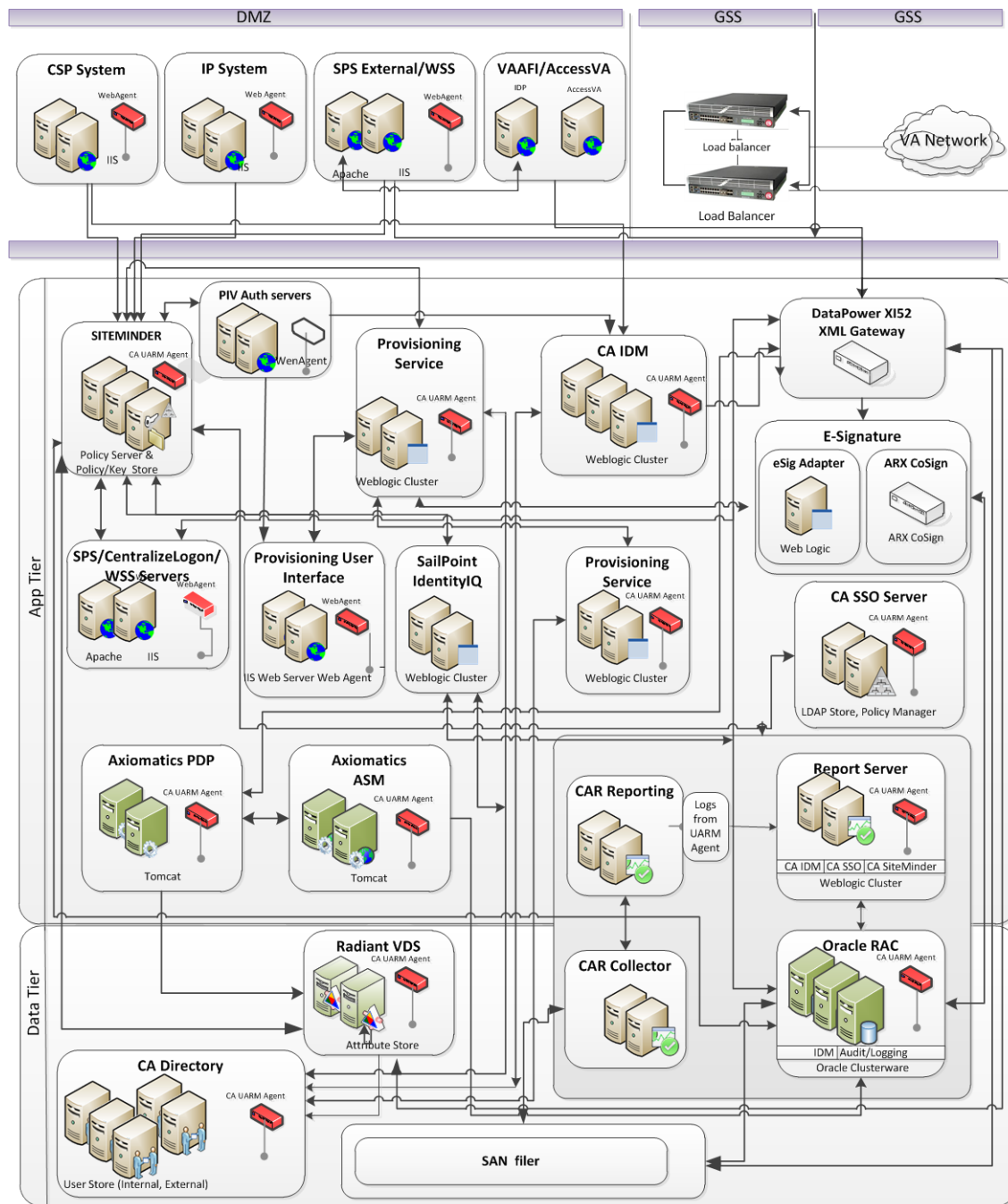


Figure 17: Logical Network String Diagram

4. System Architecture

The AcS 2.0 system architecture includes the hardware, software, and communication architectures. The hardware architecture describes the physical components needed in the system and their relationship to one another. The software architecture describes the software products, components, and code needed to provide the AcS 2.0. The communication architecture describes the connection and security requirements needed between the hardware components.

4.1. Hardware Architecture

This SDD, tailored to document detailed information required to enable CSP/IP functionality upon the COTS software contained within the infrastructure, does not introduce additional hardware.

In brief, the CSP/IP solution architecture is composed of following COTS-based building blocks:

- CA Identity Manager is an integrated identity administration solution that serves as the foundation for CSP.
- CA SiteMinder Policy Server and CA SiteMinder Federation Services is the CSP/IP federation engine service component.
- CA Directory stores user and configuration information.
- Identity Manager Workflow/Oracle Database Server stores CA Identity Manager data.
- Report Server contains information from the Identity Manager object store and the Identity Manager user store.
- Microsoft IIS Server/ SiteMinder Web Agent is an embedded IIS agent which allows secured access to the CSP/IP UIs.

Being Developed

Figure 18: Network Communication Architecture

The following table provides information for the hardware appliances used for the VA AcS 2.0.

Notes:

- X150 DataPower is currently being used in lower environment and will be upgraded.
- Production and DR are using X152 DataPower.

Table 25 : Hardware Appliance

Hardware Appliance	Descriptions	High Availability (HA)
IBM DataPower	A critical component of AcS infrastructure to securing web service message flows as a proxy using IBM DataPower Appliance	For High Availability configuration, the DataPower XI52 appliances will reside behind a Citrix Netscaler. This setup will have no effect on the existing DataPower configurations, as each transaction will be independent and processed separately by each DataPower appliance. The load balancer will serve as a reverse-proxy to distribute network traffic. The goal is to improve the overall burden of a single machine by enabling an industry standard algorithm.

The uniform resource locators (URLs) for CSP, IP, CAR, Provisioning, SAC, SSOi, VDS, and eSig for production, pre-production and SQA are provided in the table below. The AcS components residing in the DMZ are the external facing web servers that contain the CSP pages and federation components. These components will be load balanced by the Citrix Netscalers located in the Terremark GSS. DataPower, along with the remaining AcS application components, will reside in the GSS. The following table provides details on the AcS 2.0 machines such as ports, URLs, protocols hostnames for each application in every environment.

SQA (AITC)

Table 26 : Virtual Machines and Appliances

Application	Number of VMs	Number of Physical Servers	Hostname
IP, Federation Services WebUI, SPS, WSS (IIS- Single instance on each, Tomcat)	5	N/A	
IdentityMinder supporting (Identity Proofing) WebLogic cluster Admin service on primary node	3	N/A	
CA Directory (IP)	3	N/A	
Oracle RAC	N/A	2	
DataPower XI52 (Appliance)	N/A	2	Not Applicable

Pre-Production (Terremark Culpeper, VA)

Table 27 : Pre-Production (Terremark Culpeper, VA)

Application	Number of VMs	Number of Physical Servers	Hostname
-------------	---------------	----------------------------	----------

Application	Number of VMs	Number of Physical Servers	Hostname
IP, Federation Services WebUI/SPS/WSS (IIS, Tomcat) Single IIS instance on each	4	N/A	[REDACTED]
IdentityMinder supporting (Identity Proofing) (WebLogic) Admin service on primary node	2	N/A	[REDACTED] v
CA Directory (IP)	2	N/A	[REDACTED] v
Oracle Database	N/A	2	[REDACTED]
DataPower XI52 (Appliance)	N/A	N/A	Not Applicable Note: Placed inside the VAAFI Enclave

Production (Terremark Culpeper, VA)

Table 28 : Production (Terremark Culpeper, VA)

Application	Number of VMs	Number of Physical Servers	Hostname
IP, Federation Services WebUI, SPS, WSS (IIS) Single IIS instance on each	4	N/A	[REDACTED]

Application	Number of VMs	Number of Physical Servers	Hostname
IdentityMinder (IP) (WebLogic) Admin service on primary node	2	N/A	[REDACTED]
CA Directory (IP)	2	N/A	[REDACTED]
Oracle Database	N/A	2	[REDACTED]
DataPower XI52	N/A	N/A	Not Applicable Note: Placed inside the VAAFI Enclave

DR (Terremark Miami, FL)

Table 29 : DR (Terremark Miami, FL)

Application	Number of VMs	Number of Physical Servers	Hostname
IP, Federation Services WebUI (IIS)	4	N/A	[REDACTED]
Provisioning Server	2	N/A	[REDACTED]
CA Directory (IP)	2	N/A	[REDACTED]

Application	Number of VMs	Number of Physical Servers	Hostname
Oracle Database	N/A	2	[REDACTED]
DataPower XI52 (Appliance)	N/A	N/A	N/A

4.2. Software Architecture

The following diagram shows the complete software architecture of the IP 2.0.

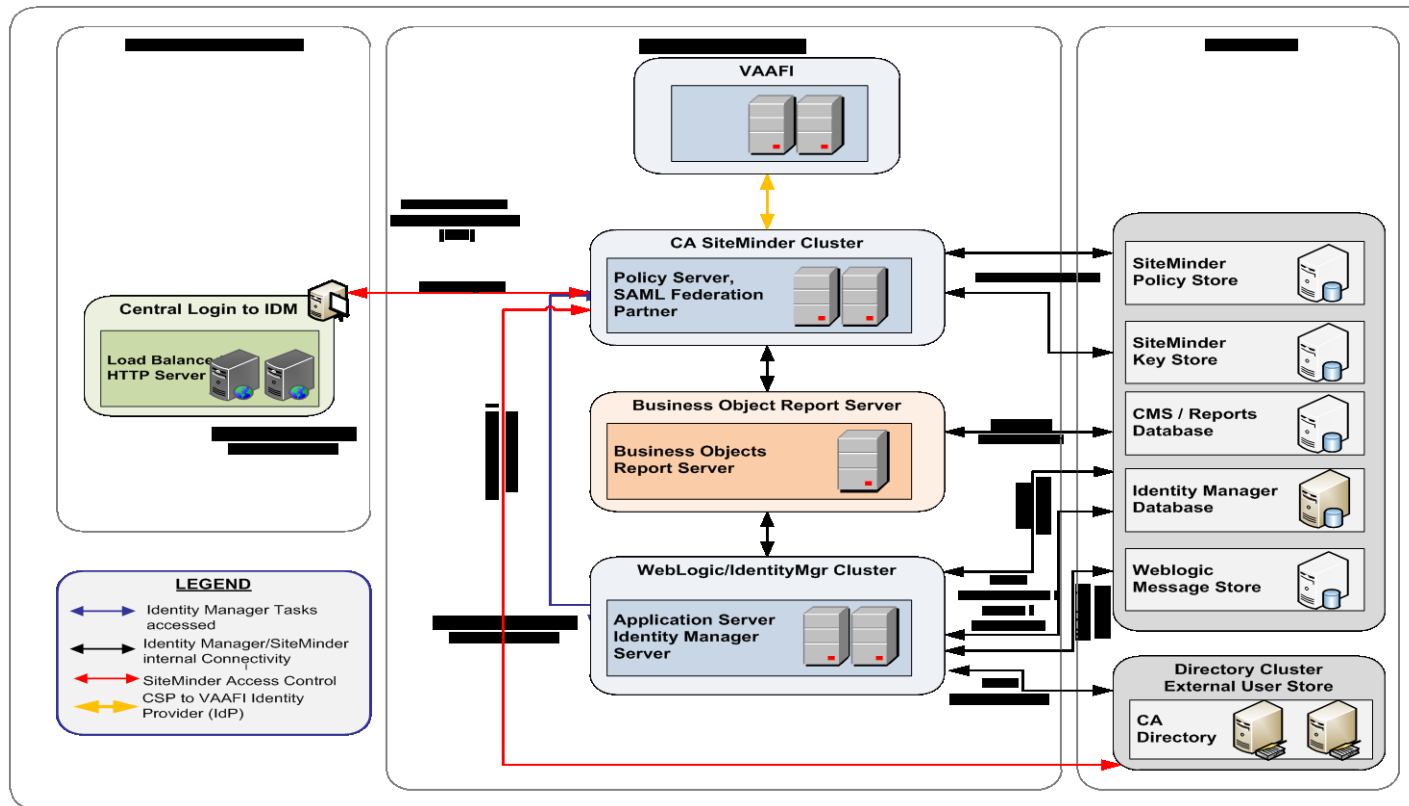


Figure 19: Software Architecture

The following table describes the AcS 2.0 products for each of the AcS services and versions.

Identity Proofing (IP)

Table 30 : Software Components

Products	Abbreviation	Product Version/Release
----------	--------------	-------------------------

Products	Abbreviation	Product Version/Release
CA IdentityMinder	CA IdentityMinder	R12.6 SP3
IIS Web Server	-	7.5
CA Web Agent	-	SM r12.5 SP3
CA Option Pack	-	SM r12.5 SP1
Servlet Exec	-	6.0 Fixpack x
WebLogic	-	10.3.6 (TRM Compliant till Q3-2016) Planned upgrade to 12c Q1-2015
Oracle Database	-	11gR2
CA Directory	LDAP directory	12.0 SP7
CA SiteMinder	CA SM	SM r12.5 SP1
IP .NET Application	IP App	ASP.NET 4
MVI Web Service Client	MVI WS	Java 1.7 (IP)

The following table provides information about the software components.

Oracle Database 11gR2

The shared database environment will maintain the following table spaces required for the components of the AcS implementation. Database High Availability and Data Guard to synchronize and replicate a HOT Oracle database environment to Terremark Miami, FL.

Table 31 : Oracle Database 11gR2

Characteristic	Description
Database Table spaces	Data Table spaces: CSPIPDM_DATA Index Table spaces: CSPIPDM_IND Users Temp Rollback Undo

Characteristic	Description
High Availability	For the AcS 2.0 IP Solution, database high availability is critical. A database outage can cause a multitude of errors to occur on the application side, thereby nullifying the high availability configurations on the application itself. It was planned for Raw Devices to be utilized by Oracle Automatic Storage Management (ASM) file system, working as the volume manager, overseeing the clusterware file systems. ASM, attached by each node, exposes the existing pool of storage and makes it available as an interface for the Oracle database files. The ASM is supported by Oracle Clusterware. If a single Oracle instance on a node fails, the ASM and database instances on the surviving nodes are designed to automatically failover. Due to the load dependency on the ASM file system storage, mirroring is needed to provide high availability.

CA Directory

The CA Directory servers are a shared resource for the IP. The CA Directory infrastructure will be configured in a multi-master replication configuration. The CA Directory comprises of various instances elaborated as follows.

Note: CA Directory structure as applicable for each of the directory instance specific to a release and will be provided in each release. The holistic view of the CA Directory structure is provided in Software Detail Design Sections.

Table 32 : CA Directory

Characteristic	Description
Directory Instances	User store CA IdentityMinder for CSP solution and Provisioning services, Policy and Key store for CA SiteMinder for CSP service Object/policy store for CA SSO for SSOi services.
High Availability	There will be a master write server for each directory. The other supporting directories will be read directories. The CA Directory will provide intelligent and transparent chaining of queries to distributed servers. It performs transparent routing to re-route requests in the event of failure on a particular CA Directory server. The CA Directory router DSA distributes incoming requests evenly among DSAs in the same site. The clients accessing router dsa are configured to maintain the list of AcS CA Directory router DSA's and the failover occurs from the client's end. This improves performance, allowing CA Directory's replication mirroring

Characteristic	Description
	<p>to provide synchronized in real-time and consistent servers. CA IdentityMinder, CA SSO, and CA SiteMinder will leverage the directories through a round robin load balancing configuration. Multiwrite-DISP replication is a replication scheme that uses Multiwrite replication for real-time updates and DISP for recovery. By default, the Directory System Agent (DSA) is configured for Multiwrite-DISP replication. This replication scheme combines the efficiency of Multiwrite when DSAs are online (real-time updates), with the robustness of DISP to allow DSAs to recover after being offline (recovery).</p> <p>The DSA uses its routing capabilities to distribute requests evenly between systems while data replication keeps the data synchronized.</p>

Web Tier – IIS Web Server

The Web Tier consists of IIS web servers that provide reverse proxy and federation to the applications.

Table 33 : Web Tier – IIS Web Server

Characteristic	Description
IIS Web Server Instances	CA IdentityMinder Registration / user profile management/admin UI for CSP service
High Availability	<p>IIS Web Servers are used by the CSP, centralized logon, PIV Auth and Federation servers to support multiple services. They will be CSP Login / Registration, Provisioning, and protected by the SiteMinder Option Pack (Federation), PIV Authentication Servers, and Centralized Logon Server Page. The CSP Login / Registration will leverage five (5) IIS web servers, behind a Citrix NetScaler load balancer with a round robin algorithm which distributes equal load between the servers. The load balancers will be configured to maintain the session for the entirety of each user transaction. In the event that all of the IIS web servers fail on Terremark Culpeper, VA site, the Citrix NetScaler load balancer will be configured to route the traffic to Terremark Miami, FL site.</p> <p>There are two IIS web servers required by CA IdentityMinder, which are load balanced by the Citrix NetScaler load balancer. The IIS web servers for provisioning service reside in Terremark.</p> <p>There are two IIS web servers required for PIV, Federation, and Centralized logon.</p>

Application Tier – WebLogic Application Server

The application tier for the Provisioning service is made up of a cluster of WebLogic application servers. The Application Tier is a shared environment for hosting application components. The AcS related applications hosted are listed below. The Report Server instance is a Business Objects environment that provides reporting services for Access Services. The CA Report server (SAP Business Objects XI R3.1 SP3) that constitutes the Reporting Infrastructure is hosted on a WebLogic cluster.

Table 34 : Application Tier – WebLogic Application Server

Characteristic	Description
WebLogic Instances	CA IdentityMinder for CSP and Provisioning solution CA SiteMinder Admin UI eSig Web Service
High Availability	<p>The WebLogic servers will be configured for high availability. These WebLogic servers will be load balanced using the Round Robin algorithm provided by the Citrix NetScaler. Persistent stores are based on file stores.</p> <ul style="list-style-type: none">• The CSP solution will consist of 3 WebLogic servers configured in a cluster.• The Provisioning will consist of 2 WebLogic servers configured in a cluster.• The SiteMinder Admin UI consists one local Single node WebLogic instance available in primary SiteMinder policy server. CA product has a limitation that Admin UI cannot automatically failover. But the High availability is achieved by configuring it to manage multiple Policy Servers including Primary and secondary servers so that alternate server can be used in case of unavailability of the primary server.• eSig web service – is within the cluster domain and is highly available through multimode cluster and is load balanced by the Citrix NetScaler and DataPower <p>The WebLogic cluster is designed as an active and passive failover. Therefore, when the instances in a Clusternode fail, they will failover to the alternate cluster node.</p>

CA IdentityMinder

The CA IdentityMinder components form an integrated identity administration solution that serves as the foundation for VA's CSP and Provisioning services. CA IdentityMinder is made up of the following components.

Table 35 : CA IdentityMinder

Characteristic	Description
Subcomponents	<p>IdentityMinder Server: Executes workflows within IdentityMinder. It includes the Management Console and the User Console deployed on a WebLogic cluster.</p> <p>Provisioning Server: Manages the lifecycle of user accounts on endpoint systems. This server is required, as the CA IdentityMinder installation will support account provisioning.</p> <p>User store: The IdentityMinder user store is maintained by CA IdentityMinder. This is an existing store that contains the user identities that a company needs to manage. The user store for VA AcS 2.0 is CA Directory as mentioned above.</p> <p>User store maintained by the Provisioning Server: The Provisioning Directory user store is maintained by the Provisioning Server. It is an instance of CA Directory and includes global users. It associates users in the Provisioning Directory with accounts on endpoints such as Microsoft Exchange, Active Directory, and SAP.</p>
High Availability	The CA IdentityMinder utilizes web logic clustering described above for high availability.

Table 36 : Operating Systems

Operating Systems
Windows Server 2008 R2
Red Hat Enterprise Linux 5.3

4.3. Network Architecture

The following diagram depicts the communication channels between the different AcS components and protocols used.

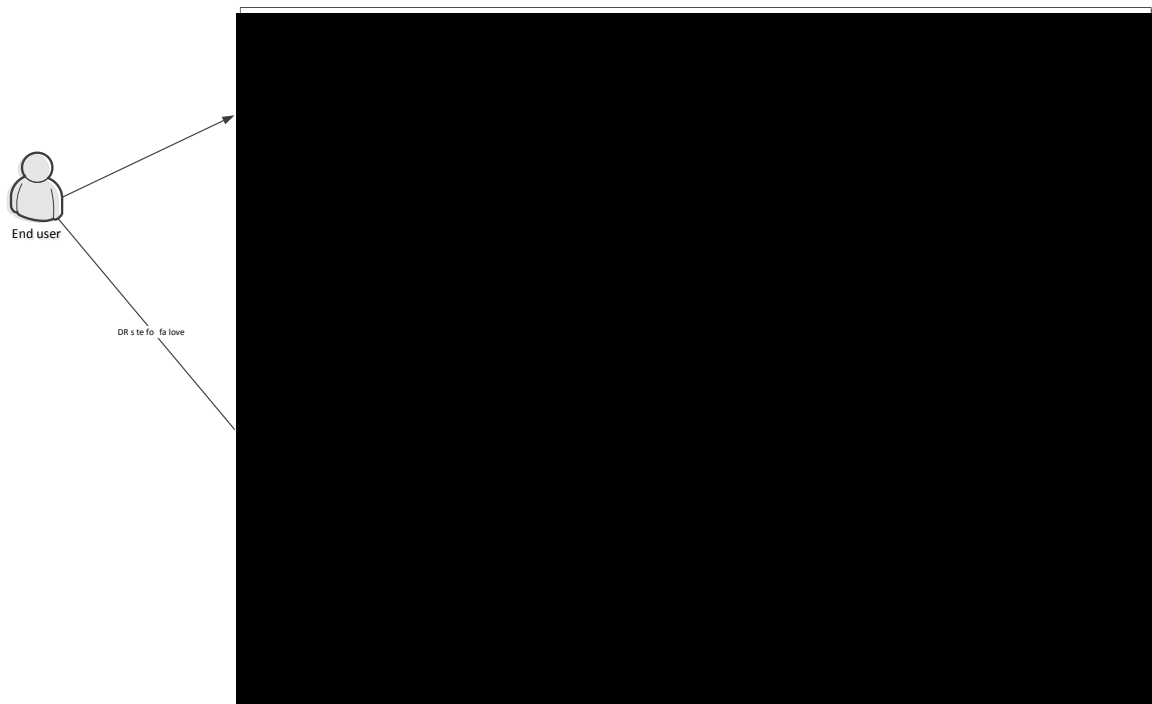


Figure 20: AcS Network Security Topology

4.4. Service Oriented Architecture / ESS

The IP system design is based on a Service Oriented Architecture (SOA) approach. The solution architecture uses accepted COTS products for each of VA AcS activity and applies the leading practices as outlined by the product vendor to the extent possible. The design of the architecture supports VA's scalability, security, extensibility, and high availability requirements to provide a flexible enterprise solution.

The VHIC system performs a search by passing ICN number to IP system to get the proofing status. IP System also performs search, retrieve, add and update function by making Web Service calls to MVI application. MVI application subsequently calls TEWS Web Service calls and perform related operations. VA Applications perform proofing operation and search for proofing status via SOAP over HTTPS calls.

IP provides the following WS interface:

Identity Proofing WS Interface – The CA IdentityMinder Task Execution Web Service (TEWS) exposes web services to applications as an interface to remotely trigger the execution of IP Service functions. This interface leverages WSDL and SOAP for integration with applications. This interface allows ID Proofer to perform IPP for LOA 2 or to retrieve the proofing status.

There are 2 major operations that occur between IP and consuming application are described below:

1. **Proof Applicant (LOA 2):** VA Identity Proofer (ID Proofer) verifies Applicant's identity in person and records information within IP Service tool for issuance of LOA 2 status.
2. **Retrieve Proofing Status:** Application or system needs to retrieve the proofing status of an individual.

4.5. Enterprise Architecture

Identity Proofing is implemented as a standards based .NET application using VA approved technologies in conformance with the TRM. The specific technologies upon which IP is based can be found in the COTS Product Roadmap located on the [AcS TSPR](#) site.

5. Data Design

This section outlines the design of the database management system (DBMS) and non-DBMS files associated with the IP solution as well as the data security implementation.

5.1. DBMS Files

The AcS 2.0 uses Oracle 11gR2 Database and CA Directory for persistent data storage. The Oracle database “ACSDb” is created and used for the following purposes:

- CA IDM schema is built during the installation via COTs pre-bundled scripts
- CA SiteMinder audit schema is built during the installation via COTs pre-bundled scripts to store audit information
- CA IDM audit schema is built during the installation via COTs pre-bundled scripts to store audit information
- Similarly, CA Directory will be used for the following purposes:
 - CSP User Store is built to store user attributes for external VA users
 - Provisioning User Store is built to store user attributes for users who are requesting access
 - SiteMinder Policy Store is built to store policy and configurations of SiteMinder
- Role manager schema is built during the installation via its pre-bundled scripts contained in the installation package

Table 37 : Database File System

Table Spaces	Data Files
SYSTEM	+ORADATA/acsdbs/datafile/system
SYSAUX	+ORADATA/acsdbs/datafile/sysaux
USERS	+ORADATA/acsdbs/datafile/users
UN DO1	+ORADATA/acsdbs/datafile/und01
UNDO2	+ORADATA/acsdbs/datafile/und02
CSPIDM_DATA	+ORADATA/acsdbs/datafile/cspipdm_data
CPIPIDM_INDX	+ORADATA/acsdbs/datafile/cspipdm_indx
PROVIDM_DATA	+ORADATA/acsdbs/datafile/providm_data
PROVIDM_INDX	+ORADATA/acsdbs/datafile/providm_indx
CASM_DATA	+ORADATA/acsdbs/datafile/casm_data
CASM_INDX	+ORADATA/acsdbs/datafile/casm_indx
ESIG_DATA	+ORADATA/acsdbs/datafile/esig_data
SACASM_DATA	+ORADATA/acsdbs/datafile/sacasm_data
SYSTEM	+ACSDb_DATA/sailpt/datafile/system.280.828271109
SYSAUX	+ACSDb_DATA/sailpt/datafile/sysaux.284.828271115

Table Spaces	Data Files
UNDOTBS1	+ACSDB_DATA/sailpt/datafile/undotbs1.290.828271119
UNDOTBS2	+ACSDB_DATA/sailpt/datafile/undotbs2.285.828271135
USERS	+ACSDB_DATA/sailpt/datafile/users.287.828271139
IDENTITYIQ_TS	+ACSDB_DATA/sailpt/datafile/identityiq_ts.286.828271127

5.2. Non-DBMS Files

For the IP solution, non-DBMS files are used for the following activities:

- **IP** User store schema within CA Directory is customized to store registered user record information (refer to section A below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions). The data dictionary for account and feed object attributes are covered as part of the **VAProvPerson** object class attributes (refer to Provisioning in section A).

5.3. Data View

For Increment 5, the IP system will interface with VHIC, CSP, and MVI for identity proofing functions.

5.3.1. IP Data Exchange with VHIC

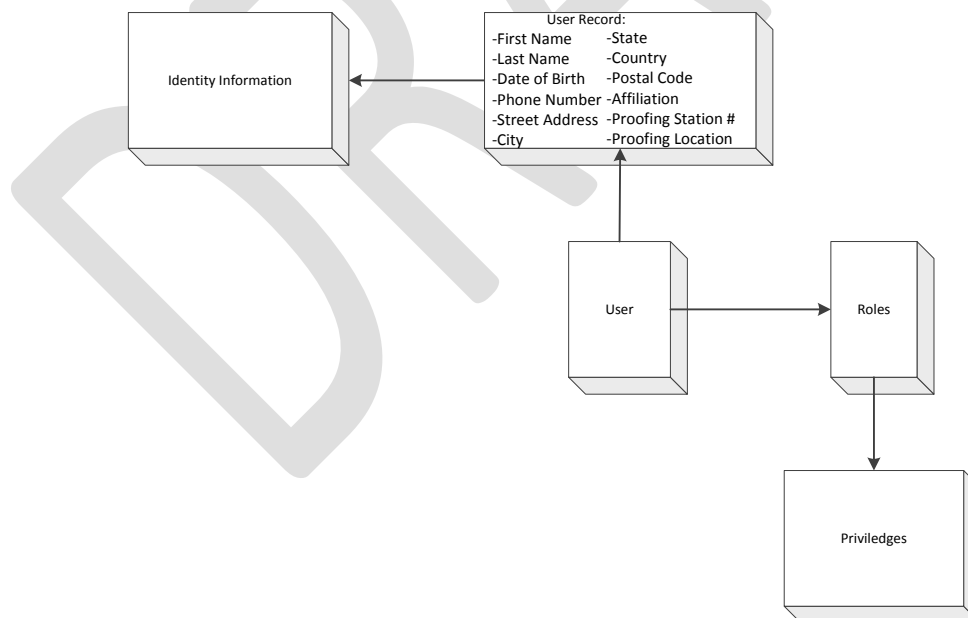


Figure 4: VHIC-IP High-level Data Exchange

Index	Identifier	Description
1	User	Entity that represents a user requesting a VHIC card, which has completed registration or has been manually added by an administrator.
2	Credential	The user ID and password of a registered user
3	Credential Type	Denotes the rules specific to credential, (e.g. E-Authentication), and level of assurance (e.g. Level 1, Level 2), the credential represents
4	User Record	Management information stored about the user
5	Identity Information	Demographic and identity-specific information stored about the user
6	Security Questions	User defined questions utilized when a user forget their credential
7	Roles	Assignment of a Role provides a set of Privileges for specific user
8	Privileges	Fine grained entitlements that grant access to specific objects with the CSP/IP

Table 38: VHIC-IP Data Exchange

Field Description	Field Required? (Yes/No)	Field Type
First Name	Yes	Static
Last Name	Yes	Static
Date of Birth	Yes	Static
Phone Number	No	Dynamic
Street Address	Yes	Static
City	Yes	Static
State	Yes	Static
Country	Yes	Static
Postal Code	Yes	Static
Affiliation	Yes	Static
Proofing Station #	No	Dynamic
Proofing Location	Yes	Static

Table 39: VHIC-IP User Data

5.3.2. IP Data Exchange with CSP

Table 40: CSP-IP Data Exchange

Index	Identifier	Description
1	User	Entity that represents a user that has completed registration or has been

Index	Identifier	Description
		manually added by an administrator. Please note, CSP/IP stakeholders that wish to use credentials to access VA services will NOT be manually created. Manual creation is available for administrators to create additional administrator accounts
2	Credential	The user ID and password of a registered user
3	Credential Type	Denotes the rules specific to credential, (e.g. E-Authentication), and level of assurance (e.g. Level 1, Level 2), the credential represents
4	User Record	Management information stored about the user
5	Identity Information	Demographic and identity-specific information stored about the user
6	Security Questions	User defined questions utilized when a user forget their credential
7	Roles	Assignment of a Role provides a set of Privileges for specific user
8	Privileges	Fine grained entitlements that grant access to specific objects with the CSP/IP

5.3.3. IP Data Exchange with MVI

CSP/IP Search for Identity Data from MVI	
Description	Required Field Type (Yes/No)
First Name	N/A
Middle Name	N/A
Last Name	N/A
SSN	N/A
Date of Birth	N/A
Gender	N/A
Home Address (Street, City, State, Zip)	N/A
Home Phone	N/A
Place of Birth (City and State)	N/A
Mother's Maiden Name	N/A
Add a CSP/IP Proofed Person Correlation to MVI	
Description	Required Field Type (Yes/No)
Fully Qualified Source ID: Assigning Authority – Value to be determined during design phase. Assigning Location – Value to be determined during design phase. Identifier Type – Value to be determined during design phase.	Yes
Assigning Authority – Value to be determined during design phase.	Yes
Assigning Location – Value to be determined during design phase.	Yes
Identifier Type – Value to be determined during design phase.	Yes
Internal Entry Number	Yes

Last Name	Yes
First Name	Yes
Middle Name (optional – the Add Person request shall include middle name when available.)	No
ICN	Yes
Gender	Yes
Date of Birth	Yes

Table 41: IP User Data Exchange with MVI

6. Detailed Design

This section describes the design for the IP solution and its activities in detail.

6.1. Hardware Detailed Design

The sections below provide the hardware information for each activity in the VA AcS 2.0. The following table displays the sizing, network, Operating System, and number of Virtual Machines required to be deployed across AcS activities:

Note: Applications will be deployed on virtual machines except Oracle (SQA) and IBM DataPower and ARX CoSign.



Microsoft Excel
97-2003 Worksheet

6.2. Software Detailed Design

This section provides final detailed information associated with the design of IP solution activity and the associated functionality.

6.2.1. Conceptual Design

The following sections provides the conceptual data design for the IP system.

The IP processes used by Government and commercial entities to establish the required level of assurance vary widely based on the target subject population, the purpose of the resulting identity proofed record, etc. A common goal for each of these identity proofing processes is to allow the enterprise to comply with legal, regulatory and due diligence requirements based on one or more of the following references FIPS 201⁷, HSPD-12⁸, OMB A-130, Appendix I⁹, VA Information Security Policies and Directives (e.g. VA Handbook 6500, Appendix F), NIST SP800-63¹⁰, and others, before the enterprise can interact with the subject, do business transactions or issue credential(s) and/or account(s) to said subject.

The IP processes are based on historical and transaction information aggregated from public and proprietary data sources. IP services can also be used as an additional interactive user authentication method for high-risk transactions, such as accessing sensitive, confidential or third party's personally identifiable information¹¹. IP services are classified as in-person, remote or

hybrid, as defined in OMB M04-04¹², is referenced to the NIST SP 800-63 Identity proofing processes and drives their scope and extensiveness.

Table 42 : Potential Impact Categories for Authentication Errors

Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod, High
Civil or criminal violations	N/A	Low	Mod	High

At VA, the IP processes are used for establishing the validity of a claim for authorization to VA applications, resources or benefits. The IP component capabilities allow for a multitude of identity proofing processes to be defined as business needs dictate and be built to suit a specific purpose.

The following diagram provides the detailed view of the complete IP system at VA and its interaction with various systems and actors.

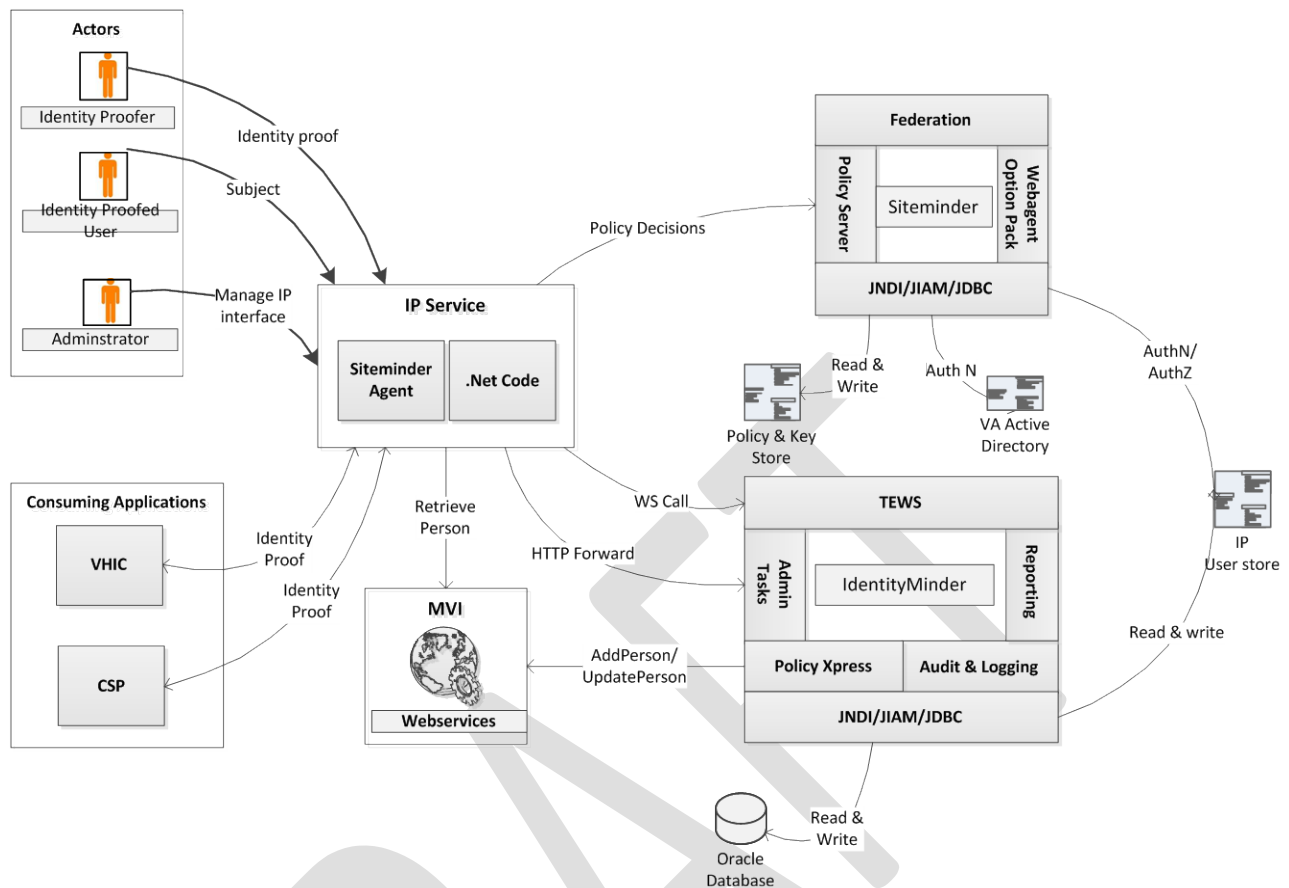


Figure 21: IP Detailed Design

CA IdentityMinder:

CA IdentityMinder is a J2EE application deployed on the WebLogic application server cluster, which implements the IP function. It is integrated with SiteMinder for Single Sign-On and access control purposes. Major modules of CA IdentityMinder used to implement the IP system, are as follows

- **Policy Xpress:** Policy Xpress helps to create complex business logic (policies) without the need to develop custom code
- **Task Execution Web Services (TEWS):** A web service interface that allows third-party client applications to submit remote tasks to CA IdentityMinder for execution

IP Service:

IP service is a combination of custom ASP.NET application deployed on IIS along with CA SiteMinder Web agent for access control

- **ASP.NET application:** This application call the CA IdentityMinder Task Execution Web services (TEWS) to execute the various tasks created for implementing the IP tasks
- **Web agent:** This acts as the policy enforcement point in the access control framework and enforces policy decision set in CA SiteMinder Policy Server, and implements the access control framework for the ASP.NET application

6.2.1.1. Product Perspective

Refer to section 3.1.3 for information on COTS products for the AcS 2.0.

6.2.1.1.1. User Interfaces

Refer to section 3.2.3 for information on user interfaces.

6.2.1.1.2. Hardware Interfaces

Refer to section 4.1 for information on hardware configurations and interfaces.

6.2.1.1.3. Software Interfaces

Refer to section 4.2 for software architecture design for the AcS 2.0.

6.2.1.1.4. Communications Interfaces

Refer to section 4.3 for the detailed communication design for the AcS 2.0.

6.2.1.1.5. Memory Constraints

This section is not applicable to the IP solution.

6.2.1.1.6. Special Operations

This section is not applicable to the IP solution.

6.2.1.2. Product Features

The AcS 2.0 is based on the foundation of CA COTS products. The table below describes the AcS IP activity products.

Table 43 : AcS 2.0 Products

#	Software	Description
1	CA IdentityMinder	A scalable, configurable identity management solution that automates onboarding, modification and off-boarding of users, enables self-service requests and automates proactive identity compliance processes.
2	WebLogic	BEA WebLogic Portal is now known as WebLogic Portal. WebLogic Portal is a well-known, widely used, Java-based portal product and a portal framework. The WebLogic Portal product is out-of-the-box software that aggregates information, content, applications, business processes and knowledge assets into a personalized display. The WebLogic Portal framework is the portal product in kit form, providing a set of tools to extensively build and customize a portal with specialized functionality. The WebLogic Portal framework comes packaged with an Eclipse-based integrated development environment (IDE) to assemble and extend the capabilities of the portal using the provided API and tools. The paired IDE is known as Oracle Workshop for WebLogic (formerly Workspace Studio). WebLogic Portal offers support for industry standards, enterprise-class portal federation, publication, and syndication capabilities including bidirectional integration with other portals and Web applications. My HealthVet (MHV) and the Clinical Information Support System (CISS) are deployed with WebLogic Portal.
3	Oracle Database	The Oracle relational database management system. There are several Oracle editions (Express, Personal, Standard, Enterprise, and Real Application Cluster). This assessment is concerned with the Standard and Enterprise editions of Oracle.

6.2.1.3. User Characteristics

Refer to section 1.5 and section 3.1.4 for user-related information.

6.2.1.4. Dependencies and Constraints

Refer to sections 2.4.1 and 2.4.2 for constraints and dependencies.

6.2.1.5. Identity Proof a User

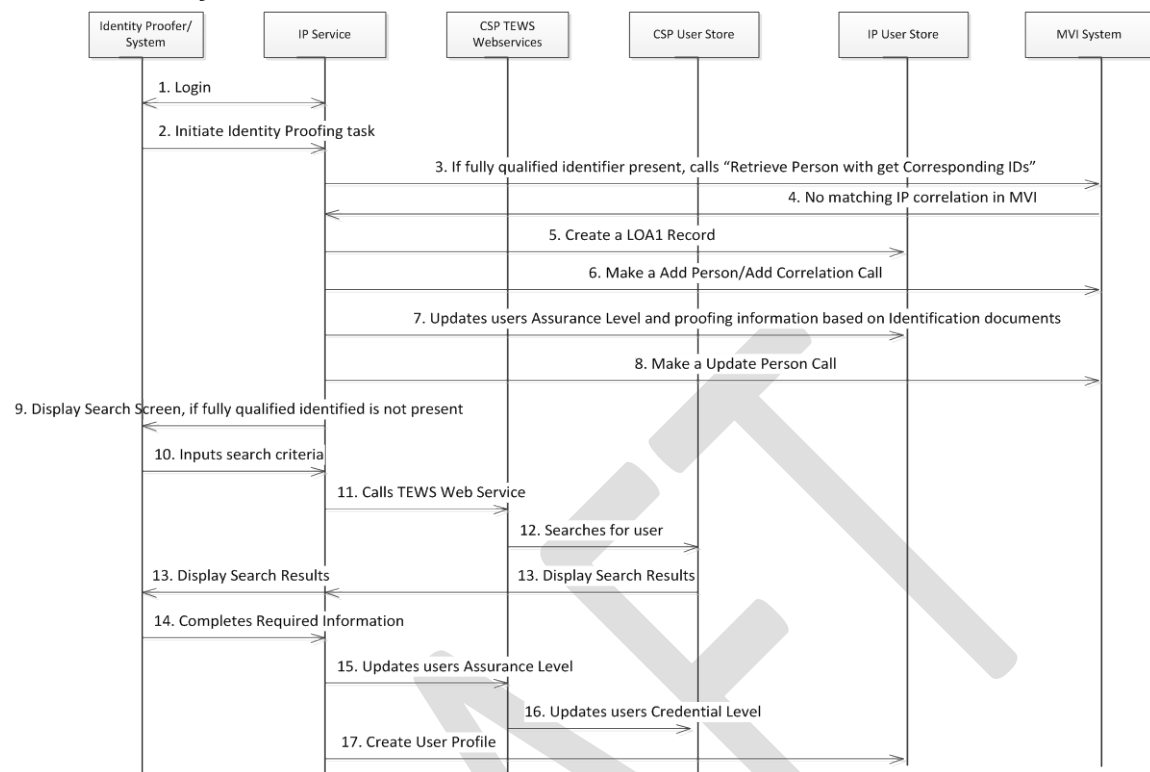


Figure 22: Identity Proof a User Sequence Diagram

Table 44 : Identity Proof a User

Field	Description
Use Case Name	Identity Proof a User
Description	This use case describes the process by which a person or a system with the role of Identity Proofer or higher can perform an in-person identity proofing.
Actors	<ol style="list-style-type: none"> 1. IP Service 2. Identity Proofer/System 3. CSP System 4. CA Identity Minder 5. MVI system
Pre-Conditions	Identity Proofer have the required access to perform the in-person proofing function
Trigger	CSP user goes to the proofing station to get identity proofed

Field	Description
Actions	<ol style="list-style-type: none"> 1. Identity Proofer/System logs into IP service 2. Identity proofer/System initiate an identity proof task on the IP service 3. If the request to IP Service contains a fully qualified identifier, then it makes a MVI call “Retrieve Person with get Corresponding IDs” to get the IP correlation from MVI system 4. If MVI do not have an existing IP correlation 5. IP service will create a LOA 1 record in IP system and makes a “Add Person/Add Correlation” call to MVI 6. Identity Proofer/System will update the user information, based on the primary and secondary identification provided by the user 7. IP service updates the user proofing information 8. IP makes a “updated person” MVI call and update the LOA value to 2 9. If the request to IP service do not contain a fully qualified identifier, then IP service will display a search screen 10. Identity Proofer enters the user information based on the primary and secondary identification document provided by the CSP user 11. IP service calls the CSP TEWS Web services 12. Searches for the user from CSP store 13. Displays search results in the IP service 14. Identity Proofer enters needed details about the CSP user, as part of proofing and submits the record 15. IP service calls the CSP TEWS Web services to update the user’s assurance level 16. CSP service updates the user credential level at the CSP user store 17. IP services creates the user profile in the IP user store
Main Success Scenarios	<ol style="list-style-type: none"> 1. User is successful proofed and a record is created in the IP user store 2. CSP user assurance level is updated to LOA 2 at the CSP system
Main Failure Scenarios	No credential gets created if an error occurs during proofing record

6.2.1.6. Create Proofing Record

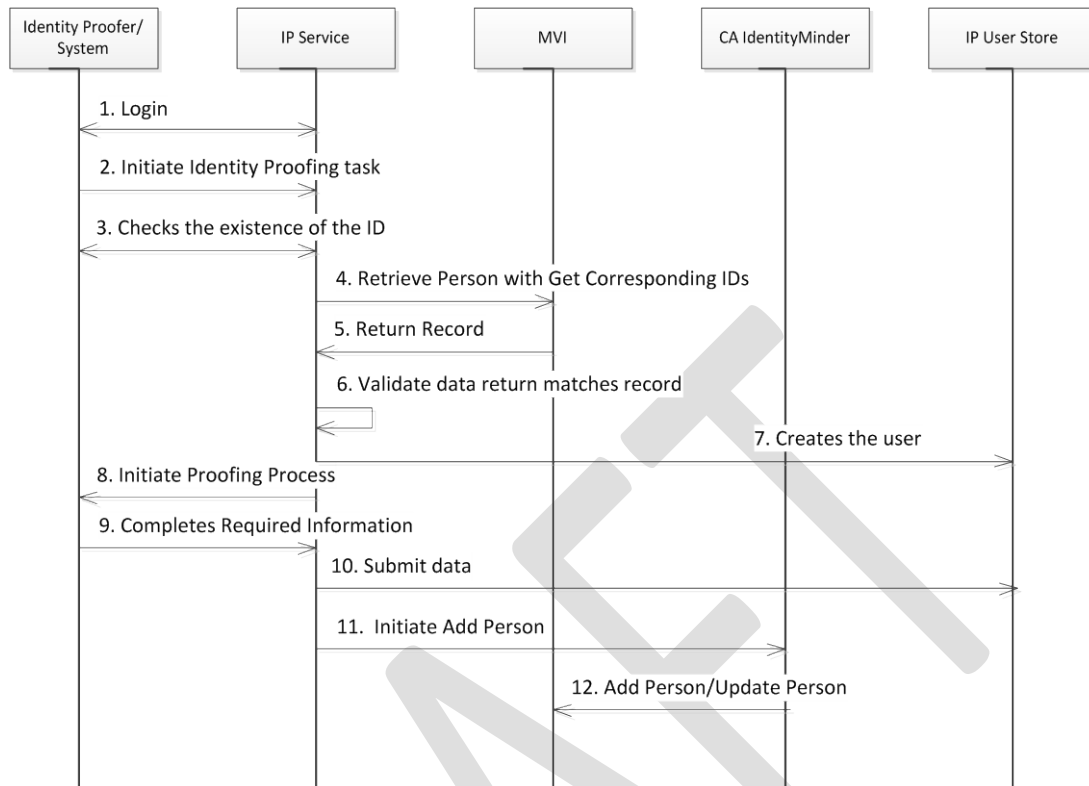


Figure 25: Create Proofing Record Sequence Diagram

Table 45 : Create Proofing Record

Field	Description
Use Case Name	Create Proofing Record
Description	This use case describes the process by which a person or a system with the role of Identity Proofer creates an identity proofing record as part of enterprise Identity Proofing.
Actors	1. IP Service 2. Identity Proofer/System 3. CSP TEWS Web services 4. CA Identity Minder
Pre-Conditions	Identity Proofer/system have the required access to perform the create proofing record function
Trigger	CSP user goes to the proofing station to get identity proofed

Field	Description
Actions	<ol style="list-style-type: none"> 1. Identity Proofer/System logs into IP service 2. Identity proofer/System initiates create identity proof task on the IP service 3. IP services receives the fully qualified identifier and checks the existence of the ID in the IP system 4. IP services get the primary view of the user and make a MVI function call “Retrieve Person with get Corresponding IDs” 5. MVI returns the person record. 6. Validates the primary data matches the retrieved person record 7. Create the user record in IP system, if it is not present already 8. Identity Proofer enters all the necessary information for identity proofing and submits the record to update the IP service 9. IP service make a TEWS call to CA IdentityMinder of the IP system 10. Submit the data to IP store 11. The policy express of IdentityMinder gets triggered and calls the MVI Add person or update person (correlation) function based on existence of user in MVI
Main Success Scenarios	Created of LOA 2 user in Identity Proofing system
Main Failure Scenarios	Error during create proofing record

6.2.2. Specific Requirements

This SDD provides the foundational detailed design for AcS activities under VA Development Support program. VA AcS components leverage the installation and configuration of COTS products to meet the technical requirements that sufficiently meet the detailed functional requirements. The design applies specific configurations and customizations made to the base infrastructure to create the technical solution necessary to meet the business requirements provided in requirements documents listed in Table 6: Project Documents above.

This increment will address following specific requirements:

Service shall be able to collect an expiration date through year 2150 when the military identification card is presented as a proofing document. Change will be made to User Interface to collect an expiration date of INDEF (indefinite) when the military identification card is presented as a proofing document. The Identity Proofing service shall require only one Primary ID in order to be In-Person Proofed, however this will be performed once this requirement is approved.

6.2.2.1. Database Repository

Not applicable for this increment.

Increment 5 presents identity proofing policies that may impact the IP database, specifically to support the following requirement:

- Requiring one Primary ID in order to be In-Person Proofed

6.2.2.2. System Features

Please refer to the AcS i5 RSD located at: [AcS 2.0 i5 RSD.PDF](#) for a complete list of IP requirements, features, and system performance specifications for this increment. The IP system features in i5 functions with VHIC for the VHIC card request process.

6.2.2.2.1. Identity Proofing

For Increment 5, IP changes break down into the following item:

- Expiration of Proofing Documentation

6.2.2.2.1.1. Expiration of Proofing Documentation

During the VHIC card request process, the in-person identity proofing process requires the expiration date to reflect current I-9 documentations. To support this requirement, the following changes will be made:

- When the military identification card is presented as a proofing document, collect an expiration date through the year 2150
- When the military identification card is presented as a proofing document, collect an expiration date of INDEF (indefinite)

6.2.2.3. Design Element Tables

N/A

6.2.2.3.1. Routines (Entry Points)

N/A

6.2.2.3.2. Templates

N/A

6.2.2.3.3. Bulletins

N/A

6.2.2.3.4. Data Entries Affected by the Design

N/A

6.2.2.3.5. Unique Records

N/A

6.2.2.3.6. File or Global Size Changes

N/A

6.2.2.3.7. Mail Groups

N/A

6.2.2.3.8. Security Keys

N/A

6.2.2.3.9.	Options
N/A	
6.2.2.3.10.	Protocols
N/A	
6.2.2.3.11.	Remote Procedure Call (RPC)
N/A	
6.2.2.3.12.	Constants Defined in Interface
N/A	
6.2.2.3.13.	Variables Defined in Interface
N/A	
6.2.2.3.14.	Types Defined in Interface
N/A	
6.2.2.3.15.	GUI
N/A	
6.2.2.3.16.	GUI Classes
N/A	
6.2.2.3.17.	Current Form
N/A	
6.2.2.3.18.	Modified Form
N/A	
6.2.2.3.19.	Components on Form
N/A	
6.2.2.3.20.	Events
N/A	
6.2.2.3.21.	Methods
N/A	
6.2.2.3.22.	Special References
N/A	
6.2.2.3.23.	Class Events
N/A	
6.2.2.3.24.	Class Methods
N/A	

6.2.2.3.25. Class Properties

N/A

6.2.2.3.26. Uses Clause

N/A

6.2.2.3.27. Forms

N/A

6.2.2.3.28. Functions

N/A

6.2.2.3.29. Dialog

N/A

6.2.2.3.30. Help Frame

N/A

6.2.2.3.31. HL7 Application Parameter

N/A

6.2.2.3.32. HL7 Logical Link

N/A

6.2.2.3.33. COTS Interface

N/A

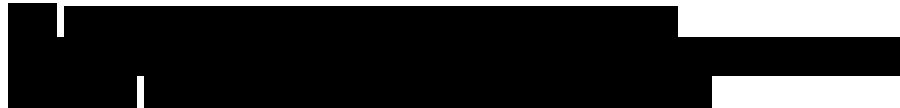
6.3. Network Detailed Design

Refer to section 6.2 for detailed communication design for the IP solution.

6.4. Service Oriented Architecture / ESS Detailed Design

IP has a web service interface to facilitate integration with other VA applications. The task that is exposed via web service is a search for an IP record that matches the submitted criteria. The web service is defined using the SOAP protocol, and web service messages are conveyed using HTTP. The IP web service is enabled through configuration of the CA Identity Manager product. The web service is described by an XML document named a Web Services Description Language (WSDL) file. The WSDL file can be found by accessing the URL for the applicable environment described below.

IP WSDL



Following diagram depicts the IP system in context with partner integrated systems and describes each integration.

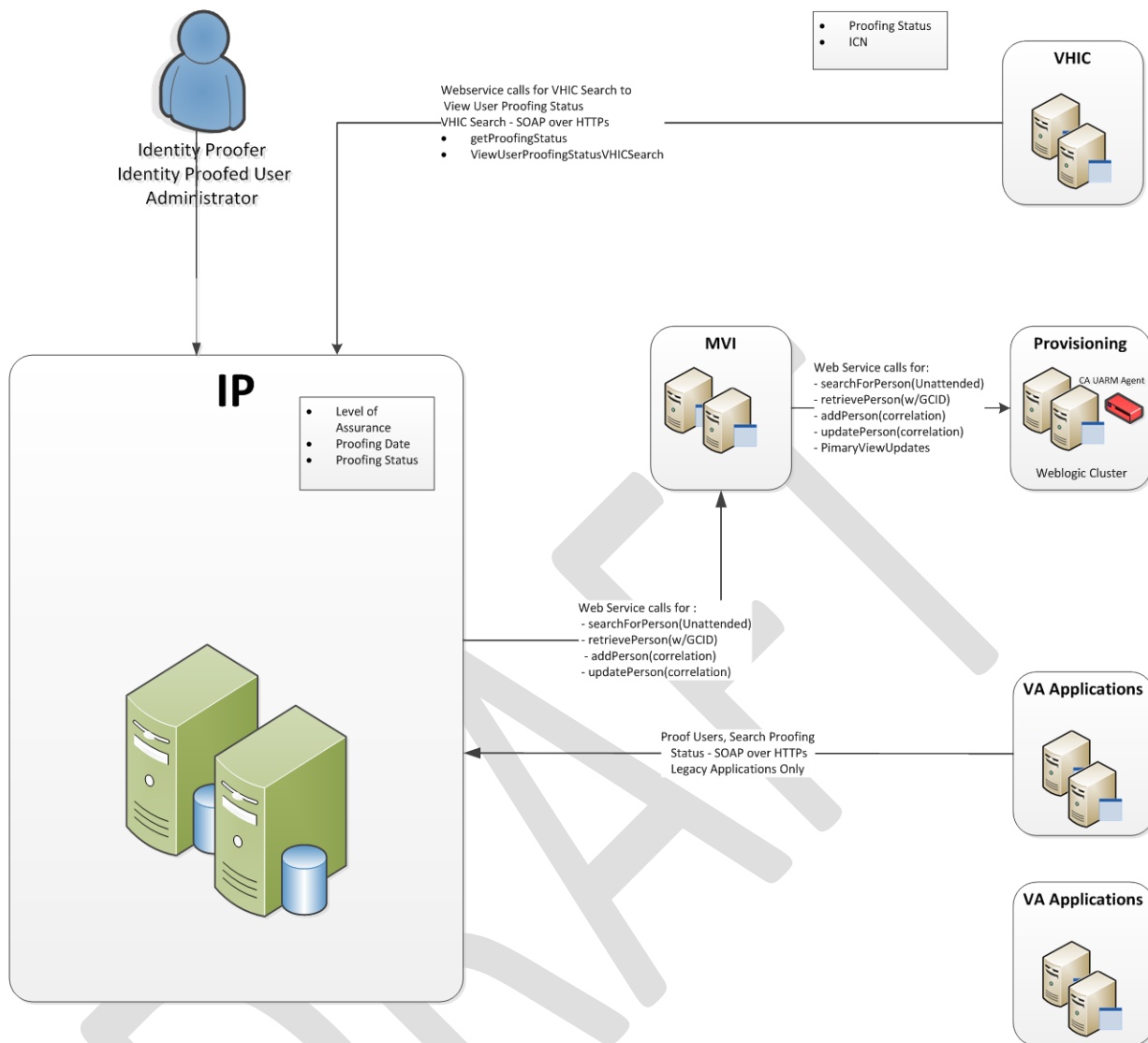


Figure 26: IP Service Oriented Architecture

IP provides the following WS interface:

Identity Proofing WS Interface – The CA IdentityMinder Task Execution Web Service (TEWS) exposes web services to applications as an interface to remotely trigger the execution of IP Service functions. This interface leverages WSDL and SOAP for integration with applications. This interface allows ID Proofer to perform IPP for LOA 2 or to retrieve the proofing status.

There are 2 major operations that occur between IP and consuming application are described below:

Proof Applicant (LOA 2): VA Identity Proofer (ID Proofer) verifies Applicant's identity in person and records information within IP Service tool for issuance of LOA 2 status.

1. Integrated applications will be able to interface with IP application via HTTPS POST messages. The POST message can contain any of the fields detailed below. A special case is when the business application submits a field named "CSPID". That field allows the IP application to load the IP record to be proofed. If that field is submitted, all other veteran data submitted with that request is ignored in favor of loading the IP data associated with that record ID. The POST message from the business application can contain a field named "ReturnURL" which contains the URL to which the business application requires the IP application to POST results after the IP application has completed the identity proof. If not included, that field will default to the URL of the page that posted the message.

Data Element Name	Definition/Description	Format
cspid	ID of the record in the IP system. If this field is included, other fields will be loaded from the IP record. Other person fields included in the POST message will be ignored.	String (any)
ReturnURL	URL of the page to be forwarded to upon completion of identity proofing. Default value is the URL of the page that submitted the POST message.	String (valid URL format)
firstname	First name of the person to be proofed.	String (A-z, ', -)
lastname	Last name of the person to be proofed.	String (A-z, ', -)
email	Email of the person to be proofed.	String (A-z, 0-9, ', - ,#,&. :. .)
dob	Date of Birth of the person to be proofed.	String ("MM/DD/YYYY")
street	Street address of the person to be proofed.	String (A-z, 0-9, ', - ,#,&. :. .)
city	City of residence of the person to be proofed.	String (A-z, ', -)
state	State of residence of the person to be proofed.	String (A-Z, length: 2)
postalcode	Postal code of the person to be proofed.	String (length: 10, ##### or #####-####)
country	Country of residence of the person to be proofed.	String (A-z, ', -)

Data Element Name	Definition/Description	Format
phone	Phone number of the person to be proofed.	String (length: 14, ###-###-#### or (###) ###-####)
origin	Origin of the identity proofing event (e.g. "VIC").	String (any)
operation	Operation for the IP system to perform (e.g. "Proof").	String (A-z)
affiliation	VA affiliation of the person to be proofed.	String (A-z)
proofinglocations	Location where the proofing event occurs.	String (A-z, ', -)
proofingcustom1	Field for custom data that needs to be returned to the business application.	String (any)
admin_id	Username of the user, requesting the Identity Proofing	String (A-z, 0-9)

Table 46: IP Web Service Interface Data Elements for Proof Applicant (LOA2) Request

Data Element Name	Definition/Description	Format
cspid	ID of the record in the IP system.	String (Any)
proofingstatus	Proofing status of the record in the IP system.	String (Any)
error	Error description	String (Any)
proofingcustom1	Echoed value from the POST to the IP system.	String (Any)

Table 47: IP Web Service Interface Data Elements for Proof Applicant (LOA2) Response

2. **Retrieve Proofing Status:** Application or system needs to retrieve the proofing status of an individual.

6.4.1. Service Description for IP

N/A

6.4.2. Service Design for IP

N/A

6.4.2.1. Introduction

N/A

6.4.2.1.1. Purpose and Scope of Service

N/A

6.4.2.1.2. Links to Other Documents

N/A

6.4.2.2. Service Details

N/A

6.4.2.2.1. Service Identification

N/A

6.4.2.2.2. Service Versions

N/A

6.4.2.2.3. Summary of Design and Platform Details

N/A

6.4.2.2.3.1. SOA Pattern(s) Implemented

N/A

6.4.2.2.3.2. COTS Platform vendor names and versions for hosting platform

N/A

6.4.2.3. Dependencies

N/A

6.4.2.4. Service Design Details

N/A

6.4.2.4.1. Interface Technical Specs

N/A

6.4.2.4.1.1. Service Invocation Type

N/A

6.4.2.4.1.2. Service Interface Type

N/A

6.4.2.4.1.3. Service Name

N/A

6.4.2.4.1.4. Interface

N/A

6.4.2.4.1.5. End Points

N/A

6.4.2.4.1.6. Operations or Methods

N/A

6.4.2.4.1.7. Message Schemas

N/A

6.4.2.4.2. Information Model

N/A

6.4.2.4.2.1. Class Diagram and Description of Entities Involved

N/A

6.4.2.4.2.2. Mappings from ELDM to Standards Based Schemas

N/A

6.4.2.4.3. Behavior Model (AKA Use Case Realization)

N/A

6.4.2.4.3.1. Use Cases (Use Case Model)

N/A

6.4.2.4.3.2. Interaction Diagrams

N/A

6.4.2.5. Gap Analysis

N/A

6.4.2.5.1. Variances from Enterprise Target Architecture

N/A

6.4.2.5.2. Variances from SLDs

N/A

6.4.2.5.3. Variances from Standards and Policies

N/A

6.4.2.5.4. Justification for Exceptions and Mitigation

N/A

6.4.3. Retrieve Proofing Status

IP has a web service interface to facilitate integration with other VA applications. The task that is exposed via web service is a search for an IP record that matches the submitted criteria. The web service is defined using the SOAP protocol, and web service messages are conveyed using HTTP. The IP web service is enabled through configuration of the CA Identity Manager product. The web service is described by an XML document named a Web Services Description Language (WSDL) file. The WSDL file can be found by accessing the URL for the applicable environment described in the table below.

The following tables describe the fields that are available to the Business Application as part of the web service interface:

Data Element Name	Definition/Description
--------------------------	-------------------------------

Data Element Name	Definition/Description
VAPERSONID	ID of the record in the IP system.
%FIRST_NAME%	First name of the person to be proofed.
%LAST_NAME%	Last name of the person to be proofed.
%EMAIL%	Email of the person to be proofed.
VADOB	Date of Birth of the person to be proofed.
postalAddress	Street address of the person to be proofed.
l	City of residence of the person to be proofed.
st	State of residence of the person to be proofed.
postalCode	Postal code of the person to be proofed.
country	Country of residence of the person to be proofed.
%USER_ID%	Username within the IP system.
Admin_id	Username of the user, requesting the Identity Proofing status

Table 48 IP Web Service Interface Data Elements For Retrieve Proofing Status Request

Data Element Name	Definition/Description
VAPERSONID	ID of the record in the IP system.
%FIRST_NAME%	First name.
%LAST_NAME%	Last name.
VAASSURANCELEVEL	Assurance level.
postalAddress	Street address.
l	City of residence.
st	State of residence.
postalCode	Postal code.
country	Country of residence.
telephoneNumber	Phone number.
VAIDPROOFSTATUS	Proofing status.
VAIDPROOFDATE	Date of proofing event (may be null).
VAIDPROOFCOMMENT	Comment for failed proofing event, will be null otherwise.

Table 49 IP Web Service Interface Data Elements for Retrieve Proofing Status Response

6.4.4.SOAP Request/Response Samples

6.4.4.1. Retrieve Proofing Status Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wSDL="http://tews6/wSDL">
  <soapenv:Header/>
  <soapenv:Body>
    <wSDL:TaskContext>
      <wSDL:admin_id>vicservice</wSDL:admin_id>
      <!--Optional:-->
      <wSDL:admin_password></wSDL:admin_password>
    </wSDL:TaskContext>
    <wSDL:ViewUserProofingStatusAppSearch>
      <wSDL:Filter index="0">
        <wSDL:Field>%FIRST_NAME%</wSDL:Field>
        <wSDL:Op>EQUALS</wSDL:Op>
        <wSDL:Value>pending</wSDL:Value>
        <!--Optional:-->
      </wSDL:Filter>
      <wSDL:Filter index="1">
        <wSDL:Field>%LAST_NAME%</wSDL:Field>
        <wSDL:Op>EQUALS</wSDL:Op>
        <wSDL:Value>veteran</wSDL:Value>
        <!--Optional:-->
        <wSDL:Conj>And</wSDL:Conj>
      </wSDL:Filter>
    </wSDL:ViewUserProofingStatusAppSearch>
  </soapenv:Body>
</soapenv:Envelope>
```

6.4.4.2. Retrieve Proofing Status Response

```
<soapenv:Envelope xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns="http://tews6/wSDL"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <soapenv:Body>
    <ViewUserProofingStatusAppSearchResult>
      <ImsStatus version="6.0">
        <transactionId>a1ccd8ec-406cd91f-5f37106d-0d15f2</transactionId>
      </ImsStatus>
      <ResultItem>
        <OID>uid=pendingveteran,ou=people,ou=csp,ou=iam,dc=va,dc=gov</OID>
        <VAPERSONID>
```

```

    <DISPLAY_NAME>CSP ID</DISPLAY_NAME>
    <ATTR_NAME>VAPERSONID</ATTR_NAME>
    <ATTR_VALUE>VACSP-dyKg1X2y</ATTR_VALUE>
    <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
</VAPERSONID>
<telephoneNumber>
    <DISPLAY_NAME>Phone Number</DISPLAY_NAME>
    <ATTR_NAME>telephoneNumber</ATTR_NAME>
    <ATTR_VALUE>111-111-1111</ATTR_VALUE>
    <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
</telephoneNumber>
<VAASSURANCELEVEL>
    <DISPLAY_NAME>Assurance Level</DISPLAY_NAME>
    <ATTR_NAME>VAASSURANCELEVEL</ATTR_NAME>
    <ATTR_VALUE>1</ATTR_VALUE>
    <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
</VAASSURANCELEVEL>
<c>
    <DISPLAY_NAME>Country</DISPLAY_NAME>
    <ATTR_NAME>c</ATTR_NAME>
    <ATTR_VALUE>UNITED STATES</ATTR_VALUE>
    <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
</c>
<postalAddress>
    <DISPLAY_NAME>Street Address</DISPLAY_NAME>
    <ATTR_NAME>postalAddress</ATTR_NAME>
    <ATTR_VALUE>Pending Street</ATTR_VALUE>
    <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
</postalAddress>
<l>
    <DISPLAY_NAME>City</DISPLAY_NAME>
    <ATTR_NAME>l</ATTR_NAME>
    <ATTR_VALUE>Burke</ATTR_VALUE>
    <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
</l>
<VAIDPROOFSTATUS>
    <DISPLAY_NAME>Identity Proof Status</DISPLAY_NAME>
    <ATTR_NAME>VAIDPROOFSTATUS</ATTR_NAME>
    <ATTR_VALUE>IdentityProofPending</ATTR_VALUE>
    <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
</VAIDPROOFSTATUS>
<st>
    <DISPLAY_NAME>State</DISPLAY_NAME>
    <ATTR_NAME>st</ATTR_NAME>
    <ATTR_VALUE>Virginia</ATTR_VALUE>
    <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
</st>
<_PCT_LAST_NAME_PCT_>
    <DISPLAY_NAME>Last Name</DISPLAY_NAME>
    <ATTR_NAME>%LAST_NAME%</ATTR_NAME>
    <ATTR_VALUE>Veteran</ATTR_VALUE>

```

```

        <ATTR_PERMISSION>ReadWrite</ATTR_PERMISSION>
    </_PCT_LAST_NAME_PCT_>
    <_PCT_FIRST_NAME_PCT_>
        <DISPLAY_NAME>First Name</DISPLAY_NAME>
        <ATTR_NAME>%FIRST_NAME%</ATTR_NAME>
        <ATTR_VALUE>Pending</ATTR_VALUE>
        <ATTR_PERMISSION>ReadWrite</ATTR_PERMISSION>
    </_PCT_FIRST_NAME_PCT_>
    <VAIDPROOFDATE>
        <DISPLAY_NAME>Identity Proof Date</DISPLAY_NAME>
        <ATTR_NAME>VAIDPROOFDATE</ATTR_NAME>
        <ATTR_VALUE/>
        <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
    </VAIDPROOFDATE>
    <VAIDPROOFINGCOMMENT>
        <DISPLAY_NAME>Reason (if Failed - Pending)</DISPLAY_NAME>
        <ATTR_NAME>VAIDPROOFINGCOMMENT</ATTR_NAME>
        <ATTR_VALUE/>
        <ATTR_PERMISSION>ReadOnly</ATTR_PERMISSION>
    </VAIDPROOFINGCOMMENT>
</ResultItem>
</ViewUserProofingStatusAppSearchResult>
</soapenv:Body>
</soapenv:Envelope>

```

6.4.4.3. Proof Applicant Request

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsdl="http://tews6/wsdl">
    <soapenv:Header/>
    <soapenv:Body>
        <wsdl:TaskContext>
            <wsdl:admin_id>imadmin</wsdl:admin_id>
            <!--wsdl:admin_password-->?</wsdl:admin_password-->
        </wsdl:TaskContext>
        <wsdl:IdentityProofUser>
            <wsdl:IdentityProofUserSearch>
                <!--Optional:-->
                <wsdl:CreateCopy>?</wsdl:CreateCopy>
                <!--Optional:-->
                <wsdl:CreateNew>?</wsdl:CreateNew>
                <!--You have a CHOICE of the next 2 items at this level-->
                <!--1 or more repetitions:-->
                <wsdl:Subject index="1">
                    <!--You have a CHOICE of the next 5 items at this level-->
                    <wsdl:UID>eddieuser01</wsdl:UID>
                    <!--wsdl:UniqueName-->?</wsdl:UniqueName-->
                    <!--wsdl:OID-->?</wsdl:OID-->
                    <!--wsdl:Name-->?</wsdl:Name-->
                    <!--wsdl:FriendlyName-->?</wsdl:FriendlyName-->
                </wsdl:Subject>
            </wsdl:IdentityProofUserSearch>
        </wsdl:IdentityProofUser>
    </soapenv:Body>
</soapenv:Envelope>

```

```

    <!--Optional:-->
    <wsdl:Check?></wsdl:Check>
</wsdl:Subject>
<!--Optional:-->
<wsdl:Organization>
    <wsdl:UniqueName?></wsdl:UniqueName>
    <wsdl:AndLower?></wsdl:AndLower>
</wsdl:Organization>
<!--You have a CHOICE of the next 2 items at this level-->
<!--1 or more repetitions:-->
<wsdl:Filter index="?">
    <wsdl:Field?></wsdl:Field>
    <wsdl:Op?></wsdl:Op>
    <wsdl:Value?></wsdl:Value>
    <!--Optional:-->
    <wsdl:Conj?></wsdl:Conj>
</wsdl:Filter>
<wsdl:Group>
    <wsdl:UniqueName?></wsdl:UniqueName>
</wsdl:Group>
</wsdl:IdentityProofUserSearch>
<wsdl:IdentityProofUserUserProfileTab>
    <!--Read Only - Next 5 items-->
    <!--wsdl:_PCT_FIRST_NAME_PCT_>Bill</wsdl:_PCT_FIRST_NAME_PCT_>
    <wsdl:_PCT_LAST_NAME_PCT_>Clinton</wsdl:_PCT_LAST_NAME_PCT_>
    <wsdl:_PCT_EMAIL_PCT_>billclinton@hotmail.com</wsdl:_PCT_EMAIL_PCT_>
    <wsdl:_PCT_USER_ID_PCT_>billclinton</wsdl:_PCT_USER_ID_PCT_>
    <wsdl:VADOB>05/12/1960</wsdl:VADOB-->
    <wsdl:VAIDPROOFLOC>Alabama</wsdl:VAIDPROOFLOC>
</wsdl:IdentityProofUserUserProfileTab>
<wsdl:IdentityProofUserAddressVerificationTab>
    <!--Read Only - Next 5 items-->
    <!--wsdl:postalAddress>8001 New Rd.</wsdl:postalAddress>
    <wsdl:l>Newark</wsdl:l>
    <wsdl:st>NJ</wsdl:st>
    <wsdl:c>UNITED STATES</wsdl:c>
    <wsdl:postalCode>27105</wsdl:postalCode-->
    <wsdl:VAADDRESSVALIDMETHOD>Primary
Identification</wsdl:VAADDRESSVALIDMETHOD>
    <wsdl:VAPOSTMARKDATE>05/12/1960</wsdl:VAPOSTMARKDATE>
</wsdl:IdentityProofUserAddressVerificationTab>
<wsdl:IdentityProofUserPrimaryIdentificationTab>
    <wsdl:VAPRIGOVPIIDTYPE>State-Issued Driver's License</wsdl:VAPRIGOVPIIDTYPE>
    <wsdl:VAPRIGOVPIIDCOUNTRY>UNITED STATES</wsdl:VAPRIGOVPIIDCOUNTRY>
    <wsdl:VAPRIGOVPIIDSTATE>California</wsdl:VAPRIGOVPIIDSTATE>
    <wsdl:VAPRIGOVPIIDNUMBER>8852041</wsdl:VAPRIGOVPIIDNUMBER>
    <wsdl:VAPRIGOVPIIDEXPDATE>05/12/2017</wsdl:VAPRIGOVPIIDEXPDATE>
    <wsdl:VAPRIPROFEXPDATE>Name</wsdl:VAPRIPROFEXPDATE>
</wsdl:IdentityProofUserPrimaryIdentificationTab>
<wsdl:IdentityProofUserSecondaryIdentificationTab>
    <wsdl:VASECGOVIDTYPE>Military ID Card</wsdl:VASECGOVIDTYPE>

```

```

    <wsdl:VASECGOVIDCOUNTRY>UNITED STATES</wsdl:VASECGOVIDCOUNTRY>
    <wsdl:VASECGOVIDSTATE>Alaska</wsdl:VASECGOVIDSTATE>
    <wsdl:VASECGOVIDNUMBER>8856972</wsdl:VASECGOVIDNUMBER>
    <wsdl:VASECGOVIDEXPDATE>04/12/2018</wsdl:VASECGOVIDEXPDATE>
    <wsdl:VASECPROFEXPDATE>Primary ID and Name</wsdl:VASECPROFEXPDATE>
  </wsdl:IdentityProofUserSecondaryIdentificationTab>
</wsdl:IdentityProofUser>
</soapenv:Body>
</soapenv:Envelope>

```

6.4.4.4. Proof Applicant Response

```

<soapenv:Envelope xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns="http://tews6/wsdl"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
  <soapenv:Body>
    <ImStatus version="6.0">
      <transactionId>76d53e5c-095cd955-c4c6f15d-071a08</transactionId>
    </ImStatus>
  </soapenv:Body>
</soapenv:Envelope>

```

7. External System Interface Design

This section describes the external interfaces with which the IP solution interacts.

The [master Interface Control Documents \(ICDs\)](#) and [integration ICDs](#) are available on the VA SharePoint site.

ID	Interface System	Description
IP Service	CSP TEWS Web Service	<ul style="list-style-type: none">- IP Calls TEWS Web Service- IP Searches for user- CSP Display Search Results- IP Updates users Assurance Level- IP Updates users Credential Level
IP Service	VHIC	<ul style="list-style-type: none">- VHIC sends an ICN and/or IP correlated identifier when checking the Proofing level of assurance.- When initiating a level 2 proofing operation, VHIC sends the ICN and Veteran name and address.- IP return the level of assurance at which a Veteran is proofed (if any) when the search is performed.- When a Proof is performed, IP returns the success or failure back VHIC.
IP Service	MVI	<ul style="list-style-type: none">- Initiate Identity Proofing task- If fully qualified identifier present, calls “Retrieve Person with get Corresponding IDs”- Create a LOA1 Record- Make a Add Person/Add Correlation Call- Updates users Assurance Level and proofing information based on Identification documents- Make a Update Person Call

Table 50: IP External System Interface

7.1. Interface Architecture

Not applicable for this increment.

7.2. Interface Detailed Design

Refer to section 3.2.3.

8. Human-Machine Interface

For user interface information related to COTS administrator functions, refer to the product documentation available at the following websites:

- CA support site: <https://support.ca.com>
- Oracle support site: <https://support.oracle.com>

Refer to section 3.2.3, which provides the interfaces that are used by AcS activities as appropriate for the end users.

8.1. Interface Design Rules

The following design rules are applicable to the user interfaces for the IP activities:

- The user and administrator interfaces comply with VA's branding specifications.
- The interface is easy to navigate with self-explanatory instructions / fields.
- The interface provides user friendly messages / information on error.
- The interface supports web browsers using Internet Explorer 7 (IE7), for Windows XP, IE9 for Windows7, and Mozilla Firefox3.6.23.
- The interface is Section 508 compliant (for non-administrator, end-user facing interfaces); the exception is CAR.
- The web interface provides necessary validation checks such as blanks for mandatory fields, special characters, and invalid email id format before form submission.

8.2. Inputs

The AcS activities are web pages, accessible via VA standard web-browsers. Navigation and data entry require no special devices beside mouse and keyboard, while meeting Section 508 compliance where appropriate.

Refer to section 3.2.3 for each of the web interface screen information regarding inputs to the system.

8.3. Outputs

In addition to web-based output and the ability to save web pages using native browser options, the following report media are generated by IP:

- PDF
- Comma Separated File (CSF)
- Excel

8.4. Navigation Hierarchy

This section documents the navigation hierarchy for IP activities that require the configuration of OOTB user interfaces.

IP supports IP and administrator functions.

IP Administrator: Performs administrative functions including controlling Identity Minder related configurations and tasks and managing the proofing registration interfaces.

Identity Proofer: Responsible for Identity Proofing users confirming identity of applicant to comply with SP 800-63 and VA 6501.

The following diagram depicts the flow for IP.

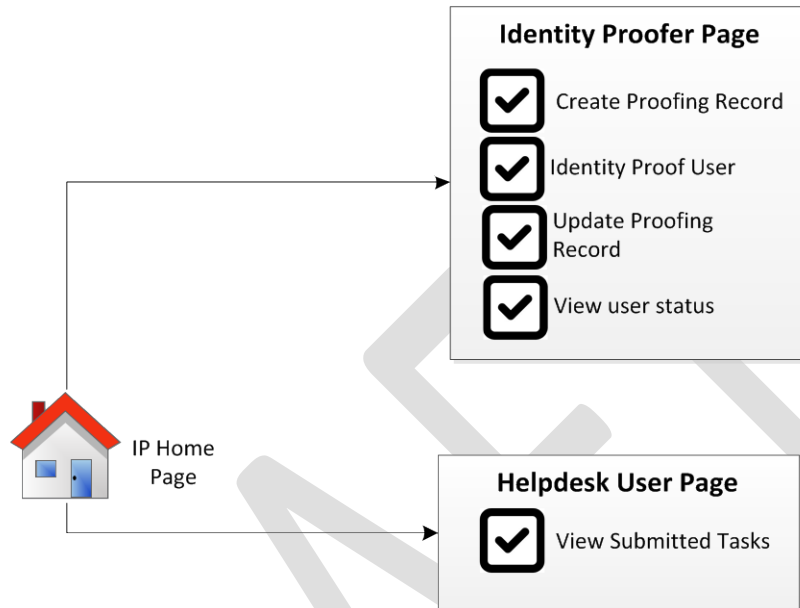


Figure 27: IP Navigation Hierarchy

9. Security and Privacy

Data security is critical for VA to safeguard user information and ensure that data in motion as well as rest is secured properly. For the AcS 2.0, the following security measures and integrity controls are in place.

Data in Motion:

Data in Motion is secured using the combination of FIPS encryption and VA issued certificates. Internal communications between CA components are encrypted using the cryptographic libraries that meet FIPS requirement. CA IdentityMinder uses the Advanced Encryption Standard (AES) adapted by the US Government. CA IdentityMinder incorporates the RSA Crypto-J v3.5 and Crypt-C ME v2.0 cryptographic libraries, which have been validated as meeting the FIPS 140-2 Security Requirements for Cryptographic Modules. CA SiteMinder Policy Server uses certified FIPS140-2 (AES) compliant cryptographic libraries.

CA UARM uses its own trusted root certificate, which is incorporated across agent and component communications. For AcS system internal communications, there is no compelling need these certificates to be replaced with VA Internal Certificate Authority (CA) or commercially trusted CA issued ones.

For communications outside of the AcS environment, certificates issued by VA Internal CA will be used for securing communications between the AcS and VA internal systems/applications and commercially trusted certificates will be used when the communication is exposed to external to VA clients and/or third parties.

9.1. Security

The requirements for Personally Identifiable Information (PII) are limited to data explicitly required in VA 6501 and NIST SP 800-63. However, the implementation adheres to the following integrity controls to ensure that acceptable security standards are met.

9.1.1. Confidentiality of Sensitive Information

The IP stores user record information required for Level 1 & Level 2 credentials for all proofing data. The data is encrypted using a FIPS 140-2 algorithm in CA Directory. The transmission of information occurs over SSL channel. In the identity proofing process, the identity proofer cannot view existing PII. The identity proofer manually enters data from the identity proofing artifacts provided by the person to be proofed, and that data are compared internally to the data stored in the IP application. Therefore, the identity proofer cannot “fish” for PII.

9.1.2. Privacy of Personal Information

The IP solution only stores the minimum PII necessary to proof the identity of the user. This information does NOT include the SSN. Sensitive data is encrypted using an approved FIPS 140-2 algorithm prior to storage. As noted, data communication occurs over TLS/SSL channels.

9.1.3. Process Integrity

The IP solution is designed to provide validation for input forms before storing the information in the user record. Each attribute that is entered in the user screens has regular expression

filtering built-in to confirm the validity prior to storage. Additionally, for data elements such as states, countries and dates, the input uses enumeration types via dropdowns to limit the data to acceptable values. The IP solution does not allow duplicate identification values. Users are required to confirm their accounts by following instructions emailed to them. Therefore, the IP users have their e-mail addresses verified prior to getting a Level 1 or Level 2 credential. The IP components have appropriate roles established to address each facet of the associated business processes. These roles clearly provide separation of duties. Additionally, due to full auditing of transactions, any misuse of authority is discernible and traceable in the audit logs and reports.

9.1.4. E-Sig Controls

The IP solution leverages e-Sig to minimize system failures, and access control to minimize human-interaction failures. The e-Sig service operates in a federated environment and requires that the user credentials that are being passed to it belongs to an authenticated Level-2 or above user.

9.2. Privacy

The IP solution only stores the minimum PII necessary to proof the identity of the user. This information does NOT include the SSN. Sensitive data is encrypted using an approved FIPS 140-2 algorithm prior to storage. As noted, data communication occurs over TLS/SSL channels.

Attachment A – Approval Signatures

This section is used to document the approval of the System Design Document. The review should be conducted face to face where signatures can be obtained ‘live’ during the review. If unable to conduct a face-to-face meeting then it should be held via LiveMeeting and concurrence captured during the meeting. The Scribe should add /es/name by each position cited. Example provided below.

The Chair of the governing Integrated Project Team (IPT), Business Sponsor, IT Program Manager, and Project Manager are required to sign.

Signed: _____

Integrated Project Team Chair and Business Sponsor Date

Signed: _____

OIS Business Sponsor Date

Signed: _____

IAM Program Manager Date

Signed: _____

AcS Program Manager Date

Signed: _____

Chief Architect Date

Signed: _____

SDE Date

A. Additional Information

The following spreadsheet provides detailed data model for IP activities:



A.1. RTM

Refer to section 1.6 for a complete list of requirements documents that are applicable to the IP solution.

A.2. Packaging and Installation

The deployment package for Infrastructure will provide details for special considerations if any for each of the components. The CA SSO client is deployed as a package to the desktop by Enterprise System Engineering (ESE) team. Using the CA SSO client installation and configuration documentation and response files provided in the deployment package, the ESE package builds and automates the process of CA SSO client to users system.

A.3. Design Metrics

A.4. Acronym List and Glossary

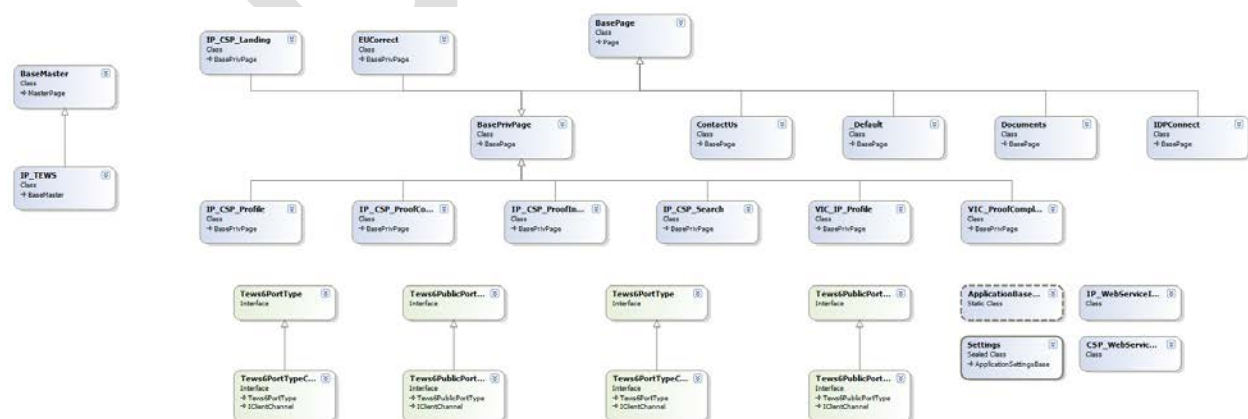
The acronyms and terms used in this SDD are defined in the [Identity and Access Services Master Glossary](#).

A.5. Required Technical Documents

A.6. Attach Documents

A.7. IP Class Diagram

The IP.NET wrapper class diagram is shown below.



Template Revision History

Date	Version	Description	Author
January 2015	2.8	Updated to latest Section 508 guidelines and remediated with Common Look Office Tool	Process Management
September 2014	2.7	Adds Enterprise Shared Services terms and requires AERB Compliance Certificate attachment.	Process Management
August 2014	2.6	Signature block update authorized by AERB CR_018934	Process Management
March 2014	2.5	Section 508 repairs to new version approved by AERB Chair approved	Process Management
August 2013	2.3	Replaced the Service Architecture sub-section with new sub-sections for consumed and provided services. Also applied miscellaneous feedback from VA team.	ASD Enterprise Shared Services (ESS) Work Group
June 2013	1.3	Upgraded to MS Office 2007-2010 format	Process Management
June 2013	1.2	Address inconsistencies in Section 3, Conceptual Design, Correct headings	Process Management
March 2013	1.1	Formatted to documentation standards and edited for Section 508 conformance	Process Management
January 2013	1.0	Initial Document	PMAS Business Office

See TOGAF® 9.1, Part III: ADM Guidelines & Techniques, Gap Analysis on TOGAF website at <http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap27.html>