

Department of Veterans Affairs

Identity and Access Management Access Services Solution 2.0 Increment 3

System Design Document



**April 2014
Version 2.2**

Revision History

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

| Date | Version | Description | Author |
|------------|---------|---|------------------------------|
| 05/08/2014 | 2.2 | Embedded email approval signatures to the PDF version to post on the AcS TSPR. Completed a quality review. | Bruce [REDACTED] HPTi/DRC |
| 04/14/2014 | 2.2 | Updated based on formal review | VetsAmerica |
| 04/04/2014 | 2.2 | Updated based on additional comments | VetsAmerica |
| 04/01/2014 | 2.2 | Updated document based on peer review feedback | VetsAmerica |
| 03/14/2014 | 2.2 | Updated design sections for increment 3 for SSOi, CAR, IP, VDS, CSP, and Provisioning | VetsAmerica |
| 1/31/2014 | 2.1 | Re-formatted to coincide with the ProPath SDD template and made some text edits. Added email approval signatures to PDF version to post on the AcS TSPR. | Bruce [REDACTED] HPTi/DRC |
| 12/18/2013 | 2.1 | Minor update to BRD reference after Formal Review | AcS Tech Leads |
| 11/22/2013 | 2.0 | Updates to include new functionality; decoupling of CSP and IP, Mobility for SSOi, CRISP Onboarding, and removal of application specific data | VetsAmerica |
| 09/12/2013 | 1.9 | Design elements to address RSD 2.0 | VetsAmerica |
| 07/02/2013 | 1.8 | Updates from peer review feedback. | HPES |
| 06/24/2013 | 1.7 | Updates from peer review feedback. | HPES |
| 06/07/2013 | 1.6 | Updates for Increment 4. Added CRISP on/off boarding workflow definitions, IP integration with MVI., Provisioning integration with MVI, PIV, AD, and TMS | HPES |
| 05/25/2013 | 1.5 | Baselined for Increment 4 | HPES |
| 02/11/2013 | 1.4 | Updates to VIP and VM tables, additional diagram updates, and additional technical clarifications following formal review | HPES; [REDACTED] |
| 01/14/2012 | 1.3 | Additional Updates from consolidated peer review feedback. Updated diagrams, tables and text to reflect Terremark environments; added technical clarifications. | HPES; [REDACTED] |

| Date | Version | Description | Author |
|-------------|----------------|--|---------------|
| 12/12/2012 | 1.2 | Updates from peer review feedback. Modification of location from AITC to Terremark and Modification of patch levels. | HPES |
| 11/30/2012 | 1.1 | Modification of Increment 2 SDD as base document to combine increment 2 and increment 3 into a single document | HPES |
| 05/11/2012 | 1.0 | Final- Addressed WP R comments. | VetsAmerica |
| 04/20/2012 | 0.1 | Initial Draft | VetsAmerica |

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 with conceptual design is required prior to the Milestone 1 Review. The as-built for each delivery must be incorporated prior to the Milestone 2 Review.

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 | 1 |
| 1.1 | Purpose of this document | 2 |
| 1.2 | Identification | 2 |
| 1.3 | Scope..... | 3 |
| 1.4 | Relationship to Other Plans | 5 |
| 1.5 | Methodology, Tools, and Techniques | 6 |
| 1.6 | Constraining Policies, Directives and Procedures..... | 6 |
| 1.7 | Constraints | 8 |
| 1.8 | Design Trade-offs | 11 |
| 1.9 | User Characteristics..... | 11 |
| 1.10 | User Problem Statement..... | 12 |
| 2 | Background | 12 |
| 2.1 | Overview of the System | 12 |
| 2.2 | Overview of the Business Process | 13 |
| 2.3 | Assumptions..... | 13 |
| 2.4 | Legacy System Retirement..... | 16 |
| 3 | Conceptual Design..... | 16 |
| 3.1 | Conceptual Application Design..... | 16 |
| 3.1.1 | Application Context..... | 16 |
| 3.1.2 | High-Level Application Design | 29 |
| 3.1.3 | Application Locations | 30 |
| 3.1.4 | Application Users | 33 |
| 3.2 | Conceptual Data Design | 34 |
| 3.2.1 | Project Conceptual Data Model | 34 |
| 3.2.2 | Database Information | 37 |
| 3.2.3 | User Interface Data Mapping | 39 |
| 3.3 | Conceptual Infrastructure Design..... | 69 |
| 3.3.1 | System Criticality and High Availability..... | 69 |
| 3.3.2 | Special Technology | 70 |
| 3.3.3 | Technology Locations..... | 70 |
| 3.3.4 | Conceptual Infrastructure Diagram..... | 70 |
| 4 | System Architecture | 73 |
| 4.1 | Hardware Architecture | 74 |
| 4.2 | Software Architecture | 85 |
| 4.3 | Communications Architecture | 99 |
| 4.4 | Communication Channel Security | 101 |

| | | |
|--------|--|-----|
| 4.5 | AcS Inter-component Communications | 101 |
| 4.5.1 | Production Server PKI Certificate List | 111 |
| 5 | Data Design | 118 |
| 5.1 | DBMS Files..... | 118 |
| 5.2 | Non-DBMS Files..... | 119 |
| 6 | Detailed Design | 119 |
| 6.1 | Hardware Detailed Design | 119 |
| 6.2 | Software Detailed Design | 120 |
| 6.2.1 | Provisioning Design | 120 |
| 6.2.2 | Role Manager (SailPoint IdentityIQ) Design | 134 |
| 6.2.3 | VDS – Attribute Exchange Service Design | 140 |
| 6.2.4 | SSOi Design | 147 |
| 6.2.5 | CSP Design | 172 |
| 6.2.6 | IP Design | 178 |
| 6.2.7 | SAC Design | 183 |
| 6.2.8 | eSig Design | 190 |
| 6.2.9 | CAR Design | 194 |
| 6.2.10 | Product Perspective | 197 |
| 6.2.11 | Specific Requirements | 199 |
| 6.3 | Communications Detailed Design..... | 199 |
| 7 | External Interface Design | 199 |
| 7.1 | Interface Architecture | 199 |
| 7.1.1 | VA CSP Federation with VAAFI | 199 |
| 7.1.2 | Master Veteran Index..... | 200 |
| 7.1.3 | VA Active Directory | 201 |
| 7.2 | Interface Detailed Design..... | 202 |
| 7.2.1 | VA CSP Federation with VAAFI | 202 |
| 7.2.2 | Master Veteran Index..... | 203 |
| 7.2.3 | VA Active Directory | 203 |
| 8 | Human-Machine Interface | 203 |
| 8.1 | Interface Design Rules..... | 203 |
| 8.2 | Inputs..... | 204 |
| 8.3 | Outputs..... | 204 |
| 8.4 | Navigation Hierarchy..... | 205 |
| 8.4.1 | CSP | 205 |
| 8.4.2 | IP | 206 |
| 8.4.3 | Provisioning | 206 |
| 9 | System Integrity Controls | 207 |

| | | |
|------------|--|------------|
| 9.1 | CSP and IP | 209 |
| 9.1.1 | Confidentiality of Sensitive Information | 209 |
| 9.1.2 | Privacy of Personal Information | 210 |
| 9.1.3 | Process Integrity | 210 |
| 9.2 | eSig..... | 210 |
| 9.2.1 | Confidentiality of Sensitive Information | 210 |
| 9.2.2 | Privacy of Personal Information | 210 |
| 9.2.3 | Process Integrity | 210 |
| 9.2.4 | System Availability | 210 |
| 9.3 | SAC..... | 211 |
| 9.3.1 | Confidentiality of Sensitive Information | 211 |
| 9.3.2 | Privacy of Personal Information | 211 |
| 9.3.3 | Process Integrity | 211 |
| 9.3.4 | System Availability | 211 |
| 9.4 | Provisioning..... | 211 |
| 9.4.1 | Confidentiality of Sensitive Information | 211 |
| 9.4.2 | Privacy of Personal Information | 212 |
| 9.4.3 | Process Integrity | 212 |
| 9.4.4 | System Availability | 212 |
| 9.5 | SSOi..... | 212 |
| 9.5.1 | Confidentiality of Sensitive Information | 212 |
| 9.5.2 | Privacy of Personal Information | 212 |
| 9.5.3 | Process Integrity | 213 |
| 9.5.4 | System Availability | 213 |
| 9.6 | CAR..... | 213 |
| 9.6.1 | Confidentiality of Sensitive Information | 213 |
| 9.6.2 | Privacy of Personal Information | 213 |
| 9.6.3 | Process Integrity | 213 |
| 9.6.4 | System Availability | 213 |
| 9.7 | Virtual Directory Service (VDS)..... | 214 |
| 9.7.1 | Confidentiality of Sensitive Information | 214 |
| 9.7.2 | Privacy of Personal Information | 214 |
| 9.7.3 | Process Integrity | 214 |
| 9.7.4 | System Availability | 215 |
| 9.8 | Role Manager..... | 215 |
| 9.8.1 | Confidentiality of Sensitive Information | 215 |
| 9.8.2 | Privacy of Personal Information | 215 |
| 9.8.3 | Process Integrity | 215 |

| | | |
|-----------|--|------------|
| 9.8.4 | System Availability | 215 |
| 10 | Approval Signatures | 216 |
| A. | Additional Information | 218 |
| A.1. | Data Dictionary | 218 |
| A.2. | CRISP Onboarding/Offboarding Attributes | 218 |
| A.3. | RTM..... | 218 |
| A.4. | Packaging and Installation | 218 |
| A.5. | Design Metrics | 218 |
| A.6. | Acronym List and Glossary | 219 |
| A.7. | Required Technical Documents | 219 |
| A.8. | CSP Class Diagram | 219 |
| A.9. | IP Class Diagram | 219 |
| A.10. | Responses to Produce WS-Security Headers..... | 220 |
| A.11. | Responses to XML Encryptions, Decryptions, and Digital Signature ... | 221 |

List of Figures

| | | |
|------------|---|----|
| Figure 1: | AcS Solution Overview | 17 |
| Figure 2: | CSP Context Diagram | 18 |
| Figure 3: | IP Context Diagram | 20 |
| Figure 4: | eSig Context Diagram | 21 |
| Figure 5: | SAC Context Diagram | 22 |
| Figure 6: | PROV Context Diagram | 23 |
| Figure 7: | SSOi Context Diagram | 25 |
| Figure 8: | CAR Context Diagram..... | 28 |
| Figure 9: | AcS Solution Application Design | 29 |
| Figure 10: | AcS Solution Conceptual Data Mode | 35 |
| Figure 11: | New VA Employee Profile Information | 39 |
| Figure 12: | New VA Contractor Profile Information..... | 40 |
| Figure 13: | New HP Trainee Profile Information | 40 |
| Figure 14: | New Volunteer Profile Information | 41 |
| Figure 15: | New VA Employee Work/Home Location Information..... | 41 |
| Figure 16: | New VA Contractor Work/Home Location Information | 42 |
| Figure 17: | New HP Trainee Work/Home Location Information..... | 42 |
| Figure 18: | New Volunteer Work/Home Location Information | 43 |
| Figure 19: | New VA Employee Organization and Employment Information..... | 43 |
| Figure 20: | New VA Contractor Organization and Employment Information | 44 |
| Figure 21: | New HP Trainee Organization and Employment Information | 45 |
| Figure 22: | New Volunteer Organization and Employment Information | 46 |

| | |
|--|-----|
| Figure 23: New VA Employee Miscellaneous Information | 47 |
| Figure 24: New VA Contractor Miscellaneous Information | 48 |
| Figure 25: New HP Trainee Miscellaneous Information | 49 |
| Figure 26: New Volunteer Miscellaneous Information | 50 |
| Figure 27: CRISP Checklist Screen | 51 |
| Figure 28: Modify Account: Step 1 User Profile | 52 |
| Figure 29: Modify Account: Step 2 Security Questions..... | 53 |
| Figure 30: Change Password | 54 |
| Figure 31: Upgrade to Level 2: Step 1 User Profile | 55 |
| Figure 32: Upgrade to Level 2: Step 2 Security Questions..... | 56 |
| Figure 33: Self-Registration: Step 1 User Profile | 57 |
| Figure 34: Self-Registration: Step 2 Security Questions | 58 |
| Figure 35: Identity Proof User: Step 1 User Profile | 59 |
| Figure 36: Identity Proof User: Step 2 Address Verification | 60 |
| Figure 37: Identity Proof User: Step 3 Primary Verification | 61 |
| Figure 38: Identity Proof User: Step 4 Secondary Identification..... | 61 |
| Figure 39: Update a User: Step 1 User Profile | 62 |
| Figure 40: Update a User: Step 2 Address Verification | 63 |
| Figure 41: Update a User: Step 3 Primary Identification..... | 64 |
| Figure 42: Update a User: Step 4 Secondary Identification..... | 64 |
| Figure 43: SSOi Centralized Login Page | 65 |
| Figure 44: SSOi PIV Only Login Page..... | 66 |
| Figure 45: Mobile Login Page | 67 |
| Figure 46: SAC PAP Landing Page..... | 68 |
| Figure 47: SAC PAP Landing Page..... | 68 |
| Figure 48: AcS Production Environments | 71 |
| Figure 49: Logical Network String Diagram..... | 73 |
| Figure 50: Network Communication Architecture | 74 |
| Figure 51: Software Architecture | 86 |
| Figure 52: AcS Network Security Topology..... | 100 |
| Figure 53: Provisioning Detail Design..... | 121 |
| Figure 54: Role Manager Detailed Design..... | 135 |
| Figure 55: VDS Detailed Design | 143 |
| Figure 56: PROV-VDS-MVI Design | 144 |
| Figure 57: SSOi Detailed Design..... | 148 |
| Figure 58: SSOi STS Architecture Diagram | 150 |
| Figure 59: Centralized Logon Page Flow | 171 |

| | |
|--|------------|
| Figure 60: Siteminder Policy Architecture for Core Centralized Authentication Flows | 172 |
| Figure 61: CSP Detailed Design | 173 |
| Figure 62: IP Detailed Design | 179 |
| Figure 63: SAC Detailed Design | 184 |
| Figure 64: eSig Detailed Design | 191 |
| Figure 65: CAR Detailed Design | 195 |
| Figure 66: CSP to VAAFI Interface Flow | 200 |
| Figure 67: MVI Interface Flow with Provisioning and IP | 201 |
| Figure 68: Provisioning – Active Directory Interface Architecture | 202 |
| Figure 69: CSP Navigation Hierarchy | 205 |
| Figure 70: IP Navigation Hierarchy | 206 |
| Figure 71: Provisioning Navigation Hierarchy | 207 |
| Figure 72: CSP Class Diagram | 219 |
| Figure 73: IP Class Diagram | 219 |

List of Tables

| | |
|--|-----------|
| Table 1: System Identification | 2 |
| Table 2: Scope Inclusions | 3 |
| Table 3: Scope Exclusion | 4 |
| Table 4: Project Documents | 5 |
| Table 5: Policies, Directives, and Procedures | 7 |
| Table 6: Assumptions and Constraints | 13 |
| Table 7: CSP Application Context Description | 18 |
| Table 8: IP Application Context Description | 20 |
| Table 9: eSig Application Context Description | 21 |
| Table 10: SAC Application Context Description | 22 |
| Table 11: PROV Application Context Description | 24 |
| Table 12: SSOi Application Context Description | 26 |
| Table 13: CAR Application Context Description | 28 |
| Table 14: Activities in the High-Level Application Design | 30 |
| Table 15: AcS Solution Application Locations | 31 |
| Table 16: AcS Solution Users | 33 |
| Table 17: Database Inventory | 35 |
| Table 18: Database Inventory | 38 |
| Table 19: Special Technology Requirements | 70 |
| Table 20: Hardware Appliance | 75 |
| Table 21: Virtual Machines and Appliances | 76 |

| | |
|--|------------|
| Table 22: AcS Products and Versions..... | 87 |
| Table 23: Software Components..... | 89 |
| Table 24: Programming Languages..... | 98 |
| Table 25: Operating Systems | 99 |
| Table 26: Port Communications and Protocols..... | 101 |
| Table 27: Pre-Production PKI Certificate List | 106 |
| Table 28: Production Cert List | 111 |
| Table 29: Database File System | 118 |
| Table 30: Potential Impact Categories for Authentication Errors | 178 |
| Table 31: AcS Solution Products | 197 |

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 solution, 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)
- Credential Service Provider (CSP)
- Electronic Signature (eSig)
- Identity Proofing (IP)
- Provisioning (PROV)
- Specialized Access Control (SAC)
- 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 solution 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 solution's primary customers are both internal and external user communities who need logical access to VA business applications. The primary subsystems for the AcS system, in part, include the following:

- Service Provider (SP)
- Identity Provider (IdP)
- Credential Service Provider (CSP)
- Secure Proxy Service
- Agentless Single Sign-On
- Mobile Authentication and Authorization
- SOA Provisioning Services
- Role Management
- Identity Management
- Fine-Grained Access Control
- WS Security
- e-Signatures
- Attribute Exchange
- Identity Access Governance

1.1 Purpose of this document

The purpose of the System Design Document (SDD) is to describe the supporting mechanics of the AcS 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 will be updated (as applicable) when modifications are incorporated and / or new capabilities are added to the solution (when appropriate).

The primary target audience is AcS 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 Solution Architects
- AcS Solution 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 AcS 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 solution. This document applies to the following systems and software:

Table 1: System Identification

| Name | Description | Abbreviation | Version | Release |
|-----------------|--|--------------|---------|-------------------------|
| VA AcS Solution | 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 2.0.0 | Release 3 (Increment 3) |

1.3 Scope

This document focuses on the technical system design to provide the foundation for the AcS 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.

Note: The remote proofing service is provided on another contract and supported through VAAFI.

Table 2: Scope Inclusions

| Includes |
|---|
| SSOi: <ul style="list-style-type: none">• Provides authentication and authorization support for VA applications• Accepts federated credentials through VA Authentication Federation Infrastructure (VAAFI) for third party providers such as: DoD Users (CAC), USAA, FCCX, and non-VA PIV• Provides VA internal users authentication and authorization support on mobile devices• Provides legacy application support for SSO• Provides support for PIV Compliant authentication (LOA 3)• Provides global log off for integrated applications/services• Provides Secure Token Service (STS) capabilities with a response message that supports the SAML format, WS-Trust protocol, and WS-Policy protocol.• Provides support for extending the SAML attributes with Provisioning data |
| CSP: <ul style="list-style-type: none">• Issues Level of Assurance (LOA) 1 and LOA 2 credentials to VA persons of interest• Federates the CSP/IP solution with VAAFI using Security Assertion Markup Language (SAML) 2.0 |
| eSig: <ul style="list-style-type: none">• Provides capability to electronically sign and verify documents using web service based task• Provides support for documents types –Word, Excel, PDF and web based email• Provides eSig enrollment services to allow the eligible external users for VA internal applications to sign the document. eSig is limited to external persons of interest, Veterans or non-Veterans that do not have credentials that carry signing certificates (hard token or soft token)• Provides functionality to delete user access |
| IP: <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• Integrates with the Master Veteran Index (MVI)• IP supports MVI error codes AE (invalid payload) and AR (MVI system components down) |
| PROV: <ul style="list-style-type: none">• Provides user account provisioning along with pre-defined roles for VA application |

| |
|--|
| Includes |
| <ul style="list-style-type: none"> • Supports onboarding of employee, contractor, volunteer, and health professionals generating a unique identifier SEC ID and utilizes the CRISP checklist to provision an account • Provisioning service is accessed and available for authorized systems serving operational and self-service based applications for both the internal and external user populations, such as AccessVA • Provides self-service capability for users to request access to integrated applications and services • Provides capability to pre-defined Privileged Users to request access (i.e., provision, de-provision, and modify user access) to integrated application • Provides automated workflows for request approval from designated approvers and provide necessary notifications via email correspondence(s) • Delegates approvals to designated approvers • Escalates approvals in case no action has been taken • Supports the update of LOA value associated with the user record for user onboarding • Virtual Directory Service (VDS) integrates with provisioning and MVI to pull pre-defined attributes for creation of a combined view (Provisioning and MVI) for MVI integration with VDS. • Provides role manager integration with authoritative source provisioning identity store (CA LDAP directory as a read only connection) to pull user identities and associated attributes (This integration with the authoritative source is used for pulling in user information to create identity cubes in SailPoint IdentityIQ) |
| SAC: |
| <ul style="list-style-type: none"> • Provides a Policy Decision Point (PDP) and Policy Administration Point (PAP) according to the OASIS eXtensible Access Control Markup Language (XACML) 3.0 standard • Provides available Software Development Kits (SDKs) for VA applications to perform Policy Enforcement Point (PEP) capabilities • Utilizes a virtual directory as the Policy Information Point (PIP) |
| CAR: |
| <ul style="list-style-type: none"> • Integrates with the AcS solution activities such as provisioning, SSOi (CA SiteMinder), CSP, IP, SAC and e-Sig to provide audit reports based on agreed upon data and alerts for daily reports |

Table 3: Scope Exclusion

| |
|---|
| Excludes |
| SSOi: |
| <ul style="list-style-type: none"> • No support of biometric authentication is provided due to limitation of current products • No support for OAuth capabilities is due to unavailability of OAuth infrastructure and required products. |

| |
|--|
| Excludes |
| CSP: <ul style="list-style-type: none"> • Issuance of Level 3 or 4 credentials are deferred • Relying Party Initiated SAML SSO with any other relying parties other than VAAFI |
| eSig: <ul style="list-style-type: none"> • Does not require a GUI, thus it does not provide registration screens for a user • User authentication is the responsibility of individual VA application • Does not support PowerPoint and client based email signing capability due to limitation of product • Does not integrate with a third party Certificate Authority (CA) |
| IP: <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 |
| PROV: <ul style="list-style-type: none"> • Role manager is not integrated with any Provisioning service for performing provisioning activities or to provide mined roles as per Increment 3 • Role manager is configured in the development environment only to perform governance activities and there will be no integration of the SailPoint tool with provisioning (CA Identity Minder) system or SSOi (CA Siteminder) system |

1.4 Relationship to Other 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 have hyperlinks to the VA IAM SharePoint and TSPR folders (as of the issuance of this artifact).

Note: The applicable standards and guidelines from the VA Handbook and NIST are identified in section 1.6 below.

Table 4: Project Documents

| Document Name | Description |
|---|---|
| I3 Requirements Specification Document: AcS 2.0 i3 RSD | Provides requirements for AcS Increment 3. |
| VA AcS FY14 Business Requirements Document: FY14 IAM Access Services BRD | Defines the “As Is” and “To Be” business area, operating environment, the system requirements and capabilities desired by stakeholders. Document provides performance and workload requirements along with availability requirements. |
| I2 Requirements Specification Document: VA AcS Solution RSD I2 | Provides requirements for AcS Increment 2. |

| Document Name | Description |
|--|--|
| I3 Requirements Specification Document: AcS Requirements Specification Document I3 v2 | Provides updated requirements for AcS Increment 3 |
| I4 Requirements Specification Document: AcS Requirements Specification Document i4 V6 | Provides updated requirements for AcS Increment 4 |
| I3 Use Cases: VA AcS Solution Use Case Model i3 rev 2.2AC | Provides use cases for AcS solution |
| I4 Use Cases: VA AcS Solution UC Model i4 AC | Provides use cases for AcS solution |
| I3 Requirements Traceability Matrix: VA AcS Solution i3 RTM | Provides the requirements traceability matrix for the AcS solution |
| I4 Requirements Traceability Matrix: VA AcS Solution i4 RTM | Provides the requirements traceability matrix for the AcS solution |
| Identity Proofing Integration to the Master Veteran Index (MVI) Requirements Specification Document iRSD - Version 0.4 CSP IP MVI Integration RSD - 050513 Document Update.docx | IP integration to the MVI |
| Provisioning Security Identifier Integration to the Master Veteran Index (MVI) iRSD Version 0.16 MVI SEC ID RSD v0_16.docx | Provisioning SEC ID integration to MVI |

1.5 Methodology, Tools, and Techniques

The system design will follow the Office of Enterprise Development (OED) ProPath methodology as outlined at [REDACTED]

Design diagrams have been created using Microsoft Visio or Microsoft PowerPoint for integration into Microsoft Word.

1.6 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: Policies, Directives, and Procedures

| # | Issuing Agency | Policy, Directive, or Procedure | Purpose |
|---|----------------|---|--|
| 1 | VA | VA 6500 Handbook | <ul style="list-style-type: none"> • Directive Information Security Program. • Defining overall Security Framework for VA. |
| 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. |
| 3 | VA | VA 6300 Directive | <ul style="list-style-type: none"> • Directive Records and Information Management. • Defines information management framework for VA Access Services. |
| 4 | NIST | SP 800-53-4 | <ul style="list-style-type: none"> • Special Publication – Recommended Security Controls for Federal Information Systems and Organizations. • Defines the required security controls for IT systems under the Federal Information Security Management Act (FISMA). |
| 5 | 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. |
| 6 | 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. |
| 7 | 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. |
| 8 | 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. |
| 9 | 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. |

| # | Issuing Agency | Policy, Directive, or Procedure | Purpose |
|----|---|---------------------------------|--|
| 10 | 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. |
| 11 | OMB | M-11-11 | <ul style="list-style-type: none"> Requirements for Accepting Externally-Issued Identity Credentials. FICAM architecture and procedures for federal agencies. |
| 12 | 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. |
| 13 | White House | NSTIC | <ul style="list-style-type: none"> National Strategy for Trusted Identities in Cyberspace (NSTIC) – Provides guidance for identity trust in cyberspace. |
| 14 | US Congress | FISMA | <ul style="list-style-type: none"> FISMA of 2002, Public Law 107-347 |
| 15 | 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. |
| 16 | US Congress | The Privacy Act of 1974 | <ul style="list-style-type: none"> § 552a. Records maintained on individuals. Defines VA Access Services Privacy assessment and control requirements. |
| 17 | National Archives and Records Administration (NARA) | Federal Records Act | <ul style="list-style-type: none"> Establishes the framework for records management programs in Federal Agencies. |
| 18 | VA | VA D 0735 | <ul style="list-style-type: none"> Homeland Security Presidential Directive 12 (HSPD-12) Program Defines Department-wide policy, roles, and responsibilities for the creation and maintenance of systems and processes to implement VA's HSPD-12 Program necessary to implement Homeland Security Presidential Directive 12 (HSPD-12) program. |
| 19 | OMB | M-05-24 | <ul style="list-style-type: none"> Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors. |

1.7 Constraints

This document is developed under the schedule and cost defined in the contract for VA AcS development support. The design is constrained to features available in the tools, technologies, and frameworks defined by VA Technical Reference Model (TRM) tools list and those that have been accepted by VA.

AcS Service - Provisioning

- **Radiant Logic:** Per VA Handbook 6500, FIPS 140-2 certified encryption must be used to encrypt data in transit if PII/PHI/VA sensitive information is involved or additional mitigating controls must be documented in an accepted System Security Plan (SSP). This system may not be used outside of the VA production network (not in a DMZ) unless otherwise approved by the Enterprise Security Change Control Board (ESCCB), along with a memorandum of Understanding and Interconnection Security Agreements (MOU/ISA), which detail the security requirements for those users and systems that share information and resources outside of the VA production network.
- **Radiant Logic (VDS):** The interfaces are SSL enabled. The consumers will require a VDS managed credentials (User ID /Password) to access the VDS via the DataPower Web service interface. This activity is necessitated by DataPower terminating the consumer's SSL session and initiating a session between DataPower and the VDS effectively removing any auditable information (IP address, PKI credentials, etc.). The attribute provider interfaces will authenticate via PKI credentials (Mutual SSL).
- **Radiant Logic (VDS):** Provisioning provides VDS access to attributes that reflect the initial creation or the most recent modification timestamp of a user record. These attributes must be indexed, of Generalized Time Syntax, and support generalizedTimeMatch (EQUALITY), generalizedTimeOrderingMatch (ORDERING). PII data sent to VDS has to be encrypted at the source (Provisioning or MVI). VDS can not encrypt data at rest prior to writing to the disk (product limitation).
- **Radiant Logic (VDS):** Provisioning will provide VDS access to attributes that reflect the initial creation or the most recent modification timestamp of a user record. These attributes must be indexed, of Generalized Time Syntax, and support generalizedTimeMatch (EQUALITY), generalizedTimeOrderingMatch (ORDERING). PII data sent to VDS has to be encrypted at the source (Provisioning or MVI). VDS cannot encrypt data at rest prior to writing to the disk (product limitation). To mitigate this risk, an implementation strategy to encrypt the data in phases is been advocated and documented in the system security plan. The various phases, on an high level to secure the data at rest are:
 1. Protect through the use of Data Center physical security controls
 2. Analyse various encryption solutions
 3. Implement the best security solution
- **CA IdentityMinder:** CA IdentityMinder's connector Xpress cannot update certain attributes – record created by, record created date, record modified by, and record modified date in to membership mapping tables. This type of functionality would require a custom connector outside of the Connector Xpress and would therefore be proprietary.
- **Unique Identifiers:** The AcS solution does not have a common single unique identifier throughout the AcS activities, increasing the complexity of the integration between activities. SECID will be used by AcS to build and link Identity records with system accounts and user information upon integration with Human Resource System.
- **SailPoint:** SailPoint does not natively support FIPs module but to meet with FIPS 140-2 standards, SailPoint IdentityIQ utilizes AES-128 symmetric key encryption for sensitive data and passwords.

- **SailPoint:** SailPoint in its current version does not support integration with the CA Identity Minder out of the box. The integration requires the development of a custom connector.
- **JRockit JRE:** Product may only be installed on machines running VA accepted WebLogic technologies. The use of different vendor JREs may create portability and configuration issues.
- **Oracle Database:** The product may be out of compliance during the implementation / functioning if proper steps to patch are not followed. Product must remain properly patched per Federal and Department standards in order to mitigate known and future security vulnerabilities. Per VA Handbook 6500 (Appendix F) systems with a Moderate or High risk assessment are required to use a FIPS 140-2 compliant DBMS solution to protect information at rest or have mitigating controls documented in an approved System Security Plan (SSP) for the system. It is the responsibility of the system owner to determine that an appropriate DBMS technology is selected or that mitigating controls are in place and documented in the SSP. Additionally, if PII/PHI/VA sensitive information is involved, FIPS 140-2 certified encryption must be used to encrypt data in transit and the technology must be implemented within the VA production network (not in a DMZ) or additional mitigating controls must be documented in an accepted System Security Plan (SSP).
- **Oracle Database:** VA has server resource limitations which constraints the Oracle server to a single Virtual machine with no load balancing or high availability. This constraint highlights a single point of failure and should be addressed by the VA in order to provide a highly available solution.

AcS Service - CAR

- **CA User Activity Reporting Module:** Version 12.5.1 or greater must be used and be configured and operated in FIPS Mode. FIPS Mode is required to provide FIPS-certified security algorithms for event transport and other communications between the CA User Activity Reporting Module and the CA Embedded Entitlements Manager (EEM). Per CA, the product is slated for end of life by year 2014 but active support will be until year 2017.
- **Operating Systems:** The CAR product only supports CentOS System which is a closed vendor provided Virtual Appliance. All the Subscription patches for the CentOS system are provided by the Vendor itself.

AcS Service - SSOi

- **CA Single Sign-On:** The product must be configured to run in FIPS only mode in order to satisfy FIPS140-2 requirements.
- **CA SiteMinder:** The SiteMinder Administration Console does not support PIV authentication. As an alternative, a link to the SiteMinder Administration Console may be accessed for authorized persons through the CA Single Sign-On product.
- **CA SiteMinder:** The product may be out of compliance during the implementation / functioning if proper steps to patch are not followed. When using SiteMinder Federation capabilities with this product, SiteMinder Federation must remain properly patched in order to mitigate known security vulnerabilities. Version Federal Information Processing

Standards (FIPS 140-2) certified encryption must be used to encrypt data in transit if Personally Identifiable Information (PII), Personal Health Information (PHI), or Veteran Affairs (VA) sensitive information is involved or additional mitigating controls must be documented in an approved System Security Plan (SSP). VA users must properly protect VA sensitive data in accordance to VA 6500 Policy and the Federal Information Security Management Act (FISMA).

- **DataPower XML Security Gateway:** Appliance must be operated on FIPS 140-2 compliant hardware with embedded hardware security modules (HSM).

AcS Service - eSig

- **ARX CoSign:** CoSign does not support access control lists. Access Control is required at the interface layer.
- **ARX CoSign:** CoSign does not support federation. The calls to the eSig service would be direct calls and would require users to be known by the system
- **ARX CoSign:** CoSign does not support PIV authentication for administrative access.

1.8 Design Trade-offs

The following are the design trade-offs for the AcS 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 to single servers that have a failover topology, the system could realize performance degradation 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.
- Since CAR, SAC, eSig, and SSOi administrative UI does not support direct PIV authentication, as an alternative, the administration console links may be provided in the CA Single Sign-On system and rely on the Desktop PIV login. However, a username and password will still be required for the administration consoles.
- Role manager uses the CA LDAP provisioning identity store as the authoritative store for user identity, as the LDAP store contains both employees and contractor information. The identity store however does not contain the manager attribute for employees who are not on-boarded via CRISP (or unless manually updated in role manager), which may impact VA's ability to perform manager-based access re-certification.
- The ARX CoSign device does not support signing of web forms.

1.9 User Characteristics

The user community for the CAR, IP, PROV, SAC, and SSOi activities consists of internal users including VA employees, contractors and affiliates. SSOi and PROV also support external business users from other government agencies like DoD for accessing VA internal business applications. The user community for eSig is external users including business partners and clients. The user community of the CSP will include both Veterans and Non-Veterans requiring logical access to VA business applications.

1.10 User Problem Statement

VA currently does not have a consistent, integrated method for managing identities of individuals requiring logical access or enforcing logical access privileges to VA applications including Veterans, beneficiaries, employees, and / or contractor affiliates across the enterprise. Each application has differing mechanisms for managing logical access. Until VA is able to definitively and consistently manage the identities that interface with VA applications, the effectiveness and efficiency by which the enterprise is securely managed will be drastically impacted. As VA attempts to increasingly function with integrated, collaborating, and Veteran-focused business processes, VA needs to implement AcS with standards and enforcement of appropriate secure access practices.

It will be necessary for VA to standardize on enterprise AcS so that an individual's access to sensitive information, irrespective of method, is consistently controlled throughout the enterprise. This enterprise-centric viewpoint will more effectively enable VA to protect access to sensitive or controlled information or Personally Identifiable Information (PII), based on least privilege and need to know criteria that is determined by an individual's specific roles and attributes in the organization, as well as the overall activity being performed.

2 Background

The purpose of VA AcS Development Support task is to design, develop, implement, integrate, operationalize, and sustain an enterprise-wide VA AcS solution 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 various AcS 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 solution 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.

2.2 Overview of the Business Process

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

2.3 Assumptions

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

Table 6: Assumptions and Constraints

| Assumptions and Constraints | |
|-----------------------------|---|
| SSOi | <ul style="list-style-type: none">• The CA SSO client will be packaged and deployed on the end user workstation. The SSOi client must be deployed, tested and certified for use on desktop deployment images prior to operationalizing the solution.• SSOi Activity OOTB standard reporting will be provided for applications integrated with CA SiteMinder and CA SSO toolset using CAR Activity.• LOA 4 “Holder Of the Key” functionality is not supported with a Federated SAML profile.• The Identity Provider (IdP), Service Provider (SP) and STS (Security Token Store) capabilities will be developed using AcS available product capabilities.• The SSOi Activity will use VA Active Directory (AD) as primary authentication store and thereby provide desktop SSO capability only to users in VA AD. SSOi will also leverage the attribute service provided by the Radiant Logic virtual directory to retrieve attributes about an authenticated user.• SSOi administrator interface, similar to SiteMinder Admin UI, does not support PIV authentication due to the COTS product limitation; therefore, PIV Authentication capability will not be enabled for the SiteMinder or CA SSO Administrator Interface.• SiteMinder has limited capability on providing STS service (i.e. SiteMinder does not provide a web service interface for the token conversion). A subset of the STS capabilities such as SAML response, WS-Trust and WS-Policy support requirements will be developed in combination with DataPower.• The SSOi centralized logon page, as well as the SSOi integrated application platforms, will have similar branding capabilities amongst one another to provide for a streamlined visual and functional perspective for integrating application• Mobile authentication will utilize SiteMinder for token issuance. Due to the larger size of the token itself, a limited number of mobile devices will be able to accept them. |
| CSP | <ul style="list-style-type: none">• The CSP design will not deny a potential user a credential, if requested, even if the user already has a DS Logon. However, design considerations have been made to direct those users with DS Logon or the ability to obtain a DS Logon to the appropriate place.• CSP information provided by the VA will be utilized for sizing estimates (refer to section A4).• CSP identity records (account data) and access controls will be separated logically from the Identity Proofing process and associated interfaces and security controls.• CSP will be a client of Identity Proofing as a separate service and provide the identity data input for completing the identity proofing process and creation of the identity proofing record. |

| Assumptions and Constraints | |
|------------------------------------|--|
| | <ul style="list-style-type: none"> • CSP credentials currently being issued are limited to Level 1 and Level 2; Levels of Assurance are defined in SP 800-63, VA 6500 handbook and 6501 Directive. • CSP utilizes in-person Identity Proofing process for vetting each LOA 2 identity record and associated account credential. • CSP Identity Proofing is limited to US-based Identity Proofing documents. • The CSP solution is designed to reduce the collection, storage, or transmission of the SSN. As such, applications currently keyed off of the SSN will need to leverage a one-time activation/synchronization method to link with the CSP credentials. |
| eSig | <ul style="list-style-type: none"> • The eSig functionality will be consumed only by external users. Internal users will use their PIV card to sign the documents. • The VA Consuming Application(s) will be responsible for authenticating the users. Mutual trust will be established between VA applications and eSig activity. • The end point applications are responsible for the authentication process (DS Logon 2 or higher) and user identity lifecycle • There is no access control list for the ARX CoSign device. • The eSig activity does not provide document hosting service(s). • The eSig solution does not provide a federated environment. • Since eSig depends on federated credentials, it is not possible to know if a credential has been revoked by the identity provider, thus triggering a removal of the user's signature capability. As a result, eSig will expose a 'remove user' service for dependent applications to invoke as credentials are inactivated or invalidated. • The eSig solution does not have access to VA global LDAP/AD directory and hence needs to maintain its own user repository. • The eSig solution does not provide administrative access to the eSig solution using PIV authentication. • The eSig solution does not provide ability to sign the web forms due to product limitation. • Horizontal scaling to increase capacity (number of users) is not a supported option for the eSig activity. |
| 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. • The Identity Proofing activity supports LOA 2 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 for versatile Identity information to be collected and used as part of user certification process. |
| PROV | <ul style="list-style-type: none"> • Initial identity feed file provided by VA AD or other VA authoritative store will be structured in a previously and mutually agreed upon format for bulk loading (one time) the VA internal users into the Provisioning user store. • The Provisioning Activity enforces separation of duties (SOD), based upon VA predefined parameters, through identity policy and execution of business rules, but does not provide |

Assumptions and Constraints

| | |
|-----------------------|--|
| | <p>runtime transaction analysis for enforcing other potential SOD violations if specific logic is not programmed directly in the solution.</p> <ul style="list-style-type: none"> • The Provisioning Activity, specifically CA IdentityMinder, provides limited enterprise role life cycle management. • The CA IdentityMinder Connector Xpress has constraints that limit functions such as: cannot update certain attributes - record created by, record created date, record modified by and record modified date in to membership mapping tables. • CRISP Onboarding processes for VA Employees and Contractors are dependent on TMS integration, which in turn is dependent on HRIS/PAID identity data feed integration with Provisioning. Such flows will be implemented as the dependency is fulfilled. • Unique Identity identification provided within AcS will be through the use of the Identity Attribute SEC_ID. |
| SAC | <ul style="list-style-type: none"> • The provisioning user store and MVI will act as data source for the Virtual Directory. • The Attribute service will only provide attributes that contain values within the Provisioning user store. • Consumers may request attributes from the Attribute service interface via Web service, Structured Query Language (SQL) and Lightweight Directory Access Protocol (LDAP). The Attribute service may query back end data sources using Web Services, SQL, and LDAP for the consumers. • Application PEPs should be able to send XACML requests and understand XACML responses from the PDP. If the consumer decides to use their own PEP then the consumer is responsible for customizing their PEP to provide context handler capabilities that translate access requests to XACML 3.0 and understand XACML 3.0 from the PDP. • PEPs that integrate with the SAC solution will have to comply with XACML 3. |
| CAR | <ul style="list-style-type: none"> • UARM does not store actual authoritative audit logs so it does not have the capability, nor is it intended, to protect the integrity of the authoritative audit data. • UARM does not support direct connections to a user store for collecting statistical information. • UARM currently in its end of life. Any future enhancement will be limited with this product • UARM does not support PIV authentication. Since it is a flash based application it also cannot integrated with CA SSO |
| Role manager | <ul style="list-style-type: none"> • The authoritative user store for role manager associated attributes will be from the Provisioning LDAP repository. • Role manager's compliance manager component will be solely used for access governance purposes, which includes access re-certification and role mining analysis. |
| Infrastructure | <ul style="list-style-type: none"> • This design assumes that Citrix Netscape Global Traffic Manager (GTM) module will be available at the time of production implementation. • Virtual machines used for the VA AcS infrastructure will be integrated in the appropriate VA Active Directory domain for each environment. • The AcS solution 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 solution such as VAAFI and Terremark, which only support 99.6% and 99.9% availability, respectively. Therefore, if the solution components support 99.9% |

| Assumptions and Constraints | |
|-----------------------------|---|
| | <p>availability, this may not be achieved due to external dependencies which may be limited to the VAAFI 99.6% figure.</p> <ul style="list-style-type: none">• The VA issues the necessary internal and external TLS/SSL certificates. Applications use self-signed certificates for internal server communications, and use VA issued certificates between remote servers to secure data and messages between applications.• Virtual machines used for VA AcS infrastructure will be integrated in the appropriate VA Active Directory domain for each environment. |

2.4 Legacy System Retirement

This section is not applicable as no legacy systems are being retired as a result of the AcS 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

This section provides the conceptual design of the AcS solution.

3.1.1 Application Context

This section provides context for each of the activities developed for VA AcS solution. The aim of AcS solution is to deploy a cohesive and consistent foundational AcS architecture which is flexible, modular, extensible, and scalable in VA's infrastructure. VA AcS foundation infrastructure enables internal users, external users and VA business partners to access various AcS activities such as:

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

Figure 1 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.

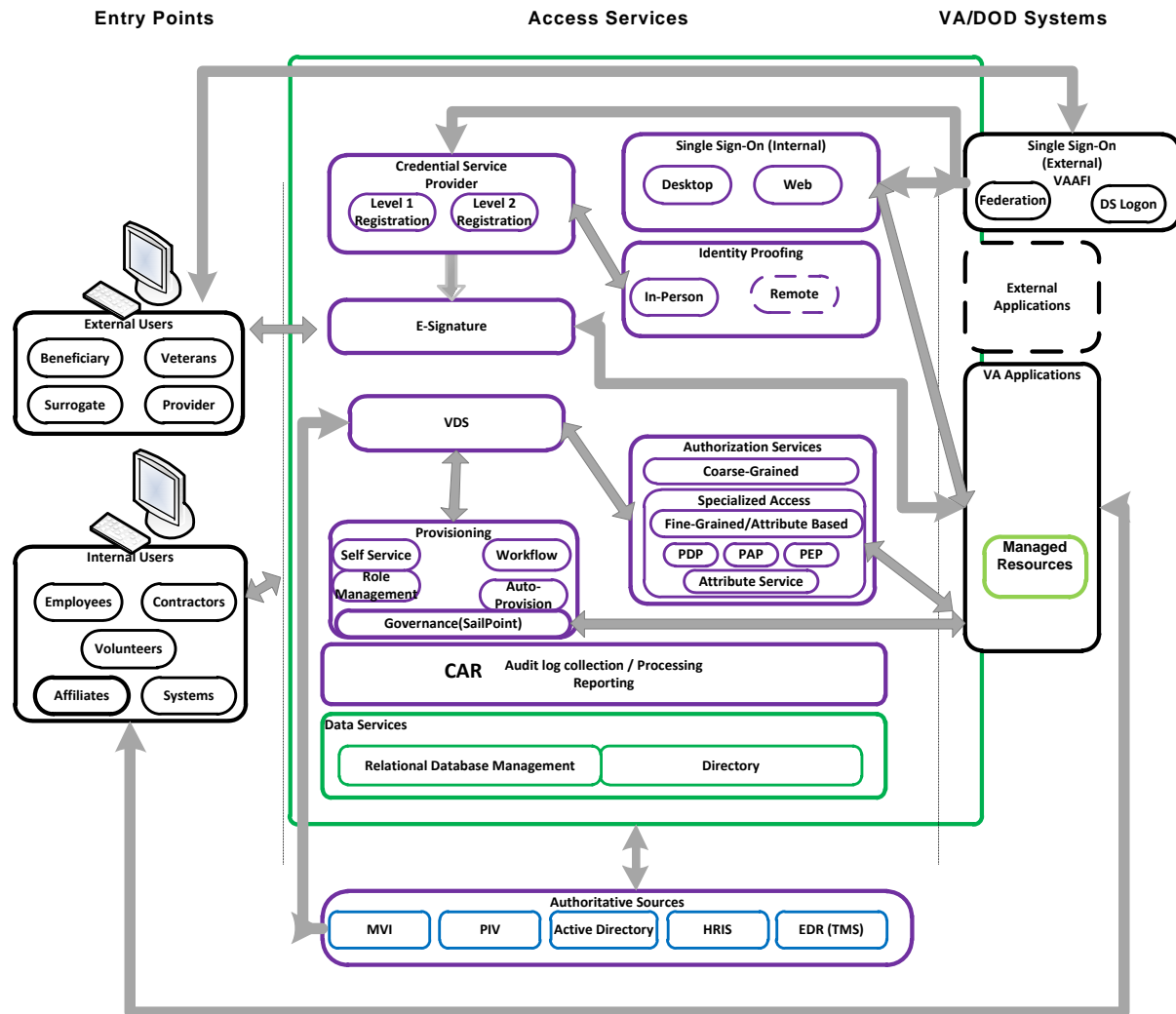


Figure 1: AcS Solution Overview

Each of the AcS solution activities is described in greater detail below.

3.1.1.1 Credential Service Provider

Credential Service Provider (CSP) is an integral component of the VA AcS solution construct and provides external end user credentials to a VA Person of Interest (POI) who is not eligible and/or does not have another VA approved credential. CSP enhances external user experience via the integrated self-service functions where a user is able to register for credentials, manage password changes and resets, administer security questions, and revise user profile information.

The activity provides an interface for federating credentials issued by CSP to relying parties. In this design the relying party is restricted to the VAAFI Federation Services. After credential issuance the CSP is responsible for receiving requests from the VAAFI service to authenticate persons with VA CSP credentials. The CSP authenticates the user and returns the authentication assertion to VAAFI for consumption. The CSP and VAAFI services together provide the end-to-end authentication services to the business application. Once the CSP passes the assertion and person attributes back to VAAFI, the role of the CSP is complete for that transaction. The access

control or authorization is done by VAAFI or is internal to the consuming business application. VAAFI validates the assertion to determine if the user should gain access to the requested application.

The primary actors interacting with the CSP application are the following:

- Administrator (Privileged User): Responsible for control and maintenance of the CSP
- External User: User requesting credential
- CSP User: User with existing CSP credential

Figure 2 below is an expansion of CSP process from Figure 1 above.

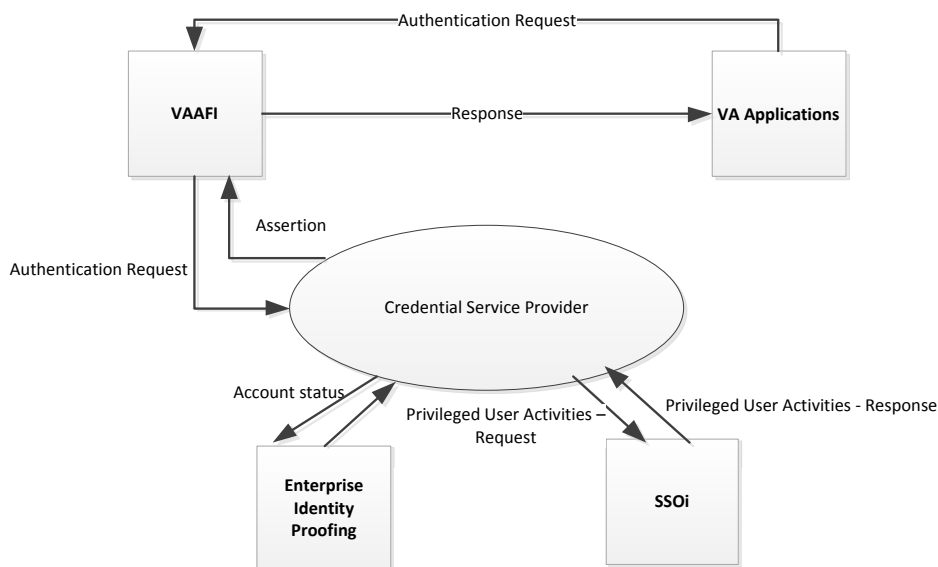


Figure 2: CSP Context Diagram

The table below provides a description of the application context for CSP.

Table 7: CSP Application Context Description

| ID | Interface Name | Input Messages | Output Messages | External Party |
|----|------------------------|------------------------|------------------------------------|-----------------------------|
| 1 | VAAFI -CSP | Authentication Request | Authentication Assertion, SAML 2.0 | NA |
| 2 | Identity Proofing -CSP | SOAP over HTTPs | SOAP over HTTPs | VA Applications (e.g., VIC) |

| ID | Interface Name | Input Messages | Output Messages | External Party |
|----|------------------------------|----------------------|----------------------|-----------------------|
| 3 | Business Applications -VAAFI | SOAP over HTTP/HTTPS | SOAP over HTTP/HTTPS | Business Applications |
| 4 | Single Sign-On - CSP | Kerberos/SPNEGO | Kerberos/SPNEGO | SSOi |

3.1.1.2 Identity Proofing

Identity Proofing (IP) is used to verify a user's identity in order to establish a level of assurance of the claim that the user is indeed who they represent themselves to be before the Identity Proofing official. 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.

The IP process is an in-person proofing process, which requires a person to be physically present at an Identity Proofing station within a VA facility or other designated location. The IP process creates a correlation between the identity proofing record and the Master Veteran Index (MVI) by performing series of steps to determine whether the person being identity proofed is already known to VA or not and act accordingly to add and/or correlate the identity proofing record with an identity record within MVI.

The primary actors interacting with the IP application are the following:

- Administrator (Privileged User): Responsible for control and maintenance of the IP
- Identity Proofer (Privileged User): User verifying identity documents and photo of an external user
- Identity Proofed User: The subject of IP

Figure 3 below is an overview of business interactions between IP, its clients and supporting systems.

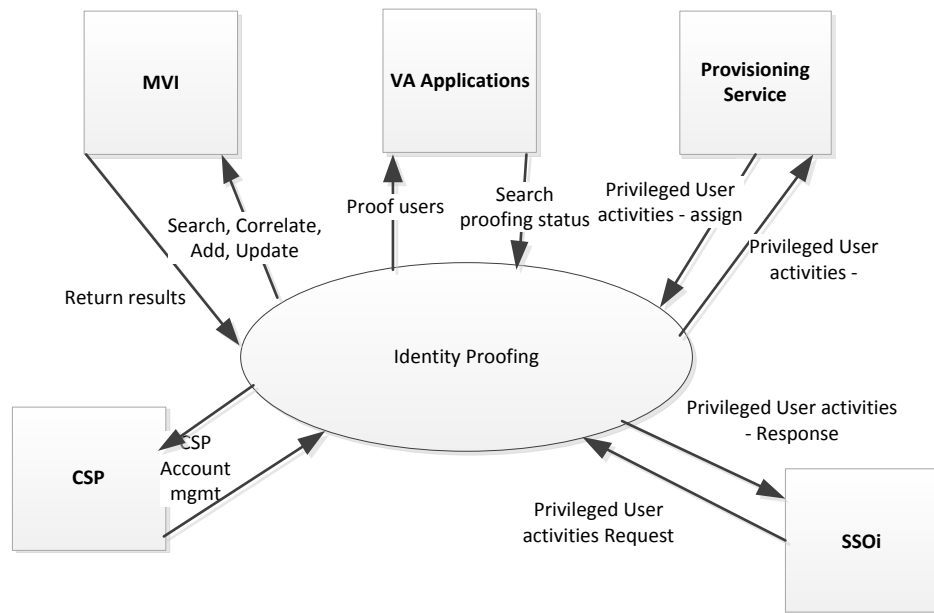


Figure 3: IP Context Diagram

The table below provides description of the application context for IP.

Table 8: IP Application Context Description

| 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 |

3.1.1.3 Electronic Signature (eSig)

Electronic signature (eSig) enables Veterans to digitally sign forms that require a high level of verification that the user signing the document is a legitimate and authorized user. The eSig activity authenticates the signer's identity, intent, and data integrity for signed digital documents for Veterans and other VA POI.

The eSig service supports machine to machine authentication. VA applications post their requests through the eSig service and once the machine to machine authentication is successfully established, the application request is received by the eSig adapter. The eSig adapter is a java application and stores each event for auditing and reporting purposes. The adapter provides the following class of APIs:

- **Sign and Verify:** The APIs allow the applications to sign a document and verify signature request
- **User Management:** The APIs allow the applications to perform user management functions such as add a user and delete a user. These APIs allow the applications to perform the lifecycle management for the eSig identities

The primary actors interacting with the eSig application are the following:

- **Administrator (Privileged User):** Responsible for control and maintenance of the eSig service
- **eSig User:** User who is using the eSig service to sign the electronic documents

Figure 4 below is an overview of business interactions between eSig, its clients, and supporting systems.

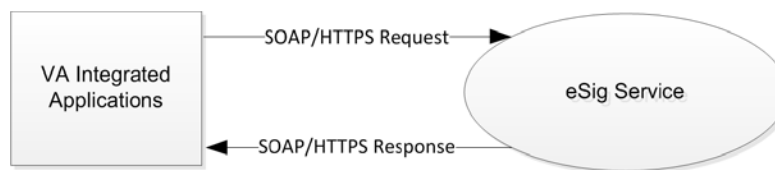


Figure 4: eSig Context Diagram

The table below provides a description of the application context for eSig.

Table 9: eSig Application Context Description

| ID | Interface Name | Input Messages | Output Messages | External Party |
|----|---------------------------------|-------------------------|--------------------------|-----------------------------------|
| 1 | eSig Application-VA application | SOAP request over HTTPS | SOAP response over HTTPS | VA applications - Signed document |

3.1.1.4 Specialized Access Control

Specialized Access Control (SAC) provides the ability to maintain and to process granular access decisions based on a set of business rules and user, resource, and environmental attributes. The SAC service enables the transition away from local application access control to evaluating and enforcing business specific, centralized access control policies, attributes, and data. The SAC application will evaluate decision requests that are formatted in a valid eXtensible Access Control Markup Language (XACML) context request. The SAC configuration evaluates requests against access policies stored internally to SAC activity. Upon evaluation of the request against the access policy, the SAC returns a XACML context response. The valid responses are limited to Permit, Deny, Indeterminate, and Not Applicable. The SAC activity is intended to enforce authorization decisions or provide support to applications for enforcement.

Figure 5 below is an overview of business interactions between SAC, its clients and supporting systems.

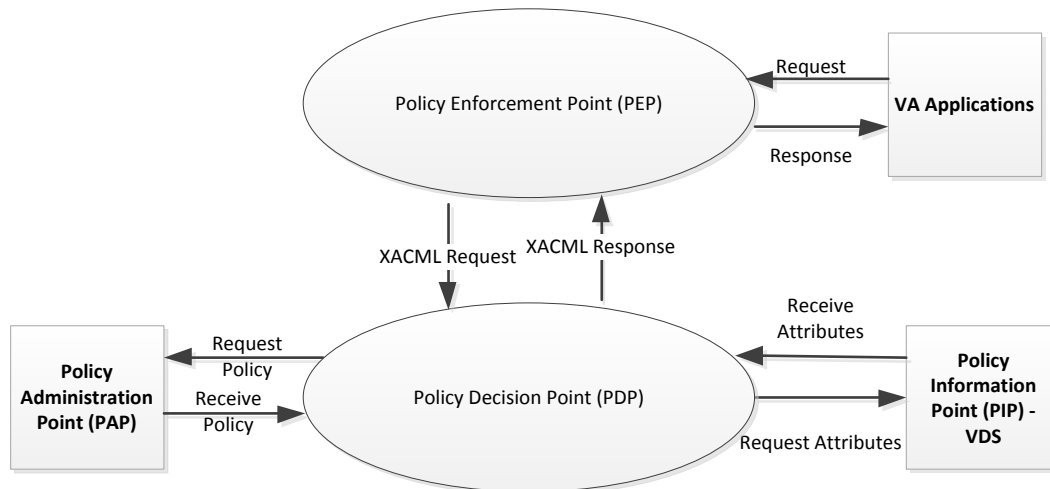


Figure 5: SAC Context Diagram

The table below provides description of the application context for SAC.

Table 10: SAC Application Context Description

| ID | Interface Name | Relegated Object | Input Messages | Output Messages |
|----|----------------------------|------------------|---|--|
| 1 | PDP Service-PEP | IAM PDP | XACML <Request> sent via a SOAP envelop over HTTP(s) | Authorization Decision Response via a SOAP envelop over HTTP(s) |
| 2 | PEP Service-VA application | Application PEP | HTTP(s) request (application dependent) | Access decisions (Permit/Deny) |
| 3 | PIP Service-PDP | IAM PIP | Dependent on Attribute data source format (LDAP, RDBMS (SQL), XML, Flat file) | Name-value attribute data pairs to be included in the XACML payload or evaluated by the PDP for rendering a decision |
| 4 | PAP Service-PDP | IAM PAP | N/A (GUI input) | N/A (Deployment artifacts – JAR file(s)) |

3.1.1.5 Provisioning

User provisioning is the process of associating an identity to one or more application accounts and associated entitlements. The Provisioning (PROV) activity involves self-service options for internal VA users for centralized creation, modification, deletion and suspension for user accounts based on business processes and interactions defined by applications or systems. The Provisioning service integrates with SSOi service to allow users to SSO to the Provisioning web

interface. Provisioning integrates with VA AD for user authentication and user information. It integrates with other VA applications for user account provisioning and de-provisioning.

The primary actors interacting with the Provisioning activity are the following internal users:

- Privileged Users: Responsible for workflow approvals, delegation, running audit reports and user access management
- Internal User: Capable of requesting and tracking access for integrated VA applications

Figure 6 below is an overview of business interactions between SAC, its clients, and supporting systems.

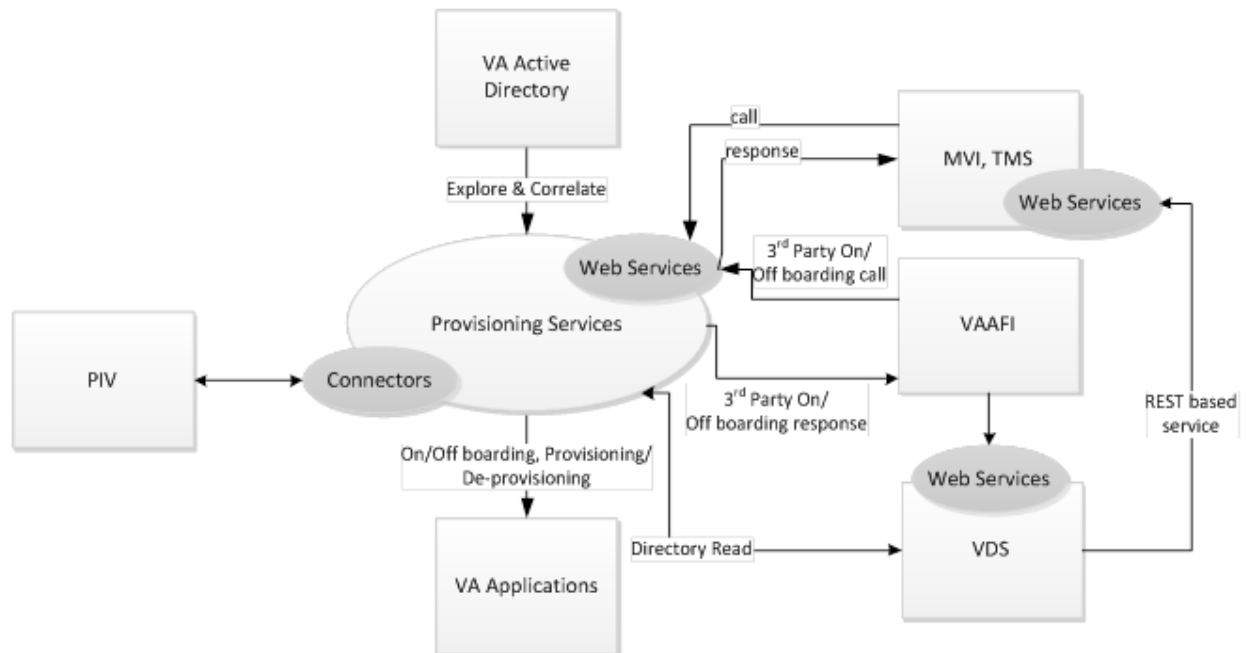


Figure 6: PROV Context Diagram

The table below provides a description of the application context for PROV.

Table 11: PROV Application Context Description

| ID | Interface Name | Relegated Object | Input Messages | Output Messages | External Party |
|----|---|----------------------|---|---|---|
| 1 | VA Active Directory (AD)-Provisioning | LDAP | LDAP queries | LDAP response / search results | LDAP Interface. VA AD is queried by IAM to obtain VA internal user information. IAM uses the LDAP protocol to communicate with AD. AD is leveraged primarily to authenticate internal VA users (via SSOi) and also as user profile data source. |
| 2 | VA Application (Web-based Front-End)-Provisioning | Provisioning Service | HTTP/HTTPS JDBC JNDI SOAP over HTTPS | HTTP/HTTPS JDBC JNDI SOAP over HTTPS | VA Applications consume the Provisioning Service using connectors (JNDI or JDBC calls) or through web services exposed as tasks for the Provisioning Service such Create User Task and Modify User Task. |
| 3 | Web-Services - Attribute Exchange-Provisioning | LDAP | LDAP queries over LDAPS SOAP over HTTPS | LDAP results over LDAPS SOAP over HTTPS | VA applications consume the attribute exchange over LDAPS or web services to retrieve user attributes. |
| 4 | VDS directory read-Provisioning | LDAP | LDAP queries over LDAPS | LDAP results over LDAPS | VDS read data from provisioning service |
| 5 | VAAFI-Provisioning | LDAP | LDAP queries over LDAPS SOAP over HTTPS | LDAP results over LDAPS SOAP over HTTPS | VAAFI receive data from VDS based on queries |
| 6 | VDS Rest based service-MVI | LDAP | LDAP queries over LDAPS SOAP over HTTPS | LDAP results over LDAPS SOAP over HTTPS | VDS read data from MVI/TMS |

3.1.1.6 Single Sign-On – Internal

Single Sign-On – Internal (SSOi) is an authentication service designated for operations-based applications. These are typically described as business applications and not Veteran self-service applications and are both externally and internally facing VA users and applications. This service provides the capability to enhance the user experience by reducing time associated with multiple log-on/log-off activities, enriched password management, and reduction in help desk support.

The SSOi service is client based service which allows internal VA users such as employees, contractors and partners within VA network to log on to integrated applications. The SSOi service connects to VA AD to validate user's credentials from desktop session or Kerberos token, uses Federation to support external cloud providers and accept users from SSOe while also utilizing HSPD-12 trust services to authenticate internal VA PIV users.

The primary actors interacting with the SSOi application are the following:

- Administrator (Privileged User): Responsible for control and maintenance of the SSOi (CA SSO and CA SiteMinder) and also responsible for running reports
- SSOi User: User who is using the SSOi service to log on to applications once they have logged on to their desktop successfully

Figure 7 below is an overview of business interactions between SSOi, its clients, and supporting systems.

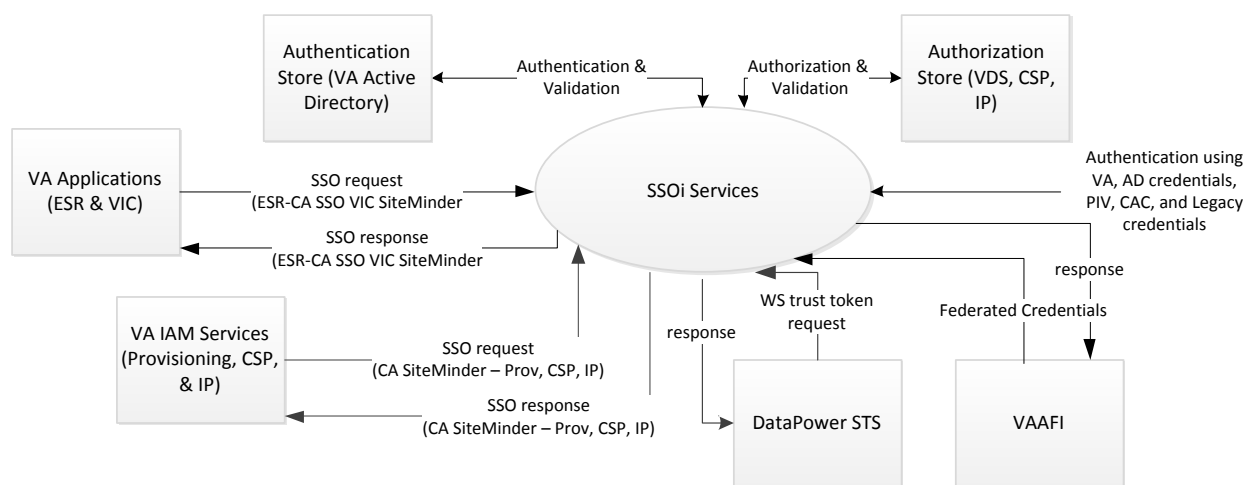


Figure 7: SSOi Context Diagram

The table below provides description of the application context for SSOi.

Table 12: SSOi Application Context Description

| ID | Interface Name | Relegated object | Input Messages | Output Messages | External Party |
|-----------|-----------------------------------|-------------------------|-----------------------|--------------------------------|---|
| 1 | VA Active Directory (AD)-SSOi | SSOi Service | LDAP queries | LDAP response / search results | LDAP Interface. VA AD is queried by SSOi Service to obtain VA internal user information. IAM (CA SiteMinder) uses the LDAP protocol to communicate with AD. AD is leveraged primarily to authenticate internal VA users. |
| 2 | Virtual Directory Service-SSOi | SSOi Service | LDAP queries | LDAP response / search results | LDAP Interface. VA VDS is queried by SSOi Service to obtain VA internal/external user information and also provide attribute authorization. IAM (CA SiteMinder) uses the LDAP protocol to communicate with VDS. VDS is leveraged primarily to authorizing VA users. |
| 3 | CSP and IP Directory Service-SSOi | SSOi Service | LDAP Queries | LDAP response / search results | LDAP Interface. VA CSP and IP Store which is CA directory instance which is queried by SSOi Service to obtain VA internal/external user information and also provide authorization response. |
| 4 | SSOi Application | SSOi Service | HTTP/HTTPS | HTTP/HTTPS | The SSOi hosted application like centralized logon pages are consumed by SSOi integrated applications |
| 5 | VA Applications-SSOi | SSOi Service | HTTP/HTTPS | HTTP/HTTPS | VA application like ESR and VIC use the CA SSO desktop native connection methods to seamlessly log in users in to their web applications. |
| 6 | VAAFI-SSOi | SSOi Service | SAML request/response | SAML request /response | VAAFI interacts with SSOi service for federation as service provider or identity provider |

| ID | Interface Name | Relegated object | Input Messages | Output Messages | External Party |
|----|----------------------|------------------|------------------------|-------------------------|---|
| 7 | DataPower – STS-SSOi | SSOi Service | WS-Trust Token request | WS-Trust Token response | DataPower acts as the STS store that supports token translation requests from the application end and will return the standard user attributes as a part of the response specification. |

3.1.1.7 Compliance Audit and Reporting

Compliance Audit and Reporting (CAR) provides the capability to monitor AcS activities to produce reports and generate alerts triggered by events or breach of predetermined event thresholds. Enabling an enterprise CAR service provides VA a common compliance auditing framework enabling the foundation for adherence within applicable government policy and regulation. VA CAR service provides Compliance Reporting and Policy Violation Alerting.

The primary actors interacting with the CAR application are the following:

- Administrator (Privileged User): Responsible for control and maintenance of CAR and to generate reports.
- Report User: Responsible for generating reports.
- Data Supplier: Responsible for providing the endpoint data needed for reporting.

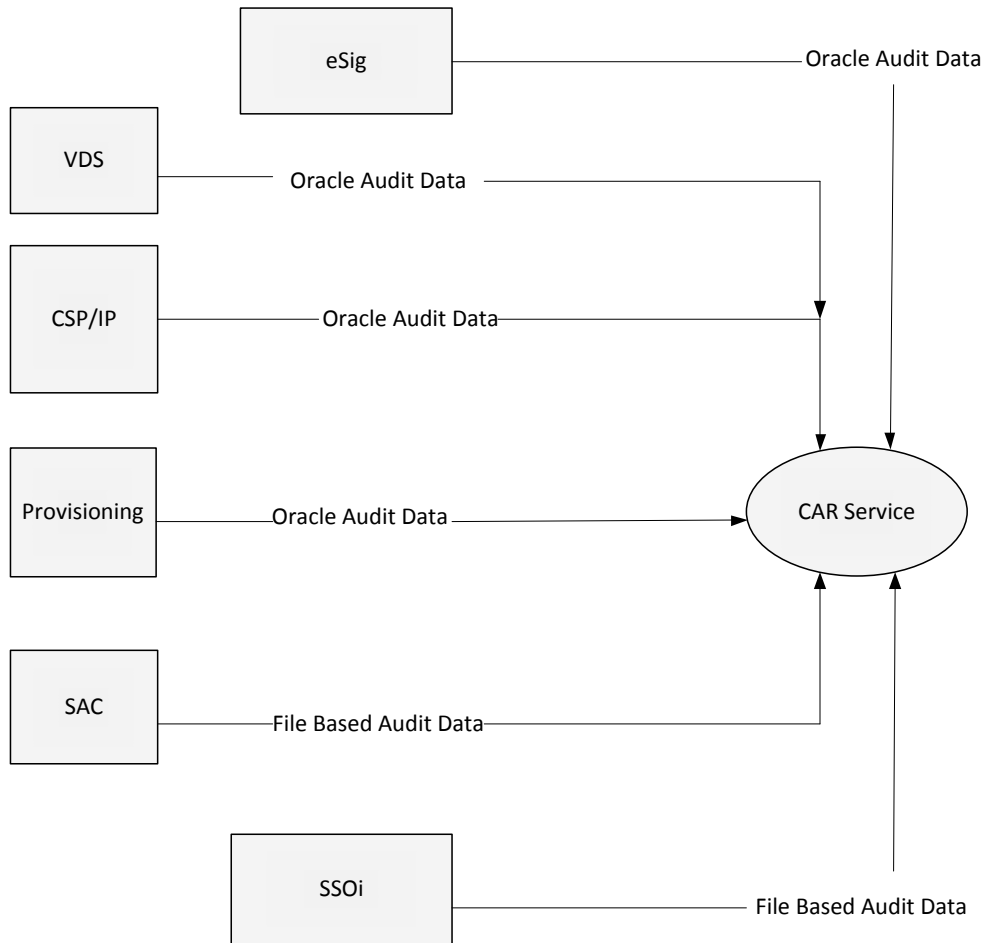


Figure 8: CAR Context Diagram

Table 13: CAR Application Context Description

| ID | Interface Name | Relegated object | Input Messages | Output Messages | External Party |
|----|----------------|------------------|----------------|-----------------|---|
| 1 | eSig | SSOi Service | ODBC queries | ODBC Response | ODBC interface is queried by CAR agent connector to collect the audit logs from the eSig Audit Source |
| 2 | VDS | SSOi Service | ODBC queries | ODBC Response | ODBC interface is queried by CAR agent connector to collect to the VDS audit source |
| 3 | CSP/IP | SSOi Service | ODBC queries | ODBC Response | ODBC interface is queried by CAR agent connector to collect the CA IDM audit source |
| 4 | Provisioning | SSOi Service | ODBC queries | ODBC Response | ODBC interface is queried by CAR agent connector to collect the CA IDM audit source |

| ID | Interface Name | Relegated object | Input Messages | Output Messages | External Party |
|----|----------------|------------------|---------------------|----------------------|---|
| 5 | SAC | SSOi Service | File Reader Queries | File Reader Response | File base Reader is used by CAR agent to collect the SAC text based audit logs |
| 6 | SSOi | SSOI Service | File Reader Queries | File Reader Response | File base Reader is used by CAR agent to collect the SSOi text based audit logs |

CAR interacts with each of the AcS solution activities and has no specific external interfaces currently.

3.1.2 High-Level Application Design

Figure 9 below provides a high-level application design for the AcS solution and identifies the major AcS activities and/or relationships with VA applications.

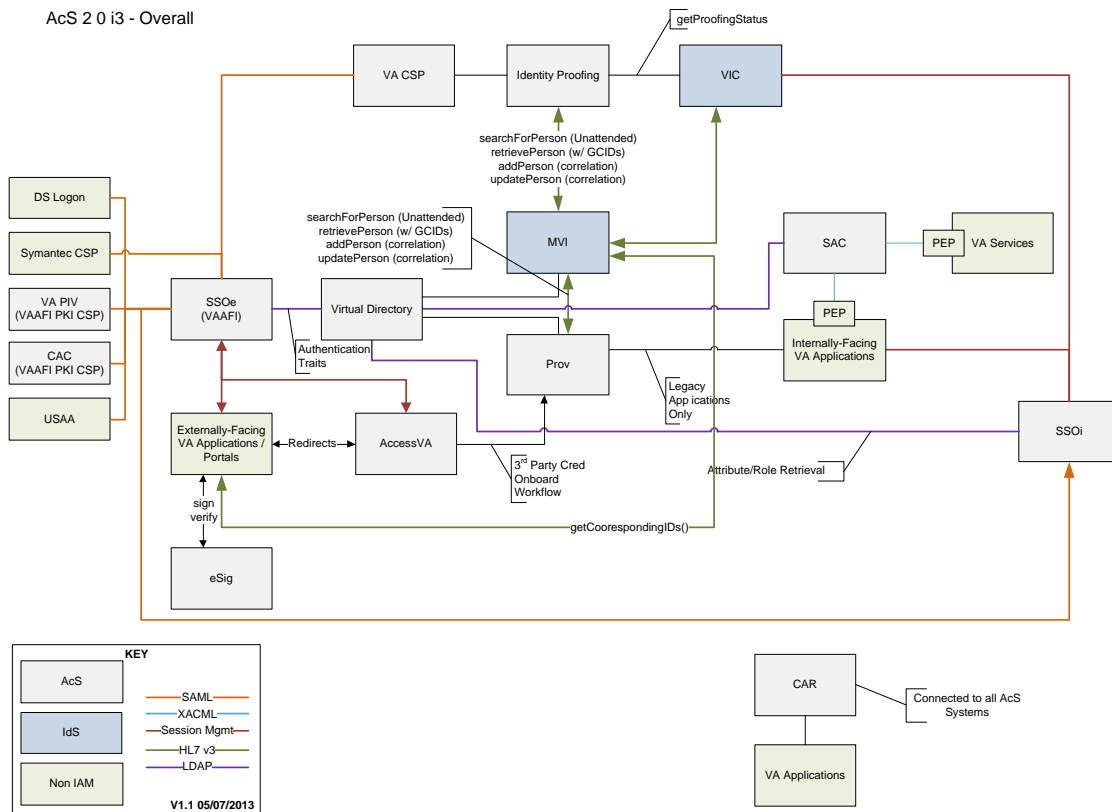


Figure 9: AcS Solution Application Design

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. For details on the PROV-VDS-MVI integration, refer to section 6.2.3.

Table 14: 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 | NA | MVI, CSP, CAR |
| 3 | eSig | eSig provides the ability to sign documents electronically. | Service | NA | CAR |
| 4 | SAC | SAC provides the ability to maintain and process granular access decisions based on a set of business rules and user attributes. | Service | NA | CAR |
| 5 | Provisioning | Provisioning associates an identity to one or more application accounts and the associated entitlements to the identity. Provisioning also provides the capabilities for managing roles and certifying entitlements. | Service | TMS | AD, CAR, EDR, MVI, PIV, VDS, IP |
| 6 | 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 is a federated partner with SSOi. | Service | Federation | AD, IP, CSP, Provisioning, SAC |
| 7 | CAR | CAR provides the ability to proactively monitor, mitigate, and recover from potential compliance infractions and incidents. | Service | NA | SSOi, Provisioning, CSP, IP, eSig, SAC |

3.1.3 Application Locations

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

Table 15: AcS Solution Application Locations

| Application Component | AcS Service | Description | Location at Which Component is Run |
|------------------------------|-----------------------------|--|---|
| IIS Web Server | SSOi, Provisioning, CSP, IP | Front end web server providing the administrative and self-service interface to CA IdentityMinder | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| Servlet Exec | SSOi | Application server for SiteMinder Federation option pack for CSP and SSOi partnerships with VAAFI. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| Oracle WebLogic | Provisioning, CSP, IP | Application server hosting CA IdentityMinder, Provisioning Server, SiteMinder and federation. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| Apache Tomcat | SAC | Application server hosting Axiomatics Services Manager, Policy Decision Point, and Policy Administration Point | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| CA IdentityMinder | Provisioning, CSP, 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) |
| CA SiteMinder | SSOi | This is a set of features that provides Single Sign-On, session management, WS Security, Authentication and Authorization Policies, Policy Decision Point, and audit reporting for access controls. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| CA Secure Proxy Server | SSOi | This is a stand-alone server that provides a proxy-based solution for access control. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| CA SSO Server | SSOi | CA desktop single sign-on solution for legacy applications. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |

| Application Component | AcS Service | Description | Location at Which Component is Run |
|------------------------------|-----------------------------|---|---|
| CA Directory | SSOi, Provisioning, CSP, 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) |
| CA UARM | CAR | User Audit and Reporting Module. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| Axiomatics ASM | SAC | The components of Axiomatics are managed from a central point, the Axiomatics Services Manager (ASM). Via ASM, policies and configurations are distributed to the authorization services and PDPs, which are deployed, managed, and monitored via the management interface. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| Axiomatics PAP | SAC | Policy Administration Point, an application for managing policies used by the policy decision point (PDP). | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| Axiomatics PDP | SAC | Policy Decision point for fine-grained authorization decision requests. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| Radiant Logic | Provisioning | COTS product for Data Virtualization. Can be used as a PIP and will be used to provide Attribute Services | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| IBM DataPower | SSOi | COTS XML Security Gateway | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| Oracle Database | SSOi, Provisioning, CSP, IP | Database to support CA IdentityMinder and audit logs from different components. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| ARX CoSign Device | eSig | Stores the Key pair for the eSig Service. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |

| Application Component | AcS Service | Description | Location at Which Component is Run |
|---|-----------------------------|--|---|
| Report Server | SSOi, Provisioning, CSP, IP | Report server for CA SiteMinder and CA IdentityMinder | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) |
| SailPoint IdentityIQ-Compliance Manager | Provisioning | COTS product for role mining, role management, and access re-certification | 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 AcS solution activities:

Table 16: AcS Solution Users

| Application Component | Description | User |
|------------------------------|--|---------------------|
| CSP | Performs administrative functions including controlling Identity Minder related configurations and tasks | CSP Administrator |
| | Responsible for managing the application and providing user lifecycle management functions including upgrading credentials, enabling/disabling accounts, and other administrative activities as needed | CSP Privileged User |
| | A user (Veteran, beneficiary, or other VA stakeholder) requesting or having a user credential of any level | End User |
| IP | Performs administrative functions including controlling Identity Minder related configurations and tasks and managing the proofing registration interfaces | IP Administrator |
| | Responsible for Identity Proofing users confirming identity of applicant to comply with SP 800-63 and VA 6501 | Identity Proofer |
| SAC | A user who attempts to access a protected VA application that subscribes to SAC activity for providing policy-based access control | End User |
| | Performs administrative functions including systems configuration, policy creation/updates, workflow management, etc. | SAC Administrator |
| eSig | Performs administrative functions including systems configuration, modifying user accounts, as well as performing and defining reporting and auditing functions | eSig Administrator |
| | A user who utilizes the eSig to electronically sign the approved document types; an eSig User is assumed to have an LOA of 2 or higher | End User |

| Application Component | Description | User |
|-----------------------|--|------------------------------|
| Provisioning | Performs administrative functions in Identity Minder including management of end users, workflows, connections to end points as well as configurations objects | Provisioning Administrator |
| | Responsible for registering, approving, and managing user provisioning and de-provisioning lifecycle | Provisioning Privileged User |
| | A user who uses provisioning to self-register, manage user profile, and check request status to gain access to integrated applications | End User |
| | A system that is authorized to use the provisioning web service functions for creating SECID and Add User. | Authorized Systems |
| | Role manager performs administrative functions including management of application connection and configuration, re-certification configuration, mining analysis reports, and advanced analytics capabilities. | Role Manager Administrator |
| | Role manager runs OOTB reports to be used for mining analysis and acts on the re-certifications triggered for the configured applications. | End User |
| SSOi | Performs administrative functions including management of SiteMinder, SSO, and associated components | SSOi Administrator |
| | A user interacts with SSOi for initial login to facilitate the integrated application login | End User |
| CAR | Performs administrative functions including management of UARM reports dashboard, generation of reports, and creating other users in UARM | CAR Administrator |
| | Runs reports and tracks audit records to verify continual system conformance with security and policy | Auditor |

3.2 Conceptual Data Design

The following sections provide the conceptual data design for the AcS solution.

3.2.1 Project Conceptual Data Model

This section describes the conceptual data model providing high-level representation of the data entities and relationships. The data objects within the AcS solution, how they are used, and how they relate to each other are provided in Figure 10. The data model is defined for CA IdentityMinder, which is used for Provisioning, CSP, and IP services for implementing VA business requirements. For specific data elements pertaining to each AcS activities, refer to [section A.1](#).

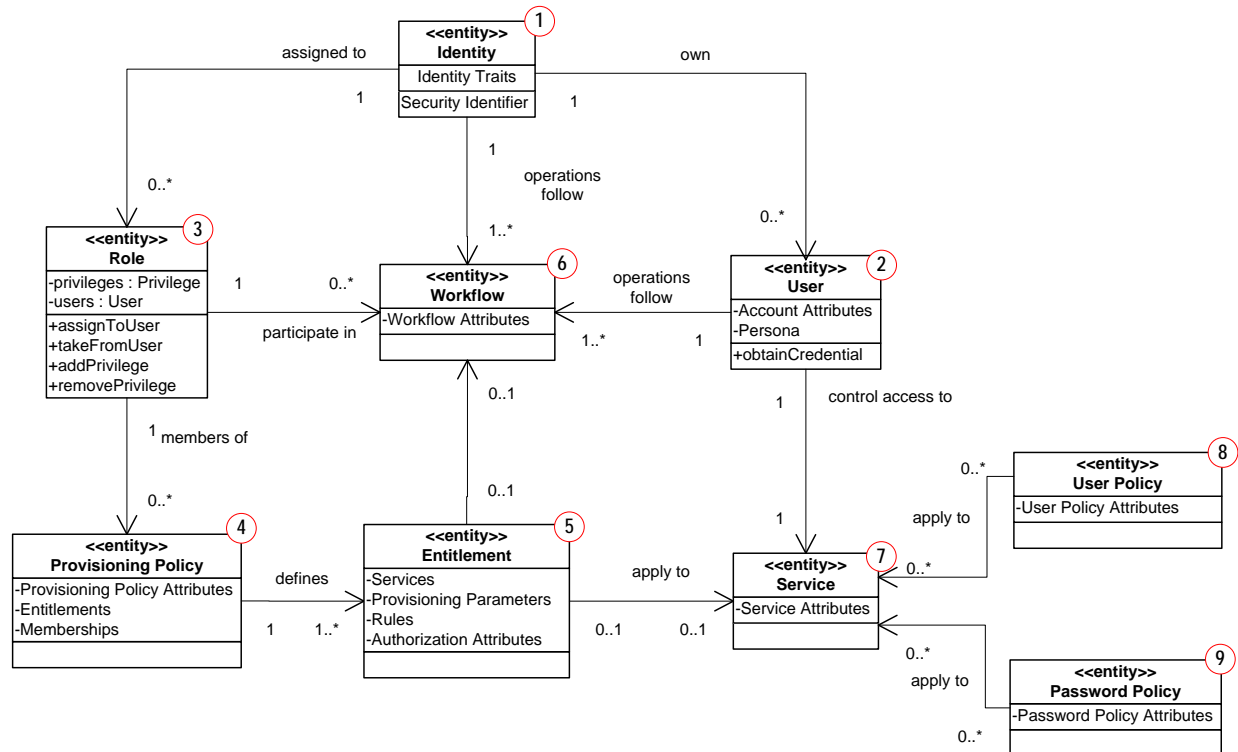


Figure 10: AcS Solution Conceptual Data Mode

The VA AcS solution uses roles, provisioning policies, entitlements and workflows to create, modify, and otherwise manage identity and account objects. These data objects are stored in repositories such as LDAP and Oracle database tables. The table below describes the AcS data objects with their input and output relationships. Detailed descriptions of each data object are provided later.

Notes:

- VDS as a product uses the data model of the consuming application such as Provisioning and MVI.
- CAR is based on a closed system (CA UARM) which does not interact with any separate repositories for its functions and therefore follows data model which is provided out of the box with the product.

Table 17: 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. | - One Identity | - 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 |

| Ref | Object | Description | Input Relationship | Output Relationship |
|-----|---------------------|---|--|---|
| | | | | identity. |
| ② | User (Account) | The User (Account) attributes defines 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. |
| 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. |

| Ref | Object | Description | Input Relationship | Output Relationship |
|-----|-----------------|---|---|--|
| 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 | |
| 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

As part of the AcS solution, the following table identifies the Oracle Database instances that will be created or interfaced with by the different activities.

Table 18: 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 Solution |
| 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 Provisioning, CSP and IP services with their corresponding instances. | Create / Replace / Interface / Modify | VRM AcS Solution |
| CA IdentityMinder – Workflow Schema | Stores runtime information for the in-session workflow engine. This store is for internal use only. The database is used by Provisioning service. | Create / Replace / Interface / Modify | VRM AcS Solution |
| 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 Provisioning, CSP and IP services with their corresponding instances. | Create / Replace / Interface / Modify | VRM AcS Solution |
| CA IdentityMinder – Task Persistence Archive Schema | Stores runtime task archives. This store is for internal use only. The database is used by Provisioning, CSP and IP services with their corresponding instances. | Create / Replace / Interface / Modify | VRM AcS Solution |
| CA IdentityMinder – Audit Schema | Provides a historical record of operations that occur in CA IdentityMinder. The database is used by Provisioning, CSP and IP services with their corresponding instances. | Create / Replace / Interface / Modify | VRM AcS Solution |
| 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 Solution |
| eSig Audit | eSig Audit data collection store where auditable transaction logs are collected for reporting purposes. | Create / Replace / Interface / Modify | VRM AcS Solution |
| Role manager - Oracle Database | Stores object definitions which are configured in role manager (roles, rules, connector configurations etc.). This database is for internal use of the tool only. Passwords (if | Create / Replace / Interface / | VRM AcS Solution |

| Database Name | Description | Type | Steward |
|---------------|--|--------|---------|
| | any) are encrypted. The database is used by Provisioning service for role manager component. | Modify | |

3.2.3 User Interface Data Mapping

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

3.2.3.1 Provisioning Screen Interface

This section provides the screens of the Graphical User Interface (GUI) that the AcS users will have access to in order to Onboard and Off Board employee, contractors, Healthcare Professional (HP) Trainees and Volunteers.

3.2.3.1.1 Profile Information Screens

The following profile information screens initiate the onboarding process for new VA employees and contractors, HP trainees, and volunteers.

New VA Employee: Profile

[New VA Employee Profile/Search: Select User](#) > New VA Employee: Profile

1 Profile 2 Profile Work Home 3 Profile Org 4 Profile Misc

• = Required

Personal Information

- First Name (required)
- Last Name (required)
- Middle Initial/Name (optional)
- Suffix (optional)
- External Email (e.g.: name@email.com)(required)
- Date of Birth (required)
- SSN (e.g.: 123456789)(required)
- Gender Choose One (required)
- Height (inches)(required)
- Eye Color Choose One (required)
- Hair Color Choose One (required)

Figure 11: New VA Employee Profile Information

New VA Contractor: Profile

[New VA Contractor Profile/Search: Select User](#) > New VA Contractor: Profile

1 Profile 2 Profile Work Home 3 Profile Org 4 Profile Misc

• = Required

Personal Information

• First Name (required)

• Last Name (required)

Middle Initial/Name (optional)

Suffix (optional)

• External Email (e.g.: name@email.com)(required)

• Date of Birth (required)

• SSN (e.g.: 123456789)(required)

• Gender (required)

• Height (inches)(required)

• Eye Color (required)

• Hair Color (required)

Figure 12: New VA Contractor Profile Information

VA Provisioning Service

Skip to main content

imadmin imadmin | [Sign out](#) | [Help](#)

1 Profile 2 Work Home 3 Profile Org 4 Profile Misc

• = Required

Personal Information

• First Name (required)

• Last Name (required)

Middle Initial/Name (optional)

Suffix (Optional)

• External Email (e.g.: name@email.com)(required)

• Date of Birth (required)

• SSN (e.g.: 123456789)(required)

• Gender (required)

• Height (inches)(required)

• Eye Color (required)

• Hair Color (required)

Tasks

- Home
- Request Access for ESR
- VA On/Off-Boarding
 - Off-Board User
 - On-Board User
 - CRISP Checklist
 - New VA Contractor Profile/Search
 - New VA Employee Profile/Search
 - New VA HPT Profile/Search
 - New VA Volunteer Profile/Search
 - Third Party Onboard Registration
 - Update TMS Profile
 - Reporting
 - Manage Users
 - Update User
- Users
- Groups
- Roles and Tasks
- Endpoints
- Provisioning Endpoints
- Policies
- Reports
- System

Figure 13: New HP Trainee Profile Information

Figure 14: New Volunteer Profile Information

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the Provisioning tab.

3.2.3.1.2 Work/Home Location Information Screens

The work/home location information for new VA employees and contractors, HP trainees, and volunteers is entered in the following screens.

Figure 15: New VA Employee Work/Home Location Information

New VA Contractor: Profile Work Home

[New VA Contractor Profile/Search: Select User](#) > New VA Contractor: Profile Work Home

1 Profile 2 Profile Work Home 3 Profile Org 4 Profile Misc

• = Required

Work / Home Location

• Work Address Street (required)

Post Office Box (if applicable)

• Work Address City (required)

• Work Address State (required)

• Work Address ZIP Code (e.g.: 12345-1234)(required)

• Work Telephone Number (e.g.: 555-555-5555)(required)

• Home Address (required)

• Home City (required)

• Home State (required)

• Home Zip (e.g.: 12345-1234)(required)

• Home Phone (e.g.: 555-555-5555)(required)

Figure 16: New VA Contractor Work/Home Location Information

VA Provisioning Service

Skip to main content

imadmin imadmin | Sign out | Help

Tasks << Home < Request Access for ESR < VA On/Off-Boarding < Off-Board User < On-Board User < CRISP Checklist < New VA Contractor Profile/Search < New VA Employee Profile/Search < New VA HPT Profile/Search < New VA Volunteer Profile/Search < Third Party Onboard Registration < Update TMS Profile < Reporting < Manage Users < Update User < Users < Groups < Roles and Tasks < Endpoints < Provisioning Endpoints < Policies < Reports < Custom

• = Required

Work / Home Location

• Work Address Street (required)

Post Office Box (if applicable)

• Work Address City (required)

• Work Address State (required)

• Work Address ZIP Code (e.g.: 12345-1234)(required)

• Work Telephone Number (e.g.: 555-555-5555)(required)

• Home Address (required)

• Home City (required)

• Home State (required)

• Home Zip (e.g.: 12345-1234)(required)

• Home Phone (e.g.: 555-555-5555)(required)

• Country (required)

Figure 17: New HP Trainee Work/Home Location Information

Figure 18: New Volunteer Work/Home Location Information

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the Provisioning tab.

3.2.3.1.3 Organization and Employment Information Screens

The organization and employment information for new VA employees and contractors, HP trainees, and volunteers is entered in the following screens.

Figure 19: New VA Employee Organization and Employment Information

New VA Contractor: Profile Org

[New VA Contractor Profile/Search: Select User](#) > New VA Contractor: Profile Org

1 Profile 2 Profile Work Home 3 Profile Org 4 Profile Misc

• = Required

Organizational and Employment Information

• Supervisor ID SEC ID (required) [Browse](#)

• VA OIT PD Project (required)

• VA Project Manager (required) [Browse](#)

• Contract Number

• HIPAA training Required Yes (required)

• Occupation Code Choose One (required)

• Employment Status Choose One (required)

• Department Choose One (required)

• Title (required)

• Sponsor (required) [Browse](#)

• Office Location Choose One (required)

• Cost Center Choose One (required)

• Special Security Access Required Choose One (required)

• Emergency Responder Choose One (required)

• Critical Employee Choose One (required)

VA Approvers

• AD Facility CIO (required) [Browse](#)

• AD ISO (required) [Browse](#)

Figure 20: New VA Contractor Organization and Employment Information

VA Provisioning Service

Tasks

- Home
- Request Access for ESR
- VA On/Off-Boarding
 - Off-Board User
 - On-Board User
 - CRISP Checklist
 - New VA Contractor Profile/Se
 - New VA Employee Profile/Se
 - New VA HPT Profile/Search
 - New VA Volunteer Profile/Se
 - Third Party Onboard Registrat
 - Update TMS Profile
 - Reporting
 - Manage Users
 - Update User
- Users
- Groups
- Roles and Tasks
- Endpoints
- Provisioning Endpoints
- Policies
- Reports
- System

Organizational and Employment Information

Supervisor ID SEC ID (required) Browse

VA OIT PD Project (required)

VA Project Manager (required) Browse

Occupation Code Choose One (required)

Employment Status Choose One (required)

Department Choose One (required)

Title (required)

Sponsor (required) Browse

Office Location Choose One (required)

Cost Center Choose One (required)

Special Security Access Required Choose One (required)

Emergency Responder Choose One (required)

Critical Employee Choose One (required)

VA Approvers

Employment Status Choose One (required)

Department Choose One (required)

Title (required)

Sponsor (required) Browse

Office Location Choose One (required)

Cost Center Choose One (required)

Special Security Access Required Choose One (required)

Emergency Responder Choose One (required)

Critical Employee Choose One (required)

VA Approvers

AD Facility CIO (required) Browse

AD ISO (required) Browse

Return to Search

Back Next Cancel

Figure 21: New HP Trainee Organization and Employment Information

VA Provisioning Service

Tasks: Home, Request Access for ESR, VA On/Off-Boarding, Off-Board User, On-Board User, CRISP Checklist, New VA Contractor Profile/Se, New VA Employee Profile/Se, New VA HPT Profile/Search, New VA Volunteer Profile/Se, Third Party Onboard Registrat, Update TMS Profile, Reporting, Manage Users, Update User, Users, Groups, Roles and Tasks, Endpoints, Provisioning Endpoints, Policies, Reports, System.

New VA Volunteer: Profile Org

1 Profile 2 Profile Work Home 3 Profile Org 4 Profile Misc

Required

Organizational and Employment Information

- Supervisor ID SEC ID (required) [Browse]
- VA OIT PD Project (required)
- VA Project Manager (required) [Browse]
- HIPAA training Required Yes (required)
- Occupation Code Choose One (required)
- Employment Status Choose One (required)
- Department Choose One (required)
- Title (required)
- Sponsor (required) [Browse]
- Office Location Choose One (required)
- Cost Center Choose One (required)

VA Approvers

- AD Facility CIO (required) [Browse]
- AD ISO (required) imadmin [Browse]

Return to Search

Back Next Cancel

Figure 22: New Volunteer Organization and Employment Information

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the Provisioning tab.

3.2.3.1.4 Miscellaneous Information Screens

The miscellaneous information for new VA employees and contractors, HP trainees, and volunteers is entered in the following screens.

New VA Employee: Profile Misc

[New VA Employee Profile/Search: Select User](#) > **New VA Employee: Profile Misc**

1 Profile 2 Profile Work Home 3 Profile Org 4 Profile Misc

• = Required

CRISP Checklist Details

These are the fields that appear at the top of the CRISP Screening Checklist tab.

•Type of Appointment Choose One (required)

•Service Choose One (required)

•Facility Choose One (required)

•SAC Background Check Initiated Date

Miscellaneous

•Mother's Maiden Name (required)

•Organization Field Choose One (required)

•Station Number Choose One (required)

•Duty Station Code Choose One (required)

•Facility or Assigned Duty Station Choose One (required)

•Street Address of Facility or Assigned Duty Station (required)

•City of Facility or Assigned Duty Station (required)

•State of Facility or Assigned Duty Station Choose One (required)

•Zip Code of Facility or Assigned Duty Station (e.g.: 12345-1234)(required)

•Foreign National Status Choose One (required)

•Name of Sponsoring Dept/Service/or Section (required)

•Mail Routing Symbol Choose One

PIV Card Info

•Type of PIV Request New ID (required)

•Type of PIV Badge Choose One (required)

Figure 23: New VA Employee Miscellaneous Information

New VA Contractor: Profile Misc

[New VA Contractor Profile/Search](#) | [Select User](#) > New VA Contractor: Profile Misc

1 Profile 2 Profile Work Home 3 Profile Org 4 Profile Misc

• = Required

CRISP Checklist Details

These are the fields that appear at the top of the CRISP Screening Checklist tab.

• Type of Appointment Choose One (required)

• Service Choose One (required)

• Facility Choose One (required)

• SAC Background Check Initiated Date

Miscellaneous

• Mother's Maiden Name (required)

• Organization Field Choose One (required)

• Station Number Choose One (required)

• Duty Station Code Choose One (required)

• Facility or Assigned Duty Station Choose One (required)

• Street Address of Facility or Assigned Duty Station (required)

• City of Facility or Assigned Duty Station (required)

• State of Facility or Assigned Duty Station Choose One (required)

• Zip Code of Facility or Assigned Duty Station (e.g: 12345-1234)(required)

• Foreign National Status Choose One (required)

• Name of Sponsoring Dept/Service/or Section (required)

• Mail Routing Symbol Choose One (required)

PIV Card Info

• Type of PIV Request New ID (required)

• Type of PIV Badge Choose One (required)

Figure 24: New VA Contractor Miscellaneous Information

VA Provisioning Service

Tasks

Home

Request Access for ESR

VA On/Off-Boarding

Off-Board User

On-Board User

CRISP Checklist

New VA Contractor Profile/Se

New VA Employee Profile/Se

New VA HPT Profile/Search

New VA Volunteer Profile/Se

Third Party Onboard Registrat

Update TMS Profile

Reporting

Manage Users

Update User

Users

Groups

Roles and Tasks

Endpoints

Provisioning Endpoints

Policies

Reports

System

CRISP Checklist Details

These are the fields that appear at the top of the CRISP Screening Checklist tab.

Type of Appointment Choose One (required)

Service Choose One (required)

Facility Choose One (required)

SAC Background Check Initiated Date (required)

Miscellaneous

Mother's Maiden Name (required)

Organization Field Choose One (required)

Station Number Choose One (required)

Duty Station Code Choose One (required)

Facility or Assigned Duty Station Choose One (required)

Street Address of Facility or Assigned Duty Station (required)

City of Facility or Assigned Duty Station (required)

State of Facility or Assigned Duty Station Choose One (required)

Facility or Assigned Duty Station Choose One (required)

Street Address of Facility or Assigned Duty Station (required)

City of Facility or Assigned Duty Station (required)

State of Facility or Assigned Duty Station Choose One (required)

Zip Code of Facility or Assigned Duty Station (e.g: 12345-1234)(required)

Foreign National Status Choose One (required)

Name of Sponsoring Dept/Service/or Section (required)

Mail Routing Symbol Choose One (required)

PIV Card Info

Type of PIV Request New ID (required)

Type of PIV Badge Choose One (required)

Return to Search

Back Finish Cancel

Copyright © 2013 CA. All rights reserved.
About VA Provisioning Service

Figure 25: New HP Trainee Miscellaneous Information

VA Provisioning Service

imadmin imadmin | Sign out | Help

Tasks

Home

Request Access for ESR

VA On/Off-Boarding

Off-Board User

On-Board User

CRISP Checklist

New VA Contractor Profile/Se

New VA Employee Profile/Se

New VA HPT Profile/Search

New VA Volunteer Profile/Se

Third Party Onboard Registr

Update TMS Profile

Reporting

Manage Users

Update User

Users

Groups

Roles and Tasks

Endpoints

Provisioning Endpoints

Policies

Reports

System

New VA Volunteer: Profile Misc

New VA Volunteer Profile/Search: Select User | New VA Volunteer: Profile Misc

1 Profile 2 Profile Work Home 3 Profile Org 4 Profile Misc

* = Required

CRISP Checklist Details

These are the fields that appear at the top of the CRISP Screening Checklist tab.

Type of Appointment Choose One (required)

Service Choose One (required)

Facility Choose One (required)

SAC Background Check Initiated Date (required)

Miscellaneous

Mother's Maiden Name (required)

Organization Field Choose One (required)

Station Number Choose One (required)

Duty Station Code Choose One (required)

Facility or Assigned Duty Station Choose One (required)

Street Address of Facility or Assigned Duty Station (required)

City of Facility or Assigned Duty Station (required)

State of Facility or Assigned Duty Station Choose One (required)

Zip Code of Facility or Assigned Duty Station (e.g: 12345-1234)(required)

Foreign National Status Choose One (required)

Name of Sponsoring Dept/Service/or Section (required)

Mail Routing Symbol Choose One (required)

PIV Card Info

Type of PIV Request New ID (required)

Type of PIV Badge Choose One (required)

Return to Search

Back Finish Cancel


Figure 26: New Volunteer Miscellaneous Information

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the Provisioning tab.

3.2.3.1.5 CRISP Checklist Screen

The following screen is used to capture the data against the checklist.

Skip to main content



VA Provisioning Service

IM Admin | [Sign out](#) | [Help](#)

» CRISP Checklist:

CRISP Screening Checklist

Checklist to be used by sponsors for tracking of completion of on-boarding requirement
 For example: (Title 5 / Title 38 / Hybrid / Fee Basis / Without Compensation (WOCs) / Residents / Contractors /
 Students / Volunteers)
 All entries on the checklist must be completed, signed and dated. Retain the OPF or applicable file

CRISP Status
Not Started

Full Name
SSN

Title
Service

SAC Background Check Adjudicated Date
Facility

Part A

Required Documentation

| Document | Completed | Last Modified by: | Date |
|---|--------------------------|-------------------|------|
| Federal Application Form or Resume | <input type="checkbox"/> | | |
| Choose One | <input type="checkbox"/> | | |
| <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> ▼ </div> | <input type="checkbox"/> | | |

Figure 27: CRISP Checklist Screen

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the Provisioning tab.

3.2.3.2 CSP Screen Interface

This section shows the screens to which the AcS users have access to perform self-service registration, profile management and password management.

3.2.3.2.1 Modify Account: Step 1 User Profile

The following screen is used to capture the user information when modifying user information and security questions.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS


Home
CSP Home
Logout

Step 1
User Profile

Step 2
Security Questions

Step 3
Modification Complete

Modify Account
* - Required

* First Name

* Last Name

Date of Birth:
DOB Month MM
DOB Day DD
DOB Year YYYY

* User ID

Phone Number

###-###-####

Street Address

City

State

* Country

Postal Code

#####-####

* Email

Back
Next
Cancel

Figure 28: Modify Account: Step 1 User Profile

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

3.2.3.2.2 Modify Account: Step 2 Security Questions

The following screen is used to capture the security questions and answers when modifying user information and security questions.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Home CSP Home Logout

Step 1 User Profile Step 2 Security Questions Step 3 Modification Complete

Modify Account

Security Question #1 [Dropdown]
Security Answer #1 [Text Field]

Security Question #2 [Dropdown]
Security Answer #2 [Text Field]

Security Question #3 [Dropdown]
Security Answer #3 [Text Field]

Security Question #4 [Dropdown]
Security Answer #4 [Text Field]

Security Question #5 [Dropdown]
Security Answer #5 [Text Field]

Back Next Cancel

Figure 29: Modify Account: Step 2 Security Questions

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

3.2.3.2.3 Change Password

The following screen allows the user to change their password.

Logged in as: [REDACTED] (Logout)

Home

Self Service

Users

Groups

Roles and Tasks

Policies

Reports

System

Change Password

User ID

First Name

Last Name

Password

Confirm Password

[REDACTED]

Passwords must:

1. Have at minimum of eight (8) non-blank characters.
2. Contain at least one:
 - a) Upper case characters (A...Z)
 - b) Lower case characters (a...z)
 - c) Base 10 digits (0...9)
 - d) Non-alphanumeric, special characters (For example, !,\$#%?)
3. Must not contain any spaces

Submit

Cancel

opyright © 2013 CA. All rights reserved.

About

Figure 30: Change Password

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

3.2.3.2.4 Upgrade to Level 2: Step 1 User Profile

The following screen captures the user information when requesting to upgrade to level 2.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS


Home
CSP Home
Logout

Step 1
User Profile

Step 2
Security Questions

Step 3
Modification Complete

Modify Account
* - Required

* First Name

* Last Name

* Date of Birth:

DOB Month MM

DOB Day DD

DOB Year YYYY

* User ID

imadmin

* Phone Number

###-###-####

* Street Address

* City

* State

Choose One:

* Country

Choose One:

* Postal Code

#####-####

* Email

Back

Next

Cancel

Figure 31: Upgrade to Level 2: Step 1 User Profile

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

3.2.3.2.5 Upgrade to Level 2: Step 2 Security Questions

The following screen captures the security questions and answers when requesting to upgrade to a Level 2 credential.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Home CSP Home Logout

Step 1 User Profile Step 2 Security Questions Step 3 Modification Complete

Modify Account

Security Question #1
Security Answer #1

Security Question #2
Security Answer #2

Security Question #3
Security Answer #3

Security Question #4
Security Answer #4

Security Question #5
Security Answer #5

Back Next Cancel

Figure 32: Upgrade to Level 2: Step 2 Security Questions

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

3.2.3.2.6 Self-Registration: Step 1 User Profile

The following screen captures the user information when self-registering.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS


Home
CSP Home
Logout

Step 1
User Profile

Step 2
Security Questions

Step 3
Modification Complete

Modify Account
* - Required

* First Name

* Last Name

Date of Birth:
DOB Month MM
DOB Day DD
DOB Year YYYY

* User ID

Phone Number

###-###-####

Street Address

City

State
Choose One:

* Country
Choose One:

Postal Code

#####-####

* Email

Back
Next
Cancel

Figure 33: Self-Registration: Step 1 User Profile

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

3.2.3.2.7 Self-Registration: Step 2 Security Questions

The following screen captures the security questions when self-registering.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Home CSP Home Logout

Step 1 User Profile Step 2 Security Questions Step 3 Modification Complete

Modify Account

Security Question #1 [Dropdown]
Security Answer #1 [Text]
Security Question #2 [Dropdown]
Security Answer #2 [Text]
Security Question #3 [Dropdown]
Security Answer #3 [Text]
Security Question #4 [Dropdown]
Security Answer #4 [Text]
Security Question #5 [Dropdown]
Security Answer #5 [Text]

Back Next Cancel

Figure 34: Self-Registration: Step 2 Security Questions

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.


3.2.3.3 IP Screen Interface

This section shows the screens to which the AcS users have access to perform IP.

3.2.3.3.1 Identity Proof User

3.2.3.3.1.1 Step 1 User Profile

The following screen captures the user information when identity proofing a user.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS


[VA Home](#)
[IP Home](#)
[About ID Proofing](#)
[Contact Us](#)

Logged in as
[Logout](#)

Step 1
User Profile

Step 2
Address Verification

Step 3
Primary Identification

Step 4
Secondary Identification

Step 5
Submit Proof

Identity Proofing (Step 1): User Profile

* - Required Identity Proofing: TBD

** - Enter the first few characters of a proofing station number in the proofing station filter to shorten the number of proofing stations listed. Please note that special characters and regular expressions are not supported by the filter.

* First Name

* Last Name

* Date of Birth

DOB Month MM

DOB Day DD

DOB Year YYYY

* User ID

* Phone Number

###-###-####

* Street Address

* City

* State

Choose One:

* Country

Choose One:

* Postal Code

#####-####

* Email

* Affiliation

Choose One:

** Proofing Station #

Filter

(Not Required)

* Proofing Location

Choose One:

☐ Create a CSP Record? [?]

Back

Next

Cancel

Figure 35: Identity Proof User: Step 1 User Profile

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.3.1.2 Step 2 Address Verification

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

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

VA Home IP Home About ID Proofing Contact Us Logged in as [redacted] Logout

Step 1 User Profile Step 2 Address Verification Step 3 Primary Identification Step 4 Secondary Identification Step 5 Submit Proof

Identity Proofing (Step 2): Address Verification

* - Required

* Address Validation Type [F]

* Postmark Date: Month MM [] [] N/A

Street Address [1]

City [C]

State [M]

Country [U]

Postal Code [6]
#####-####

Back Next Cancel

Figure 36: Identity Proof User: Step 2 Address Verification

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.3.1.3 Step 3 Primary Identification

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

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

VA Home IP Home About ID Proofing Contact Us Logged in as: [Redacted] Logout

Step 1 User Profile Step 2 Address Verification **Step 3 Primary Identification** Step 4 Secondary Identification Step 5 Submit Proof

* = Required

* ID Type [Redacted]

* Country of Issuance [Redacted]

* State of Issuance [Redacted]

* Identification Number [Redacted]

* Expiration Date: Month MM [Redacted]

* Information Provided/Verified By [Redacted]

Back Next Cancel

Figure 37: Identity Proof User: Step 3 Primary Verification

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.3.1.4 Step 4 Secondary Identification

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

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

VA Home IP Home About ID Proofing Contact Us Logged in as: [Redacted] Logout

Step 1 User Profile Step 2 Address Verification Step 3 Primary Identification **Step 4 Secondary Identification** Step 5 Submit Proof

* = Required

* ID Type [Redacted]

* Country of Issuance [Redacted]

* State of Issuance [Redacted]

* Identification Number [Redacted]

* Expiration Date: Month MM [Redacted]

* Information Provided/Verified By [Redacted]

Person being proofed: Amy Ehm

Figure 38: Identity Proof User: Step 4 Secondary Identification

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.3.2 Update a User

3.2.3.3.2.1 Step 1 User Profile

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

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

VA Home IP Home About ID Proofing Contact Us Logged in as: [Redacted] Logout

Step 1 User Profile Step 2 Address Verification Step 3 Primary Identification Step 4 Secondary Identification Step 5 Submit Proof

Identity Proofing (Step 1): User Profile

Identity Proofing: Rajesh Radhakrishnan

* - Required

** - Enter the first few characters of a proofing station number in the proofing station filter to shorten the number of proofing stations listed. Please note that special characters and regular expressions are not supported by the filter.

* First Name
* Last Name
* Date of Birth
* User ID
* Phone Number
###-###-####
* Street Address
* City
* State
* Country
* Postal Code
#####-####
* Email
* Affiliation
** Proofing Station #
* Proofing Location

Back Next Cancel

Figure 39: Update a User: Step 1 User Profile

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.3.2 Step 2 Address Verification

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

The screenshot shows the 'Step 2 Address Verification' screen. At the top is a blue header with the 'UNITED STATES DEPARTMENT OF VETERANS AFFAIRS' logo and navigation links: 'VA Home', 'IP Home', 'About ID Proofing', 'Contact Us', 'Logged in as [redacted]', and 'Logout'. Below the header is a yellow banner with five steps: 'Step 1 User Profile', 'Step 2 Address Verification' (highlighted with a yellow arrow), 'Step 3 Primary Identification', 'Step 4 Secondary Identification', and 'Step 5 Submit Proof'. Below the banner, a legend indicates '* = Required'. The main form area is titled 'Person being proofed: FIRST TESTER TWO'. It contains several fields: '* Address Validation Type', '* Postmark Date: Month MM', 'Street Address', 'City', 'State', 'Country', and 'Postal Code' (with a hint '#####-####'). A large black redaction box covers the input area for these fields. At the bottom right are three buttons: 'Back', 'Next', and 'Cancel'.

Figure 40: Update a User: Step 2 Address Verification

Refer [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.3.2.3 Step 3 Primary Identification

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

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

VA Home IP Home About ID Proofing Contact Us Logged in as: [Redacted] Logout

Step 1 User Profile Step 2 Address Verification Step 3 Primary Identification Step 4 Secondary Identification Step 5 Submit Proof

* = Required

* ID Type [Redacted]

* Country of Issuance [Redacted]

* State of Issuance [Redacted]

* Identification Number [Redacted]

* Expiration Date: Month MM [Redacted]

* Information Provided/Verified By [Redacted]

Amy Ehm

Back Next Cancel

Figure 41: Update a User: Step 3 Primary Identification

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.3.2.4 Step 4 Secondary Identification

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

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

VA Home IP Home About ID Proofing Contact Us Logged in as: [Redacted] Logout

Step 1 User Profile Step 2 Address Verification Step 3 Primary Identification Step 4 Secondary Identification Step 5 Submit Proof

* = Required

* ID Type [Redacted]

* Country of Issuance [Redacted]

* State of Issuance [Redacted]

* Identification Number [Redacted]

* Expiration Date: Month MM [Redacted]

* Information Provided/Verified By [Redacted]

Person being proofed: Amy Ehm

Figure 42: Update a User: Step 4 Secondary Identification

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the IP tab.

3.2.3.4 SSOi Screen Interface

This section shows the screens to which the AcS users have access to authenticate to VA applications through the centralized login page.

3.2.3.4.1 Centralized Login Page

To support VA applications, the SSOi activity provides a centralized logon page to support one or more authentication mechanisms. These authentication mechanisms include userID / Password, PIV, or Microsoft Windows authentication. This page is modifiable for each application to reflect only the authentication mechanisms selected by the integrating VA application.


The following screen is accessed by end users to authenticate to integrated VA applications with SSOi.

UNITED STATES
DEPARTMENT OF VETERANS AFFAIRS

Home Contact Us

VA Identity and Access Management System (IAM)

Select Log In Method to Access: [target URL, if IdP to SP consumer application URL (SPID)]

| VA Network User ID and Password | PIV Card |
|--|--|
| Enter your VA Active Directory (AD) user ID (i.e. vhaismsmithj) and password below, then click Login. | Insert your PIV card into your card reader and click Login. Please enter your PIN when prompted. |
| <p>User ID <input type="text"/></p> <p>Password <input type="password"/></p> <p>Login</p> | <p></p> <p>Login</p> |
| If you do not remember your VA Network user ID and password, please contact the National Service Desk Support: | If you do not remember your PIN or experience other issues with your PIV card, please contact the National Service Desk Support: |
| Phone: 800-877-4328 (Option 1) Email: NSDSecurity@va.gov | Phone: 800-877-4328 (Option 1) Email: PIVHelpRequests@va.gov |

If authentication failed using your VA Network ID and PW, or your PIV card, please contact National Service Desk Support:
Phone: 800-877-4328
For general questions regarding the IAM authentication service, please contact the National Service Desk Support, VBA Philadelphia, at 855-673-4357 (Option 3)

WARNING
WARNING
WARNING

You have accessed a United States Government computer. Unauthorized use of this computer is a violation of federal law and may subject you to civil and criminal penalties. This computer and the automated systems, which run on it, are monitored. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. Communications made using this system may be disclosed as allowed by federal law.

Department of Veterans Affairs | [Privacy Policy](#)

Figure 43: SSOi Centralized Login Page

3.2.3.4.2 Centralized PIV-Only Login page

For applications that require PIV-only authentication, the SSOi system provides a centralized login page where a user selects the PIV login method.

The following screen is accessed by end users to authenticate to integrated VA applications with SSOi using only a PIV card.

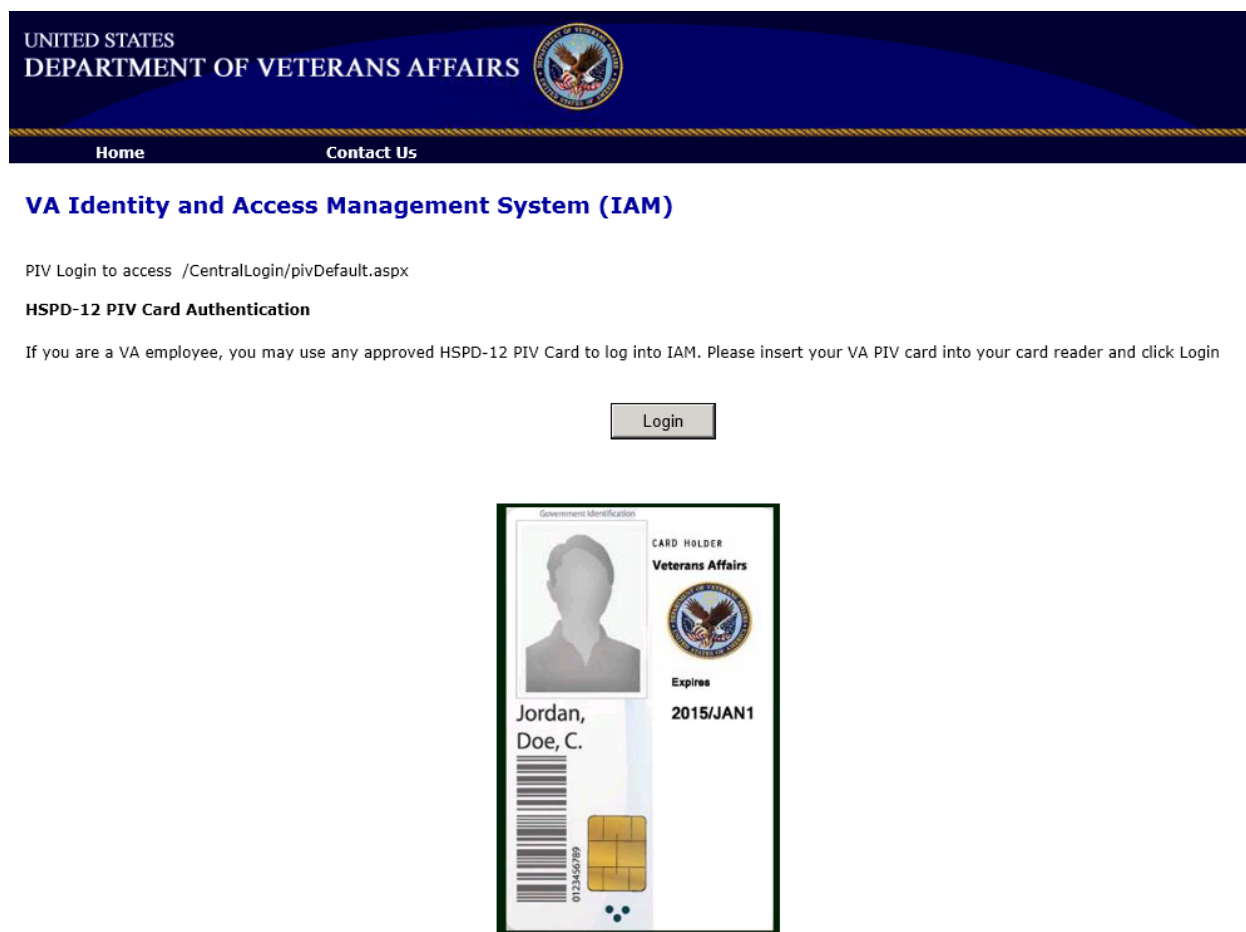


Figure 44: SSOi PIV Only Login Page

3.2.3.4.3 Mobile Login Page

The following screen is accessed by end users to authenticate to integrated VA applications with SSOi through a mobile device. To support accessing VA applications with mobile devices, a static mobile webpage is built within SSOi to provide userID / Password authentication. Like the centralized login page, this mobile login page could also provide PIV and x509 based authentication as defined by application policy.



| UNITED STATES DEPARTMENT OF VETERANS AFFAIRS  | | |
|--|---|---|
| Home Contact Us | | |
| VA Identity and Access Management System (IAM) | | |
| Select Log In Method to Access: [target URL, if IdP to SP consumer application URL (SPID)] | | |
| <p>VA Network User ID and Password</p> <p>Enter your VA Active Directory (AD) user ID (i.e. vhaismsmithj) and password below, then click Login.</p> <p>User ID <input type="text"/></p> <p>Password <input type="password"/></p> <p><input type="button" value="Login"/></p> <p>If you do not remember your VA Network user ID and password, please contact the National Service Desk Support:</p> <p>Phone: 800-877-4328 (Option 1) Email: NSDSecurity@va.gov</p> | <p>PIV Card</p> <p>Insert your PIV card into your card reader and click Login. Please enter your PIN when prompted.</p>  <p><input type="button" value="Login"/></p> <p>If you do not remember your PIN or experience other issues with your PIV card, please contact the National Service Desk Support:</p> <p>Phone: 800-877-4328 (Option 1) Email: PIVHelpRequests@va.gov</p> | <p>Windows Authentication</p> <p>This option allows you to login using your current Windows session. This option is only available for users logged onto a VA issued computer. Click Login to authenticate.</p> <p><input type="button" value="Login"/></p> <p>If you experience issues trying to use Windows Authentication, please contact the National Service Desk Support, VBA (Philadelphia):</p> <p>Phone: 855-673-4357 (Option 3) Email: ITSC@va.gov</p> |
| <p>If authentication failed using your VA Network ID and PW, or your PIV card, please contact National Service Desk Support: Phone: 800-877-4328 For general questions regarding the IAM authentication service, please contact the National Service Desk Support, VBA Philadelphia, at 855-673-4357 (Option 3)</p> | | |
| <p>WARNING WARNING WARNING</p> <p>You have accessed a United States Government computer. Unauthorized use of this computer is a violation of federal law and may subject you to civil and criminal penalties. This computer and the automated systems, which run on it, are monitored. Individuals are not guaranteed privacy while using government computers and should, therefore, not expect it. Communications made using this system may be disclosed as allowed by federal law.</p> | | |
| <p align="center"> Department of Veterans Affairs Privacy Policy </p> | | |

Figure 45: Mobile Login Page

3.2.3.5 SAC Screen Interface

This section shows the screens to which the AcS users have access to administer the SAC service.

3.2.3.5.1 PAP Landing Page

The following screen is accessible to SAC privileged users once they initiate the Axiomatics thick client to create or open workspaces for policy authoring.

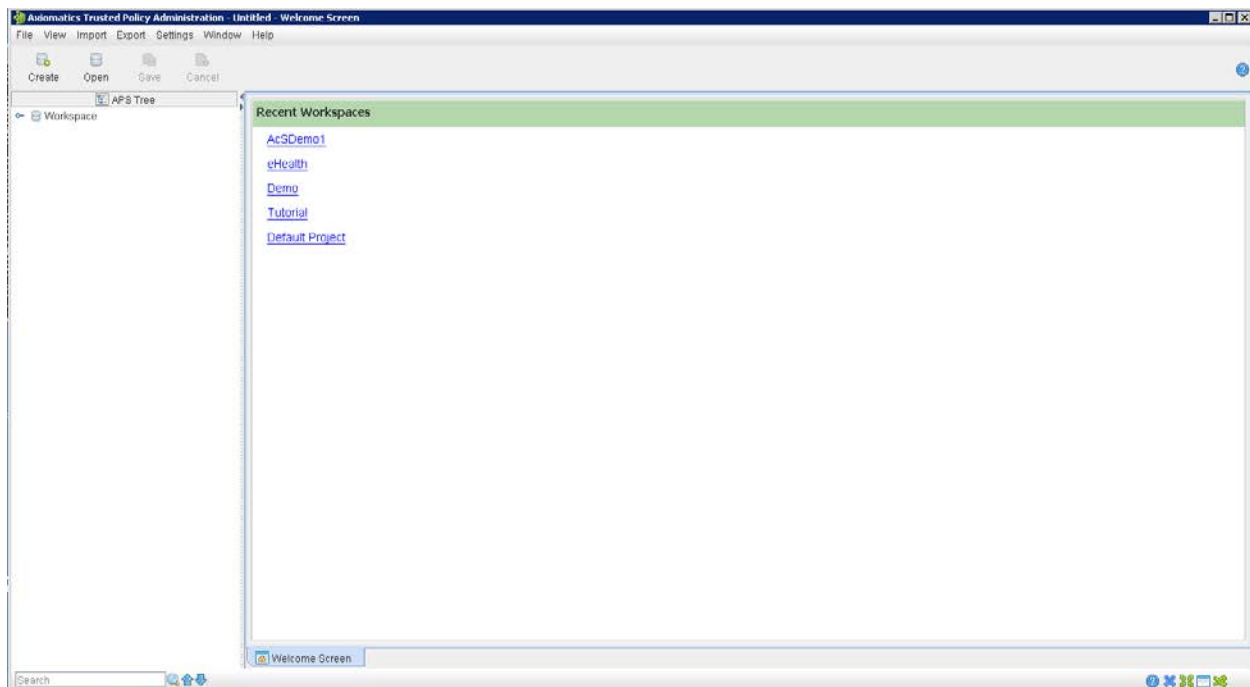


Figure 46: SAC PAP Landing Page

3.2.3.5.2 PAP Authoring Page

Once a workspace is opened or created by the privileged user, the following screen displays in which the SAC privileged user creates/edits XACML 3.0 policies.

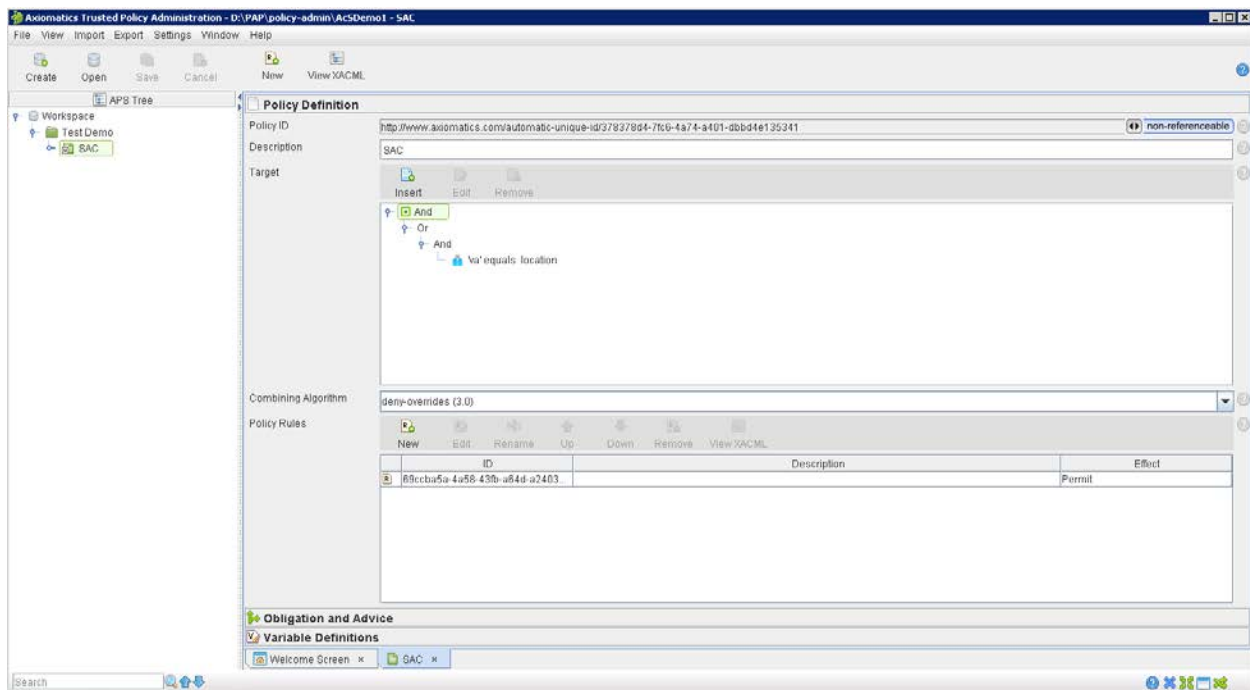


Figure 47: SAC PAP Landing Page

3.2.3.6 AcS Solution Report Interface

The reporting interface for the AcS solution is provided via the CAR activity.

3.2.3.7 Unmapped Data Element

Refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions.

3.3 Conceptual Infrastructure Design

The section provides a conceptual design of the infrastructure needed for the core capabilities of the AcS solution. The section focuses on the primary environments and locations where the AcS activities are installed. The information provided is preliminary design and is elaborated in later detailed design section.

The performance and capacity requirements information is provided in the following:



Performance_Growth
_Scalability.docx

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

The following table provides information about the special technologies implemented as part of the AcS solution.

Table 19: Special Technology Requirements

| Special Technology | Description | Notional Location | TRM Status |
|---------------------------|---|--------------------------|-------------------|
| WebSphere DataPower XI50 | DataPower provides the needed WebService capabilities to VAAFI and to AcS. | All | Yes |
| ARX Co-Sign (eSig) | Provides a PKI-based solution for digital signing documents, forms, and transactions. | All | Yes |

3.3.3 Technology Locations

Refer to section 3.3.4.1 below for technology locations.

3.3.4 Conceptual Infrastructure Diagram

This section depicts the AcS solution 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

The high-level conceptual infrastructure diagram for the VA AcS infrastructure is shown in Figure 48 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.

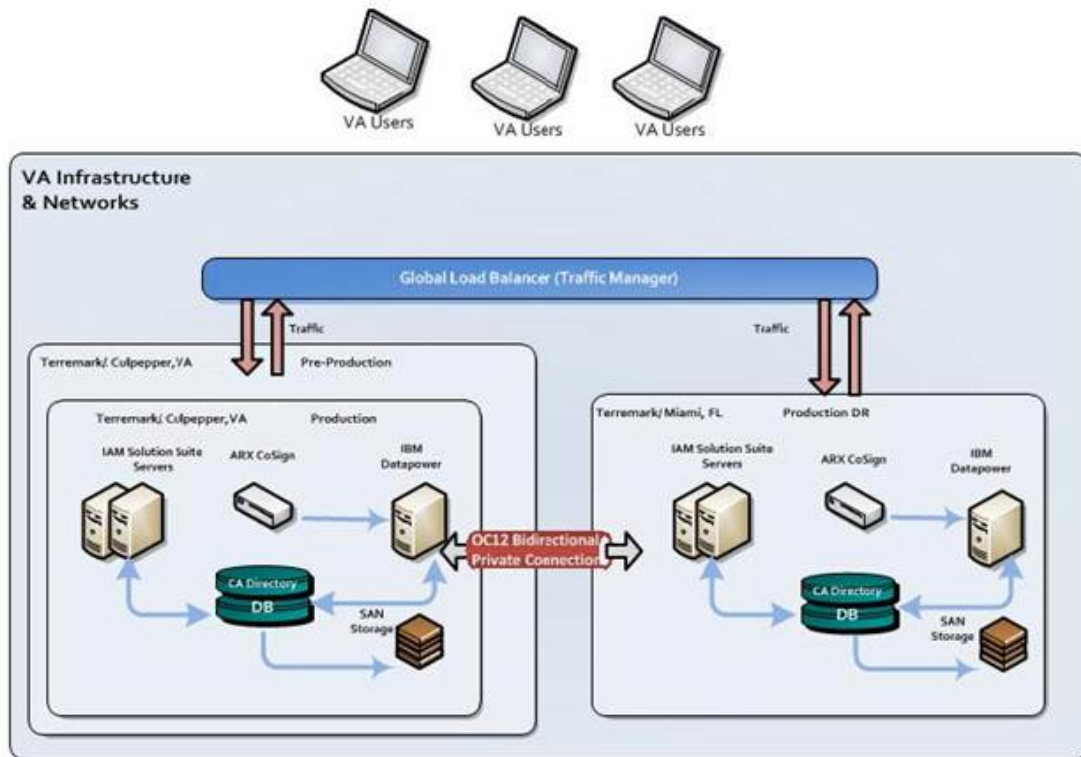


Figure 48: AcS Production Environments

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.

3.3.4.2 Conceptual Production String Diagram

The following diagram provides a logical view of the AcS solution components.

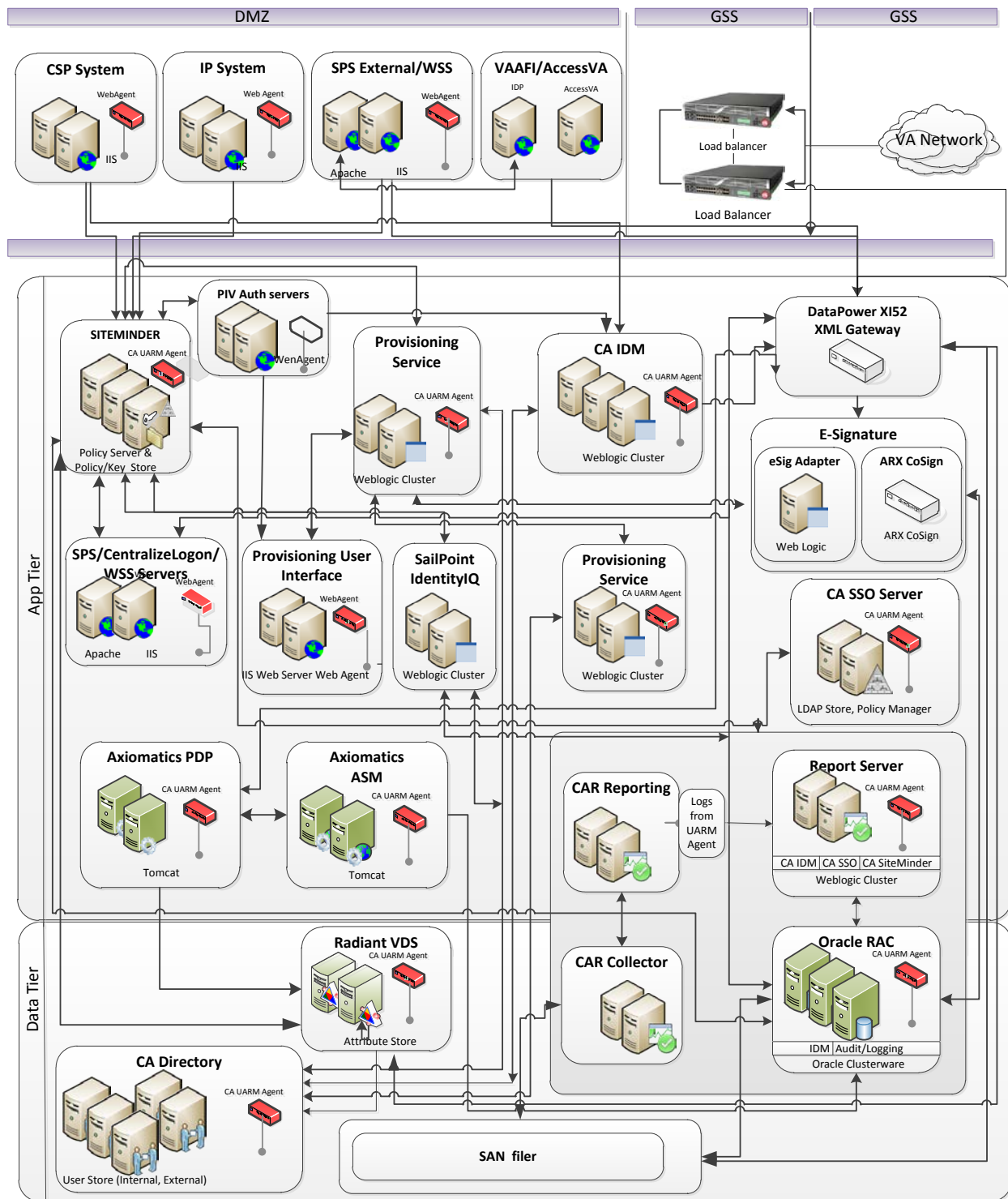


Figure 49: Logical Network String Diagram

4 System Architecture

The AcS solution 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 solution. The communication architecture describes the connection and security requirements needed between the hardware components.

4.1 Hardware Architecture

The following diagram shows the AcS solution hardware architecture and network topology.

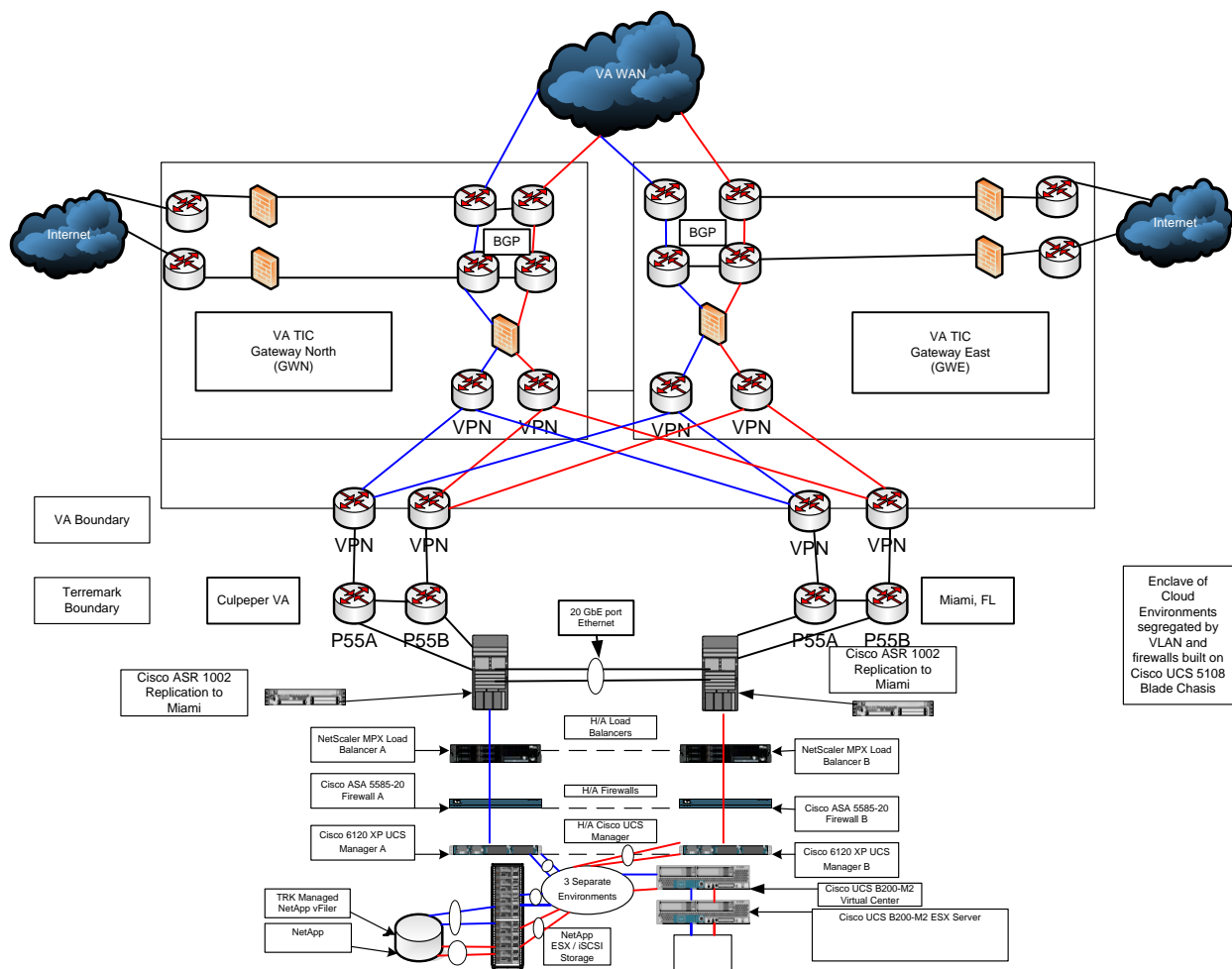


Figure 50: Network Communication Architecture

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

Notes:

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

Table 20: Hardware Appliance

| Hardware Appliance | Descriptions | High Availability (HA) |
|---------------------------|---|--|
| ARX Co-Sign (eSig) | The ARX CoSign device is a PKI-based, off-the-shelf digital-signature solution enabling VA to embed digital signatures in various documents, forms, and transactions. CoSign is a turnkey, hardware-based solution that is easily and quickly deployed in the network and provides cost-effective digital-signature capabilities for the organization. CoSign stores the signature credentials in a secure server, and maintains that the signer has exclusive access user's signature credentials, while still maintaining a centrally managed solution. | The ARX CoSign device has a built-in mechanism to provide HA capability. For high availability, several CoSign appliances are installed where one of the CoSign appliances is defined as the primary while the others are designated as the alternate CoSign appliances. Information is replicated securely from the primary to the alternate appliances using the IPSEC protocol. In case of a failure, another attempt is made. The device will give up after a total of ten tries and an alert will be sent to the administrator. The eSig adapter talks to the primary device. The secondary device pulls the changes from primary and be completely synchronized with the primary device. |
| IBM DataPower | A critical component of AcS infrastructure to | 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 solution machines such as ports, URLs, protocols hostnames for each application in every environment.

Table 21: Virtual Machines and Appliances

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|---------------|----------------------------|---|
| SQA (AITC) | | | |
| CSP/IP/Federation Services WebUI/SPS/WSS (IIS- Single instance on each, Tomcat) | 5 | N/A | VAAUSIAMWEB151.vha.med.va.gov VAAUSIAMWEB152.vha.med.va.gov VAAUSIAMWEB153.vha.med.va.gov VAAUSIAMWEB154.vha.med.va.gov VAAUSIAMWEB155.vha.med.va.gov |
| IdentityMinder supporting (Credential Service Provider and Identity Proofing) WebLogic cluster Admin service on primary node | 3 | N/A | VAAUSIAMIDM600.vha.med.va.gov VAAUSIAMIDM601.vha.med.va.gov VAAUSIAMIDM602.vha.med.va.gov |
| Centralized Logon page, SPS, WSS (IIS- Single instance on each) | 1 | N/A | VAAUSIAMWEB631.vha.med.va.gov |
| PIV Authentication Handler (IIS) Single instance on each No OCSP responder or CRL configuration | 1 | N/A | VAAUSIAMWEB630.vha.med.va.gov |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|---------------|----------------------------|---|
| IdentityMinder support (Provisioning Service) (WebLogic) Admin service on primary node | 2 | N/A | VAAUSIAMIDM603.vha.med.va.gov VAAUSIAMIDM604.vha.med.va.gov |
| Provisioning WebUI (IIS) Single instance on each | 2 | N/A | VAAUSIAMWEB600.vha.med.va.gov VAAUSIAMWEB601.vha.med.va.gov |
| Provisioning Server | 2 | N/A | VAAUSIAMPRV600.vha.med.va.gov VAAUSIAMPRV601.vha.med.va.gov |
| CA Directory (CSP and IP) | 3 | N/A | VAAUSIAMLDP600.vha.med.va.gov VAAUSIAMLDP601.vha.med.va.gov VAAUSIAMLDP602.vha.med.va.gov |
| CA Directory (Provisioning) | 2 | N/A | VAAUSIAMLDP603.vha.med.va.gov VAAUSIAMLDP604.vha.med.va.gov |
| CA SSO Server | 2 | N/A | VAAUSIAMSSO600.vha.med.va.gov VAAUSIAMSSO601.vha.med.va.gov |
| CA SSO | 2 | N/A | VAAUSIAMWEB620.vha.med.va.gov VAAUSIAMWEB621.vha.med.va.gov |
| CA UARM (Tomcat) | 4 | N/A | VAAUSIAMLOG600.vha.med.va.gov VAAUSIAMLOG601.vha.med.va.gov VAAUSIAMLOG602.vha.med.va.gov VAAUSIAMLOG603.vha.med.va.gov (not in cluster currently) |
| CA Report Server (Weblogic) | 2 | N/A | VAAUSIAMRPT600.vha.med.va.gov VAAUSIAMRPT601.vha.med.va.gov |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|----------------|----------------------------|---|
| CA SiteMinder (Weblogic) includes CA Directory instance for SiteMinder Admin service on primary node Admin UI on primary node | 3 | N/A | VAAUSIAMSMP600.vha.med.va.gov VAAUSIAMSMP601.vha.med.va.gov VAAUSIAMSMP602.vha.med.va.gov |
| Axiomatics PDP (Tomcat) | 1 | N/A | VAAUSIAMAPS600.vha.med.va.gov |
| Axiomatics ASM/PAP (Tomcat) | 1 | N/A | VAAUSIAMAPS601.vha.med.va.gov |
| Axiomatics Policy Auditor | 1 | N/A | VAAUSIAMAPA600.vha.med.va.gov |
| Radiant Logic VDS | Not Applicable | 1 | VAAUSIAMVDS600.vha.med.va.gov |
| Oracle RAC | Not Applicable | 2 | VAAUSIAMDBS600.vha.med.va.gov VAAUSIAMDBS601.vha.med.va.gov |
| DataPower XI50 (Appliance) | Not Applicable | 2 | Not Applicable |
| ARX CoSign (Appliance) | Not Applicable | 1 | Not Applicable |
| eSig Weblogic Servers Admin service on primary node | 2 | N/A | VAAUSIAMARX600.vha.med.va.gov VAAUSIAMARX601.vha.med.va.gov |
| Role manager (SailPoint) servers (WebLogic) Admin service on primary node | 2 | NA | VAAUSIAMAPP620.VHA.MED.VA.GOV VAAUSIAMAPP621.VHA.MED.VA.GOV |
| Pre-Production (Terremark Culpeper, VA) | | | |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|---------------|----------------------------|--|
| CSP/IP/Federation Services WebUI/SPS/WSS (IIS, Tomcat) Single IIS instance on each | 4 | N/A | vateriamweb410.preprod.acs.iam.vha.med.va.gov vateriamweb411.preprod.acs.iam.vha.med.va.gov vateriamweb412.preprod.acs.iam.vha.med.va.gov vateriamweb417.preprod.acs.iam.vha.med.va.gov |
| Centralized Logon page, SPS, WSS (IIS) Single IIS instance on each Web403/404 will replace 413/414 | 2 | N/A | Vateriamweb413.preprod.acs.iam.vha.med.va.gov Vateriamweb414.preprod.acs.iam.vha.med.va.gov Vateriamweb403.vha.med.va.gov – new server in VA domain Vateriamweb404.vha.med.va.gov – new server in VA domain |
| PIV Authentication Handler (IIS) Single IIS instance on each | 2 | N/A | Vateriamweb415.preprod.acs.iam.vha.med.va.gov Vateriamweb416.preprod.acs.iam.vha.med.va.gov |
| IdentityMinder supporting (Credential Service Provider and Identity Proofing) (Weblogic) Admin service on primary node | 2 | N/A | vateriamidm410.preprod.acs.iam.vha.med.va.gov vateriamidm411.preprod.acs.iam.vha.med.va.gov |
| IdentityMinder support (Provisioning Service) (Weblogic) Admin service on primary node | 3 | N/A | vateriamidm430.preprod.acs.iam.vha.med.va.gov vateriamidm431.preprod.acs.iam.vha.med.va.gov vateriamidm432.preprod.acs.iam.vha.med.va.gov |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|---------------|----------------------------|---|
| Provisioning WebUI (IIS) Single IIS instance on each | 2 | N/A | vateriamweb430.preprod.acs.iam.vha.med.va.gov vateriamweb431.preprod.acs.iam.vha.med.va.gov |
| Provisioning Server | 2 | N/A | vateriamprv430.preprod.acs.iam.vha.med.va.gov vateriamprv431.preprod.acs.iam.vha.med.va.gov |
| CA Directory (CSP and IP) | 2 | N/A | vateriamldp410.preprod.acs.iam.vha.med.va.gov vateriamldp411.preprod.acs.iam.vha.med.va.gov |
| CA Directory (Provisioning) | 2 | N/A | vateriamldp430.preprod.acs.iam.vha.med.va.gov vateriamldp431.preprod.acs.iam.vha.med.va.gov |
| CA SSO Server | 2 | N/A | vateriamsso450.vha.med.va.gov vateriamsso451.vha.med.va.gov |
| CA UARM | 3 | N/A | vateriamlog470.preprod.acs.iam.vha.med.va.gov vateriamlog471.preprod.acs.iam.vha.med.va.gov vateriamlog472.preprod.acs.iam.vha.med.va.gov |
| CA Report Server | 1 | N/A | vateriamrpt490.preprod.acs.iam.vha.med.va.gov |
| CA SiteMinder (Weblogic) includes CA Directory instance for SiteMinder Admin service on primary node Admin UI on primary node | 3 | N/A | vateriamsmp450.preprod.acs.iam.vha.med.va.gov vateriamsmp451.preprod.acs.iam.vha.med.va.gov vateriamsmp452.preprod.acs.iam.vha.med.va.gov |
| Axiomatics PDP (Tomcat) | 2 | N/A | vateriamdp430.preprod.acs.iam.vha.med.va.gov vateriamdp431.preprod.acs.iam.vha.med.va.gov |
| Axiomatics ASM/PAP (Tomcat) | 1 | N/A | vateriamasm430.preprod.acs.iam.vha.med.va.gov |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|---|----------------|----------------------------|--|
| Radiant Logic VDS | N/A | 1 | VATERIAMVDS402.preprod.acs.iam.vha.med.va.gov |
| Oracle Database | N/A | 2 | vateriamdbs400.preprod.acs.iam.vha.med.va.gov |
| DataPower XI52 (Appliance) | Not Applicable | N/A | Not Applicable Note: Placed inside the VAAFI Enclave |
| ARX CoSign (Appliance) | Not Applicable | N/A | Not Applicable |
| eSig WebLogic Servers Admin service on primary node | 2 | N/A | vateriamarx470.preprod.acs.iam.vha.med.va.gov vateriamarx471.preprod.acs.iam.vha.med.va.gov |
| Role manager (SailPoint) servers (WebLogic) Admin service on primary node | 2 | N/A | VATERIAMAPP433.PREPROD.ACS.IAM.VHA.MED.VA.GOV VATERIAMAPP434.PREPROD.ACS.IAM.VHA.MED.VA.GOV |
| Production (Terremark Culpeper, VA) | | | |
| CSP/IP/Federation Services WebUI/SPS/WSS (IIS) Single IIS instance on each | 4 | N/A | vateriamweb210.prod.acs.iam.vha.med.va.gov vateriamweb211.prod.acs.iam.vha.med.va.gov vateriamweb212.prod.acs.iam.vha.med.va.gov vateriamweb217.prod.acs.iam.vha.med.va.gov |
| Centralized Logon page, SPS, WSS (IIS , Tomcat) Single IIS instance on each | 2 | N/A | vateriamweb213.prod.acs.iam.vha.med.va.gov vateriamweb214.prod.acs.iam.vha.med.va.gov |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|---------------|----------------------------|---|
| PIV Authentication Handler (IIS) Single IIS instance on each No OCSP or CRL | 2 | N/A | vateriamweb215.prod.acs.iam.vha.med.va.gov vateriamweb216.prod.acs.iam.vha.med.va.gov |
| IdentityMinder (CSP and IP) (Weblogic) Admin service on primary node | 2 | N/A | vateriamidm210.prod.acs.iam.vha.med.va.gov vateriamidm11.prod.acs.iam.vha.med.va.gov |
| IdentityMinder (Provisioning) (Weblogic) Admin service on primary node | 3 | N/A | vateriamidm230.prod.acs.iam.vha.med.va.gov vateriamidm231.prod.acs.iam.vha.med.va.gov vateriamidm232.prod.a cs.iam.vha.med.va.gov |
| Provisioning WebUI (IIS) Single IIS instance on each | 2 | N/A | vateriamweb230.prod.acs.iam.vha.med.va.gov vateriamweb231.prod.acs.iam.vha.med.va.gov |
| Provisioning Server | 2 | N/A | vateriamprv230.prod.acs.iam.vha.med.va.gov vateriamprv231.prod.acs.iam.vha.med.va.gov |
| CA Directory (CSP/IP) | 2 | N/A | vateriamldp210.prod.acs.iam.vha.med.va.gov vateriamldp211.prod.acs.iam.vha.med.va.gov |
| CA Directory (Provisioning) | 2 | N/A | vateriamldp230.prod.acs.iam.vha.med.va.gov vateriamldp231.prod.acs.iam.vha.med.va.gov |
| CA SSO Server | 2 | N/A | vateriamsso250.vha.med.va.gov vateriamsso251.vha.med.va.gov |
| CA UARM | 3 | N/A | vateriamlog270.prod.acs.iam.vha.med.va.gov vateriamlog271.prod.acs.iam.vha.med.va.gov vateriamlog272.prod.acs.iam.vha.med.va.gov |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|----------------|----------------------------|--|
| CA Report Server (WebLogic) | 1 | N/A | Vateriamrpt290.prod.acs.iam.vha.med.va.gov |
| CA SiteMinder (WebLogic) includes CA Directory instance for SiteMinder Admin service on primary node Admin UI on primary node | 3 | N/A | vateriamsmp250.prod.acs.iam.vha.med.va.gov vateriamsmp251.prod.acs.iam.vha.med.va.gov vateriamsmp252.prod.acs.iam.vha.med.va.gov |
| Axiomatics PDP (Tomcat) | 2 | N/A | vateriamdp230.prod.acs.iam.vha.med.va.gov vateriamdp231.prod.acs.iam.vha.med.va.gov |
| Axiomatics ASM/PAP (Tomcat) | 1 | N/A | vateriamasm230.prod.acs.iam.vha.med.va.gov |
| Radiant Logic VDS | N/A | 2 | VATERIAMVDS202.prod.acs.iam.vha.med.va.gov VATERIAMVDS203.prod.acs.iam.vha.med.va.gov |
| Oracle Database | N/A | 2 | vateriamdbs200.prod.acs.iam.vha.med.va.gov |
| DataPower XI52 | Not Applicable | N/A | Not Applicable NOTE: Placed inside the VAAFI Enclave |
| ARX CoSign | Not Applicable | N/A | Not Applicable |
| eSig WebLogic Servers | 2 | N/A | vateriamarx270.prod.acs.iam.vha.med.va.gov vateriamarx270.prod.acs.iam.vha.med.va.gov |
| Role manager (SailPoint) servers (WebLogic) | 2 | N/A | VATERIAMAPP233.PROD.ACS.IAM.VHA.MED.VA.GOV VATERIAMAPP234.PROD.ACS.IAM.VHA.MED.VA.GOV |
| DR (Terremark Miami, FL) | | | |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|---------------|----------------------------|--|
| CSP/IP/Federation Services WebUI (IIS) | 4 | N/A | vateriamweb210.dr.acs.iam.vha.med.va.gov vateriamweb211.dr.acs.iam.vha.med.va.gov vateriamweb212.dr.acs.iam.vha.med.va.gov vateriamweb217.dr.acs.iam.vha.med.va.gov |
| Centralized Logon page, SPS, WSS (IIS, Tomcat) | 2 | N/A | vateriamweb213.dr.acs.iam.vha.med.va.gov vateriamweb214.dr.acs.iam.vha.med.va.gov |
| PIV Authentication Handler (IIS) | 2 | N/A | vateriamweb215.dr.acs.iam.vha.med.va.gov vateriamweb216.dr.acs.iam.vha.med.va.gov |
| IdentityMinder (CSP) (WebLogic) | 2 | N/A | vateriamidm210.dr.acs.iam.vha.med.va.gov vateriamidm211.dr.acs.iam.vha.med.va.gov |
| IdentityMinder (Provisioning) (WebLogic) | 3 | N/A | vateriamidm230.dr.acs.iam.vha.med.va.gov vateriamidm231.dr.acs.iam.vha.med.va.gov vateriamidm232.dr.acs.iam.vha.med.va.gov |
| Provisioning WebUI (IIS) | 2 | N/A | vateriamweb230.dr.acs.iam.vha.med.va.gov vateriamweb231.dr.acs.iam.vha.med.va.gov |
| Provisioning Server | 2 | N/A | vateriamprv230.dr.acs.iam.vha.med.va.gov vateriamprv231.dr.acs.iam.vha.med.va.gov |
| CA Directory (CSP and IP) | 2 | N/A | vateriamldp210.dr.acs.iam.vha.med.va.gov vateriamldp211.dr.acs.iam.vha.med.va.gov |
| CA Directory (Provisioning) | 2 | N/A | vateriamldp230.dr.acs.iam.vha.med.va.gov vateriamldp231.dr.acs.iam.vha.med.va.gov |
| CA SSO Server | 2 | N/A | vateriamssso250.dr.acs.iam.vha.med.va.gov vateriamssso251.dr.acs.iam.vha.med.va.gov |
| CA UARM | 3 | N/A | vateriamlog270.dr.acs.iam.vha.med.va.gov vateriamlog271.dr.acs.iam.vha.med.va.gov vateriamlog272.dr.acs.iam.vha.med.va.gov |
| CA Report Server (WebLogic) | 1 | N/A | Vateriamrpt290.dr.acs.iam.vha.med.va.gov |

| Application | Number of VMs | Number of Physical Servers | Hostname |
|--|---------------|----------------------------|--|
| CA SiteMinder (WebLogic) includes CA Directory instance for SiteMinder | 2 | N/A | vateriamsmp250.dr.acs.iam.vha.med.va.gov vateriamsmp251.dr.acs.iam.vha.med.va.gov |
| Axiomatics PDP (Tomcat) | 2 | N/A | VATERIAMAPSXXX.dr.acs.iam.vha.med.va.gov VATERIAMAPSXXX.dr.acs.iam.vha.med.va.go |
| Axiomatics ASM/PAP (Tomcat) | 1 | N/A | VATERIAMAPSXXX.dr.acs.iam.vha.med.va.gov |
| Radiant Logic VDS | N/A | 2 | VAAUSIAMVDSXXX.dr.acs.iam.vha.med.va.gov VAAUSIAMVDSXXX.dr.acs.iam.vha.med.va.go |
| Oracle Database | N/A | 2 | vateriamdbs200.dr.acs.iam.vha.med.va.gov vateriamdbs201.dr.acs.iam.vha.med.va.gov |
| DataPower XI52 (Appliance) | N/A | N/A | N/A |
| ARX CoSign (Appliance) | N/A | N/A | N/A |
| eSig WebLogic Servers | 2 | N/A | vateriamarx270.dr.acs.iam.vha.med.va.gov vateriamarx270.dr.acs.iam.vha.med.va.gov |

4.2 Software Architecture

The following diagram shows the complete software architecture of the VA AcS solution.

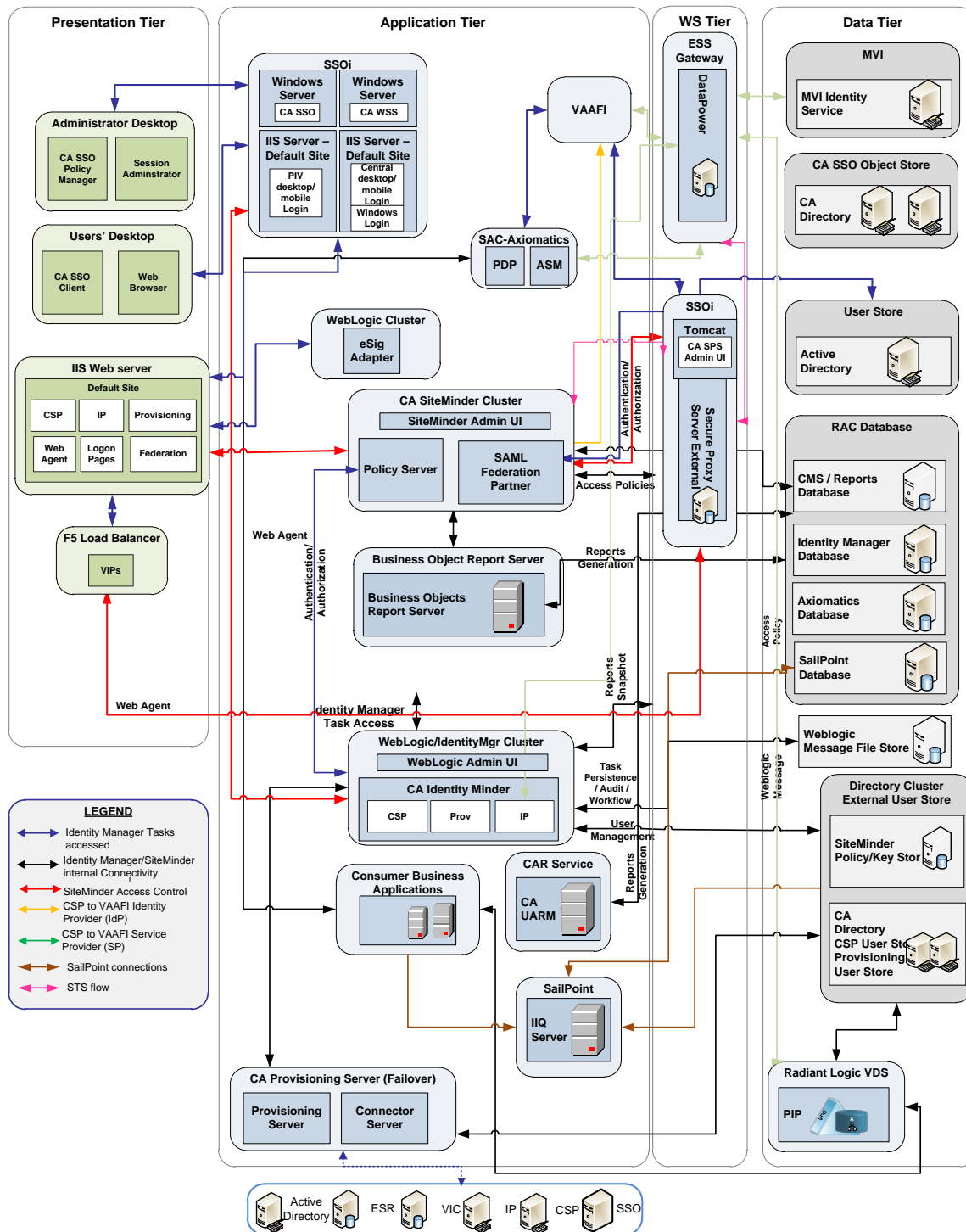


Figure 51: Software Architecture

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

Table 22: AcS Products and Versions

| Activity Name | Products | Abbreviation | Product Version/Release |
|-----------------------------------|------------------------------------|------------------------|-------------------------|
| Credential Service Provider (CSP) | 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 |
| | Oracle Database | - | 11gR2 |
| | CA Directory | LDAP directory | 12.0 SP7 |
| | CA SiteMinder | CA SM | SM r12.5 SP1 |
| | CSP .NET Application | CSP App | ASP.NET 4 |
| Single Sign-On – Internal (SSOi) | CA Single Sign On | CA SSO | 12.1 / R12.1 |
| | Oracle Database | - | 11gR2 |
| | CA Directory | CA LDAP | 12.0 SP7 |
| | CA SiteMinder | CA SM | SM r12.51 |
| | CA Option Pack for Federation | - | SM r12.51 |
| | Login Page | LP | ASP.NET 4 |
| Provisioning (PROV) | CA IdentityMinder | CA IdentityMinder | R12.6 SP3 |
| | IIS Web Sever | - | 7.5 |
| | CA Web Agent | - | SM r12.51/12.0SP3 |
| | WebLogic | - | 10.3,6 |
| | Oracle Database | - | 11gR2 |
| | CA Directory | LDAP directory | 12.0 SP7 |
| | CA SiteMinder | CA SM and Proxy Server | SM r12.51 |
| | CA WorkPoint | CA WP | R12.6 SP3 |
| | BLTH (Business Logic Task Handler) | BLTH | Java 1.7 |
| | MVI Web Service Client | MVI WS | Java 1.7 |

| Activity Name | Products | Abbreviation | Product Version/Release |
|--------------------------------------|---|--|--------------------------|
| | Radiant Logic VDS | Attribute Service & Policy Information Point | 6.2.2 |
| | SailPoint - Compliance Manager | SailPoint IdentityIQ Access Governance Manager | v6.1p2 |
| Specialized Access Control (SAC) | Axiomatics PDP | Policy Decision Point | 5.2.1 |
| | Axiomatics ASM | Services Manager | 5.2.1 |
| | Axiomatics PAP | Policy Administration Point | 5.2.1 |
| | Axiomatics APA | Axiomatics Policy Auditor | 1.1.3 |
| | Apache Tomcat | Axiomatics Application Server | 7.0.42 |
| Compliance Audit and Reporting (CAR) | CA User Activity Reporting Module | CA UARM | 12.5 SP3 (12.5) |
| | CA User Activity Reporting Module Agent | CA UARM Agent | 12.5 SP3 (12.5) |
| | SAC Connector | SAC Connector | UARM Regular Expressions |
| e-Signature (eSig) | ARX Co-Sign | Digital Signature | v6.3 |
| Identity Proofing (IP) | 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 |
| | 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.

Table 23: Software Components

| Software Component | |
|---|---|
| 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. | |
| Database Table spaces | <p>4 Data Table spaces: PROVIDM_DATA, CSPIPIDM_DATA, CASMAUDIT_DATA,ESIGAUDIT_DATA,VDSAUDIT_DATA, SACASM_DATA</p> <p>3 Index Table spaces: PROVIDM_INDX, CSPIPIDM_INDX, CASMAUDIT_INDX</p> <p>Users</p> <p>Temp</p> <p>Rollback</p> <p>Undo</p> |
| High Availability | For the AcS 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 | |
| <p>The CA Directory servers are a shared resource for the AcS solution. The CA Directory infrastructure will be configured in a multi-master replication configuration. The CA Directory comprises of various instances elaborated as follows.</p> <p>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.</p> | |
| 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. |

| Software Component | |
|--|---|
| | |
| High Availability | <p>There will be a master write server for each directory. The other supporting directories will be read directories.</p> <p>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 to provide synchronized in real-time and consistent servers.</p> <p>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 is comprised of the IIS web servers which provide reverse proxy and federation to the applications. | |
| 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.</p> <p>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</p> |

| Software Component | |
|--|--|
| | <p>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 | |
| <p>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.</p> | |
| WebLogic Instances | <p>CA IdentityMinder for CSP and Provisioning solution</p> <p>CA SiteMinder Admin UI</p> <p>eSig Web Service</p> |
| 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> |
| Application Tier –Tomcat Application Server | |
| <p>The application tier for the SAC solution is comprised of Tomcat application servers. The Application Tier is a shared environment for hosting application components. The AcS related applications hosted are listed below. The Axiomatics PDP and ASM components are hosted on</p> | |

| Software Component | |
|---|--|
| the Tomcat application servers. | |
| Tomcat Instances | Axiomatics ASM Axiomatics PDP Axiomatics APA |
| High Availability | Tomcat will not be configured as an application cluster. Tomcat is used to as an applications container for the Axiomatics product. No other applications will be deployed to the container. High Availability will be provided through load balancing of the service requests via DataPower and F5 VIP. Each TCP connection will be alternated between application nodes without a sticky bit. Each connection is stateless. |
| Report Server /Reporting Infrastructure | |
| CA Report Server is powered by Business Objects Enterprise XI to use the reports provided with IdentityMinder. | |
| Axiomatics | |
| The Axiomatics components are integral to the specialized access control solution. It provides the necessary components for externalizing authorization. Axiomatics is comprised of the following components. | |
| Subcomponents | <p>Axiomatics Services Manager: System for managing an APS installation from a central point by providing for the deployment, configuration, and monitoring of PDPs, as well as for the management of attributes and audit services. ASM makes possible the remote management of PDP configurations, including policies, attribute sources and various other run-time configurations. ASM provides functionality for declaring attribute sources and also allows users to create and maintain attribute definitions for use in the Axiomatics PAP Client. In addition, ASM monitors the operational status of PDPs. Applicable data needed by ASM is stored in an external database.</p> <p>Policy Decision Point: Service that provides XACML-based authorization to Policy Enforcement Points (PEPs). The Axiomatics PDP provides externalized authorization and runs as a service on the network, exposing a web service interface that is secured by SSL/TLS.</p> <p>Policy Administration Point: Development environment for XACML 3 policies is used in the Axiomatics authorization infrastructure. Provides graphical XACML policy editor, attribute dictionary, and simulating and tracing policies. Policies will check in to ClearCase when finalized and can be checked out by an administrator when policy updates are needed.</p> |

| Software Component | |
|--|--|
| | Policy Auditor: Simplifies the analysis and validation process of XACML policies. Provides a user-friendly web-based graphical interface. |
| High Availability | The PDPs are stateless and will use the F5 for high availability. |
| 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. | |
| 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 solution 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. |
| CA SiteMinder | |
| CA SiteMinder is an integral component of Access Services solution, providing CSP solution federation capabilities to integrate with VAAFI. CA SiteMinder is also utilized to protect the CA IdentityMinder application. CA SiteMinder is comprised of the following components. | |
| Subcomponents | <p>SiteMinder Policy Server: The Policy Server provides advanced authentication and password services to protected applications such as CA IdentityMinder. The policy server communicates with the CA Directory, which stores the required policy objects, key objects and user data to provide federation services as well.</p> <p>Secure Proxy Server: The Secure Proxy Server provides agentless web based integration as well as provides secure web services calls supported by centralized policies defined in SiteMinder.</p> <p>Policy/Key Store: The policy store / key store is CA</p> |

| Software Component | |
|---|---|
| | <p>Directory instance which stores configured policies, objects and keys required by CA SiteMinder.</p> <p>Web Agents: The agents to be installed on the web server protect the resources.</p> <p>Admin User Interfaces: The Admin UI hosted in admin VLAN to manage CA SiteMinder and policies.</p> <p>FSS Administrative UI: The Federation Admin UI is hosted on same VM as CA SiteMinder to manage CA SiteMinder for federation configuration. It requires a web server as provided in the web tier above.</p> <p>Audit: The SiteMinder Audit sub-system stores audit events for SiteMinder authentication and authorization transactions. The data is stored in the oracle database and is secured from modifications.</p> |
| High Availability | <p>CA SiteMinder will be installed on three (3) servers. These servers will be load balanced using the native CA SiteMinder software configuration.</p> <p>The CA SiteMinder web agent HA is depending on Application Web server HA. If there are multiple IIS instance for the protected application, webagent is also on HA as it is installed on individual Web server. Webagent configured to talk to all the Siteminder Policy Server available and internally it load balance the request in a round robin mode.</p> |
| CA SSO | |
| <p>The CA SSO server, Authentication services, and CA SSO desktop client enable the SSOi services for desktop single sign on usage. The authentication services communicate with the user store to provide credentials and authenticate the user to the SSOi solution. It also interacts with the CA Directory to maintain user logon information. The CA SSO is installed and configured in FIPS only mode as approved by TRM.</p> | |
| Subcomponents | <p>CA SSO Server: The CA SSO Server is the main component of the CA SSO suite. It manages resources and provides services to the CA SSO Client. A CA SSO server farm will be created for clustering. The data on each server can then be replicated to the servers contained within the farm.</p> <p>CA Policy Manager: The Policy Manager is the user interface to manage the SSO Server and the data stores (CA Access Control and CA Directory). It is usually installed on an administrator's workstation for remote management of SSO Servers using TCP/IP.</p> <p>CA SSO Desktop Client: The CA SSO Client is the desktop component of CA SSO must be installed on every end-user workstation that requires SSOi solution.</p> |

| Software Component | |
|--|---|
| High Availability | <p>There are a number of components for CA SSO which will be configured for High Availability.</p> <p>CA SSO Server: A CA SSO server farm will be created. It is a system of two networked CA SSO Servers. The data on each server will be replicated to servers in the farm. The Terremark Culpeper, VA site and Terremark Miami, FL site will contain two (2) servers in each site to create the server farm. One server in each server farm is assigned as hub. The hub server is the server that receives the incoming updates from external server farms, and propagates the data to its peers within its own server farm to achieve failover between sites. The load is be balanced between two servers in the server farm using the Citrix NetScaler load balancer.</p> <p>CA Policy Manager: The Policy Manager is the user interface that enables the management of the SSO Server and the data stores (CA Access Control and CA Directory). It is installed on an administrator's workstation for remote management of SSO Servers using TCP/IP.</p> <p>CA SSO Desktop Client: The CA SSO Client is the desktop component of CA SSO. It must be installed on every end-user workstation that requires SSOi solution. The CA SSO Client has built-in failover between the CA SSO Client and the authentication host, and between the CA SSO Client and CA SSO Server. The fully qualified domain name (FQDN) for both Terremark Culpeper, VA server farm and Terremark Miami, FL server farm is defined in the CA SSO client configuration for built-in failover.</p> |
| CA UARM | |
| <p>CA User Activity Reporting Module collects logs from a variety of applications and devices using agentless or agent-based methods. It then normalizes the log to CA Common Event Grammar (CEG) and reduces the volume of logs by filtering unwanted events based on pre-defined event filtering policies. Processed events are available for reporting, alerting, and multi-dimensional investigation. Based on log archival policy, CA UARM compresses logs and stores them on external storage systems for long term storage. The CA UARM component is installed and configured in FIPS only mode as per TRM.</p> <p>CA UARM only supports CentOS System which is a closed vendor provided Virtual Appliance. This Product is procured and properly licensed to VA. All the Subscription patches for the CentOS system are provided by the Vendor itself.</p> | |
| Subcomponents | <p>Management/Reporting Server: There will be one active management server in the User Activity Reporting Module network. The second server will be a failover (inactive) management server. The management server stores predefined and user-defined content and configurations. The management server also authenticates users and authorizes feature access.</p> |

| Software Component | |
|---|--|
| | <p>Collection Server: Collection server will be responsible to collect and normalize the log events sent by respective UARM agents. Agent is responsible to failover to respective collector servers in case one of collector servers is not available.</p> |
| High Availability | <p>The CAR architecture maintains two (2) Collector Servers and one (1) Reporting Server. The Collector Servers are the main actors that collect the data events and are designed to have an instant failover. The agents for the collectors would failover to the appropriate collector, which will reduce the likelihood of data loss in transit.</p> <p>The reporting servers are designed with a hot and cold instance. Since the reporting server is not responsible for any data collection, the hot and cold instance addresses HA requirements in that the collector server will be switched to the cold instance in case of a failure.</p> |
| eSig Adapter | |
| <p>eSig Adapter is the engine that provides the basis for the eSig capability. eSig uses the CoSign appliance as a building block and provides the capability to digitally sign documents to various applications within VA. Moreover, the events are recorded and made available to the CAR service for reporting. The eSig system utilizes an inherent defense mechanism to reduce potential system security compromises.</p> | |
| Subcomponents | <p>DataPower devices: The DataPower devices are used to authenticate the machine to machine sessions.</p> <p>WebLogic Server: The WebLogic Server hosts the eSig adapter. The eSig adapter has the following components:</p> <p>eSig Servlet: The eSig Servlet receives the request and passes on to the eSig Façade. The Servlet currently receives only API calls but can be extended if required to include the web interface.</p> <p>eSig Façade: The eSig façade component carries out the following categories of operation:</p> <ul style="list-style-type: none"> ○ User Management: The user management function allows the service to add or remove a particular user. ○ Sign and Verify: This allows the applications to sign a given document. ○ Reporting Events: This category allows the eSig service to record events that will be reported via CAR service. <p>CoSign Device: The CoSign device is a hardware appliance that stores the user certificates.</p> |
| High Availability | <p>The DataPower appliances have an inherent, self-contained HA feature where the appliance will auto failover to the other appliance; however, the DataPower appliances do not</p> |

| Software Component | |
|--|--|
| | <p>support internal load balancing.</p> <p>WebLogic domains are created in clusters consisting of multiple WebLogic Server instances running simultaneously and working together to provide increased scalability and reliability. A cluster appears to clients to be a single WebLogic Server instance. The server instances that constitute a cluster can run on the same system, or be located on different systems. The eSig Servlet and eSig Façade run within the cluster domain and is highly available through multimode cluster and is load balanced by F5 and DataPower.</p> <p>CoSign is highly available through internal functions that keep the appliances in sync with each other.</p> <p>The (limited) High availability feature within the ARX CoSign appliances (in the production environment with two CoSign appliances) is handled manually through swap of the primary and secondary appliances in case of failure of the primary one. There is no option for load balancing of the requests among the two devices. Only local replication of the configuration and user data is ensured between the two devices, thus allowing for manually initiated failover with limited amount of downtime. The communication interface between the ARX CoSign WebLogic servers and the appliance(s) is through a DNS registered FQDN, pointing to an IP address, registered with the Primary appliance. At the time of the manual failover the IP address configuration is also swapped, thus allowing for uninterrupted communication from the WebLogic App Server custom eSig component to the appliances.</p> |
| Radiant Logic VDS | |
| Radiant Logic VDS acts as an abstraction layer, extracting identity and context information from various (in-scope) applications and data silos. | |
| Subcomponents | The Radiant Logic product is Virtual Directory (VDS) for VA Policy Information Points (PIP) and is an integral component of the specialized access control solution. |
| High Availability | Identically configured VDS servers are configured behind a hardware load balancer to provide horizontal scalability to support query performance and capacity (concurrent consumers). VDS instances are configured for data replication. Provisioning will write user data to one instance and VDS will replicate the data to the other instance. The MVI Rest service (data provider) has to be highly available since VDS is not persisting that data. A virtual IP (Load balancer) will be configured as a front end to the two production instances. |
| Role Manager (SailPoint) | |

| Software Component | |
|---|---|
| <p>Role manager (SailPoint) is the centralized tool which will support the role mining and access governance requirements at VA. A web application deployed on the application server has an Oracle database as its backend for storing applicable object configurations including authoritative, application account data. The data that is reconciled in the tool periodically (based upon a pre-defined timeframe) is used to re-certify user access and streamline the role management process.</p> | |
| Subcomponents | <p>Compliance Manager: The Compliance Manager is a SailPoint module which is provided within the base installation.</p> <p>This component provides a graphical user interface to perform access governance activities which include:-</p> <ol style="list-style-type: none"> 1- Configure authoritative and other target applications. 2- Perform role mining analysis from the aggregated data 3- Configure access re-certifications <p>Reporting and Advanced Analytics: The tool provides an in-build reporting and searching capability to assist in the audit/analyzing requirements.</p> |
| High Availability | The role manager tool utilizes WebLogic clustering mechanism for high availability. |

The following table defines the programming languages used for development within the VA AcS solution.

Table 24: Programming Languages

| Programming Languages | Definition/Description |
|-----------------------|---|
| Java | Java language was used to develop custom class/jar file for IdentityMinder Business Logic Task Handler BLTH. |
| C#/.NET | C#/.NET for development of custom applications. |
| HTML / DHTML | Provides basic web page language. |
| ASP.NET | Active Server Pages for development of web-pages. The SiteMinder login.fcc page was customized using this language. |
| XML | Common configurations are stored as XML files. |
| XACML | XML-based language for development of privileges/role management. |
| JavaScript | Scripting language. |
| RegEX | Regular Expression. |
| BeanShell | Scripting language for development of SailPoint configuration objects |

The following table lists the operating systems used for the VA AcS solution.

Table 25: Operating Systems

| Operating Systems |
|------------------------------|
| Windows Server 2008 R2 |
| CentOS 5.5 |
| Red Hat Enterprise Linux 5.3 |

4.3 Communications Architecture

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

4.4 Communication Channel Security

In order for AcS system components to communicate internally (within the boundaries of AcS) or externally in a secure manner, the supporting software PKI infrastructure components need to be configured. Every Hypervisor Virtual machine, physical server, hardware or software appliance, and applicable other AcS-exposed service is issued a VA internal or commercial (publicly trusted) CA signed server certificate and configured for runtime use. If auto-enrollment service for PKI certificates is not available for any of the AcS' virtual or physical system components, certificate signing requests (CSR) (in the form of Certificate Signing Request [CSR] file) will be generated for each component and sent to the VA PKI helpdesk at [REDACTED]. The following lists the server certificates for the AcS components:

- The publicly accessible AcS URLs requiring user authentication are protected by SSL/TLS encryption. The client SSL/TLS connections will be terminated at the Citrix NetScaler load balancer and subsequently proxied to the appropriate AcS DMZ component.
- The SSL/TLS certificates assigned to the AcS' external access URLs were requested from and issued by VAs commercial (publicly trusted) certificate authority - GTE Cybertrust
- The AcS native components communicating TCP/IP layer secured FIPS mode of encryption.
- VA Internal User Access
- AcS Infrastructure Security

4.5 AcS Inter-component Communications

The following table displays the necessary port communications and protocols used for each component-based server. The ports described must be open for both inbound and outbound communications. The ports mentioned below indicate inbound ports and are opened to AcS components for communication.

Table 26: Port Communications and Protocols

| Application | Network | Port(s) | Reason | Protocol(s) |
|-----------------|----------|------------|--|-------------|
| Oracle Database | Internal | [REDACTED] | Oracle SQL Net Listener | TCP (JDBC) |
| | | [REDACTED] | DataGuard | TCP |
| | | [REDACTED] | Connection Manager | TCP |
| | | [REDACTED] | Oracle Management Agent | TCP |
| | | [REDACTED] | Oracle Enterprise Database Console (HTTP Port) | HTTP |
| | | [REDACTED] | Oracle Enterprise Database Console (RMI Port) | TCP |

| Application | Network | Port(s) | Reason | Protocol(s) |
|---|----------|---------|---|-------------|
| | | ████ | Oracle Enterprise Database Console (JMS Port) | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM collection server | TCP |
| | | ████ | SAILPT – Role manager internal database | TCP |
| CA Directory (CSP/IP, Provisioning) | Internal | ████ | Provisioning router dsa | TCP |
| | | ████ | Provisioning main dsa | TCP |
| | | ████ | Provisioning common objects dsa | TCP |
| | | ████ | Provisioning inclusions dsa | TCP |
| | | ████ | Provisioning notify dsa | TCP |
| | | ████ | DXWebserver Listener (SSL) | HTTPS |
| | | ████ | DXWebserver Listener for shutdown command | TCP |
| | | ████ | Dxmanager-DXadmin communication | TCP |
| | | ████ | CSP/PROV/SMPS Router DSA | LDAPS |
| | | ████ | CSP Data DSA | LDAPS |
| | | ████ | SMPS Data DSA | LDAPS |
| | | ████ | PROV Data DSA | LDAPS |
| | | ████ | DXadmin Secure LDAP | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM Collection Server | TCP |
| Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI) | DMZ | ████ | Accounting port | TCP |
| | | ████ | Authentication port | TCP |
| | | ████ | Authorization port | TCP |
| | | ████ | Auditing Port | TCP |
| | | ████ | SSL port for reverse proxy | HTTPS |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM Collection Server | TCP |
| CA Report | Internal | ████ | WebLogic Port for Report Server | HTTPS |

| Application | Network | Port(s) | Reason | Protocol(s) |
|---|--------------|---------|---|-------------|
| Server | | ████ | Central Management Console Server Port | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM Collection Server | TCP |
| Federation Option Pack | DMZ | ████ | ServletExec port for listening incoming requests from IIS | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM Collection Server | TCP |
| CA Identity Manager (CSP/IP, Provisioning) | Internal | ████ | Administration Port | HTTPS |
| | | ████ | Manage Server Port | TCP |
| | | ████ | Node Manager | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM Collection Server | TCP |
| Provisioning Server | Internal | ████ | Provisioning Server | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM Collection Server | TCP |
| CA SiteMinder | Internal | ████ | Accounting port | TCP |
| | | ████ | Authentication port | TCP |
| | | ████ | Authorization port | TCP |
| | | ████ | Auditing Port | TCP |
| | | ████ | SSL port for reverse proxy | HTTPS |
| | | ████ | WebLogic port for SiteMinder Admin UI | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM Collection Server | TCP |
| CA Siteminder SPS | DMZ/Internal | ██ | Apache HTTP Port | HTTP |
| | | ██ | Apache SSL port | HTTPS |
| | | ████ | Tomcat/ SPS HTTP Port | HTTP |
| | | ██ | Tomcat/SPS SSL Port | HTTPS |

| Application | Network | Port(s) | Reason | Protocol(s) |
|----------------|----------|---------|--|-------------|
| CA UARM | Internal | ████ | Administration Port for CA UARM | TCP |
| | | ████ | SSL Port (reverse proxy to administration port 5250) for CA UARM | HTTPS |
| | | ████ | Syslog port (UDP) for CA UARM server | TCP |
| | | ████ | Syslog TCP listening port for CA UARM | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | Communication port for ODBC /JDBC driver | TCP |
| | | ████ | Audit client communication with port-mapper | TCP |
| | | ████ | Dispatcher SME listener | TCP |
| | | ████ | CA Directory LDAP DXadmin port (CA Directory bundled with CA UARM) | TCP |
| | | ████ | Dispatcher Service in SSL mode for events from Client Connector | TCP |
| CA SSO Server | Internal | ████ | Port for ticket granting agent (Windows Authentication Agent) | TCP |
| | | ████ | Access Control port bundled with CA SSO | TCP |
| | | ████ | LDAP communication port for CA Directory bundled with CA SSO for user directory | LDAPS |
| | | ████ | LDAP communication port for CA Directory bundled with CA SSO for token directory | LDAPS |
| | | ████ | TCP SSL port where the SSO Server will listen. | TCP |
| | | ████ | Agent command and control listening port | TCP |
| | | ████ | CA UARM Collection Server | TCP |
| DataPower XI52 | Internal | ████ | Administration port | TCP |
| | | ████ | Web services | HTTPS |
| ARX CoSign | Internal | ████ | API Calls | HTTPS |

| Application | Network | Port(s) | Reason | Protocol(s) |
|--------------------------|----------|----------|-------------------------------|-------------|
| eSig WebLogic | Internal | ████ | Administration Port | HTTPS |
| | | ████ | Manage Server Port | TCP |
| | | ████ | Node Manager | TCP |
| Radiant Logic VDS | Internal | ████ | LDAP SSL port | LDAPS |
| | | ████ | Application server Admin Port | HTTP |
| | | ████ | Application server HTTP Port | HTTP |
| | | ████ | Application server HTTPS port | HTTPS |
| | | ████ | Application server JMX port | TCP |
| | | ████ | Control Panel Web server port | HTTP |
| | | ████ | Control Panel Web server Port | HTTPS |
| | | ██ | Web Services Port | HTTPS |
| Axiomatics | Internal | ████ | HTTP Connector Port | HTTP |
| | | ████ | AJP Connector Port | TCP |
| | | ████ | Server Shutdown Port | TCP |
| | | ████ | HTTPS Connector Port | HTTPS |
| SailPoint | Internal | ████████ | HTTPS Connector Port | HTTPS |

The following tables provide the AcS solution inter-component communications details.

Table 27: Pre-Production PKI Certificate List

| Computer Name (Hostname) | Common Name (CN) | FQDN | Cert Type | Issuer | Cert Function | Description | Comments |
|-----------------------------|------------------|------|-----------|--------|---------------|--------------------------------|----------|
| | | | Internal | VA | Device | Citrix NetScaler Load balancer | |
| | | | Internal | VA | Device | Citrix NetScaler Load balancer | |
| | | | External | VA | Web URL | Internet-facing URL | |
| | | | Internal | VA | Web URL | Internet-facing URL | |
| | | | Internal | VA | Web URL | Provisioning WebLogic Cluster | |
| | | | Internal | VA | Web URL | Provisioning IIS | |
| | | | Internal | VA | Web URL | SSOi Server | |
| | | | | | | | |
| | | | Internal | VA | Device | DataPower (SAC) | |
| | | | Internal | VA | Web URL | Data Power Mgmt. (SAC) | |
| | | | Internal | VA | Web URL | DataPower (SAC) | |
| | | | Internal | VA | Web URL | Data Power Mgmt. (SAC) | |
| | | | Internal | VA | Web URL | Siteminder SPS | |
| | | | External | VA | Web URL | Siteminder WSS | |
| | | | Internal | VA | Web URL | Siteminder WSS | |
| | | | Internal | VA | Web URL | PIV authentication | |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Cert Type | Issuer | Cert Function | Description | Comments |
|-----------------------------|------------------|------|-----------|--------|---------------|-------------------------------|------------|
| | | | Internal | VA | Web URL | PIV authentication | |
| | | | External | VA | Web URL | SiteMinder SPS | |
| | | | | | | | |
| | | | Internal | VA | Server/Web | CSP WebLogic Cluster | |
| | | | | | | | |
| | | | Internal | VA | Server/Web | CSP WebLogic Cluster | |
| | | | | | | | |
| | | | Internal | VA | Server/Web | CSP WebLogic Cluster | |
| | | | | | | | |
| | | | Internal | VA | SSL | Provisioning WebLogic Cluster | Management |
| | | | | | | | |
| | | | Internal | VA | SSL | Provisioning WebLogic Cluster | Management |
| | | | | | | | |
| | | | Internal | VA | SSL | CA SiteMinder | Management |
| | | | | | | | |
| | | | Internal | VA | SSL | CA SiteMinder | Management |
| | | | | | | | |
| | | | Internal | VA | SSL | CA SiteMinder | Management |
| | | | | | | | |
| | | | Internal | VA | Web Service | CA Directory | LDAPS |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Cert Type | Issuer | Cert Function | Description | Comments |
|-----------------------------|------------------|------|-----------|--------|---------------|--------------|----------------------------|
| | | | | | | | |
| | | | Internal | VA | SSL | CA Directory | Management |
| | | | Internal | VA | Web Service | CA Directory | LDAPS |
| | | | | | | | |
| | | | Internal | VA | SSL | CA Directory | Management |
| | | | Internal | VA | Web Service | CA Directory | LDAPS |
| | | | | | | | |
| | | | Internal | VA | SSL | CA Directory | Management |
| | | | Internal | VA | Web Service | CA Directory | LDAPS |
| | | | | | | | |
| | | | Internal | VA | SSL | CA Directory | Management |
| | | | Internal | VA | Web Service | CA Directory | LDAPS |
| | | | | | | | |
| | | | Internal | VA | SSL | CA SSO | SSL listener |
| | | | Internal | VA | Web Service | CA SSO | SSL listener |
| | | | Internal | VA | Web Service | CA SSO | LDAPS with CA Directory |
| | | | | | | | |
| | | | Internal | VA | SSL | CA SSO | SSL listener |
| | | | Internal | VA | Web Service | CA SSO | SSL listener |
| | | | Internal | VA | Web Service | CA SSO | LDAPS with CA Directory |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Cert Type | Issuer | Cert Function | Description | Comments |
|-----------------------------|------------------|------|-----------|--------|---------------|-------------|----------------------|
| | | | | | | | |
| | | | Internal | VA | URL | CA UARM | |
| | | | Internal | VA | Server | CA UARM | |
| | | | Internal | VA | SSL | CA UARM | Management interface |
| | | | Internal | VA | Web Service | CA UARM | Dispatcher Service |
| | | | | | | | |
| | | | Internal | VA | URL | CA UARM | |
| | | | Internal | VA | Server | CA UARM | |
| | | | Internal | VA | SSL | CA UARM | Management interface |
| | | | Internal | VA | Web Service | CA UARM | Dispatcher Service |
| | | | | | | | |
| | | | Internal | VA | URL | CA UARM | |
| | | | Internal | VA | Server | CA UARM | |
| | | | Internal | VA | SSL | CA UARM | Management interface |
| | | | Internal | VA | Web Service | CA UARM | Dispatcher Service |
| | | | | | | | |
| | | | Internal | VA | URL | CA UARM | |
| | | | Internal | VA | Server | CA UARM | |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Cert Type | Issuer | Cert Function | Description | Comments |
|-----------------------------|------------------|------|-----------|--------|---------------|-----------------------|-----------------------------|
| | | | Internal | VA | SSL | CA UARM | Management interface |
| | | | Internal | VA | Web Service | CA UARM | Dispatcher Service |
| | | | | | | | |
| | | | Internal | VA | Server | Oracle 11g | Also serve as auditing cert |
| | | | Internal | VA | SSL | Oracle 11g | Management |
| | | | | | | | |
| | | | Internal | VA | Server | Oracle 11g | Also serve as auditing cert |
| | | | Internal | VA | SSL | Oracle 11g | Management |
| | | | | | | | |
| | | | Internal | VA | Server | Oracle 11g | Also serve as auditing cert |
| | | | Internal | VA | SSL | Oracle 11g | Management |
| | | | | | | | |
| | | | Internal | VA | Server | Oracle 11g | Also serve as auditing cert |
| | | | Internal | VA | SSL | Oracle 11g | Management |
| | | | | | | | |
| | | | Internal | VA | SSL | Reporting | WebLogic port |
| | | | Internal | VA | SSL | Reporting | WebLogic port |
| | | | Internal | VA | SSL | eSig WebLogic Cluster | |
| | | | Internal | VA | SSL | eSig WebLogic Cluster | |
| | | | Internal | VA | Device | ARX-CoSign | |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Cert Type | Issuer | Cert Function | Description | Comments |
|--------------------------|------------------|------|-----------|--------|---------------|-------------|----------|
| | | | Internal | VA | Device | ARX-CoSign | |
| | | | | | | | |

Table 28: Production Cert List

| Computer Name (Hostname) | Common Name (CN) | FQDN | Certificate Type | Issuer | Cert Function | Comments |
|--------------------------|------------------|------|------------------|-------------|---------------|--|
| | | | Internal | VA | SSL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | External | External CA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | External | VA | Device | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | External | External CA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | | | | |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Certificate Type | Issuer | Cert Function | Comments |
|-----------------------------|------------------|------|---------------------|----------------|------------------|--|
| | | | External | External CA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | SSL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | External | External CA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | External | VA | Device | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | | | | |
| | | | External | External CA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Certificate Type | Issuer | Cert Function | Comments |
|-----------------------------|------------------|------|---------------------|-------------|------------------|--|
| | | | Internal | VA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | External | External CA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | Internal | VA | Web URL | FQDNs for Citrix NetScaler Load balancer N/A |
| | | | | | | |
| | | | Internal | VA | Device | FQDNs & Hostname for DataPower N/A |
| | | | | | | |
| | | | Internal | VA | Device | FQDNs & Hostname for DataPower N/A |
| | | | | | | |
| | | | Internal | VA | Device | FQDNs & Hostname for DataPower N/A |
| | | | | | | |
| | | | Internal | VA | Device | FQDNs & Hostname for DataPower N/A |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | | | | |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Certificate Type | Issuer | Cert Function | Comments |
|-----------------------------|------------------|------|---------------------|--------|------------------|------------|
| | | | Internal | VA | SSL | Management |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | Internal | VA | Web Service | LDAPS |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | Internal | VA | Web Service | LDAPS |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | Internal | VA | Web Service | LDAPS |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | Internal | VA | Web Service | LDAPS |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | Internal | VA | Web Service | LDAPS |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Certificate Type | Issuer | Cert Function | Comments |
|-----------------------------|------------------|------|---------------------|--------|------------------|----------------------------|
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | Internal | VA | Web Service | LDAPS |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | Internal | VA | Web Service | LDAPS |
| | | | | | | |
| | | | Internal | VA | SSL | Management |
| | | | Internal | VA | Web Service | LDAPS |
| | | | | | | |
| | | | Internal | VA | SSL | |
| | | | Internal | VA | Web Service | SSL listener |
| | | | Internal | VA | Web Service | LDAPS with CA Directory |
| | | | | | | |
| | | | Internal | VA | SSL | |
| | | | Internal | VA | Web Service | SSL listener |
| | | | Internal | VA | Web Service | LDAPS with CA Directory |
| | | | | | | |
| | | | Internal | VA | URL | |
| | | | Internal | VA | Server | |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Certificate Type | Issuer | Cert Function | Comments |
|-----------------------------|------------------|------|---------------------|--------|------------------|-----------------------------|
| | | | ternal | VA | SSL | Management interface |
| | | | ternal | VA | Web Service | Dispatcher Service |
| | | | | | | |
| | | | ternal | VA | URL | |
| | | | ternal | VA | Server | |
| | | | ternal | VA | SSL | Management interface |
| | | | ternal | VA | Web Service | Dispatcher Service |
| | | | | | | |
| | | | ternal | VA | URL | |
| | | | ternal | VA | Server | |
| | | | ternal | VA | SSL | Management interface |
| | | | ternal | VA | Web Service | Dispatcher Service |
| | | | | | | |
| | | | ternal | VA | URL | |
| | | | ternal | VA | Server | |
| | | | ternal | VA | SSL | Management interface |
| | | | ternal | VA | Web Service | Dispatcher Service |
| | | | | | | |
| | | | ternal | VA | Server | Also serve as auditing cert |

| Computer Name (Hostname) | Common Name (CN) | FQDN | Certificate Type | Issuer | Cert Function | Comments |
|-----------------------------|------------------|------|---------------------|--------|------------------|--------------------------------|
| | | | Internal | VA | SSL | Management |
| | | | | | | |
| | | | Internal | VA | Server | Also serve as auditing cert |
| | | | Internal | VA | SSL | Management |
| | | | | | | |
| | | | Internal | VA | Server | Also serve as auditing cert |
| | | | Internal | VA | SSL | Management |
| | | | | | | |
| | | | Internal | VA | Server | Also serve as auditing cert |
| | | | Internal | VA | SSL | Management |
| | | | | | | |
| | | | Internal | VA | SSL | WebLogic port |
| | | | | | | |
| | | | Internal | VA | SSL | WebLogic port |
| | | | Internal | VA | SSL | WebLogic port |
| | | | Internal | VA | SSL | WebLogic port |
| | | | | | | |
| | | | Internal | VA | Device | |
| | | | Internal | VA | Device | |

5 Data Design

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

5.1 DBMS Files

The AcS solution 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 29: 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/cspipidm_data |
| CPIPIDM_INDX | +ORADATA/acsdbs/datafile/cspipidm_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 |

| Table Spaces | Data Files |
|---------------|---|
| SYSAUX | +ACSDb_DATA/sailpt/datafile/sysaux.284.828271115 |
| 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 AcS solution, non-DBMS files are used for the following activities:

- **CSP, IP, and Provisioning:** User store schema within CA Directory is customized to store registered user record information (refer to [section A.1](#) 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.1](#)).
- **CAR:** Stores data in UARM logs and leverages information present in AcS activities and integrated applications for reporting (refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions).
- **Provisioning:** VDS does not have a directory tree structure but each time builds a structure for namespace similar to application connected to, for example in this case similar to provisioning.

6 Detailed Design

This section describes the design for the AcS 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 solution. 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), IBM DataPower, and ARX CoSign.



20131108 - AcS IAM
TerreMark PreProd ar

6.2 Software Detailed Design

This section provides final detailed information associated with the design of each AcS solution activity and the associated functionality that is being delivered.

6.2.1 Provisioning Design

The Provisioning service is an integral component of the AcS solution, which aims to institute an automated, streamlined approval workflow process to augment the existing identity life cycle model of the VA. Provisioning encompasses various aspects of user access management, including initial assignment of user entitlements, subsequent modification of those entitlements, and de-provisioning of entitlements. The entitlements that a user may be associated with include predefined roles or groups with specified privileges related to each role and application access rights. The service will provide the foundation for an enterprise-wide method for managing the provisioning life cycle for an integrated application.

The Provisioning activity provides centralized management of user account creation, termination, and modification for VA applications. It provides VA users a means to initiate self-service requests for account creation and modification for integrated applications, then automatically route the provisioning request to the designated Approver. Once approved, accounts will be provisioned automatically.

The following diagram provides a detailed view of the complete provisioning activity at VA, including interactions with various business partners as well as end users. The following sections provide a detailed description of each component.

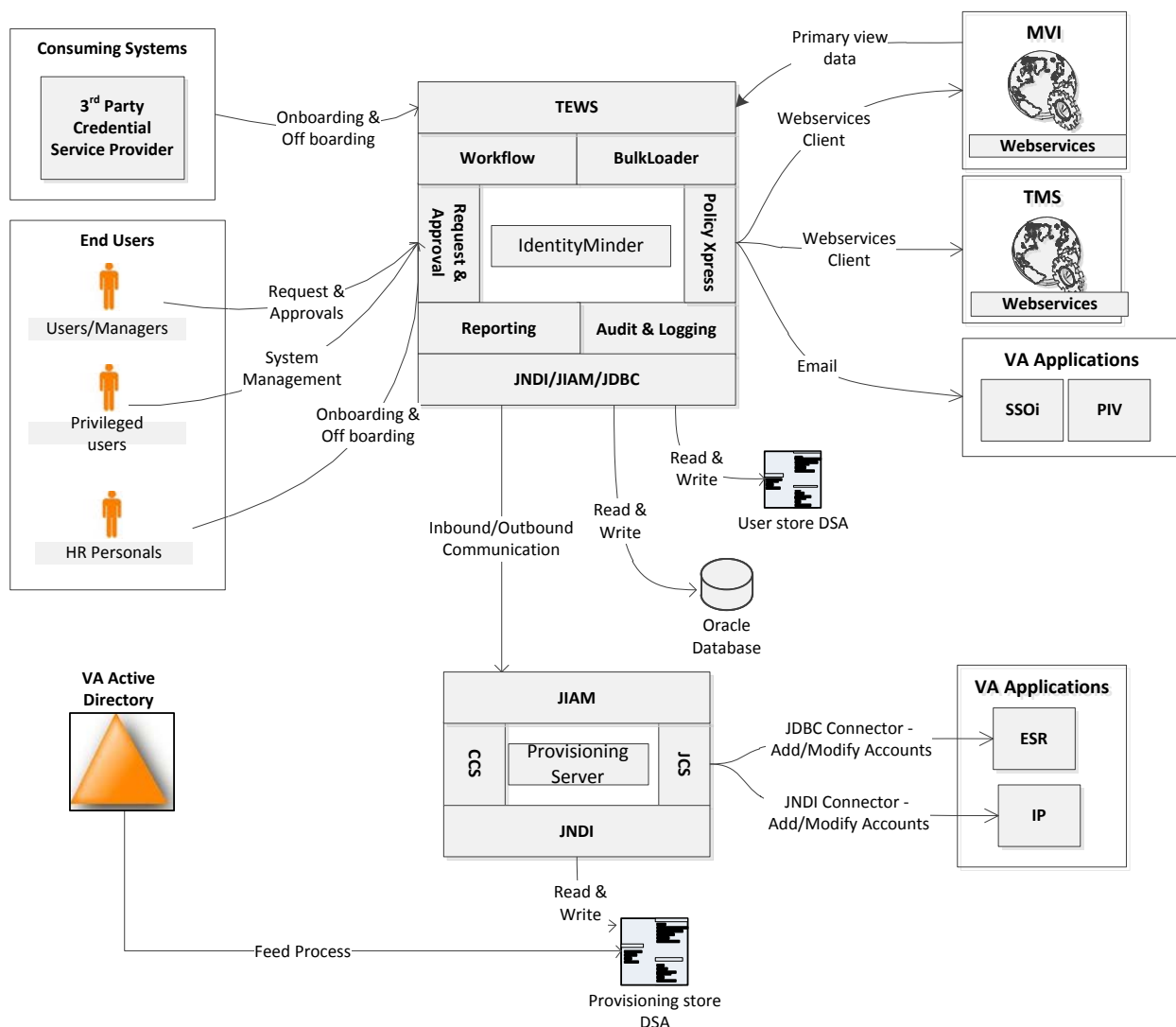


Figure 53: Provisioning Detail Design

The different end points interacting with the Provisioning activity include the following.

- **TMS and PIV:** These are email based connectors as an email will be sent to the account administrators to provision/de-provision the users. Future releases will automate this process.
- **MVI:** Integrated with MVI via web services to determine whether a user already exists in the system by searching for a user before user is added and a unique identifier SEC ID is issued. Provisioning connects to MVI to capture primary view data to facilitate Provisioning-VDS-MVI integration. The changes in the primary view data (Last Name, First Name, Middle Name, SSN, Suffix, Gender, and DOB) at MVI side will trigger a web service call to provisioning system, to update the attributes.
- **Active Directory:** The user accounts are correlated to the IdentityMinder global user based on samAccountName and email-based provisioning is setup as part of user onboarding.

Note: Individual interface control documents provide details on the integration of these applications with Provisioning.

CA IdentityMinder:

The Provisioning activity leverages the capabilities of CA IdentityMinder to minimize software development using standard capabilities of the suite. The Provisioning service creates, modifies, and disables access to consuming applications.

CA IdentityMinder is central component of the Provisioning activity. It is a J2EE application deployed on the WebLogic application server cluster, which implements the provisioning activity. It is integrated with SiteMinder providing SSO capability and supporting access control to VA users for accessing the registration features. The major modules of CA IdentityMinder implemented for VA include the following:

- **Workflow:** A feature that helps control the flow of provisioning and de-provisioning across the VA enterprise. For the AcS solution, it is mostly used for approvals and delegations.
- **Policy Express:** Policy Express 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 applications to submit remote tasks to CA IdentityMinder for execution.
- **Provisioning server:** Provisioning engine of the architecture, which acts as a broker between IdentityMinder and Connector server
- **Connector Server:** Endpoint server which connects with various endpoints for provisioning and de-provisioning

The following sections provide an overview of the use cases / functionality being implemented by the Provisioning activity.

The user onboarding and user offboarding follow the same technical flow for employees/contractors/HP trainees/volunteers, except that the required and optional attributes (refer to [section A.2](#) below) may change for each of them, and/or the approvers context may change.

6.2.1.1 Provisioning: User Onboarding

| Field | Description |
|---------------|---|
| Use Case Name | User CRISP Onboarding |
| Description | This use case describes the process by which a new VA Employee/Contractor/HP Trainees/Volunteers is on boarded. |
| Actors | 1. Provisioning Service (CA Identity Minder) (Provisioning forms,workflow,policy express) 2. HR/Sponsor/COR (Requestor) 3. VA Manager (Approver) 4. User Store 5. MVI |

| Field | Description |
|----------------|---|
| | 6. Account Administrators |
| Pre-Conditions | <ol style="list-style-type: none"> 1. All the human actors have appropriate access privileges in provisioning service to perform the actions 2. Connectivity between provisioning service and MVI and Sec ID generation |
| Trigger | <ol style="list-style-type: none"> 1. The New Employee/Contractor/HP Trainees/Volunteers accepts VA employment offer |
| Actions | <ol style="list-style-type: none"> 1. HR/Sponsor/COR: with required privileges login to CA IdentityMinder to complete user registration process 2. HR/Sponsor/COR: access the access form and fill in the details of the user to be on boarded and submit the IdentityMinder task 3. IdentityMinder makes a call to MVI, to check the existence of the record 4. If the user record exists with corresponding Sec ID, then the CA IdentityMinder creates a new identity record with the SEC ID returned from MVI and correlates it to the MVI record. 5. If the user record exists without an associated SEC ID, then the CA IdentityMinder generates the SEC ID and initiates an "Add Person" and correlates it to the MVI record. 6. If the user does not exists in MVI, then the CA IdentityMinder generates the SEC ID and call the "Add Person-implicit" MVI service to create an identity record within the MVI System and correlates the SEC ID to that record 7. Workflow associated with the task gets triggered and appends a work item to the VA Manager/Sponsor queue and sends an email to the VA Manager/Sponsor to Approve/Reject the addition of user to the provisioning system 8. Approver logs into the CA IdentityMinder and selects the work item specific to the on boarding and validates the user data to approve / reject the request with proper justification 9. Upon successful approval, Policy Express script associated with the task gets triggered and email will be sent to associated TMS administrators for implementing the birth right privileges, which are not managed through the provisioning system 10. The user will be created in the user store of provisioning system 11. HR/Sponsor/COR: with required privileges login to CA IdentityMinder, the system which implements the provisioning system 12. HR/Sponsor/COR access the CRISP checklist select the "TMS training completed" checkbox 13. Workflow associated with the task gets triggered and sends notification to Active Directory administrators and PIV system administrators 14. Active Directory administrator will log into the provisioning system and provide details of Active Directory specific user details, as part of user profile and proceed the workflow process 15. The PIV system administrator will log into the provisioning system and provide details of PIV as part of user profile and proceed the workflow process 16. The user will be created in the user store of provisioning system |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram actor Requestor participant Provisioning Forms participant User store participant Workflow participant Approver participant Policy Express participant Account Administrators participant MVI Requestor->>Provisioning Forms: 1. User Logs in Provisioning Forms->>Provisioning Forms: 2. Completes onboarding forms Provisioning Forms->>MVI: 3. Calls MVI related to SEC ID generation MVI->>User store: 4. If user record exists with corresponding SEC ID, create a new identity record and correlate it with MVI MVI->>User store: 5. If user record exists without corresponding SEC ID, generate SEC ID, initiate Add Person and correlate with MVI MVI->>User store: 6. If user does not exist in MVI, generate SEC ID, initiate Add Person implicit and correlate with MVI MVI->>Workflow: 7. Workflow triggered, email sent to Approver Workflow->>Approver: 8. Approver Access Application & selects work item Approver->>Workflow: 9. Validate and approve Workflow->>Policy Express: 10. Sent a notification to TMS admins Policy Express->>User store: 11. User is created in User Store Requestor->>Provisioning Forms: 12. User logs in Provisioning Forms->>Provisioning Forms: 13. Completes TMS training Provisioning Forms->>Policy Express: 14. Notify AD and PIV administrators Policy Express->>User store: 15 & 16. Approved and update user values User store->>User store: 17. User is created </pre> |
| Main Success Scenarios | <ol style="list-style-type: none"> 1. Successful generation of SEC ID for VA employee/contractor/HP Trainees/Volunteers 2. Creation of VA Employee/Contractor/HP Trainees/Volunteers in provisioning system with Sec ID as unique identifier |
| Main Failure Scenarios | <ol style="list-style-type: none"> 1. SEC ID creation process error out 2. Failure in creation of user in provisioning system |

6.2.1.2 Provisioning: Third-Party / DoD Onboarding

| Field | Description |
|----------------|--|
| Use Case Name | Third-Party Onboarding |
| Description | This use case describes the process by which a VA / External System calls the provisioning web service for onboarding a third party or DoD user |
| Actors | <ol style="list-style-type: none"> 1. Provisioning Service – web service 2. VA / External System 3. Provisioning Service – CA IdentityMinder 4. MVI 5. VDS |
| Pre-Conditions | <ol style="list-style-type: none"> 1. The VA system have appropriate access privileges to access provisioning service to onboard user |
| Trigger | <ol style="list-style-type: none"> 1. The VA / External System calls Provisioning service for onboarding |
| Actions for | <ol style="list-style-type: none"> 1. The VA / External System calls provisioning web service function VATHirdPartyOnboardUserProfile() and passes the primary user traits to CA IdentityMinder system for user creation including First Name, Last Name, Middle Name(optional), SSN, Prefix, Suffix, Address, Date of Birth, Email(optional), Gender , EDIPI(optional), CSP ID and LOA. Along with the |

| Field | Description |
|-------|--|
| | <p>attributes, a self-asserted Boolean value will be passed, to inform whether the attribute value is self-asserted or CSP provided</p> <ol style="list-style-type: none"> 2. The Task Execution Web Service (TEWS) calls the business logic task handler (BLTH), which has the custom code for the implementation 3. If the request contains EDIPI value, BLTH invokes SearchbyEDIPI() MVI function to retrieve the user and If the request do not contain EDIPI value, the BLTH invokes SearchbyTraits() MVI function, passing First Name, Last Name, Middle Name (optional), SSN (optional), Date of Birth, and Gender as traits to search the user. 4. If the user record exists with corresponding Sec ID in MVI, search the provisioning store to retrieve the user attributes <ol style="list-style-type: none"> a. If the provisioning record has a lower LOA value than the incoming request, then the provisioning attributes (including the MVI_ attribute set) will be updated along with LOA and end the process. b. If the provisioning record had a higher LOA value than the incoming request then the CSPID and MVI_ attributes of the record will be update in provisioning c. If the provisioning record has the same LOA value as the request, then the provisioning attributes (including the MVI_ attribute set) will be updated and end the process d. If the provisioning record is not found for the corresponding SecID, an error message is thrown to the VA/External system and end the process 5. If the user record exists without an associated SEC ID in MVI, then the BLTH will generates the SEC ID and invokes an “Add Person (Add Correlation)” MVI function and correlates it to the MVI record. 6. The user will be created in the user store of provisioning system, with all the attributes including MVI_ attributes returned from the search. 7. If the user does not exists in MVI, then the BLTH generates the SEC ID and call the “Add Person-implicit” MVI service to create an identity record within the MVI System and correlates the SEC ID to that record. 8. The user will be created in the user store of provisioning system, with all MVI attribute values 9. The provisioning record is provisioned to VDS system 10. The provisioning system sends a response to the VA system on the status of the operation |

| Field | Description |
|------------------------|---|
| Sequence Diagram | <pre> sequenceDiagram participant VA as VA / External System participant PWS as Provisioning Web Service participant BLTH as CA IdentityMinder BLTH participant MVI as MVI participant VDS as VDS VA->>PWS: 1. Calls & send the primary user traits PWS->>BLTH: 2. Invoke the custom code BLTH->>MVI: 3. Search by traits or Search by EDIPI, based on the request MVI-->>BLTH: 4. If the user record exists with corresponding Sec ID in MVI, update the LOA value of the user in provisioning BLTH-->>PWS: 5. If record does not exist, SECID is generated and correlated with MVI PWS->>PWS: 6. User is created in provisioning store PWS->>MVI: 7. If user does not exist in MVI, person is added and correlation with MVI MVI->>PWS: 8. User is created in provisioning store PWS->>VDS: 9. User provisioned to VDS PWS-->>VA: 10. Send the status as response </pre> |
| Main Success Scenarios | <ol style="list-style-type: none"> 1. Successful generation of Sec ID for third-party user 2. Creation of third-party user in provisioning system with Sec ID as a unique identifier and update VDS |
| Main Failure Scenarios | <ol style="list-style-type: none"> 1. Sec ID creation process error out 2. Failure in creation of user in provisioning system or VDS |

6.2.1.3 Provisioning: Update Provisioning Record from MVI

| Field | Description |
|----------------|--|
| Use Case Name | Update Provisioning Record from MVI |
| Description | This use case describes the process by which the MVI system calls the provisioning web service for updating the user data as part of the primary view change |
| Actors | <ol style="list-style-type: none"> 1. Provisioning Service – web service 2. Provisioning Service – CA IdentityMinder 3. MVI 4. VDS |
| Pre-Conditions | 1. MVI system have appropriate access privileges to access provisioning service to update the user |
| Trigger | 1. If a user record in MVI is updated and SECID correlation exists for that record |
| Actions | <ol style="list-style-type: none"> 1. The MVI system calls provisioning web service function UpdateProvisioning() and passes SECID and primary user traits which are changed as part of MVI primary view update to CA IdentityMinder system for user update including First Name, Last Name, Middle Name(optional), SSN, Prefix, Suffix, Date of Birth, Gender. 2. The Task Execution Web Service (TEWS) calls the business logic task handler (BLTH), which has the custom code for the implementation 3. BLTH updates the VDS system with new user information passed from MVI 4. The provisioning system updates the user record in provisioning store 5. The provisioning system sends a response to the VA system on the status of the operation |

| Field | Description |
|------------------------|---|
| Sequence Diagram | <pre> sequenceDiagram participant MVI participant PWS as Provisioning Web Service participant CA as CA Identity/Vinder BLTH participant VDS MVI->>PWS: 1. Calls & send the update user traits PWS->>CA: 2. Invoke the custom code CA->>VDS: 3. User provisioned to VDS CA->>CA: 4. User is created in provisioning store CA->>MVI: 5. Send the status as response </pre> |
| Main Success Scenarios | Successful update of user record in provisioning and VDS |
| Main Failure Scenarios | Failure in update of user in provisioning system or VDS |

The **Provisioning web service function description** is provided in the following table.

Note: The format for data elements is elaborated in the AcS data elements spreadsheet in [section A.1](#) below.

| Method /Function | Description of Method/Function | Input | Output |
|----------------------------------|--|---|-----------------------------|
| VAThirdPartyOnboardUserProfile() | Onboard a third party user into provisioning store | <ol style="list-style-type: none"> 1. First Name (Required) 2. FNSelfAssert (Required - Boolean) 3. Last Name (Required) 4. LNSelfAssert (Required - Boolean) 5. DOB (Required - MM/DD/YYYY format) 6. DOBSelfAssert (Required - Boolean) 7. Email (Required) 8. EmailSelfAssert(Required - Boolean) 9. Gender (Required) 10. GenderSelfAssert(Required - Boolean) 11. CSPID (Required) 12. CSPIDSelfAssert(Required - Boolean) 13. LOA(Required) 14. LOASelfAssert(Required - Boolean) 15. 16. Middle Name (Optional) 17. MNSelfAssert (Optional - Boolean) 18. Suffix (Optional) 19. SuffixSelfAssert (Optional - Boolean) 20. SSN (Optional – 9 digits) 21. SSNSelfAssert (Optional - Boolean) 22. EDIPI(Optional) 23. EDIPISelfAssert (Optional - Boolean) 24. Home Address(Optional) 25. HASelfAssert (Optional - Boolean) 26. Home Phone(Optional) 27. HPSelfAssert (Optional - Boolean) | SECID (10 digits – string) |

6.2.1.4 Provisioning: User Offboarding

| Field | Description |
|----------------|--|
| Use Case Name | User Offboarding |
| Description | This use case describes the process by which an existing VA Employee/Contractor/HP Trainees/Volunteers is off boarded. |
| Actors | <ol style="list-style-type: none">1. Provisioning Service (CA Identity Minder) (Provisioning forms, workflow, policy express, Connector Server)2. HR/Sponsor/COR (Requestor)3. VA Manager (Approver)4. User Store5. Account Administrators |
| Pre-Conditions | <ol style="list-style-type: none">1. All the human actors have appropriate access privileges in provisioning service to perform the actions |
| Trigger | <ol style="list-style-type: none">1. VA Employee/Contractor/HP Trainees/Volunteers provides notice for separating from employment to VA Manager.2. VA Manager/Sponsor is notified of breach of rules by VA Employee |
| Actions | <ol style="list-style-type: none">1. Requester with proper privileges login to CA IdentityMinder to initiate user off boarding process2. Requestor access the appropriate form to submit a request for off boarding a user3. Workflow associated with the task gets triggered and appends a work item to the HR/Sponsor/COR queue.4. Workflow sends an email to the HR/Sponsor/COR to Approve/Reject the off boarding of user to the provisioning system5. Approver logs into CA IdentityMinder and selects the work item specific to the off boarding and validates the user data and approves the request to off board the user6. Policy Express script associated with the task gets triggered and email will be sent to TMS administrators, Active Directory administrators and PIV administrators for de-provisioning the accesses, which are not managed through the provisioning system7. Provisioning system will de provision accounts for managed endpoints via connector server8. User is deactivated in the user store and roles / group membership are updated accordingly |

| Field | Description |
|------------------------|---|
| Sequence Diagram | <pre> sequenceDiagram participant Requestor participant Provisioning Forms participant User store participant Workflow participant Approver participant Policy Express participant Account Administrators participant Connector Server Requestor->>Provisioning Forms: 1. User Logs in Provisioning Forms->>Provisioning Forms: 2. Complete forms and Submits Provisioning Forms->>Workflow: 3. Task submitted Workflow->>Approver: 4. Workflow triggered, email sent to Approver Approver->>Provisioning Forms: 5. Approver Access Application & selects work item Approver->>Policy Express: 6. Validate and approve Policy Express->>Account Administrators: 6. Sent a notification to all account admins Account Administrators->>Connector Server: 7. Deprovision the managed accounts Connector Server->>User store: 8. Deactivate the user </pre> |
| Main Success Scenarios | <p>VA Employee/Contractor/HP Trainees/Volunteers is deactivated in the provisioning system</p> <p>Associated accounts of VA Employee/Contractor/HP Trainees/Volunteers are removed from the VA applications</p> |
| Main Failure Scenarios | Error during deactivation of VA Employee/Contractor/HP Trainees/Volunteers in the provisioning system |

6.2.1.5 Provisioning: User Provisioning

| Field | Description |
|----------------|---|
| Use Case Name | User Provisioning |
| Description | This workflow describes the technical activities and associated data exchanges through which a VA users self-registers for an integrated application. |
| Actors | <ol style="list-style-type: none"> Provisioning Service (Provisioning system, workflow, policy express) Employee/Contractor (Requestor) VA Manager (Approver) Managed Endpoints (via Account Administrators for non-managed endpoints) |
| Pre-Conditions | <ol style="list-style-type: none"> All the human actors have appropriate access privileges in provisioning service to perform the actions |
| Trigger | <ol style="list-style-type: none"> VA Employee/Contractor/HP Trainees/Volunteers requires access to VA application to perform their job function |
| Actions | <ol style="list-style-type: none"> Requester with proper privileges login to CA IdentityMinder to request access to a managed endpoint Requestor accesses the access request form and submits a request for access to an endpoint Workflow associated with the task gets triggered and appends a work item to the appropriate approver's queue Workflow sends an email to the approver to Approve/Reject the provisioning request |

| Field | Description |
|------------------------|---|
| | <ol style="list-style-type: none"> Approver logs into CA Identity Minder and selects the work item specific to the access request and validates the user data and approves the request to grant access to the endpoint If the endpoint is not managed through CA IdentityMinder, a policy express script associated with the task gets triggered and corresponding emails will be sent to account administrators of the endpoint to provisioning the access If the endpoint is managed through CA IdentityMinder, then CA IdentityMinder evaluates the requested role and calls the Provisioning Server to provision the access. Provisioning Server connects with the appropriate connector server and provision the request privileges at the endpoint |
| Sequence Diagram | <pre> sequenceDiagram participant Requestor participant Provisioning System participant Workflow participant Approver participant Policy Express participant Managed Endpoints Requestor->>Provisioning System: 1. User logs in Requestor->>Provisioning System: 2. Submits request for access Workflow->>Requestor: 3. Workflow triggered, append item to user's queue Workflow->>Approver: 4. Send email to Approver Provisioning System->>Approver: 5. Selects work item, validates user data & grants access Workflow->>Policy Express: 6. For non managed endpoints, policy express script is triggered to send email Policy Express->>Managed Endpoints: 6. Provision request privileges Provisioning System->>Managed Endpoints: 7. Endpoint is managed Provisioning System->>Managed Endpoints: 8. For managed endpoints, access is provisioned within the endpoint </pre> |
| Main Success Scenarios | VA Employee/Contractor/HP Trainees/Volunteers is provisioned to the requested VA application |
| Main Failure Scenarios | VA Employee/Contractor/HP Trainees/Volunteers is not provisioned to the requested VA application |

6.2.1.6 User De-Provisioning

| Field | Description |
|---------------|--|
| Use Case Name | User De-provisioning |
| Description | This workflow describes the technical activities and associated data exchanges through which a VA user is de-provisioned for an integrated application. |
| Actors | <ol style="list-style-type: none"> Provisioning Service (Provisioning system, workflow, policy express) Employee/Contractor (Requestor) VA Manager (Approver) Managed Endpoints (via Account Administrators for non-managed endpoints) |

| Field | Description |
|------------------------|---|
| Pre-Conditions | 1. All the human actors have appropriate access privileges in provisioning service to perform the actions |
| Trigger | 1. VA Employee/Contractor/HP Trainees/Volunteers transfers from one organization unit to another 2. VA Employee/Contractor/HP Trainees/Volunteers job function is changed |
| Actions | <ol style="list-style-type: none"> 1. Requester with proper privileges login to CA IdentityMinder to request de-provisioning of a to a managed endpoint 2. Requestor accesses the access request form and submits a request for de-provisioning an access 3. Workflow associated with the task gets triggered and appends a work item to the appropriate approver's queue 4. Workflow sends an email to the approver to Approve/Reject the provisioning request 5. Approver logs into CA IdentityMinder and selects the work item specific to the access request and validates the user data and approves the request to revoke access from the endpoint 6. If the endpoint is not managed through CA IdentityMinder, a policy express script associated with the task gets triggered and corresponding emails will be sent to account administrators of the endpoint to de-provisioning the access 7. If the endpoint is managed through CA IdentityMinder, then CA IdentityMinder evaluates the requested role and calls the Provisioning Server to de-provision the access. 8. Provisioning Server connects with the appropriate connector server and connects to the endpoint and de-provision the request privileges |
| Sequence Diagram | <pre> sequenceDiagram participant Requestor participant Provisioning System participant Workflow participant Approver participant Policy Express participant Managed Endpoints Requestor->>Provisioning System: 1. User logs in Requestor->>Provisioning System: 2. Submits request for de-provisioning Provisioning System->>Workflow: 3. Workflow triggered, append item to user's queue Workflow->>Approver: 4. Send email to Approver Provisioning System->>Workflow: 5. Access Provisioning, validates user data & revokes access Workflow->>Policy Express: 6. For non managed endpoints, policy express script is triggered to send email Provisioning System->>Workflow: 7. For managed endpoints, evaluate the role Workflow->>Managed Endpoints: 8. For managed endpoints, access is de-provisioned within the endpoint </pre> |
| Main Success Scenarios | VA Employee/Contractor/HP Trainees/Volunteers is de-provisioned from the requested VA application |
| Main Failure Scenarios | VA Employee/Contractor/HP Trainees/Volunteers is not de-provisioned from the requested VA application |

6.2.1.7 Explore and Correlate from Endpoints

| Field | Description |
|----------------|---|
| Use Case Name | Explore and Correlate from Endpoints |
| Description | <p>This workflow describes the technical activities and associated data exchanges through which user identity record is explored and correlated with integrated endpoints. The explore correlate functionality only maps user identities, and no user attributes are changed (provisioning does not get updated based on endpoint, but endpoints get updated by provisioning). Provisioning only is updated by authoritative source (in this case VA AD feed), which is consumed through identity feed. Active Directory samAccountName is mapped to Provisioning user id, for user feed.</p> <p>During the feed process, if the samAccountName of a user is not found for the corresponding provisioning record, the record will be ignored and manual suspension of the account will be carried out. During the explore and correlate process, the accounts which do not find a matching samAccountName in provisioning, will be correlated to the orphan bucket named “default user”. The users correlated to “default user” will be reported to the application endpoint custodian and the provisioning system will not delete, suspend the users tagged under “default user”. The explore and correlate policy is configured to only correlate the endpoint accounts with the provisioning records and not update the provisioning user attributes</p> <p>Note: The VA application ESR is explored-correlated as an endpoint during initial set up of Provisioning service integration with ESR. Provisioning uid(samAccountName) is used as the correlation key with ESR ID.</p> |
| Actors | <ol style="list-style-type: none">1. Provisioning Service (Connector server, provisioning server, CA IdentityMinder)2. Managed endpoint |
| Pre-Conditions | VA application should be a managed application under IdentityMinder |
| Trigger | The daily batch job is the starting point. |
| Actions | <ol style="list-style-type: none">1. A batch job or a manual explore and correlate, triggers the Connector Server to start the explore and correlate operation2. Connector Server searches the endpoint and explores the account and pass it to the provisioning server3. Provisioning server reconciles the explored accounts with the existing global user for correlation4. Provision server does the inbound call to the IdentityMinder on the explored and correlate accounts5. IdentityMinder global users will be correlated to the associated endpoints accounts and accounts which do not match the global user id will be tagged into the orphan account6. The accounts that do not match global users are tagged to be orphaned |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram participant Endpoints participant Connector Server participant Provisioning Server participant Identity Minder Endpoints->>Connector Server: 1. Explore & Correlate trigger Connector Server->>Provisioning Server: 2. Search and explores accounts Provisioning Server->>Provisioning Server: 3. Reconcile accounts Provisioning Server->>Identity Minder: 4. Inbound call with account info Identity Minder->>Identity Minder: 5. IM Global users are correlated to associated endpoint accounts Identity Minder->>Identity Minder: 6. Accounts that do not match global users Are tagged to be orphaned </pre> |
| Main Success Scenarios | The identities from the VA application are explored and correlated successfully |
| Main Failure Scenarios | Failure to run the explore and correlate job |

6.2.2 Role Manager (SailPoint IdentityIQ) Design

The role manager tool is an integral component of the AcS solution, which aims to institute an automated, streamlined role mining and access governance process to improve the existing governance landscape at VA. The current implementation is limited to development environment. Role mining is the process of defining roles which includes reconciliation of data from target repositories and then logical structuring of the associated data (entitlements) into enterprise level roles (which may be organizational, business or IT roles). The tool also assists in performing the mining activity across multiple applications that have been aggregated in it.

The tool provides the capability to perform access re-certification on the application data or the roles created by the mining activity previously. The re-certification can be configured either on the role composition (what makes the role) or role assignment (who is assigned the role). This helps VA's reporting / re-certification related activities by performing these periodic reviews which minimize the risk of having inappropriate access. This process can reduce the complexity of roles existing in the VA environment, by assisting the application teams to better model the roles specific to their environment.

The following diagram provides a detailed view of the role manager tool including interactions with various repositories and the end users.

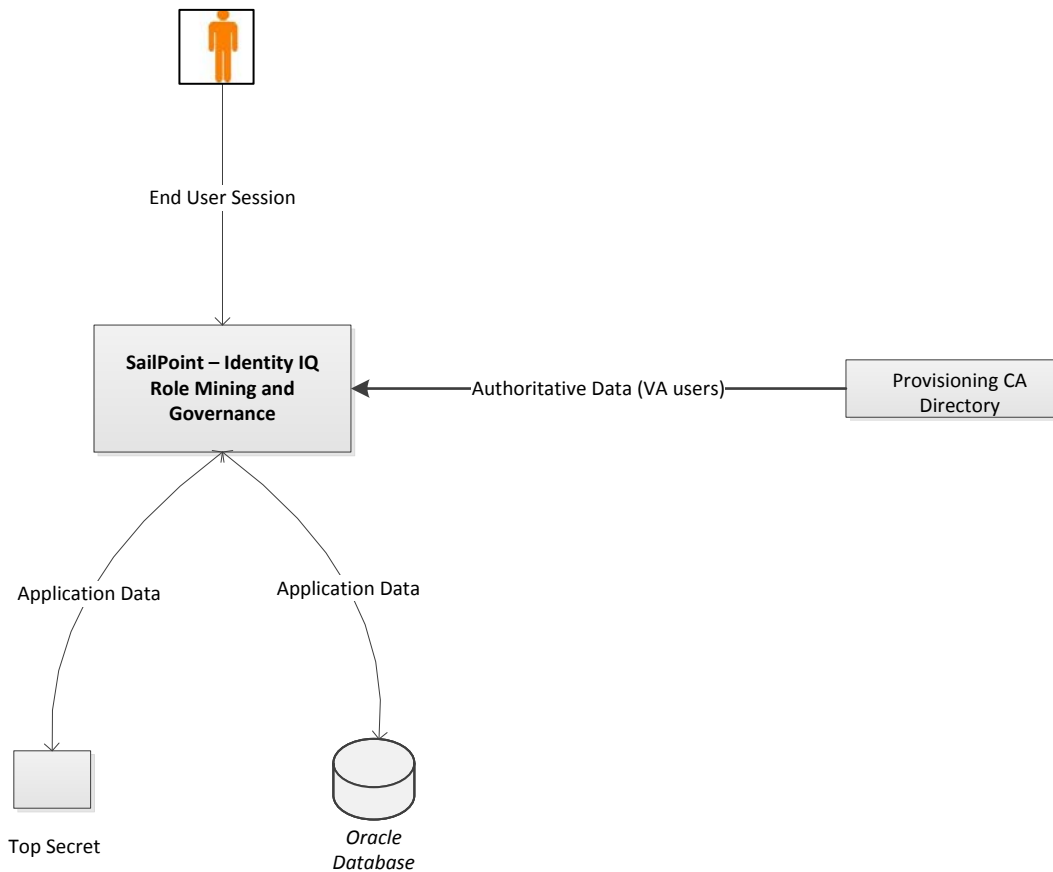


Figure 54: Role Manager Detailed Design

The VA users access the role manager tool to perform re-certification or role mining activities. The tool defines the capability internally upon which the end user's access is defined within the tool's interface.

Role Manager Components:

- Role Manager:** The role component is involved in mining the roles from the aggregated application data which has been reconciled in the system and then configuring them in the tool. The role manager generates the mined results (CSV, Excel) of the application data which are readable by the business users. These results are then analysed to generate well-structured roles.
- Compliance Manager:** This module provides a unified platform for access governance activities. The key area which the tool assists in is the entitlements, roles that have been configured in Role Manager tool can then be certified by the end users (owner, manager etc.), which helps in reducing any inappropriate access by a user. The module further helps in defining SoD (Segregation of Duty) policies surrounding the application data to mitigate risk associated around them.

6.2.2.1 Authoritative Source – VA Repository

| Field | Description |
|----------------|--|
| Use Case Name | Authoritative Source – VA Repository |
| Description | This use case describes the process through which the authoritative source of user population is pulled in Role Manager from the target Provisioning LDAP Repository. |
| Actors | 1. CA LDAP (Authoritative Source Repository) 2. Role Manager 3. Oracle DB (hosting SailPoint database) |
| Pre-Conditions | 1. No firewall exists between the deployed Role Manager application and the authoritative source data repository. |
| Trigger | 1. This activity is a one-time data load activity which will pull the VA user population inside Role Manager. This reconciliation task may be configured to run based on how frequently the data population needs to be refreshed. |
| Actions | <ol style="list-style-type: none">1. The authoritative application is configured in Role Manager to connect to the target CA LDAP source.2. The LDAP source sends out a test connection successful to complete the bind with Role Manager.3. The aggregation task is configured in Role Manager which connects to the target repository.4. Authoritative user information is pulled inside Role Manager and update is made in the Oracle database (hosting the SailPoint application). The following attributes are pulled in for the users:<ul style="list-style-type: none">• cn• givenName• objectClass• departmentNumber• l• manager• mail• sn• title• uid <p>The Role Manager tool returns success to the LDAP application repository on completion of the reconciliation task.</p> |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram participant CA LDAP participant SailPoint participant Oracle DB CA LDAP->>SailPoint: 1. Authoritative App Bind SailPoint-->>CA LDAP: 2. Bind Successful CA LDAP->>SailPoint: 3. Reconciliation Task SailPoint->>Oracle DB: 4. SailPoint Database Updated SailPoint-->>CA LDAP: Return Success Status </pre> |
| Main Success Scenarios | The authoritative user population for VA users is reconciled inside Role Manager. |
| Main Failure Scenarios | The authoritative user repository fails to connect and pull the user population inside Role Manager. |

6.2.2.2 Role Mining – VA Application

| Field | Description |
|----------------|---|
| Use Case Name | Role Mining – VA Application |
| Description | This use case describes the process through which role mining activity is performed on the reconciled data from a VA application source |
| Actors | <ol style="list-style-type: none"> 1. Application Repository 2. Role Manager (Role Mining) 3. Oracle DB (hosting SailPoint database) 4. Business Users |
| Pre-Conditions | 1. No firewall exists between the deployed Role Manager application and the application data repository. |
| Trigger | 1. This reconciliation task may be configured to run based on how frequently the data population needs to be updated to perform the role mining activity. |
| Actions | <ol style="list-style-type: none"> 1. The VA application is configured in Role Manager to connect to the target repository where data has to be aggregated for performing role mining activities. 2. The target repository source sends out a “test connection” successful to complete the bind with Role Manager. 3. The aggregation task is configured in Role Manager which connects to the |

| Field | Description |
|-------|---|
| | <p>target repository for pulling in mining data.</p> <p>4. User information is pulled inside Role Manager and update is made in the Oracle database (hosting the SailPoint application). The following attributes are pulled in for the users:-</p> <ul style="list-style-type: none"> • ACID • ACID SIZE • ACID TYPE • COUNT • CPU • DATE CREATED • DATE LAST MODIFIED • DATE LAST USED • DEPT ACID • DEPT NAME • DIV ACID • DIV NAME • FAC • INSDATA • NAME • NOATS • PASSWORD EXPIRES DATE • PASSWORD INTERVAL • PROFILE ACID • SEGMENT • TSODEST • TSOLACCT • TSOLPROC • TSOLSIZE • TSOMSIZE • TSOOPT • TSOUDDATA • TSOUNIT • ZONE ACID • ZONE NAME • TIME LAST MODIFIED • TIME LAST USED <p>5. The aggregated data is used to perform role mining activities to generate the mining reports which are communicated to the business users.</p> <p>6. The business users can then create the identified roles on the target system and/or in Role Manager.</p> <p>The Role Manager tool returns success to the target CA Directory (LDAP) on</p> |

| Field | Description |
|------------------------|---|
| | successful reconciliation. |
| Sequence Diagram | <pre> sequenceDiagram participant CUPS as Application Repository (CUPS) participant SailPoint participant OracleDB as Oracle DB participant BusinessUsers as Business Users CUPS->>SailPoint: 1. Target App. Bind SailPoint-->>CUPS: 2. Bind Successful CUPS->>SailPoint: 3. Reconciliation Task SailPoint->>OracleDB: 4. SailPoint Database Updated SailPoint-->>CUPS: 5. Mining Activity Completed SailPoint->>BusinessUsers: 6. Business Users receive Role Mining results </pre> |
| Main Success Scenarios | The user data is reconciled inside Role Manager and the role mining results are successfully completed. |
| Main Failure Scenarios | The target repository fails to connect and pull the user information inside Role Manager for the mining activities. |

6.2.2.3 Access Re-certification – Role Composition

| Field | Description |
|----------------|--|
| Use Case Name | Access Re-certification – Role Composition |
| Description | This use case describes the process through which the roles/entitlements data in Role Manager is certified for its composition or assignment (to end users) by the application owner. |
| Actors | <ol style="list-style-type: none"> 1. Business User/Manager 2. Role Manager (Compliance Manager) 3. Oracle DB (hosting SailPoint database) 4. User administration team 5. Role Manager Administrator |
| Pre-Conditions | 1. The user data from the target repository has been reconciled and is up-to-date in the Role Manager database. |
| Trigger | 1. This reconciliation task has been completed and an “Access Review” or a “Role Composition Access Review” has been initiated by the Role Manager administrator. |
| Actions | <ol style="list-style-type: none"> 1. The application repository has successfully reconciled in Role Manager to aggregate the most up-to-date VA user information (from the target source). 2. The mining activity has been completed successfully on the application data with roles created and also assigned to users in Role Manager. 3. In order to certify users access an “Access Review” is triggered in Role |

| Field | Description |
|------------------------|--|
| | <p>Manager which is hosted on the database by the Role Manager administrator.</p> <p>4. In order to certify a role composition a “Role Composition Access Review” is triggered in Role Manager which is hosted on the database by the Role Manager administrator.</p> <p>5. The application owner can access the Role Manager dashboard and complete the access re-certification staged above to either approve/revoke users’ access.</p> <p>6. Any revocation request from the access re-certification is communicated to the user administrator team manually.</p> |
| Sequence Diagram | <pre> sequenceDiagram participant AR as Application Repository participant SP as SailPoint participant OD as Oracle DB participant BU as Business Users participant UAT as User Administration Team AR->>SP: 1. Data Aggregated (Current) SP->>SP: 2. Mining Activity Completed SP->>OD: 3. Manager Access Review Initiated SP->>OD: 4. Role Composition Access Review Initiated BU->>SP: 5. Business Users access Sailpoint SP->>UAT: 6. User Admin Notification </pre> |
| Main Success Scenarios | The access re-certification is completed successfully on the application data (roles or entitlements) |
| Main Failure Scenarios | The access re-certification is incomplete and/or the application data was not reconciled successfully. |

6.2.3 VDS – Attribute Exchange Service Design

The VDS is a supporting component of the AcS solution that provides authoritative user attributes to other AcS components and VA applications. The VDS connects to systems and/or applications and retrieves user attributes and either stores a copy to disk or maintains a memory based cache of the data.

6.2.3.1 Design Constraints

- Provisioning interface to VDS
 - SSL-enabled
 - Simple Authentication (BindDN / password)
 - PII data is transmitted in an encrypted format
 - VDS stores data in the transmission format

- Provisioning is responsible for ensuring VDS and Provisioning remain synchronized
- Provisioning has full read/write/obliterate access
- VAAFI interface to VDS
 - SSL-enabled
 - Protected by DataPower
 - Requires VDS-managed credentials to enforce access controls in VDS
 - VAAFI has read-only access
- VDS interface to MVI
 - SSL-enabled
 - Does not require authentication
 - PII data is transmitted in an encrypted/one-way-hashed format
 - VDS stores data in the transmission format
 - VDS has read-only access
- VDS supports both PKI authentication (Mutual SSL) and Userid/Password

6.2.3.2 Use Case

| Field | Description |
|----------------|---|
| Use Case | Retrieve User by CSPID |
| Actors | 1. VAAFI (consumer) 2. MVI 3. VDS (Attribute Exchange Service(AES)) 4. DataPower |
| Pre-Conditions | 1. VDS has ingested Provisioning Attribute data |
| Sequences | 1. Submits SOAP query with credentials 2. Data Power relays query 3. VDS searches local copy of Provisioning by CSPID 4. VDS queries MVI by SECID 5. VDS returns SOAP results 6. DataPower relays SOAP results |

| Field | Description |
|------------------|---|
| Sequence Diagram | <pre> sequenceDiagram participant Consumer participant DataPower participant AES as Attribute Exchange Service (AES) participant MVI Consumer->>DataPower: 1. Submit Query DataPower->>AES: 2. Submit Query AES->>AES: 3. Local Query AES->>MVI: 4. Query MVI MVI-->>AES: 5. Return Results AES-->>DataPower: 6. Return Results </pre> |
| Success | <ol style="list-style-type: none"> 1. VDS found CSPID (locally) and SecID (MVI) returning one result 2. VDS did not find CSPID (locally) returning zero results |
| Failures | <ol style="list-style-type: none"> 1. VDS found multiple CSPIDs locally 2. VDS found CSPID (locally) and no MVI record returning one result 3. VDS found CSPID (locally) and did not find SecID (MVI) 4. Any non-response/time-out of a remote system |

6.2.3.3 Detailed Design

The detailed design is depicted in the following diagram. The blue box defines the VDS system boundary. The following sections discuss the interfaces and design.

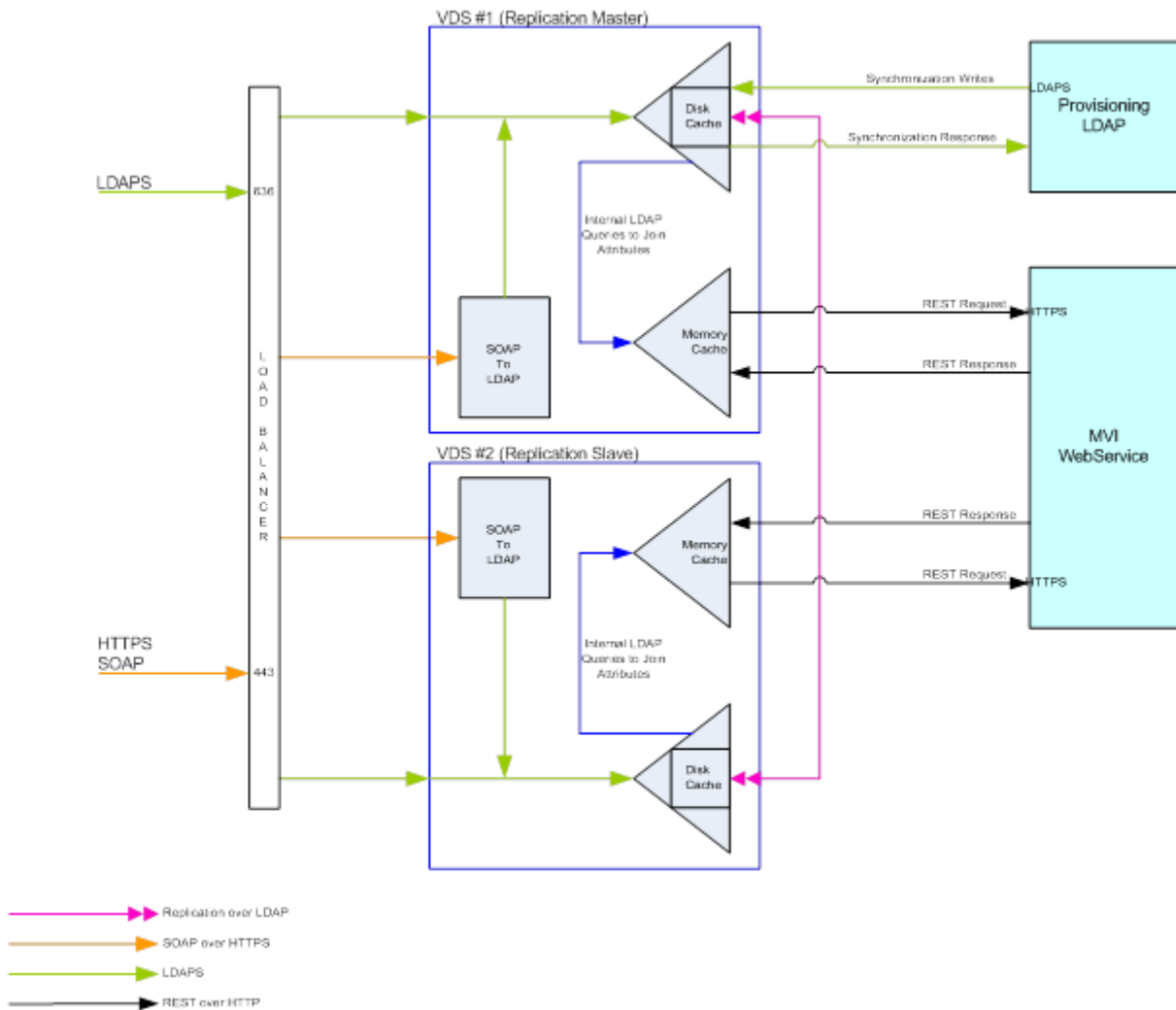


Figure 55: VDS Detailed Design

The solution is comprised of two or more instances of VDS with one configured as a replication master and the balance are configured as replication slaves. Finally, there are two Virtual IP addresses that act as a load-balancer front-end to the VDS instances. The LDAPS protocol (port 636) and the HTTPS/SOAP (port 443) are configured to listen for consumer facing connections. The HTTPS/SOAP load balanced port is configured to listen for requests from the DataPower appliance.

6.2.3.4 Context Diagram

The following context diagram provides VDS with three interfaces. The PROV and MVI interfaces are attribute sources; the SSOe (VAAFI) interface is an attribute consumer.

MVI-VDS Integration
(supporting Target Portal Strategy)

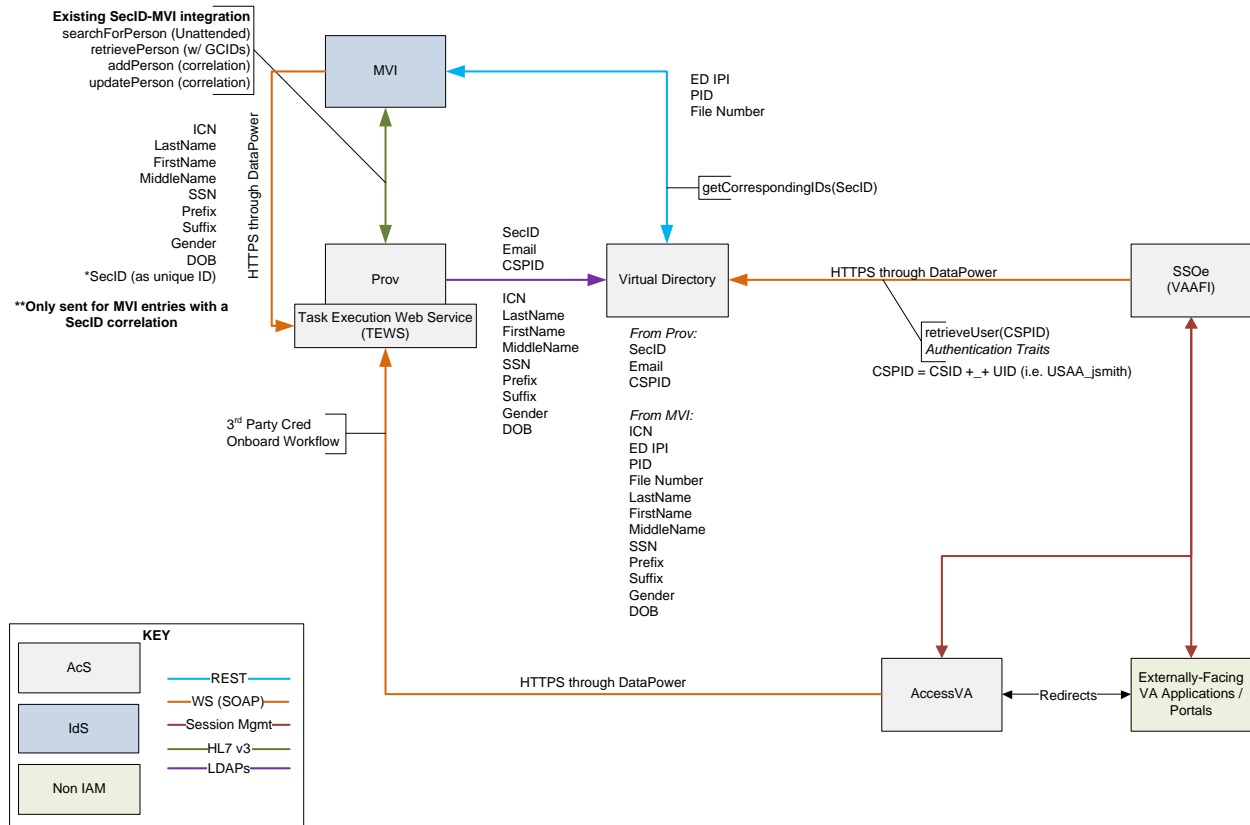


Figure 56: PROV-VDS-MVI Design

6.2.3.5 Provisioning LDAP Interface

The VDS is configured to ingest a set of data from provisioning LDAP data store. The following table identifies the VDS interface and the attributes to be ingested.

Table 31: Composite View Attributes

| Attribute | VDS Interface | Value |
|------------|---------------|--------|
| CSP ID | PROV | Multi |
| ICN | PROV | Single |
| PID | MVI | Multi |
| SEC ID | PROV MVI | Single |
| dodedipnid | MVI | Multi |
| LastName | PROV | Single |

| Attribute | VDS Interface | Value |
|-----------------------------------|---------------|--------|
| FirstName | PROV | Single |
| MiddleName | PROV | Single |
| SSN | PROV | Single |
| Prefix | PROV | Single |
| Suffix | PROV | Single |
| Gender (Format Male/Female) | PROV | Single |
| DOB (MM/DD/YYYY format) | PROV | Single |
| Email | PROV | Single |
| File Number (BIRLS) | MVI | Multi |
| Date of Death (MM/DD/YYYY format) | PROV | Single |
| Identity Theft | PROV | Single |

The ingested attributes are protected by Access Control Instructions (ACIs) that grants authorized consumers read only access. PII data will be encrypted/one-way-hashed by the VDS data provider and VDS will store the data in its encrypted/hashed. This will prohibit VDS consumers from querying the PII data by their clear text values. Non-PII data will be indexed and queryable by authorized VDS consumers.

The Provisioning LDAP data is initially ingested via a snap shot and loaded into VDS. The Provisioning application then utilizes its internal workflow and makes appropriate changes to VDS to ensure VDS remains accurately synchronized. Refer to the Provisioning design for details regarding the synchronization management.

6.2.3.6 MVI Webservice Interface

The VDS-MVI Webservice is an AcS developed extension to the VDS application. The VDS application defines a developer modifiable Java interface that can be extended to interface non-LDAP interfaces to the VDS LDAP engine. The basic interface is defined below.

```
package com.rli.scripts.intercept;

public class CLASSNAME implements UserDefinedInterception2 {

    public void select(InterceptParam prop) {...}

    public static SearchResult processresult(InterceptParam prop, SearchResult anEntry) {...}

    public void authenticate(InterceptParam prop) {...}

    public void insert(InterceptParam prop) {...}

    public void update(InterceptParam prop) {...}

    public void delete(InterceptParam prop) {...}
```

```
public void compare(InterceptParam prop) {...}
}
```

In the MVI interface, the select (Search) and SearchResult methods will be implemented to facilitate searching MVI and processing the search results. The balance of the methods will be coded to return errors if they are ever called.

The Search method will take the InterceptParam object which contains a number of basic LDAP session parameters such as timelimits, sizelimits, search depth, and a search filter. The interception script will get the search filter; construct a HTTPS REST call to the MVI Webservice end point. Next the interception script parses the HTTPS REST response and constructs a LDAP search result consisting of multiple LDAP Attributes that will be returned in the InterceptParam object to the LDAP engine.

The MVI Webservice interface will be configured with an ACI that prevents any consumer from making direct calls to the interface. PII data will be encrypted/one-way-hashed by the VDS data provider and VDS will cache the data in transmission format. All queries will be the result of a Webservice or LDAP query of the provisioning LDAP cache. ACIs will be put in place to grant authorized users read only access and denying all others.

MVI Webservice properties will be stored in a VDS connection profile.

| Method /Function | Description of Method/Function | Input | Output |
|------------------|---|--------------------------------------|--|
| SearchRequest | Searches the VDS via the LDAP interface | REST Representation of a LDAP filter | REST Representation of a LDAP SearchResponse. SearchResults can be Zero results (not found), a non-zero error code, or a set of attributes the consumers is authorized by access control instructions to access. |
| ModifyRequest | Not used | Not used | Not used |
| AddRequest | Not used | Not used | Not used |
| DelRequest | Not used | Not used | Not used |
| ModifyDNRequest | Not used | Not used | Not used |
| CompareRequest | Not used | Not used | Not used |
| AbandonRequest | Not used | Not used | Not used |
| ExtendedRequest | Not used | Not used | Not used |

The COTS VDS WSDL is provided below for reference. This WSDL effectively implements the LDAP protocol via REST services.



A sample SOAP request/response for calling attribute exchange service of VDS is provided below for reference:



Request_Response
payload.docx

6.2.3.7 Solution Operations

Example: Consumer queries VDS Webservice with a filter “(cspid=USAA_BJohnson)”.

1. VDS Webservice authenticates the consumer and translates the SOAP request into a valid LDAP query.
2. VDS Webservice passes the consumers identity with the query to the LDAP engine for processing.
3. Query of the internal cache of the provisioning attribute data with the filter “(cspid=USAA_BJohnson).”
4. A record is found with a SECID attribute with a value of 0001.
5. The VDS LDAP engine make a query to the internal LDAP interface that represents the MVI Webservice with a filter of “(secid=0001).”
6. The InterceptParam object is passed via the Select method of the Java interface, and the VDS code calls the MVI Webservice and processes the results, creating LDAP attributes for each key/value returned from MVI.
7. The LDAP engine merges the LDAP data from the MVI call with the LDAP data returned from the provisioning LDAP data and returns the data to the VDS Webservice.
8. The VDS Webservice translates the LDAP response into a valid SOAP response and returns to the consumer.

6.2.4 SSOi Design

The existence of multiple applications accessed by the VA user community creates a problem where users have to remember multiple passwords for multiple applications. Each application is using disparate logon capabilities that commensurate with the risk-level associated with the specific application security requirements. The SSOi activity addresses these identified issues of multiple passwords, re-authentication and security challenges by providing seamless authentication from application to application without prompting user's for their credentials again. To simplify users' experience, the SSOi activity will provide a common entry point for SSOi enabled applications. The authentication events for users will be logged and audited as required to produce necessary reports.

A detailed view of the SSOi activity is depicted in the following diagram.

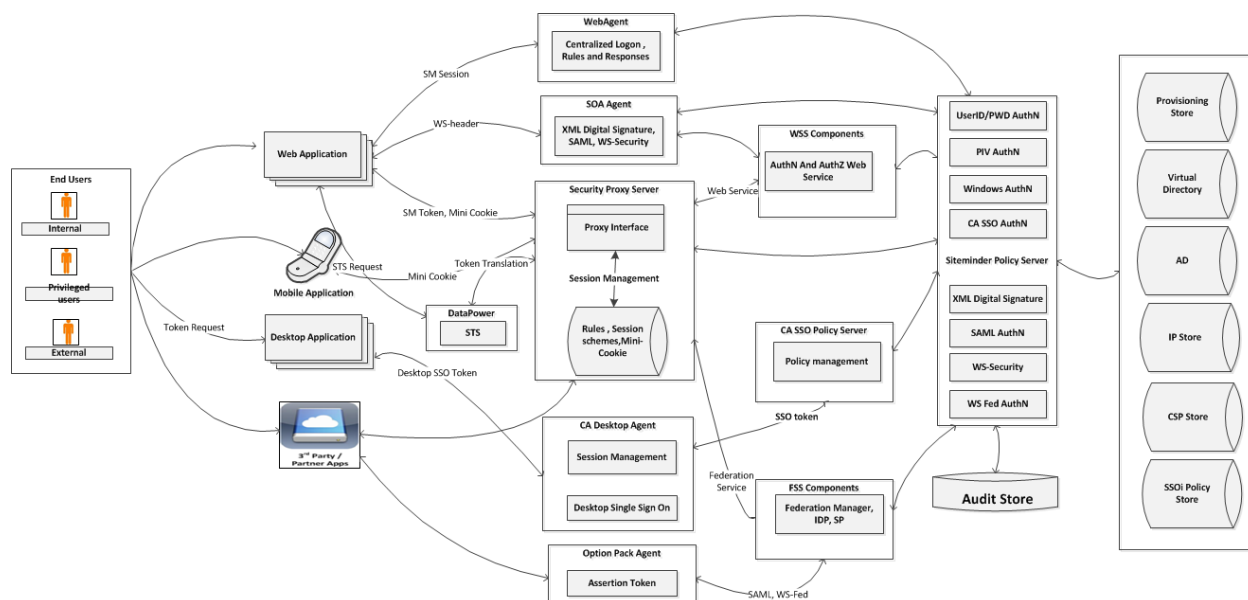


Figure 57: SSOi Detailed Design

SSOi leverages the capabilities of the CA SiteMinder and SSO COTS suite to minimize software development. The basic components of SSOi are comprised of enforcement agents, service endpoints, centralized policy engine, proxy services, and data tier to support various application types.

Enforcement Agents:

The enforcement agent enforces policies and protects the end applications.

- **Web Agent:** A Web agent protects web and application containers. Agents are installed on application web servers to intercept authentication requests to determine authorization permissions defined by the access policies.
- **SOA Agent:** This Agent protects the web service endpoints and enforces necessary policies to secure access. SOA Agents provide the capability to read SOAP/REST messages and add / update security headers with a user's SSO session.
- **Secure Proxy Server (SPS):** The SPS provides proxy services for application authentication and authorizations. SPS enables mobile applications in a similar way it does for web applications by issuing mini cookies. These cookies are compliant with native mobile applications and browsers. A web application can also call the SSOi Authentication and Authorization web service interface to authenticate and validate the SSOi sessions via SOAP and REST messages.
- **Desktop Agent:** Desktop agent provides SSO functionality to desktops / thick clients and provides user access by validating their internal desktop session. The desktop agent is also used to support web application SSO capability (protected by web agents) by redirecting the request to the web application.
- **Option Pack Agent:** This agent specifically enforces policies for federation application. It has the ability to generate and consume SAML assertion as well as WS Trust. The option pack agent communicates with the Federation Security Service (FSS) to manage federation partners.

Service Endpoints:

- **Web Service Security (WSS):** SSOi supports WS-Security tokens through WSS for various web service methods such as SOAP and REST. WSS also provides authentication and authorization web services to validate XML requests from client and generate sessions through XML response.
- **Federation Security Service (FSS):** FSS supports legacy through option pack agent and partnership federation through federation manager. It supports various federation standards such as SAML and WS-Federation. This provides the Identity Provider (IdP) and Service Provider (SP) objects for application integration.
- **Security Token Store Service (STS):** DataPower acts as the STS store that supports token translation requests from application end, where it supports WS-Trust token as input request having user's Siteminder session as part of request. STS store validates Token request and will returns the standard user attributes as a part of response specification

Centralized Policy Engine:

The SSOi policy engine is made up of CA SiteMinder and SSO policy server. All policy configuration, administration, and evaluation are managed through a centralized policy engine. The policy engine receives the requests from the different enforcement agents and service components. It then evaluates and takes action on the requests by providing an appropriate response back to the integrated application. The centralized policy engine provides various ways to authenticate a user such as: user ID/password, Microsoft Windows authentication using Kerberos and NTLM token, PIV and PKI authentication, conversion of desktop token to a Web token, XML digital signature, SAML, and WS-Federation. SSOi validates credentials against the back end user store and provides the SSO token as well as the user attributes to enforcement point for response back to the application.

Data Tier:

The data tier consists of user stores and a policy store. The policy server uses directory plugins to connect to each user directory for authentication and authorization. Currently SSOi supports Active Directory (AD), Provisioning Store, CSP, IP, and VDS as a user authentication and authorization store. The policy store contains all the policies used to enforce the authentication and authorization requests.

The sections below provide detailed technical flows for the SSOi activity and the associated interactions amongst the system components. The functionality and features provided below focus solely on the requirements directly related to the SSOi activity.

The SSOi STS architecture is depicted in the following diagram.

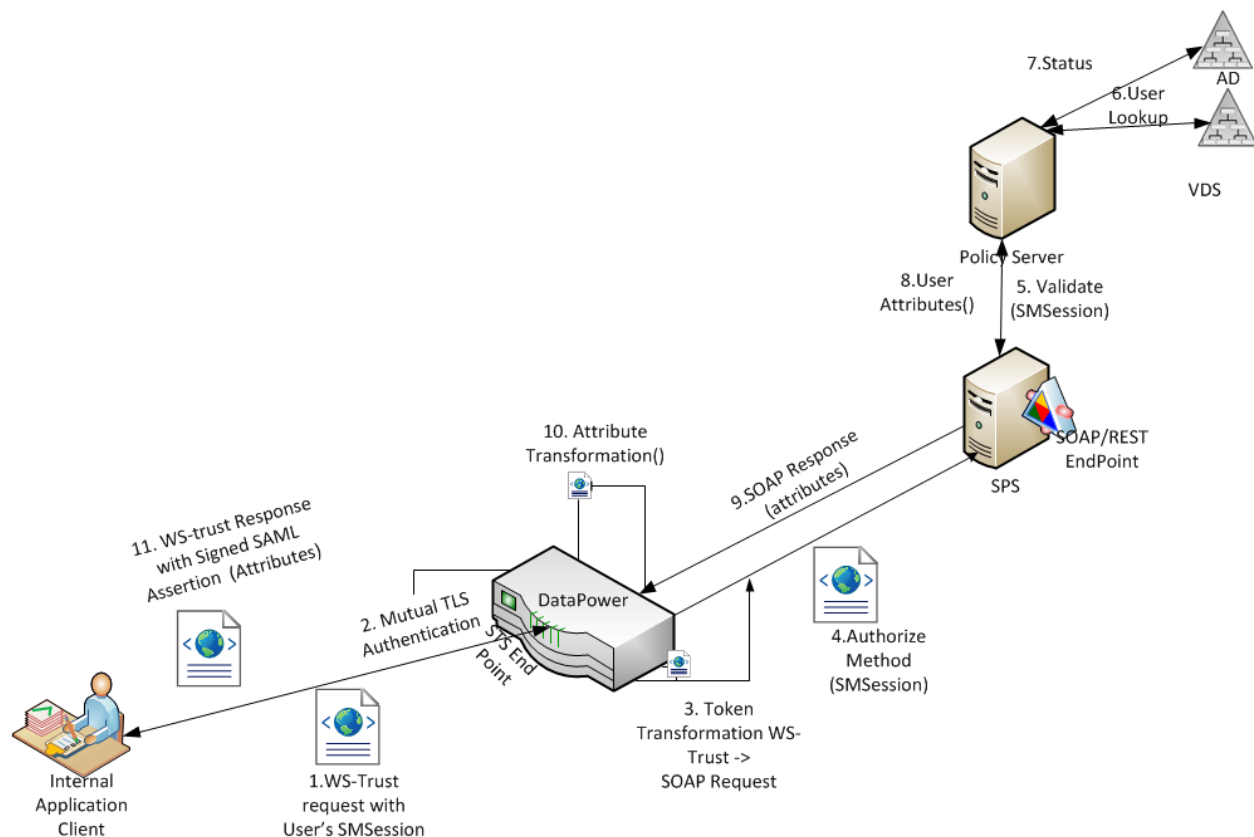


Figure 58: SSOi STS Architecture Diagram

The details of the SSOi STS architecture flow is described in section 6.2.4.9.

6.2.4.1 SSOi Support for LOA 2/3 Internal Users

| Field | Description |
|----------------|---|
| Use Case Name | Authentication Support for Level of Assurance (LOA 2/3) |
| Description | This use case describes the process through which a user authenticates to the SSOi service using approved LOA 2/3 |
| Actors | 1. Internal Users 2. SSOi 3. Centralized Logon Page 4. SSOi Integrated Application(s) 5. User Directory |
| Pre-Conditions | User has valid credential for each type of authentication method and tries to access the protected application. Invalid credentials are supported through error flows. |
| Trigger | The internal user tries to access the application protected by SSOi. |
| Actions | Centralized Log On Page with Windows Authentication 1. SSOi Web Agent Intercepts the request to access integrated application and |

| Field | Description |
|-------|--|
| | <p>verifies it with policy server</p> <ol style="list-style-type: none"> 2. Web Agent redirects the request to centralized log on page with Windows authentication. 3. The IIS Windows Authentication Logon Server 4. The logon server collects the Kerberos credentials. 5. SSOi authenticates the user against the Active Directory. 6. The Logon Server passes the control to SiteMinder Policy server to authorize the user 7. If the user is authorized to access the resource then a token is generated by SSOi (SiteMinder Policy Server) 8. SSOi creates SiteMinder Token and then Notifies Windows Authentication Logon Server 9. The Logon server redirects the user to application 10. The Application is presented to the user. <p>Centralized Log On Page with Userid/Password Authentication</p> <ol style="list-style-type: none"> 1. SSOi Web Agent Intercepts the user request to access integrated application 2. The Web Agent verifies it with policy server if the application is protected 3. If the resource is protected Web Agent redirects to Logon server 4. Logon Server prompts for credentials 5. The user enters the credentials 6. The Logon Server passes the control to SiteMinder Policy server to authorize the user 7. SiteMinder Policy Server authenticates and authorizes user against Active Directory 8. SiteMinder Policy Server create SiteMinder Token 9. User is authenticated and authorized to access the resource by SiteMinder Policy Server 10. The Logon server redirects the user to application <p>Centralized Log On Page with PIV Authentication</p> <ol style="list-style-type: none"> 1. SSOi Web Agent Intercepts the user request to access integrated application 2. The Web Agent verifies it with Policy Server if the application is protected 3. If the resource is protected Web Agent redirects to centralized log on page where a user can select PIV Logon from the list of supported authentication methods. 4. PIV Logon prompts to select Client certificate 5. The user selects the client certificate and enters the PIN 6. The SSL server maps the user's certificate to the server. 7. CA SiteMinder verifies the user exists. 8. CA SiteMinder verifies the user's basic credentials. 9. CA SiteMinder verifies that the certificate credentials and the basic credentials represent the same user. |

| Field | Description |
|------------------|--|
| | <p>10. If the user look up failed on AD by SiteMinder then it generates user OnAuthattempt rule which redirects the user back to failed logon page or else it authorizes the access to the resource and redirects the user back to application with valid Siteminder session cookie.</p> <p>Centralize Page With PIV-Only Authentication (LOA3)</p> <ol style="list-style-type: none"> 1. SSOi Web Agent Intercepts the user request to access integrated application 2. The Web Agent verifies it with Policy Server if the application is protected by higher level 10 authentication. 3. If the resource is protected Web Agent redirects to centralized PIV log on page where a user can hit login button to login using PIV card. 4. Central login server sends the requests to PIV logon server. 5. PIV Logon prompts to select Client certificate 6. The user selects the client certificate and enters the PIN 7. The SSL server maps the user's certificate to the server 8. PIV certificate authentication happens at the TLS layer, higher authentication level (10) configured on policy server 9. CA SiteMinder verifies the user exists. 10. CA SiteMinder verifies the user's basic credentials. 11. CA SiteMinder verifies that the certificate credentials and the basic credentials represent the same user. 12. If the user is authorized to access the resource, the PIV Logon server redirects the user to application |
| Sequence Diagram | <pre> sequenceDiagram participant User participant Application participant LogOnServer as Log On Server For Windows Authentication(IIS) participant AD participant PolicyServer as Policy Server participant UserDirectory as User Directory User->>Application: 1. User Access Application Application->>LogOnServer: 2. Redirect to Windows Authentication Logon Server LogOnServer->>User: 3. Gather NTLM V2 Credentials from User Desktop LogOnServer->>AD: 3. Authenticate User Against AD AD->>LogOnServer: 5. Authorize user LogOnServer->>PolicyServer: 6. Authorize user against AD PolicyServer->>UserDirectory: 7. Create SM Token UserDirectory-->>PolicyServer: PolicyServer->>LogOnServer: 8. User Authenticated and Authorized LogOnServer->>Application: 9. Redirect to TARGET Application Application->>User: 10. Application Presented to User </pre> |

| Field | Description |
|------------------------|---|
| | <div data-bbox="407 243 1464 722"> <p>Centralized Log on page with UserID/password authentication</p> <pre> sequenceDiagram participant User participant Application participant Log On Server participant Policy Server participant User Directory User->>Application: 1. User Access Application Application->>Log On Server: 2. Verifies the resource is protected Application->>Log On Server: 3. Redirect to Logon Server Log On Server->>User: 4. Prompt for Credentials User->>Log On Server: 5. User enters credentials Log On Server->>Policy Server: 6. Validate user Policy Server->>User Directory: 6.a Authenticate and Authorize user against user directory User Directory-->>Policy Server: 6.b Create SM Token Policy Server->>Log On Server: 7. User Authenticated and Authorized Log On Server->>Application: 8. Redirect to TARGET Application Application->>User: Application Presented to User </pre> </div> <div data-bbox="407 758 1464 1461"> <p>Centralized Log on page with PIV authentication</p> <pre> sequenceDiagram participant User participant Application participant PIV Log On Server participant Policy Server participant User Directory User->>Application: 1. User Access Application Application->>PIV Log On Server: 2. Verifies the resource is protected Application->>PIV Log On Server: 3. Redirect to PIV Logon Server PIV Log On Server->>User: 4. Prompt for Client Certificate User->>PIV Log On Server: 5. User Selects certificate and enter PIN PIV Log On Server->>User: 6. Validate PIN PIV Log On Server->>Policy Server: 7. Authenticated response with client certificate Policy Server->>PIV Log On Server: 8. Authorize User call with client certificate Policy Server->>User Directory: 9. Validate certificate Issuer against certmap User Directory-->>Policy Server: 10.a Collect user principal name from client certificate Policy Server->>User Directory: 10.b Authorize user against user directory User Directory-->>Policy Server: 10.c User Authorized Policy Server->>PIV Log On Server: 11. Redirect to TARGET Application PIV Log On Server->>Application: Application Presented to User </pre> </div> |
| Main Success Scenarios | User is authenticated successfully and application is presented to the user. |
| Main Failure Scenarios | <p>No failed authorization may occur but system had been designed to handle to scenario if at all it may</p> <ul style="list-style-type: none"> Default failed Kerberos authentication will redirect the user to the centralized log Username/Password page but can be customized to redirect to any application page based on the policies. Default failed Kerberos authorization will redirect the user to centralized login page but can be customized to redirect to any application page based on the policies. Default failed UserId/Password authentication will redirect the user to the |

| Field | Description |
|-------|---|
| | <p>centralized log Username/Password page but can be customized to redirect to any application page based on the policies.</p> <ul style="list-style-type: none"> • Default failed UserID/Password authorization will redirect the user to centralized login page but can be customized to redirect to any application page based on the policies. • Default failed PIV authentication will redirect the user to the centralized log Username/Password page but can be customized to redirect to any application page based on the policies. • Default failed PIV authorization will redirect the user to centralized login page but can be customized to redirect to any application page based on the policies. • Default Session Timeout redirects the users back to the centralize logon page • Default Authorization Failure to the application will redirect the user to the centralize failedlogin page • Default Application Logout Page will redirect the user back to the centralize logon page |

6.2.4.2 SSOi Support for LOA 2/3 External Users

| Field | Description |
|----------------|--|
| Use Case Name | LOA 2/3-SSOi Integration Flow |
| Description | This use case describes the process by which an SSOi User performs SSO to one or more integrated application. |
| Actors | <ol style="list-style-type: none"> 1. External User 2. VAAFI 3. SSOi Integrated Application(s) 4. User Directory |
| Pre-Conditions | <ol style="list-style-type: none"> 1. The SECID which will be received from VAAFI and will be available as correlated attribute in Provisioning store 2. A valid external card user access the SSOi protected application through Access VA |
| Trigger | External User initiates the application session by clicking on the target application from Access VA |
| Actions | <ol style="list-style-type: none"> 1. An external user accesses an application which is SSOi service provider via public URL. 2. The user will be redirected to IdP (VAAFI) for credentials 3. The IdP will authenticate the external user and generate the SAML assertion with user attributes as defined in integration RSD/SDD. 4. VAAFI SAML service posts the generate SAML Assertion to the SSOI SAML Assertion Consumer URL. SPS will proxy the internal URL access for external users. |

| Field | Description |
|------------------------|--|
| | <ol style="list-style-type: none"> SSOI SAML Consumer server makes a call to the SiteMinder Policy server to validate SAML assertion. SM Policy server validates SAML assertion against SAML auth scheme and by verifying the digital signature. It consumes the assertion and after that decrypts the SAML Assertion. SM Policy server validates the user retrieved from SAML assertion against Provisioning User directory by validating SECID If the SECID is valid, Policy server creates the SM token and redirect to the target application with the required header variables such as Firstname, csid, icn, Lastname, EDIPI, email address, assurance level, and other attributes received as a part of assertion mentioned in the following table If the user is valid, Policy server creates the SM token and redirect to the target application with required header variables based on the policy configured for the integrated application and SPID |
| Sequence Diagram | <pre> sequenceDiagram participant User participant VAAFI participant Application participant SPS as SPS With Option Pack participant PolicyServer as Policy Server participant ProvisioningDir as Provisioning User Directory User->>VAAFI: 1. External User Access Application VAAFI->>Application: 2. Redirect to VAAFI For credentials Application->>VAAFI: 3. Validate User Credentials VAAFI->>Application: 4. Create SAML Assertion With Attributes Application->>VAAFI: 5. Post SAML Assertion to SSOI VAAFI->>PolicyServer: 6. Validate SAML Assertion PolicyServer->>PolicyServer: 7. Validate Assertion Against SAML Auth Scheme PolicyServer->>PolicyServer: 8. Consume SAML Assertion PolicyServer->>ProvisioningDir: 9. Validate SECID ProvisioningDir->>PolicyServer: 10. Create SM Token PolicyServer->>Application: 11. Generate Response headers Application->>User: 12. Redirect to TARGET Application with header information </pre> |
| Main Success Scenarios | User is authenticated and Application is presented to the user. |
| Main Failure Scenarios | <p>In the event of an exception or error during attribute consumption default SAML assertion error will be generated and returned it to VAAFI</p> <p>The failure scenarios like Session timeout, authentication and authorization failures will covered similar to Centralized Logon page for each integration using SPS,</p> |

VAAFI IdP SAML Integration:

| | |
|-----------------------------|-----------|
| IDPID: | |
| Siteminder Affiliate Domain | N/A |
| NameID | SubjectDN |
| AuthN Director | NA |

| | |
|----------------------|------------|
| Encryption Algorithm | [REDACTED] |
| SLO | NA |
| Attribute Details | [REDACTED] |
| Signature Algorithm | [REDACTED] |

6.2.4.3 SSOi Mobility Support

| Field | Description |
|----------------|--|
| Use Case Name | SSOi Mobility Support |
| Description | This use case describes the process by which SSOi user performs authentication through mobile devices. Mini and SM Session cookies are supported. |
| Actors | <ol style="list-style-type: none"> 1. Mobile User 2. SSOi Integrated Application(s) 3. User Directory |
| Pre-Conditions | The user has a mobile device with access to VA applications. |
| Trigger | Mobile User initiates authentication to application via a mobile device. |
| Actions | <p>Http Session Cookie Is Valid</p> <ol style="list-style-type: none"> 1. Mobile User accesses the application URL through a mobile device 2. CA Secure Proxy Server (SPS) intercepts the requests and check for the mini cookie availability 3. If http Session cookie is valid then SPS will validate and update the session cookie with updated time stamp and pass the control back to the application 4. After user entering the credentials, SPS validates the user by making a call to the Policy Server 5. Policy Server validates the credentials by verifying it against user directory 6. SiteMinder Policy Server validates the user 7. SiteMinder Policy Server redirects to Mobile application 8. Browser presents application to the Mobile user <p>Http Session Cookie Does Not Exist Or Is Not Valid</p> <ol style="list-style-type: none"> 1. If http Session Cookie is not valid or does not exist it will redirect to the login server 2. Prompt for the Centralized Mobile authentication Page with UserID/Password option and PIV/PIN option (both authentication mechanisms follow the same process that is described in section 6.2.4.2) |

| Field | Description |
|------------------|--|
| | <ol style="list-style-type: none"> 3. User enters credentials based on the option selected 4. Policy Server validates the credentials 5. Verify the credentials against user directory 6. Receive valid user response 7. After user validation completed, redirect to the application 8. SPS creates and sets the http Session cookie 9. Pass the control to the application. 10. Present application to the Mobile User <p>Access to Mobile Application Using Native Apps</p> <ol style="list-style-type: none"> 1. A native app calls the authentication SOAP/REST based web service exposed by Secure Proxy server Authentication web service with respective input parameters such as username, password and resource Uri. (Note - Currently SPS Webservice Solution does not support X509 tags due to limitation of the product) 2. Authentication Web service validates the credentials 3. Validate against policy server/user store. 4. Receive validated user notification 5. If successful then mini session cookie is returned as part of response code 6. Application call Authorization service to get permit /deny response from Authorization web service else fail result code is returned as response |
| Sequence Diagram | |

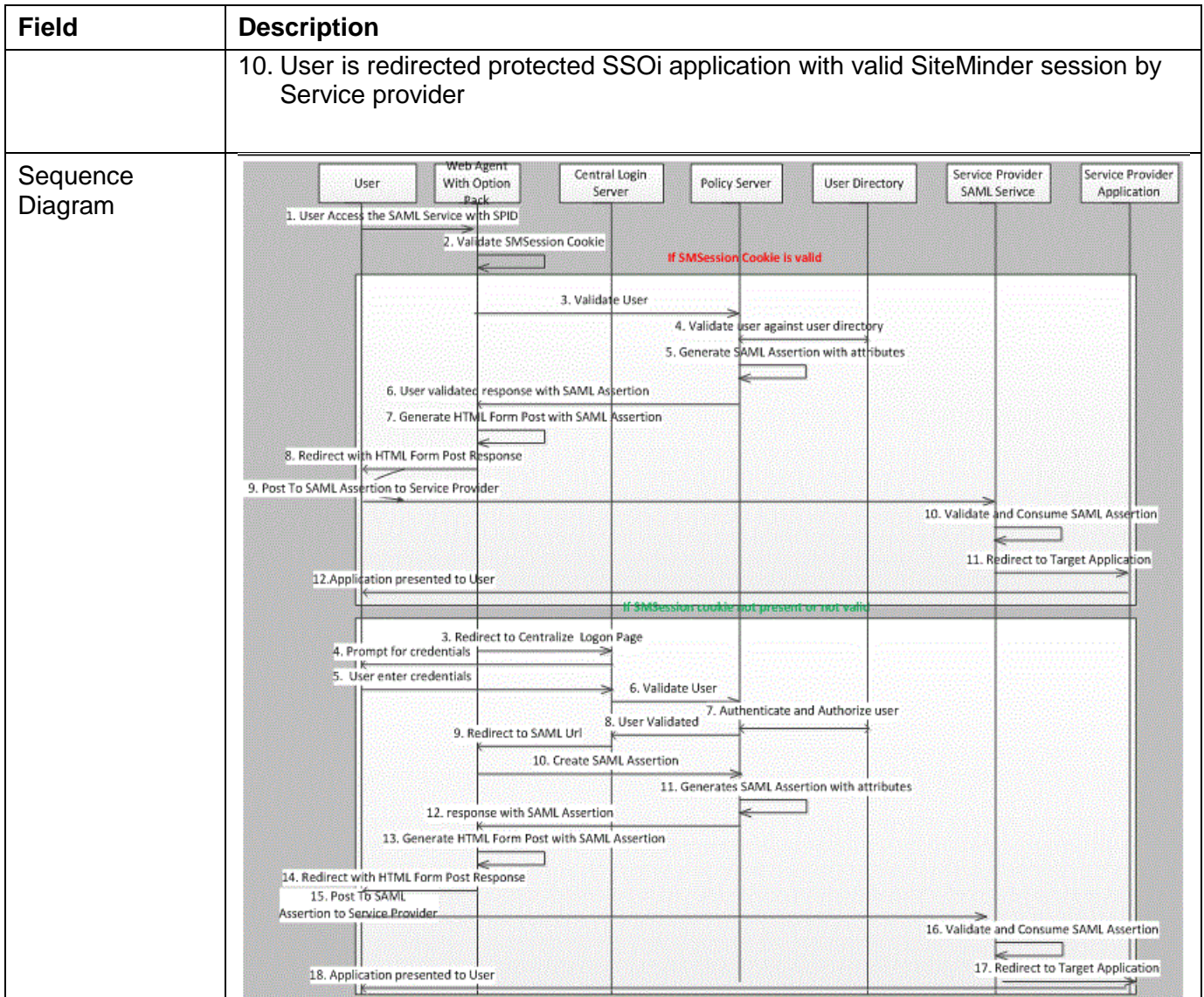
| Field | Description |
|------------------------|---|
| | <pre> sequenceDiagram participant MU as Mobile User participant SPS participant App as Application participant LOS as Log On Server participant PS as Policy Server participant UD as User Directory MU->>SPS: 1. User Access Mobile Application SPS->>SPS: 2. Validate Mini Cookie SPS->>App: 3. Validate User SPS->>UD: 4. Validate user against user directory UD-->>PS: 5. User Validated PS->>App: 6. Redirected to Mobile application App->>MU: 7. Application presented to Mobile User SPS->>LOS: 3. Redirect to Login Server LOS->>MU: 4. Prompt for credentials MU->>LOS: 5. Mobile User enter credentials LOS->>PS: 6. Validate User PS->>UD: 7. Authenticate and Authorize User UD-->>PS: 8. User Validated PS->>App: 9. Redirect to Application App->>SPS: 10. Set Http Session Cookie SPS->>App: 11. Present Mobile App App->>MU: 12. Application presented to Mobile User </pre> <p>Access Mobile Application using Native Apps</p> <pre> sequenceDiagram participant MU as Mobile User Native App participant SPS participant PS as Policy Server participant UD as User Directory MU->>SPS: 1. Authenticate User SOAP/REST Call with username, password and resource name) SPS->>PS: 2. Validate User SPS->>UD: 2.a Validate user against user directory UD-->>PS: 2.b User Validated PS->>MU: 3. Response with success/failure, and If success Mini cookie is returned MU->>SPS: 4. Authorize user </pre> |
| Main Success Scenarios | User is authenticated successfully and application is presented to the user |
| Main Failure Scenarios | <ul style="list-style-type: none"> Default failed UserId/Password authentication will redirect the user to the centralized log Username/Password page but can be customized to redirect to |

| Field | Description |
|-------|---|
| | <p>any application page based on the policies.</p> <ul style="list-style-type: none"> • Default failed UserID/Password authorization will redirect the user to centralized login page but can be customized to redirect to any application page based on the policies. • Default Session Timeout redirects the users back to the centralize Mobile logon page • Default Authorization Failure to the application will redirect the user to the centralize Mobile failedlogin page • Default Application Logout Page will redirect the user back to the centralize Mobile logon page • For Native apps, since it utilizes the SSOi web service, the error codes are mentioned in the table 6.2.2.11 |

6.2.4.4 Federation Identity Provider (IdP) and Service Provider (SP) for Internal Users

| Field | Description |
|----------------|--|
| Use Case Name | Federation Identity Provider (IdP) and Service Provider (SP) Services |
| Description | This use case describes the process by which a federated user is authenticated to the SSOi activity. |
| Actors | <ol style="list-style-type: none"> 1. Internal Users 2. SSOi 3. SSOi Integrated Applications |
| Pre-Conditions | A valid integration/trust between Identity Provider (IdP) and Service Provider (SP) |
| Trigger | User Access application protected with SAML federation authentication mechanism |
| Actions | <p>Identity Provider (IdP) – Without a Valid Session Cookie</p> <ol style="list-style-type: none"> 1. An internal user accesses an application (IdP-protected URL) which is at service provider without a SiteMinder session cookie. 2. Web server redirects user to centralize log on page and prompted for authentication credential 3. User enters the credentials 4. SiteMinder Policy server validates against User store. 5. SiteMinder Policy server authenticates and authorizes the user 6. SiteMinder Policy Server creates valid user token 7. SiteMinder Policy server redirects to SAML URL 8. SiteMinder Policy server generates the SAML Assertion by: 9. SiteMinder Policy Server adds the required attributes such as user Principal Name (UPN), email, firstname and lastname 10. IdP posts the SAML assertion to the Service Provider SAML Assertion |

| Field | Description |
|-------|---|
| | <p>Consumer service:</p> <ol style="list-style-type: none"> 11. SiteMinder Policy Server (IdP) generates HTML Form Post with SAML assertion 12. SiteMinder Policy Server (IdP) redirects with HTML form post response 13. SiteMinder Policy Server (IdP) posts SAML assertion to Service Provider 14. Service provide Consumes the SAML assertion generated by SSOi and grants the access to the user 15. Service provider redirect to protected SSOi application with valid SiteMinder session 16. Service provider present application to the end user <p>Identity Provider (IdP) – With a Valid Session Cookie</p> <ol style="list-style-type: none"> 1. An internal user accesses an application (IdP protected URL) which is at service provider with a SiteMinder Session cookie. 2. The user is validated by SiteMinder Policy Server. 3. SiteMinder Policy Server generates the SAML assertion by adding all the required attributes such as user Principal Name (UPN), email, firstname and lastname 4. IdP posts the SAML assertion to the Service Provider SAML Assertion <p>Consumer service:</p> <ol style="list-style-type: none"> 5. IdP generates HTML form post with SAML Assertion 6. IdP redirects with HTML Form Post Response 7. IdP posts to SAML Assertion to Service Provider 8. Service provider consumes the SAML assertion generated by SSOi and grants the access to the user 9. Service provider redirects to protected SSOi application with valid SiteMinder session 10. Service provider presents application to the end user <p>Service Provider (SP)</p> <ol style="list-style-type: none"> 1. An internal user accesses an application which is protected by a separate IdP other than SSOi. 2. User enters the credentials and validated with IdP 3. The SAML assertion is generated by adding the required attributes such as user Principal Name (UPN), email, firstname, and lastname by IdP 4. IdP posts the SAML assertion to the Service Provider which is configured at SiteMinder 5. SPS / Webagent option pack validates the SAML Assertion with the Policy Server 6. Service provider consumes the SAML assertion generated by IdP 7. Service provider validates the user attributes. 8. Service provider creates SiteMinder Token 9. SAML Assertion is consumed by Service provider |



| Field | Description |
|------------------------|--|
| | <p>an application which is protected by a separate IDP other than SSOi</p> <pre> sequenceDiagram participant User participant IDP as IDP SAML Service participant Application participant SPS as SPS With Option Pack participant Policy as Policy Server participant UserDir as User Directory User->>IDP: 1. User Authenticates to IDP IDP->>Application: 2. Request to Access Application IDP->>IDP: 3. Create SAML Assertion With Attributes IDP->>SPS: 4. Post SAML Assertion to SSOI SPS->>Policy: 5. Validate SAML Assertion Policy->>Policy: 6.a Validate Assertion Against SAML Auth Scheme Policy->>Policy: 6.b Consume SAML Assertion Policy->>UserDir: 6.c Validate User Policy->>Policy: 6.d Create SM Token Policy->>SPS: 7. Assertion Validated and consumed SPS->>Application: 8. Redirect to TARGET Application Application->>User: Application Presented to User </pre> |
| Main Success Scenarios | User is authenticated and Application is presented to the user. |
| Main Failure Scenarios | <p>VA as IdP:</p> <ul style="list-style-type: none"> • Default failed Kerberos authentication will redirect the user to the centralized log Username/Password page but can be customized to redirect to any application page based on the policies. • Default failed Kerberos authorization will redirect the user to centralized login page but can be customized to redirect to any application page based on the policies. • Default failed UserID/Password authentication will redirect the user to the centralized log Username/Password page but can be customized to redirect to any application page based on the policies. • Default failed UserID/Password authorization will redirect the user to centralized login page but can be customized to redirect to any application page based on the policies. • Default failed PIV authentication will redirect the user to the centralized log Username/Password page but can be customized to redirect to any application page based on the policies. • Default failed PIV authorization will redirect the user to centralized login page but can be customized to redirect to any application page based on the policies. • Default Session Timeout redirects the users back to the centralize logon page • Default Authorization Failure to the application will redirect the user to the centralize failedlogin page |

| Field | Description |
|-------|---|
| | <ul style="list-style-type: none"> • Default Logout will redirect the user back to the centralize logon page VA as SP: • SSOi consumes the assertion and generates the SMsession to provide the access to the application. The application policy will drive the failure conditions. • Default Session Timeout redirects the users back to the centralize logon page • Default Authorization Failure to the application will redirect the user to the centralize failed login page • Default Logout will redirect the user back to the centralize logon page |

6.2.4.5 WS Federation for Internal Users

| Field | Description |
|----------------|--|
| Use Case Name | WS Federation for Internal Users |
| Description | This use case describes the process by which a user gets seamless access to the relying partner application using WS trust. |
| Actors | <ol style="list-style-type: none"> 1. Internal Users 2. SSOi 3. SSOi Integrated Application(s) 4. User Directory |
| Pre-Conditions | A valid WS integration/ trust between Identity provider and relying partner |
| Trigger | User access application protected with WS federation authentication |
| Actions | <ol style="list-style-type: none"> 1. User accesses the application without a valid SiteMinder session 2. Web server redirects to Login Server 3. User prompted for credentials 4. User enters the credentials 5. Validated against SiteMinder Policy server 6. Authenticate and authorize user against User store 7. Notify Log On Server of validated user 8. Generate the WS Federation Assertion token: 9. Redirect to WS Federation URL 10. Create WS Federation Assertion 11. Generate WS Federation assertion with attributes such as User Principal Name (UPN), email, firstname, and lastname 12. Notify Web Agent of transaction 13. SiteMinder posts the WS Federation assertion to the Relying party configured 14. Redirect with HTML Form Post 15. Relying party validates the WS federation token generated 16. Relying party consumes WS- Federation |

| Field | Description |
|------------------------|--|
| | <p>17. Redirect to Target Application</p> <p>Alternate Flow</p> <ol style="list-style-type: none"> 1. User accesses the application with a valid SiteMinder session 2. Validate user credentials: 3. Validated against SiteMinder Policy server User store. 4. Authenticate and authorize user against User store 5. SiteMinder Policy server generates the WS Federation Assertion token by adding all the required attributes such as user Principal Name (UPN), email, firstname, lastname. 6. SiteMinder posts the WS Federation assertion to the Relying party configured. 7. Redirect with HTML Form Post 8. Relying party validates the WS federation token generated 9. Relying party consumes WS-Federation 10. Redirect to Target Application |
| Sequence Diagram | <pre> sequenceDiagram participant User participant WebAgent as Web Agent With Option Pack participant LogOnServer as Log On Server participant PolicyServer as Policy Server participant UserDirectory as User Directory participant ResourcePartner as Resource Partner Service participant ServiceProvider as Service Provider Application Note over User, WebAgent: 1. User Access the WS-FED Service with ParterID WebAgent->>WebAgent: 2. Validate SMSession Cookie Note over WebAgent, PolicyServer: 3. Validate User Note over PolicyServer, UserDirectory: 4. Validate user against user directory Note over PolicyServer: 5. Generate WS federation assertion attributes PolicyServer->>PolicyServer: 6. User validated response with WS-FED Assertion PolicyServer->>WebAgent: 7. Generate HTML Form Post with WS-FED Assertion WebAgent->>User: 8. Redirect with HTML Form Post Response Note over User, ResourcePartner: 9. Post To WS-FED Assertion to Resource Partner ResourcePartner->>ResourcePartner: 10. Validate and Consume WS-FED Assertion ResourcePartner->>ServiceProvider: 11. Redirect to Target Application Note over User, WebAgent: 3. Redirect to Login Server Note over WebAgent, LogOnServer: 4. Prompt for credentials LogOnServer->>LogOnServer: 5. User enter credentials LogOnServer->>PolicyServer: 6. Validate User Note over PolicyServer, UserDirectory: 8. User Validated Authenticate and Authorize user PolicyServer->>PolicyServer: 10. Create WS-FED Assertion PolicyServer->>PolicyServer: 11. Generates WS-FED Assertion with attributes PolicyServer->>WebAgent: 12. response with WS-FED Assertion WebAgent->>User: 13. Generate HTML Form Post with WS-FED Assertion User->>WebAgent: 14. Redirect with HTML Form Post Response Note over User, ResourcePartner: 15. Post To WS-FED Assertion to Resource Partner ResourcePartner->>ResourcePartner: 16. Validate and Consume WS-FED Assertion ResourcePartner->>ServiceProvider: 17. Redirect to Target Application </pre> |
| Main Success Scenarios | User is authenticated and Application is presented to the user. |

| Field | Description |
|------------------------|---|
| Main Failure Scenarios | Assertion failure errors generated by Relying party unable to consume WS-Federation assertions. |

6.2.4.6 SSOi Support for Attribute Service

| Field | Description |
|----------------|--|
| Use Case Name | SSOi Support for Attribute Service |
| Description | This use case describes the process by which SiteMinder calls the attribute service from VDS during authorize policy evaluation. |
| Actors | <ol style="list-style-type: none"> 1. Users 2. SSOi 3. SSOi Integrated Application(s) 4. User Directory 5. VDS |
| Pre-Conditions | A valid WS integration/ trust between Identity and Relying partner |
| Constraints | SSOi will be depend the capability of VDS attribute service capability to get appropriate attributes |
| Trigger | User authenticated with SSOi and needs specific attributes from VDS |
| Actions | <ol style="list-style-type: none"> 1. User authenticates in to SSOi 2. SSOi redirects to Logon Server 3. Logon server prompts for Credentials 4. User enters credentials 5. SSOi authenticates and authorize user against user store 6. SiteMinder session token is generated by SiteMinder Policy Server 7. During evaluation of authorization policies SiteMinder policy server call the attribute service exposed by VDS and provided user information (UPN) as input and specific attribute names such as Firstname, lastname, SECID required by application policy 8. Attribute service returns the attribute set to SiteMinder policy server at the run time. 9. SiteMinder set them on http headers as response and provide it back to the application. |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram participant User participant Application participant Log On Server participant Policy Server participant User Directory participant VDS User->>Application: 1. User Access Application Application->>Log On Server: 2. Redirect to Logon Server Log On Server->>User: 3. Prompt for Credentials User->>Log On Server: 4. User enters credentials Log On Server->>Policy Server: 5. Authenticate and Authorize user against user directory Policy Server->>User Directory: 6. Create SM Token Policy Server->>VDS: 7. Call VDS attributes service VDS->>Policy Server: 8. Return the user attributes Policy Server->>Log On Server: 9. Returns the attribute as HTTP headers Log On Server->>Application: 10. Application Presented to User </pre> |
| Main Success Scenarios | User is authenticated and Application is presented to the user. |
| Main Failure Scenarios | Failure to receive attribute will result in blank response which will be handled by application to display application specific error codes. |

6.2.4.7 SSOi Proxy Authentication Request

| Field | Description |
|----------------|--|
| Use Case Name | SSOi Proxy Authentication Request |
| Description | This use case describes the process by exchanges which SiteMinder offers proxy capability for the authentication request. The centralized login page will be integrated with SPS for implementing SSOI using multiple authentication methods (LOA2, LOA3,). |
| Actors | <ol style="list-style-type: none"> 1. Users 2. SSOi 3. SSOi Integrated Application(s) |
| Pre-Conditions | All application access requests go through SPS |
| Trigger | User accesses application protected and proxy through SPS |
| Actions | <ol style="list-style-type: none"> 1. The user access to the application which proxy through Secure proxy server 2. The Secure proxy Server verifies the policy server to check the resource is protected 3. If the resource is protected SPS, it prompts the user for credentials 4. User submits credentials 5. Secure proxy server validates the credentials with policy server 6. SiteMinder Policy Server authenticates and authorizes user against User Store 7. SiteMinder Policy server sets the cookie and passes control back to SPS 8. Secure Proxy Server invokes proxy engine and passes control to the application |

| Field | Description |
|------------------------|---|
| Sequence Diagram | <pre> sequenceDiagram participant User participant SPS participant Application participant Policy Server participant User Directory User->>SPS: 1. User Access the Application SPS->>Policy Server: 2. Is Resource Protected Policy Server->>User: 3. Prompt for credentials User->>SPS: 4. User enters the credentials SPS->>Policy Server: 5. Validate user Policy Server->>User Directory: 6. Authenticate and Authorize user against User directory User Directory-->>Policy Server: 7. User Authenticated and Authorized Response Policy Server->>Application: 8. Redirect to Target Application Application->>User: 10. Application presented to user </pre> |
| Main Success Scenarios | User is authenticated and Application is presented to the user |
| Main Failure Scenarios | <ul style="list-style-type: none"> • Default Session Timeout redirects the users back to the logon handler • Default Authorization Failure to the application will redirect the user to the failedlogon handler • Default Application Logout Page will redirect the user back to the logon handler |

6.2.4.8 Session Management

| Field | Description |
|----------------|--|
| Use Case Name | Session Management |
| Description | This use case describes the process by which SiteMinder manages session tokens. |
| Actors | 1. Users 2. Client 3. Web Service |
| Trigger | 1. User stays idle (more than 60 minutes) after getting access to the application. 2. User clicks log out button available in the application |
| Pre-Conditions | A user has a valid single sign-on token |
| Actions | SSOi Session idle time out 1. A user logs in to the SiteMinder protected application 2. Validate the SiteMinder Cookie |

| Field | Description |
|------------------------|--|
| | <ol style="list-style-type: none"> 3. Send session specs to Policy Server 4. Policy Server evaluates the session time set for each authorization 5. If the user idles greater than the time out set on SSOi policy it will log out the user 6. Redirect to the Logon page for re-authentication <p>Limit refresh session token</p> <ol style="list-style-type: none"> 1. A user logs in to the SiteMinder protected application 2. Validate the SiteMinder Cookie 3. Send session specs to Policy Server 4. SiteMinder evaluates the max session time set for each authorization request 5. If the user session is greater than the max time out set on policy, it will log out the user 6. Prompt for the authentication again <p>SSOi Session Logout</p> <ol style="list-style-type: none"> 1. A user clicks log out on SiteMinder protected application 2. Validate the session cookie 3. Web agent calls logout method call to policy server 4. Policy Server clears all the session cookie 5. Web agent redirected it to log on page |
| Sequence Diagram | <pre> sequenceDiagram participant User participant SPS/WebAgent participant Application participant Log On Server participant Policy Server participant User Directory Note over User, SPS/WebAgent: 1. valid session SPS/WebAgent->>SPS/WebAgent: 2. Validate SM Cookie SPS/WebAgent->>Application: 3. Send Session Spec Application->>Policy Server: 4. Calculate IdleTime & Max time allowed Note over Policy Server: IdleTimeOut/ Max Time Out Policy Server->>Policy Server: 5. Invalidate Session Spec Policy Server->>Log On Server: 6. Redirect to Logon page based on policy Log On Server->>User: 6. Redirect to Logon page based on policy Note over User, Application: 1. valid session and click log out Application->>SPS/WebAgent: 2. Validate session Cookie SPS/WebAgent->>Application: 3. Logout() Application->>Policy Server: 4. Terminate Spec and Clear Cache Note over Policy Server: Global LogOut Policy Server->>Log On Server: 5. Redirect to Logon page based on policy Log On Server->>User: 5. Redirect to Logon page based on policy </pre> |
| Main Success Scenarios | Session management policy is enforced |

| Field | Description |
|------------------------|-------------|
| Main Failure Scenarios | N/A |

6.2.4.9 SSOi STS Architecture Flow

| Field | Description |
|----------------|--|
| Use Case Name | SSOi STS Architecture Flow |
| Description | This use case describes the process through which SSOi translates various session tokens and provides a gateway for attribute service |
| Actors | <ol style="list-style-type: none"> 1. Users 2. Client 3. Web Service 4. User Directory |
| Pre-Conditions | A user has a valid single sign-on token |
| Trigger | Client accesses a web service endpoint at DataPower |
| Actions | <ol style="list-style-type: none"> 1. SSO STS architecture implements DataPower in conjunction with Secure Proxy Server (SPS) Web service. Internal application creates a WS-Trust request message with the user's session cookie as part of SOAP body and send it to the enterprise service on behalf of the user 2. DataPower front-end gets the input request from the client application. The request will be mutually authenticated with TLS 3. DataPower extracts SMSession from input request and transforms it into a SOAP request as per the published SPS authorize service 4. STS Service calls the SPS web service to validate the user session extracted on earlier step and request for additional attributes 5. SPS requests for validation of SMSession to Siteminder Policy Server. 6. Policy Server decrypts the SMSession and validates the token. It extracts the user context from the session and performs an user lookup in to the user directory 7. User status is returned to the policy server 8. Policy Server returns the user attributes to SPS based on the policy definition 9. SPS packages the user attributes and returns it to DataPower as a SOAP response 10. STS Service extracts user attributes including caller context. The user attributes are packaged in a SAML assertion signed with DataPower. The complete assertion is packaged inside WS-Token 11. DataPower returns the WS-Token to the requesting internal application. Application consumes the WS-Token and receives the user attribute sets with |

| Field | Description |
|------------------------|---|
| | <p>the updated SMSession token</p> <p>SPS Authorization Web service</p> <ol style="list-style-type: none"> 1. Client formulate a SOAP base request to SSOi Authorization web service with AppID, resource string , action, Session token as inputs 2. SiteMinder detects the request and passes it to the endpoint. 3. SSOi web service validates SSOi token and evaluates the user authorization based on the policy configuration 4. SiteMinder Policy Server authorizes 5. SiteMinder Policy Server gets session attribute from SOAP request 6. SiteMinder Policy Server authorizes user against user store 7. SiteMinder Policy Server return updated session specs if valid 8. SiteMinder Policy Server returns the result code and updated SSOi session token as response code back to the client. 9. SiteMinder Policy Server send the SOAP authentication response with the user attributes 10. Client receives updated SOAP response with user session and attributes |
| Sequence Diagram | <pre> sequenceDiagram participant Client participant SPS participant AuthN/AuthZ Web service participant Policy Server participant User Directory Note over Client: 1. Client request SOAP message to Authenticate/ Authorize a user Client->>SPS: Note over SPS: 2. SPS detect the request and pass it to endpoint SPS->>AuthN/AuthZ Web service: Note over AuthN/AuthZ Web service: 3. Validates the token AuthN/AuthZ Web service->>AuthN/AuthZ Web service: 4. authorize () Note over AuthN/AuthZ Web service: 5. Get the session attribute from SOAP request AuthN/AuthZ Web service->>User Directory: 6. Authorize user against User directory User Directory-->>AuthN/AuthZ Web service: Note over AuthN/AuthZ Web service: 7. Returns the updated session spec if valid AuthN/AuthZ Web service-->>SPS: 8. Returns updated SSOi token SPS-->>Client: 9. SOAP AZ Response with user attributes Note over Client: 10. Client gets the update SOAP response with user session </pre> |
| Main Success Scenarios | <ol style="list-style-type: none"> 1. User is authorized 2. Application is presented to the user |
| Main Failure Scenarios | <ol style="list-style-type: none"> 3. The Authorization web service will return Access denied error message when Authorization failure occurs. 4. Any communication error at service end point will result in SOAP fault codes as response <p>Web service methods throws below error message upon failure authentication –</p> |

| Field | Description |
|-------|--|
| | <p>Sample message for Authorize()</p> <pre><message>Authorization Failed</message> <resultCode>NOTAUTHORIZED</resultCode>.</pre> |

6.2.4.10 Centralized Login Page

To support accessing VA applications with multiple authentication mechanisms at one place, the SSOi activity provides a static centralized logon page to support userID / Password, PIV, or Microsoft Windows authentication. This page is modifiable for each application to reflect only the authentication mechanisms selected by the integrating VA application. Also to support VA applications with PIV compliance, the SSOi activity provides a static PIV only centralized logon page to support only using PIV card. A pre-condition to this is client has certificate to support mutual TLS authentication.

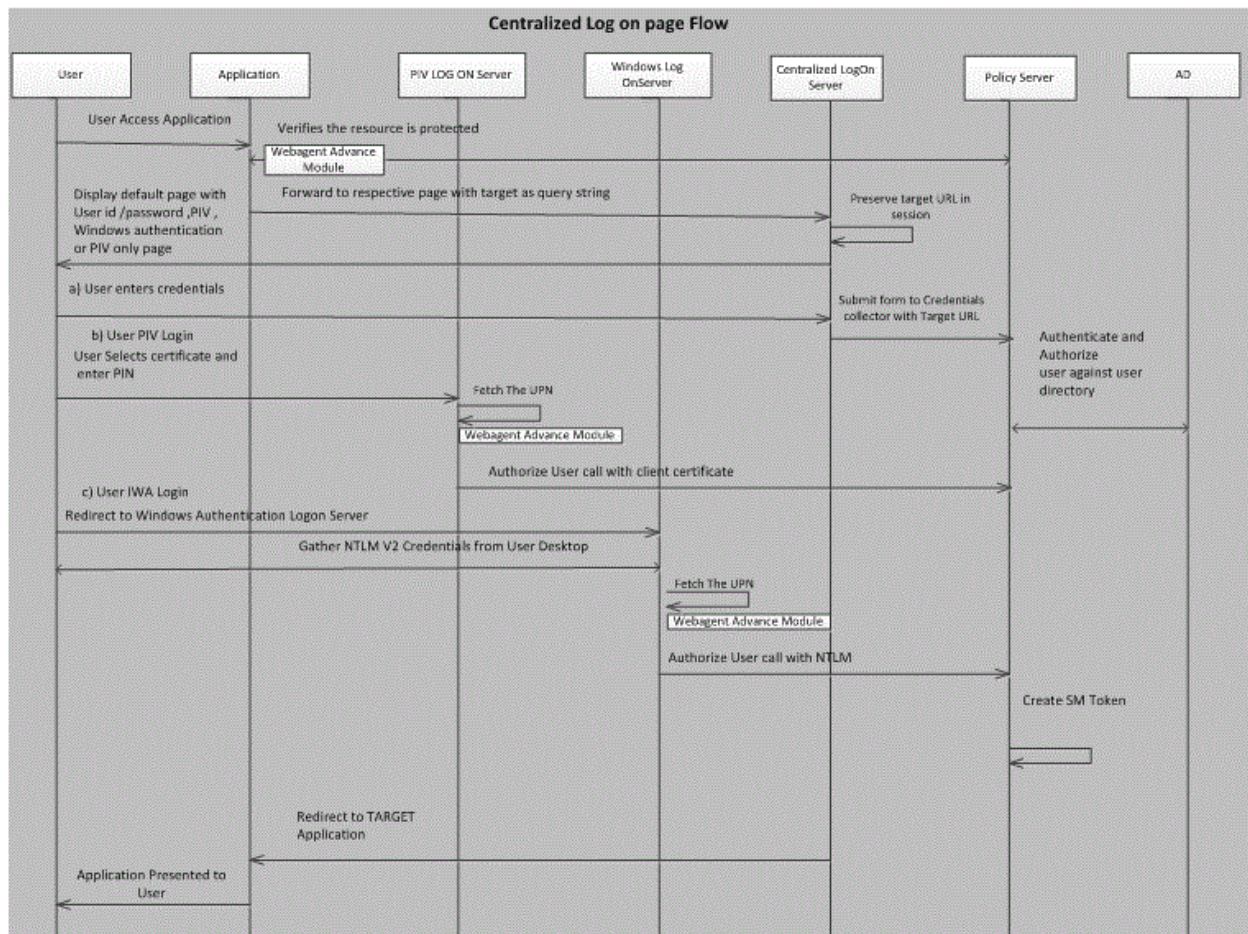


Figure 59: Centralized Logon Page Flow

The centralized logon page flow includes the following steps:

1. User attempts to access VA application protected by SiteMinder multiple authentication

2. Web Agent Intercepts the request to access integrated application and verifies it with policy server
3. SiteMinder redirects the request to respective (PIV or Default) static centralized log on page with application name and target URL of the application as query string.
4. Central login page handler preserves the target and displays static central login page to user.
5. For multiple authentication supported applications, central login page handler provides user with an option to choose either user ID, password, PIV card, or windows authentication method to log into application.
6. For PIV only and PIV compliance supported applications, PIV only central login page handler displays PIV only login page.
7. If user submits user ID and password, the request is sent by the browser to central login handler which submits the credentials to login FCC SiteMinder credential collector.
8. If user login with Windows authentication, the request is sent by the browser to windows NTLM logon sever which checks with policy server for authentication.
9. If user login with PIV card and for PIV only login, the request is sent by the browser to PIV logon sever which checks with policy server for authentication
10. Policy server authenticates the user against the Active Directory.
11. If the user is authorized by Policy Server to access the resource then a token is generated
12. SSOi creates SiteMinder Token and redirects the user to application

The following diagram depicts the Siteminder policy architecture for core centralized authentication flows that was described above.

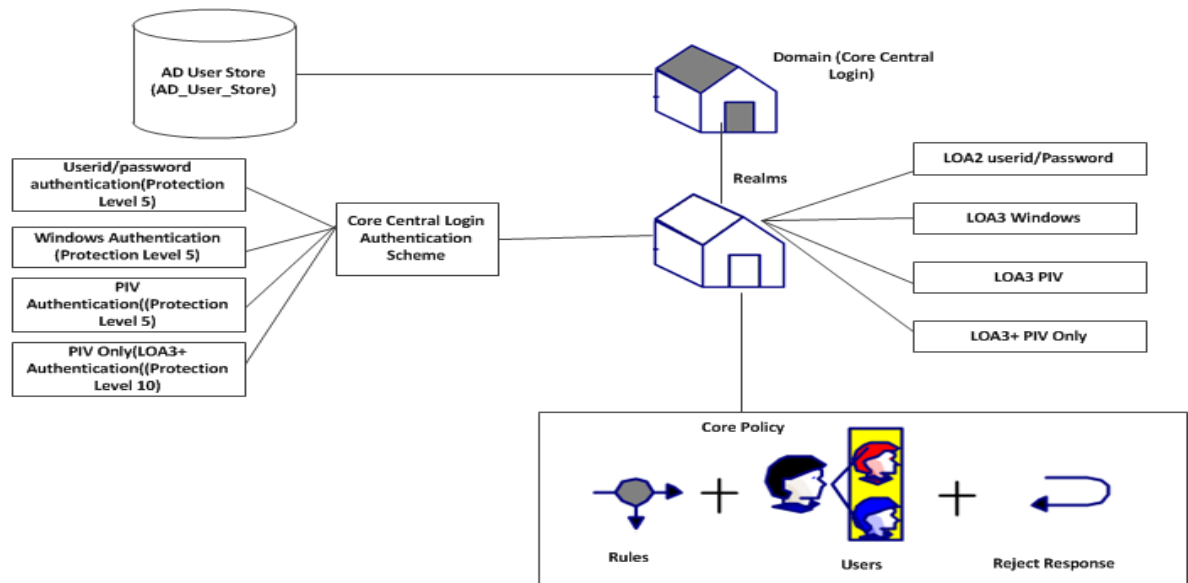


Figure 60: Siteminder Policy Architecture for Core Centralized Authentication Flows

6.2.5 CSP Design

The CSP provides the external end-user credentials for accessing multiple VA application behind the VAAFI infrastructure. It acts a federation partner with VAAFI and asserts LOA 1 and LOA 2

credentials. It provides a self-service interface for external users to perform self-service functions such as forgot password, change password, forgot userID and ability to modify account

The following diagram provides a detailed view of the complete CSP system at VA and its interaction with VAAFI and other actors.

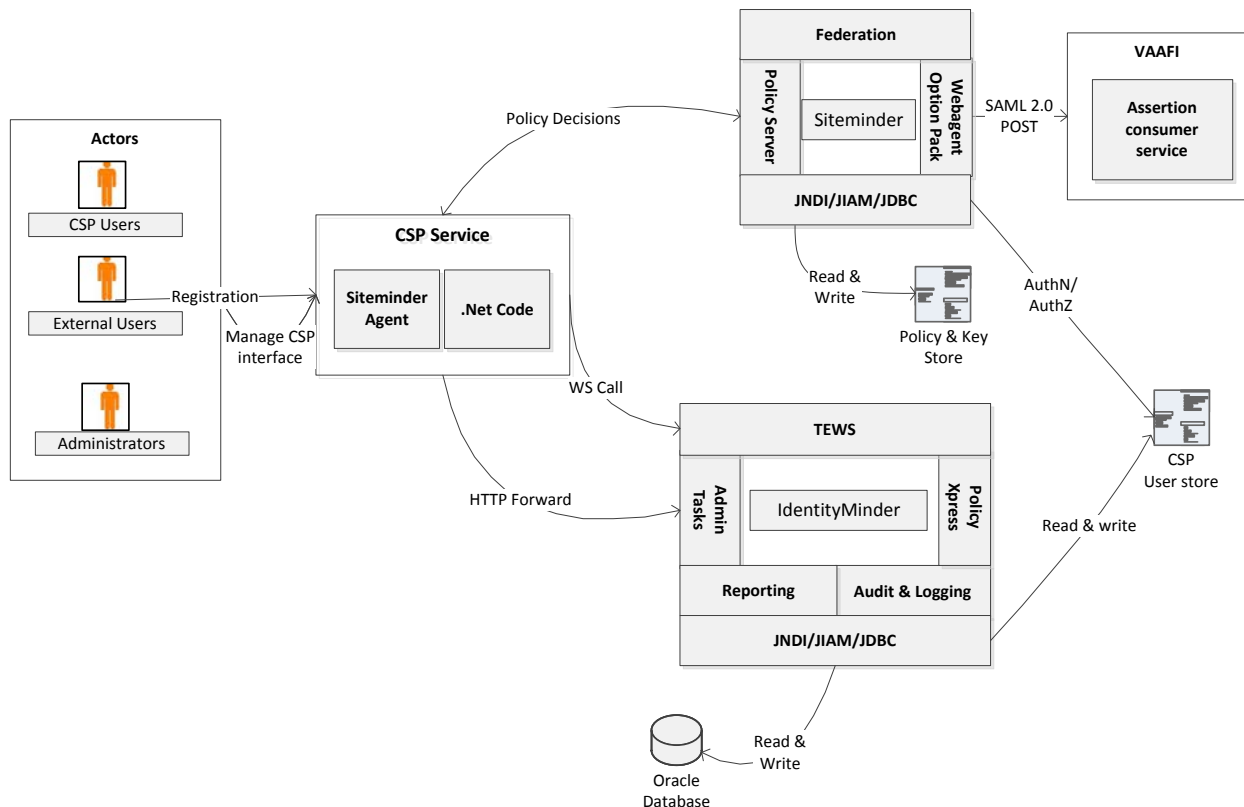


Figure 61: CSP Detailed Design

CA IdentityMinder:

This is a J2EE application deployed on the Web logic application server cluster, which implements the CSP function. It is integrated with SiteMinder for Single Sign On and Access Control purposes. Major modules of CA IdentityMinder, which are leveraged to implement the CSP, 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

CSP Service:

The CSP 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 calls the CA IdentityMinder Task Execution Web services (TEWS) to execute the various tasks created for implementing the CSP activities

- **Web agent:** This acts as the policy enforcement point and enforces policy decision set in CA SiteMinder Policy Server, and implements the access control framework for the ASP.NET application

CSP-VAAFI Integration:

CSP is responsible for receiving requests from the VAAFI service to authenticate persons with VA CSP credentials. The CSP authenticates the user and returns the authentication assertion to the requesting service (VAAFI). The CSP and VAAFI services together provide the end-to-end authentication services to the business application. Once the CSP passes the assertion and person attributes back to VAAFI and does a handshake, the role of the CSP is complete for that transaction. The access control or authorization is done by VAAFI or is internal to the consuming business application. VAAFI validates the assertion to determine if the user should gain access to the requested application.

SiteMinder federation services implements and establishes the federation partnership between CSP and VAAFI. In the context of the design CSP service will act as an Identity Provider and VAAFI acts as a service provider

6.2.5.1 Credential Issuance

| Field | Description |
|----------------|--|
| Use Case Name | Credential Issuance |
| Description | This workflow describes the technical activities and associated data exchanges through which an external user gets a LOA 1/ 2 credential, which could be used to access applications managed under VAAFI requiring LOA1/2 credentials. |
| Actors | 1. CSP Service 2. External User 3. CA Identity Minder Tasks |
| Pre-Conditions | External user have a valid email address |
| Trigger | An external user requires LOA1 or 2 credential |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram participant EU as External User participant CSP as CSP Service .NET Application participant CIM as CA Identity Minder Tasks participant PE as Policy Express participant CUS as CSP User Store EU->>CSP: 1. Access Landing Page CSP->>CSP: 2. Navigate to registration page & initiate self registration CSP->>CSP: 3. Complete details, answer security questions & Submit CSP->>CIM: 4. Submit registration request CIM->>CUS: 5. Create User Profile CUS->>PE: 6. User created successfully PE->>CSP: 7. Trigger email to be sent CSP->>EU: 8. If user has requested LOA 2, send Identity Proofing email EU->>CSP: 9. User accesses CSP managed account link CSP->>EU: 10. Prompt user to change password </pre> |
| Actions | <ol style="list-style-type: none"> 1. External user access the CSP service landing page 2. Navigate to the registration page and initiate the self-registration process for requesting a LOA 1 or LOA 2 3. Provide the user related details, and register answers for security questions and submit the request 4. The CSP Service ASP.NET code make a web service call to CA IdentityMinder TEWS interface and submits the registration request 5. CA IdentityMinder task creates the user profile in CSP user store 6. Notify policy express the user was successfully created 7. The policy express rule gets triggered to send the user with user ID and temporary password in two separate emails 8. If the user has requested for LOA 2, then an separate email to the user to appear in-person for identity proofing will be sent 9. User follows the instructions provide in the email sent from CSP service and access the CSP manage account link 10. User will be prompted for password change and on successful change the user will be redirected to the Manage user link |
| Main Success Scenarios | Successful generation of CSP user profiles in CSP user store |
| Main Failure Scenarios | Failure to create the user in CSP user store |

6.2.5.2 Revoke/Reissue Credential

| Field | Description |
|------------------------|--|
| Use Case Name | Credential Issuance |
| Description | This workflow describes the technical activities and associated data exchanges through which CSP user credential is revoked or reissued. |
| Actors | 1. CSP Service 2. CSP Service administrator |
| Pre-Conditions | CSP Service administrator have the required access to perform the credential revoke/reissue function |
| Trigger | Credential revocation/ reissue request received from a trusted partner system |
| Sequence Diagram | <p>Third-party system</p> <pre> sequenceDiagram participant CSPAdmin as CSP Administrator participant NETApp as .NET Application participant CAM as CA Identity Minder participant CSPUS as CSP User Store CSPAdmin->>NETApp: 1. Login NETApp->>CAM: 2. Select Revocation/Reissue Link CAM->>NETApp: 3. Search for user NETApp->>CSPUS: 4. If user is found, Revoke or Enable User appropriately CSPUS->>NETApp: 5. Provide status of the user NETApp->>CSPAdmin: </pre> |
| Actions | <ol style="list-style-type: none"> 1. CSP administrator log into CSP service .NET application as an administrator 2. Administrator click on the revocation/reissue of credential link, which gets forwarded to the specific CA Identity Minder task 3. Administrator search for the specific user and if the user is found, based on the type of request the user will be revoked or enabled in CSP user store 4. CSP administrator respond to the trusted partner system on the status of the task |
| Main Success Scenarios | User is successful revoke or reissued a credential |
| Main Failure Scenarios | Failure during revoke or reissue of credential |

6.2.5.3 Federation with VAAFI

| Field | Description |
|---------------|--|
| Use Case Name | Federation with Consuming Application |
| Description | This workflow describes the technical activities and associated data exchanges |

| Field | Description |
|------------------------|---|
| | through which a CSP user who poses LOA 1/ 2 credential, federate to VAAFI, to access the application behind VAAFI. |
| Actors | <ol style="list-style-type: none"> 1. CSP Service 2. CSP User 3. CA SiteMinder Federation Service |
| Pre-Conditions | CSP user have a valid LOA 1 or LOA 2 credential |
| Trigger | A CSP user wants to access applications behind VAAFI |
| Sequence Diagram | <pre> sequenceDiagram participant End User participant VAAFI participant CSP Service participant CA Federation Option Pack participant CSP User Store End User->>VAAFI: 1. Accesses VAAFI VAAFI->>End User: 2. Redirects user to VA CSP Link CA Federation Option Pack->>End User: 3. Prompt user for credentials End User->>CSP Service: 4. Inputs credentials and submits CSP Service->>CSP User Store: 5. Authenticate and Authorize user CSP User Store-->>CSP Service: 6. User Authenticated/Authorized CA Federation Option Pack->>CA Federation Option Pack: 7. Generates SAML CA Federation Option Pack->>VAAFI: 8. POST SAML VAAFI->>End User: 9. Consumes token and displays appropriate applications </pre> |
| Actions | <ol style="list-style-type: none"> 1. CSP user access VAAFI, for accessing application behind VAAFI 2. VAAFI redirects the user to VA CSP link, which is a protected federation link by CA SiteMinder 3. The SiteMinder agent prompts the user for user credentials 4. CSP user type in the credentials and submit the request 5. The CSP service authenticate and authorize the user against the CSP user store is 6. The user is successfully authenticated and authorized. 7. SiteMinder federation option pack generated a SAML 2.0 token with assurance level of the user as an attribute 8. The option pack redirects the user with a SAML POST to VAAFI 9. VAAFI consumes the SAML token and based on the assurance level (LOA 1 or LOA2) it displays the list of application the user can access |
| Main Success Scenarios | Successfully single sign on to VAAFI application |
| Main Failure Scenarios | Failure to Single Sign on to VAAFI application |

6.2.6 IP Design

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 201¹, HSPD-12², OMB A-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 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 information⁵. IP services are classified as in-person, remote or hybrid.

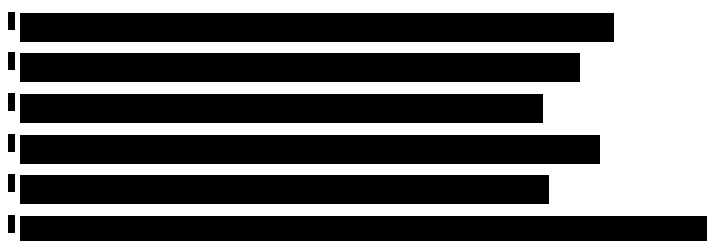
The following table, as defined in OMB M04-04⁶, is referenced to the NIST SP 800-63 Identity proofing processes and drives their scope and extensiveness.

Table 30: 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 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.



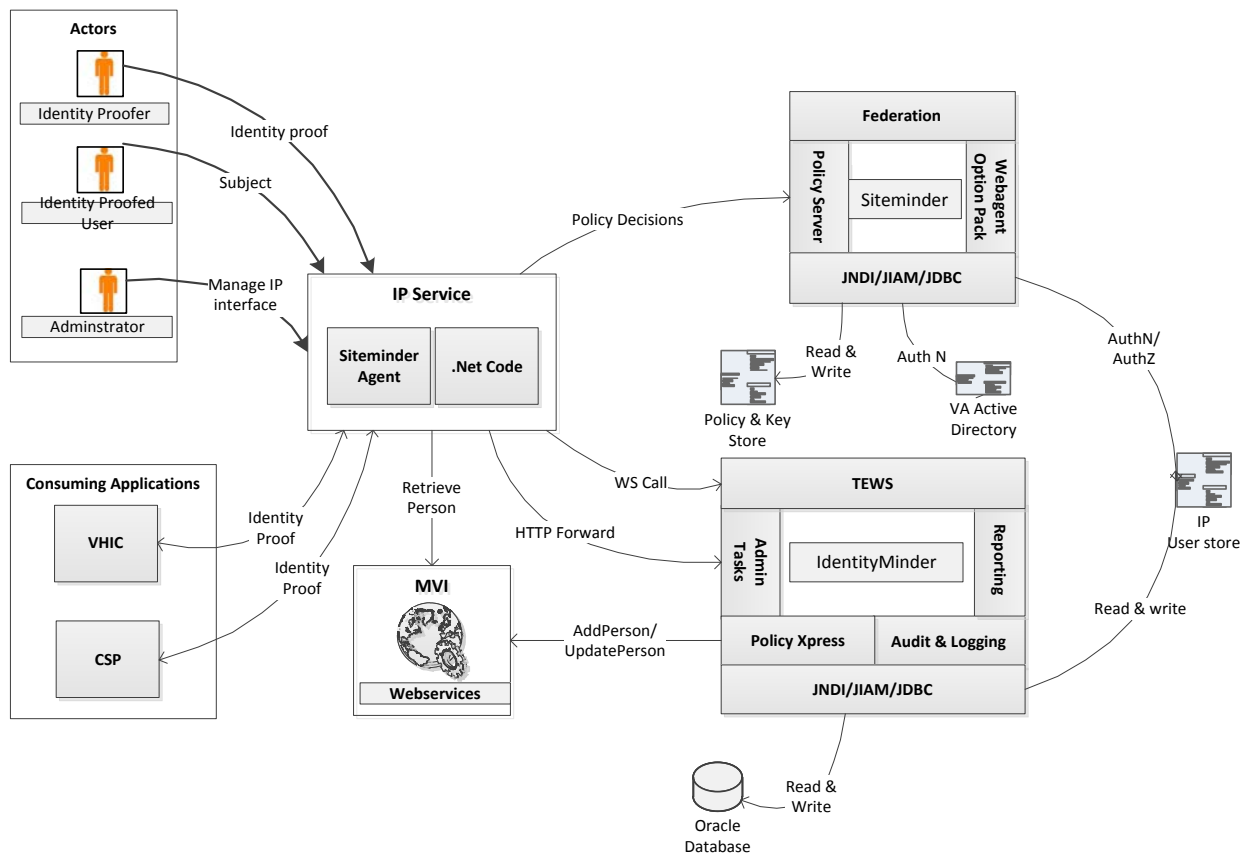


Figure 62: IP Detailed Design

CA IdentityMinder:

CA IdentityMinder is a J2EE application deployed on the Web logic 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

6.2.6.1 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 |
| 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 |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram participant IP as Identity Proofer/ System participant IS as IP Service participant TEWS as CSP TEWS Webservices participant CUS as CSP User Store participant IUS as IP User Store participant MVI as MVI System IP->>IS: 1. Login IS->>IP: 2. Initiate Identity Proofing task IS->>MVI: 3. If fully qualified identifier present, calls "Retrieve Person with get Corresponding IDs" MVI-->>IS: 4. No matching IP correlation in MVI IS->>CUS: 5. Create a LOA1 Record IS->>MVI: 6. Make a Add Person/Add Correlation Call IS->>CUS: 7. Updates users Assurance Level and proofing information based on Identification documents IS->>MVI: 8. Make a Update Person Call IS->>IP: 9. Display Search Screen, if fully qualified identified is not present IP->>IS: 10. Inputs search criteria IS->>TEWS: 11. Calls TEWS Web Service TEWS->>CUS: 12. Searches for user CUS-->>IS: 13. Display Search Results IS->>IP: 13. Display Search Results IP->>IS: 14. Completes Required Information IS->>CUS: 15. Updates users Assurance Level IS->>IUS: 16. Updates users Credential Level IS->>IUS: 17. Create User Profile </pre> |
| 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 |

6.2.6.2 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 | <ol style="list-style-type: none">1. IP Service2. Identity Proofer/System3. CSP TEWS Web services4. 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 |
| Actions | <ol style="list-style-type: none">1. Identity Proofer/System logs into IP service2. Identity proofer/System initiates create identity proof task on the IP service3. IP services receives the fully qualified identifier and checks the existence of the ID in the IP system4. 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 record7. Create the user record in IP system, if it is not present already8. Identity Proofer enters all the necessary information for identity proofing and submits the record to update the IP service9. IP service make a TEWS call to CA IdentityMinder of the IP system10. Submit the data to IP store11. 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 |

| Field | Description |
|------------------------|---|
| Sequence Diagram | <pre> sequenceDiagram participant IP as Identity Proofer/ System participant IS as IP Service participant MVI as MVI participant CIM as CA IdentityMinder participant IUS as IP User Store IP->>IS: 1. Login IS->>IS: 2. Initiate Identity Proofing task IS->>IS: 3. Checks the existence of the ID IS->>MVI: 4. Retrieve Person with Get Corresponding IDs MVI->>IS: 5. Return Record IS->>IS: 6. Validate data return matches record IS->>IUS: 7. Creates the user IS->>IP: 8. Initiate Proofing Process IP->>IS: 9. Completes Required Information IS->>IUS: 10. Submit data IS->>CIM: 11. Initiate Add Person CIM->>IUS: 12. Add Person/Update Person </pre> |
| Main Success Scenarios | Created of LOA 2 user in Identity Proofing system |
| Main Failure Scenarios | Error during create proofing record |

6.2.7 SAC Design

VA currently maintains customized code to manage user's fine-grained access control decisions based on policies. The maintenance of custom code is cumbersome and each information security aspect needs to be addressed individually by independent applications. VA applications have the need for more granular or specialized access controls that are not inherent in the applications. The SAC activity addresses this need by providing fine- and coarse-grained resource access and attribute based permissions controlling what functionality and information is available to each user. It provides the capability to simplify the process and enhances information security by providing the ability to make fine-grained access control decisions based on pre-defined policies and user attributes.

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

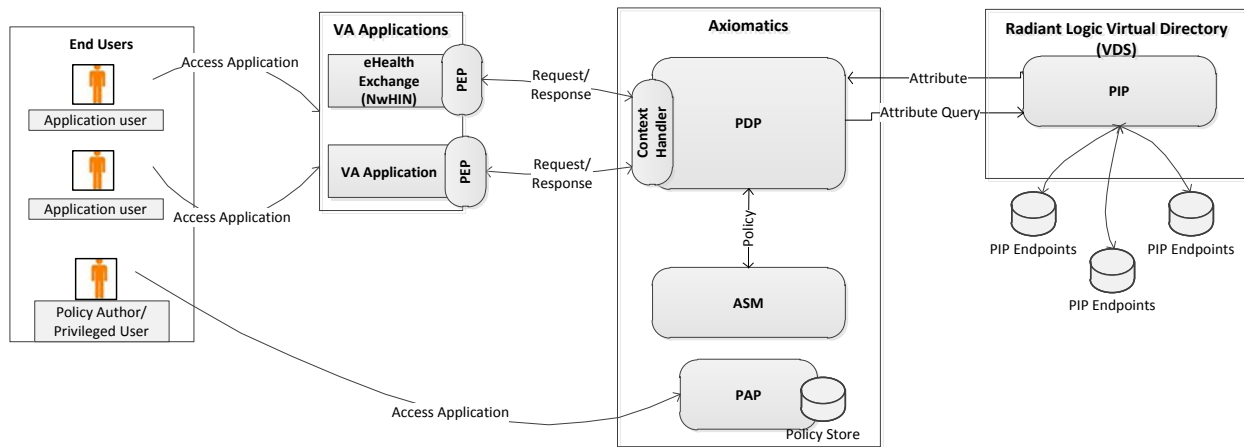


Figure 63: SAC Detailed Design

SAC leverages the capabilities of Axiomatics, Radiant Logic, and DataPower products to minimize software development. The basic components of Axiomatics are the Policy Enforcement Point (PEP), Policy Decision Point (PDP), Axiomatics Policy Auditor (APA), Axiomatics Services Manager (ASM), and Policy Administration Point (PAP). The Radiant Logic product is Virtual Directory (VDS) for VA Policy Information Points (PIP). DataPower is used as a security measure to protect the web service communication between the PEP and PDP.

Natively, the Policy Administration Point (PAP) tool, provided as part of the Axiomatics software suite for SAC does not have its own security framework. The current implementation of the SAC solution relies on OS-level authentication/access controls to allow or disallow access to the PAP. At this time the Policy Author and Privileged users for SAC, as related to policy administration have to be provided specific access to the system hosting the PAP tool at Windows OS level in order for them to be able to use it.

Axiomatics:

- Policy Enforcement Point (PEP):** PEP enforces authorization decisions. It intercepts user requests to protected resources and enforces access control decisions. The PEP software component enforces the access decisions made by the PDP. It first intercepts access requests to protected applications then sends an authorization requests to the PDP. It is responsible for granting or denying access to a protected resource. Custom PEPs can be built using the Software Development Kit (SDKs) provided by Axiomatics to speed up integration with the SAC PDP. The PEPs have to conform to XACML 3.0 to integrate with the SAC enterprise PDP.
- Policy Decision Point (PDP):** PDP is a XACML policy evaluation engine that can retrieve the access control parameters from sources at various levels of the enterprise to render a decision. The PDP receives authorization requests from PEP and evaluates these requests against authorization policies authored from the PAP. The XACML 3.0 security policies are cached at the PDP. It has two web service interfaces used for communication with the ASM and PEPs. The ASM communicates with the PDP through the management interface web service on the PDP. PEPs communicate with the PDP through the PDP endpoint address web service. The PEP sends XACML 3.0 requests to the PDP for access control decisions. The PDP then determines the correct security policy to use then determines which attributes are needed for a decision. The PDP queries the attribute

service to retrieve any attribute not in the PEP's request. After the PDP uses attributes from within the XACML request and from the attribute service along with the corresponding XACML 3.0 policy it will generate an access control decision, which is sent back to the PEP that made the request.

- **Policy Administration Point (PAP):** The PAP facilitates creation of policies and policy sets and retains these policies in policy stores with the intent of making them available to the PDP. Axiomatics PAP is a stand-alone Java application providing a full-featured graphical XACML 3.0 policy editor. The interface provides administrators authoring, testing, and troubleshooting capabilities. The PAP is used in the SAC solution for authoring XACML 3.0 security policies. The security policies represent the business rules for access control that restrict access based on client preferences, data restrictions, user security, and contextual constraints. The policies are exported from the PAP as policy packages.
- **Axiomatics Services Manager (ASM):** Axiomatics ASM is a web based application that provides a centralized configuration management interface for the PDPs. It provides the capability to manage and provision configurations to remotely managed PDPs. The PDPs can be grouped logically for easier management. New and updated XACML 3.0 policies can be pushed to individual PDPs or to PDPs within groups for easier policy management.
- **Axiomatics Policy Auditor (APA):** Axiomatics APA is a web-based application that provides a tool for analysing the behaviour of XACML policies. This analysis and process provides compliance with consumers business rules, increases policy controls, and supports accountability. It can also help determine unexpected policy behaviour.

Radiant Logic:

- **Virtual Directory Store (VDS):** VDS aggregates attributes across the enterprise from different data sources while providing the flexibility to receive requests via SQL (JDBC driver), LDAP, and Web Services SPML and DSML. It can perform mapping and transformation of attributes from data sources across the enterprise that can then be exposed through virtual views to consumers. The views can be configured to provide a single view of identities that may reside in multiple data sources. Radiant Logic VDS is a Java application that provides attribute service functionality. VDS has the capability to aggregate attributes across the enterprise from different authoritative PIPs. Custom views can be created and modified easily for the PDP to consume attributes for access control decisions. Onboarding procedures are followed for onboarding of data sources.
- **Policy Information Point (PIP):** The PIP retrieves user information by sharing, federating, exchanging and accessing various attributes associated with a user from variety of authoritative identity stores such as directories and databases. The attributes in the PIPs are required for the PDP to perform access control decisions at runtime.

6.2.7.1 Enforce Access Control Decision

| Field | Description |
|----------------|--|
| Use Case Name | Enforce Access Control Decision |
| Description | This use case describes the process by which a Policy Enforcement Point (PEP) interacts with a consuming application and the SAC service to facilitate an authorization request and enforce an access control decision. |
| Actors | <ol style="list-style-type: none">1. Application2. PEP3. DataPower4. PDP |
| Pre-Conditions | <ol style="list-style-type: none">1. Enter User has authenticated session with Application2. TLS session is established between the Application and PEP |
| Trigger | The PEP receive a request for an authorization from an application |
| Actions | <ol style="list-style-type: none">1. End-User attempts to access protected application.2. PEP intercepts access request3. The PEP can reside between the end user and the application4. The PEP can reside within the application itself5. PEP verifies request is valid and contains authentication attributes that can be used to uniquely identify the user6. PEP translates access request to XACML 3.07. Includes authentication attributes (SECID, ICN, unique identifier)8. May include client preferences, data restrictions, user security, contextual constraints9. Forwards XACML 3.0 request to DataPower10. DataPower performs XML threat reduction and forwards request to PDP11. PDP evaluates appropriate policy (ies) and attributes (within XACML request and from PIPs (VDS)) and generates an access control decision. *Note - "eHealth" initiated requests, PIP is not consulted.12. The PDP response is sent to DataPower13. DataPower sends PDP response to the PEP. PEP receives XACML 3.0 access control decision response from the PDP.14. PEP enforces access control that it received from PDP. |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram participant Application participant PEP participant DataPower participant PDP Application->>PEP: 1. End User access application PEP->>PEP: 2. Intercepts Request PEP->>PEP: 3. Verifies Request PEP->>DataPower: 4. Translates Request to XACML 3.0 and sends to PDP through DataPower DataPower->>PDP: PDP->>PDP: 5. Evaluates Message PDP->>DataPower: 6. Send response DataPower->>PEP: 7. PEP gets Response PEP->>Application: 8. Enforces Decision </pre> |
| Main Success Scenarios | <ol style="list-style-type: none"> 1. If Decision is Permit, access is granted to the user to access the protected resource. 2. If Decision is Deny, access is denied. The user is not allowed to access the protected resource. 3. The processing of Indeterminate or Not Applicable is determined by the application requirements. |
| Main Failure Scenarios | <ol style="list-style-type: none"> 1. Message format/contents are not valid 2. PDP is non-responsive and decision is not provided to application |

6.2.7.2 Security Policy Authoring

| Field | Description |
|----------------|---|
| Use Case Name | Security Policy Authoring |
| Description | This use case describes the process through which a SAC Privileged User authors security control policies. |
| Actors | <ol style="list-style-type: none"> 1. Privileged User 2. PAP 3. APA |
| Pre-Conditions | Privileged user has access to PAP. |
| Trigger | The privileged user starts up Axiomatics Policy Administration Point thick client GUI interface to author and test XACML 3.0 policies. |
| Actions | <ol style="list-style-type: none"> 1. Privileged User creates workspace to organize and store policies 2. The policies and configurations are stored locally 3. Privileged User authors and tests XACML 3.0 policies |

| Field | Description |
|------------------------|---|
| | <ol style="list-style-type: none"> Once completed, the privileged user exports policy package to dedicated file location Privileged User logs into APA and configures attributes from the PEP perspective Privileged User creates queries for validation and runs validation tests Policy is authorized successfully upon successful testing |
| Sequence Diagram | <pre> sequenceDiagram participant User as Privileged user participant PAP participant APA User->>PAP: 1. Logs in and creates workspace activate PAP PAP->>PAP: 2. Authors and Tests policies deactivate PAP PAP->>PAP: 3. Exports policies deactivate PAP User->>APA: 4. Logs in to APA and configures attributes activate APA APA->>APA: 5. Queries for validation and runs test deactivate APA APA->>APA: 6. Policy successfully created deactivate APA </pre> |
| Main Success Scenarios | Policy is created successfully. |
| Main Failure Scenarios | Policy creation fails and user has to start over. |

6.2.7.3 Manage Access Control Policies

| Field | Description |
|----------------|--|
| Use Case Name | Manage Access Control Policies |
| Description | This use case describes the process through which a SAC Privileged User manages access control policies across PDPs. |
| Actors | <ol style="list-style-type: none"> Privileged User ASM |
| Pre-Conditions | Privileged user has access to ASM component. |
| Trigger | The privileged user is logged in to ASM and is ready to deploy policy package. |
| Actions | <ol style="list-style-type: none"> Privileged User determines proper PDP group to deploy policy package Upload validated policy package Push policies to managed PDP within PDP group |

| Field | Description |
|------------------------|--|
| | 4. Policies are pushed via web service call over TLS 5. Privileged user checks PDP status and pushes policies 6. Privileged user tests PDP with XACML requests to verify policy |
| Sequence Diagram | <pre> sequenceDiagram participant PU as Privileged user participant ASM Note over PU: 1. Determines PDP group to deploy PU->>ASM: Note over ASM: 2. Upload policy package ASM->>ASM: Note over ASM: 3. Push policies to PDP group ASM->>ASM: Note over ASM: 4. Checks PDP status ASM->>ASM: Note over ASM: 5. Test policy ASM->>ASM: </pre> |
| Main Success Scenarios | Policy is pushed to PDP successfully |
| Main Failure Scenarios | Policy upload fails and user has to start over. |

6.2.7.4 Make Access Control Decisions

| Field | Description |
|----------------|--|
| Use Case Name | Make Access Control Decisions |
| Description | This use case describes the process through which a Policy Decision Point (PDP) gathers and evaluates the necessary information (access control policy (ies) and attributes) and makes an access control decision. |
| Actors | 1. PEP 2. DataPower 3. PIP 4. PDP |
| Pre-Conditions | The application authorization policy and needed attributes exist |
| Trigger | PDP receives XACML request from PEP via DataPower |

| Field | Description |
|------------------------|---|
| Actions | <ol style="list-style-type: none"> 1. PEP request is received and PDP examines the request attributes to determine the correct policy to apply 2. Once the correct policies have been determined the PDP queries the PIP for attributes required by policy (ies) 3. The PDP uses the attributes found in the XACML 3.0 request, the attributes retrieved from the PIP, and the XACML 3.0 security policies to generate an access control decision 4. The XACML 3.0 response/access control decision is sent to DataPower 5. DataPower sends the XACML 3.0 response/access control decision to the requested PEP 6. PDP logs the access request and response |
| Sequence Diagram | <pre> sequenceDiagram participant PEP participant DataPower participant PDP participant PIP PEP->>PDP: 1. Sends request for authorization PDP->>PIP: 2. Queries for attributes PDP->>PDP: 3. Generate decision PDP->>DataPower: 4. Decision sent DataPower->>PEP: 5. Sends Decision to PEP PDP->>PDP: 6. Logs the event </pre> |
| Main Success Scenarios | Decision is generated and passed to PEP |
| Main Failure Scenarios | Policy is not found or attributes are missing and decision is not generated |

6.2.8 eSig Design

The VA business processes require that for many activities the nations Veterans, VA business partners and other persons of interest must provide signatures. The eSig activity provides the ability for users to submit a signature electronically when doing business electronically with VA.

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

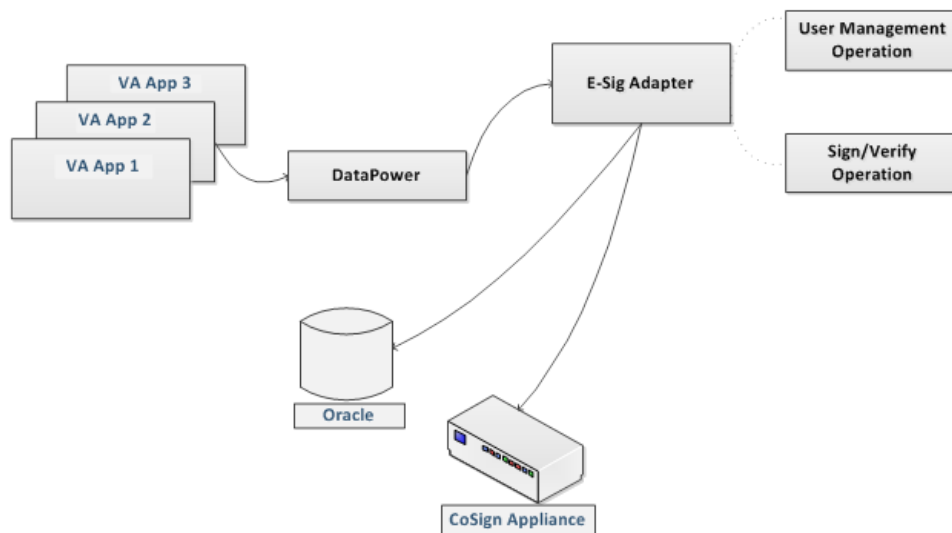


Figure 64: eSig Detailed Design

The eSig adapter will be implemented using a Servlet. This configuration will allow integration for both web based and machine to machine calls. The eSig adapter will utilize the façade design pattern which will allow the flexibility to add more classes and abstraction from various complexities that are likely to result in new integrations. With the façade approach, any changes to the CoSign appliance will not result in major changes on the eSig adapter. If the profile of the user instantiating a class becomes relevant in the future, the façade pattern will disallow certain function calls based on the profile. Since the request to the eSig adapter is stateless, many parallel instances of the Servlet and the façade class can be instantiated. This will be imperative as the design is optimized in terms of scaling out.

The request from the end application is completely decoupled from the CoSign appliance and hence more controls can be built before the request reaches the CoSign appliance. This is imperative because the CoSign appliance has no access control list and no security inherent capabilities other than the password for the public private key pair. The functionality is similar to the Chain of Responsibility pattern but façade pattern is preferred for other reasons listed above.

Visible Signature:

The visible signature will include the signer's common name on the left side of the signature box, followed by the common name, with the email address under the common name (if supplied), and the reason (if supplied) under the email address, and with the signature date and time with GMT offset value positioned under the reason on the right side of the signature box.

Example:



6.2.8.1 User Management – Sign Document

| Field | Description |
|----------------|---|
| Use Case Name | User Management – Sign Document |
| Description | This Use Case describes the process through which a User signs a document electronically. |
| Actors | <ol style="list-style-type: none">1. Signing user2. DataPower3. eSig Adapter4. ARX CoSign5. Oracle RAC |
| Pre-Conditions | The document allows electronic signature to be captured. |
| Trigger | The user authenticates to the VA application and clicks to signs a document electronically. The VA application sends the request to eSig for signing. |
| Actions | <ol style="list-style-type: none">1. DataPower intercepts the signature request from the user and sends it to the eSig Adapter.2. Upon receipt, the ARX CoSign device checks to see whether the user exists.3. If the user exists:<ol style="list-style-type: none">3a) ARC CoSign returns the user information3b) The eSig Adapter compares the CN3c) The eSig Adapter updates the user information in the ARX CoSign3d) The eSig Adapter logs the sign event with the Oracle RAC4. If the user does not exist, eSig Adapter generates and stores the encrypted password and user data.5. The eSig Adapter signs the document and sends the success response to ARX CoSign.6. The eSig Adapter logs the sign event and returns results to DataPower. |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram participant DP as DataPower participant EA as eSig Adapter participant ARX as ARX CoSign participant ORAC as Oracle RAC DP->>EA: 1. Sign Request EA->>ORAC: 2. Check if User Exists alt If user exists ORAC-->>EA: 3. Retrieve user info EA->>EA: 4. Compare the CN EA->>ARX: 5. Update user info EA->>ORAC: 6. Log sign event else If user does not exists EA->>ARX: 3. Generate & store password and user data EA->>ARX: 4. Sign the document ARX-->>EA: SuccessResponse EA->>ORAC: 5. Log sign event end ORAC->>DP: 6. Return Results </pre> <p>The diagram illustrates the electronic signature process involving four components: DataPower, eSig Adapter, ARX CoSign, and Oracle RAC. The process begins with DataPower sending a '1. Sign Request' to the eSig Adapter. The eSig Adapter then sends '2. Check if User Exists' to Oracle RAC. A green dashed box indicates the 'If user exists' path, where Oracle RAC returns '3. Retrieve user info' to the eSig Adapter, which then performs '4. Compare the CN' (self-call), sends '5. Update user info' to ARX CoSign, and finally sends '6. Log sign event' to Oracle RAC. A red dashed box indicates the 'If user does not exists' path, where the eSig Adapter sends '3. Generate & store password and user data' to ARX CoSign, followed by '4. Sign the document' to ARX CoSign. ARX CoSign returns a 'SuccessResponse' to the eSig Adapter, which then sends '5. Log sign event' to Oracle RAC. Finally, Oracle RAC sends '6. Return Results' back to DataPower.</p> |
| Main Success Scenarios | The electronic signature is captured and provided on the document. |
| Main Failure Scenarios | The electronic signature fails and is not captured on the document. |

6.2.8.2 User Management – Verify Document

| Field | Description |
|----------------|---|
| Use Case Name | User Management – Verify Document |
| Description | This Use Case describes the process through which a signed document is verified |
| Actors | <ol style="list-style-type: none"> 1. DataPower 2. eSig Adapter 3. ARX CoSign 4. Oracle RAC |
| Pre-Conditions | The document being verified was previously signed with eSig. |

| Field | Description |
|------------------------|---|
| Trigger | An already signed document is presented for verification. |
| Actions | <ol style="list-style-type: none"> 1. DataPower intercepts a request to validate a signature and sends it to the eSig Adapter. 2. Upon receipt, the ARX CoSign device checks to see whether the user exists. 3. The eSig Adapter verifies the signature against the ARX CoSign data 4. ARX CoSign verifies the signature 5. The eSig Adapter logs the verify event with the Oracle RAC 6. The eSig Adapters returns success to DataPower. |
| Sequence Diagram | <pre> sequenceDiagram participant DP as DataPower participant eSig as eSig Adapter participant ARX as ARX CoSign participant ORAC as Oracle RAC DP->>eSig: 1. Sign Request eSig->>ORAC: 2. Check if User Exists ORAC-->>eSig: eSig->>ARX: 3. Verify the signature ARX-->>eSig: 4. Verification response eSig->>ORAC: 5. Log verify event ORAC-->>eSig: eSig-->>DP: 6. Return Results </pre> |
| Main Success Scenarios | The electronic signature is verified and response is sent to requestor. |
| Main Failure Scenarios | The electronic signature is not valid. |

6.2.9 CAR Design

The CAR activity consolidates monitoring and audit reporting to a single solution for multiple AcS activities. The CAR activity is based on the User Activity Reporting Module (UARM) COTS and integrates with the following AcS activities:

- Credential Service Provider (CSP)
- Identity Proofing (IP)
- Provisioning (PROV)
- Specialized Access Control (SAC)
- Single Sign-On – Internal (SSOi)
- Electronic Signature (eSig)
- Virtual Directory Store (VDS)

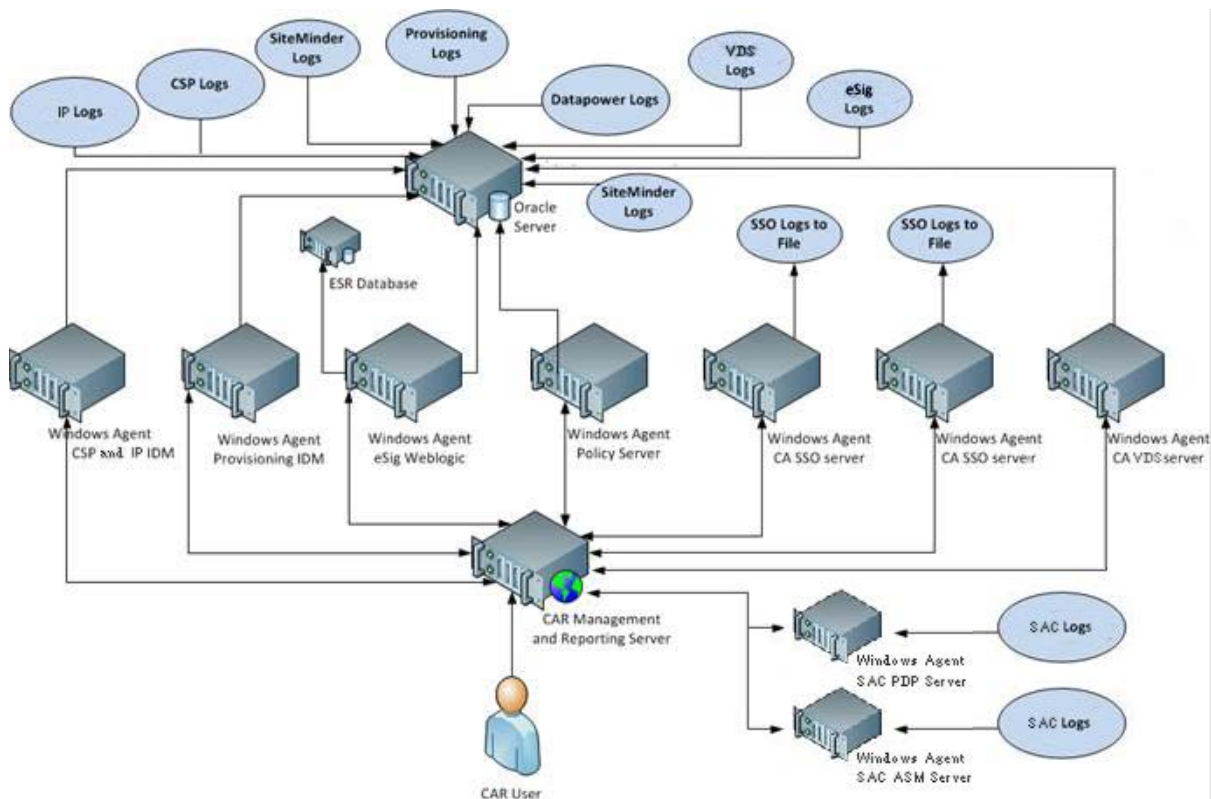


Figure 65: CAR Detailed Design

The CAR activity architecture contains agents and server communications where agents would be deployed on the destination systems that invoke a connector that is designed to recognize a specific log pattern and normalize into a common event grammar format that is stored on UARM collector server.

- **Agent and Server Communications:** Agent collects the normalized events in to its queue. The queue manager then sends the normalized events to the UARM collector server using dispatcher service.
- **Connectors:** Current implementation of UARM would be using three out-of-box connectors (i.e., CA IdentityMinder, CA SiteMinder, CA SSO and three custom connectors for Axiomatics, ARX CoSign, and ESR)
- **Connector Data Mapping File:** Data mapping file would defining global definition and provide the output as the normalized events.
- **Connector Parser File:** Parser would be disassembling the raw events and normalizing this information to common event grammar.
- **Oracle Connectors:** The connectors for Oracle audit source use ODBC connections to connect and fetch audit events.

6.2.9.1 Process Activity Logs to generate reports

| Field | Description |
|------------------------|--|
| Use Case Name | Process Activity Logs |
| Description | This Use Case describes the process through which CAR will consume and process the data from the audit logs to generate reports. |
| Actors | <ol style="list-style-type: none"> 1. Agent 2. Connector 3. UARM Connector 4. Oracle RAC/File Log |
| Pre-Conditions | The AcS activities has captured the audit logs and CAR is setup to connect with audit log store |
| Trigger | The audit logs connector is invoked by the AcS activity agent. |
| Actions | <ol style="list-style-type: none"> 1. The agent invokes the connector. 2. The agent makes an ODBC connection to the Oracle RAC to obtain the audit file. 3. The Oracle RAC returns the raw audit file data 4. The connector normalizes the data 5. The connector submits the data to the collection queue 6. The agent executes the Dispatcher Service and sends the data to the UARM Collector for generation of reports. |
| Sequence Diagram | <pre> sequenceDiagram participant Agent participant Connector participant UARM Connector participant Oracle RAC/File Log Agent->>Connector: 1. Invokes Connector Connector->>Oracle RAC/File Log: 2. Makes ODBC connection Oracle RAC/File Log-->>Connector: 3. Retrieve the Raw Audit Logs Connector->>Connector: 4. Normalize the events Connector->>Collection Queue: 5. Collection Queue Agent->>UARM Connector: 6. Dispatcher Service </pre> |
| Main Success Scenarios | The Management and Reporting server uses the internal UARM logs to provide the ad-hoc and standard reports/alerts. |
| Main Failure Scenarios | No Audit Logs are retrieved to generate reports. |

6.2.10 Product Perspective

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

6.2.10.1.1 User Interfaces

Refer to section 3.2.3 for information on user interfaces.

6.2.10.1.2 Hardware Interfaces

Refer to section 6.1 for information on hardware configurations and interfaces.

6.2.10.1.3 Software Interfaces

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

6.2.10.1.4 Communications Interfaces

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

6.2.10.1.5 Memory Constraints

This section is not applicable to the AcS solution.

6.2.10.1.6 Special Operations

This section is not applicable to the AcS solution.

6.2.10.2 Product Features

The AcS solution is based on the foundation of CA COTS products. The table below describes the AcS solution products.

Table 31: AcS Solution Products

| # | Software | Description |
|---|----------------------------------|---|
| 1 | CA IdentityMinder | A scalable, configurable identity management solution that automates on-boarding, modification and off-boarding of users, enables self-service requests and automates proactive identity compliance processes. |
| 2 | CA SiteMinder Web Access Manager | SiteMinder Web Access Manager is a web access management system that enables user authentication and secure Internet SSO (single sign-on), policy-driven authorization, federation of identities, and auditing of access to the web applications it protects. |

| # | Software | Description |
|---|--|--|
| 3 | CA Directory | <p>CA Directory provides directory services and security for online applications for organizations. For example, it enables customers to access their electronic accounts; employees can access critical business data.</p> <p>This product is generally considered a highly scalable and distributable implementation of directory services, including security services (e.g., authentication).</p> <p>CA Directory is supported on a variety of Windows and UNIX platforms, as well as 64-bit operating systems such as Linux 64, Solaris 10/Intel 64, UltraSparc 64, IBM Power5 64 and HP-UX Itanium 64.</p> <p>CA Directory supports open standards including: LDAP (and related RFCs), X.500 (DAP, DSP, DISP), Security (SSL, TLS, password hashes), Management (SNMP and related RFCs), Network (IPv6, RFC1006), and US Federal Government standards (FIPS 140-2, Common Criteria EAL3, and Section 508).</p> |
| 4 | WebLogic | <p>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).</p> <p>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 Health_eVet (MHV) and the Clinical Information Support System (CISS) are deployed with WebLogic Portal.</p> |
| 5 | 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 | CA Single Sign-On | CA Single Sign-On improves security and simplifies user access by automating login to applications through a single authentication. This enables implementation of stronger security practices without burdening users with remembering multiple username and password combinations. |
| 7 | CA User Activity Reporting Module (UARM) | CA User Activity Reporting Module is a high-performance log management solution. |

| # | Software | Description |
|----|--------------------------------|---|
| 8 | Axiomatics | The Axiomatics Policy Server (APS) is a powerful access control system that allows users to manage, simulate and enforce fine-grained policies written in the eXtensible Access Control Markup Language (XACML). The Axiomatics Policy Server (APS) provides a full-fledged, XACML-based authorization service. The components are managed from a central point, the Axiomatics Services Manager (ASM). |
| 9 | Radiant Logic | Radiant Logic acts as a virtual user store from multiple endpoints. It has evolved into an easy-to-use, enterprise-grade solution for stronger authentication and richer authorization. |
| 10 | SailPoint – Compliance Manager | A centralized access governance tool which streamlines the execution of compliance controls and improves audit performance through automated access re-certifications, role and policy management. |

6.2.10.3 User Characteristics

Refer to section 1.9 and section 3.1.4 for user-related information.

6.2.10.4 Dependencies and Constraints

Refer to section 1.7 and section 2.3 for AcS solution constraints and dependencies.

6.2.11 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 section 1.4 in Table 4 above.

6.3 Communications Detailed Design

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

7 External Interface Design

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

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

7.1 Interface Architecture

7.1.1 VA CSP Federation with VAAFI

The CSP activity interfaces with VAAFI via SSOi service where CSP asserts identity credentials using SSOi to VAAFI via the SAML Web SSO Profile, HTTPS POST binding. The following diagram depicts the high level flow of an authentication event between VAAFI and CSP (via SSOi).

In the following diagram, VAAFI is the Service Provider; CSP using SSOi is the Identity Provider; the User Agent is the web browser of the user accessing the VAAFI protected applications.

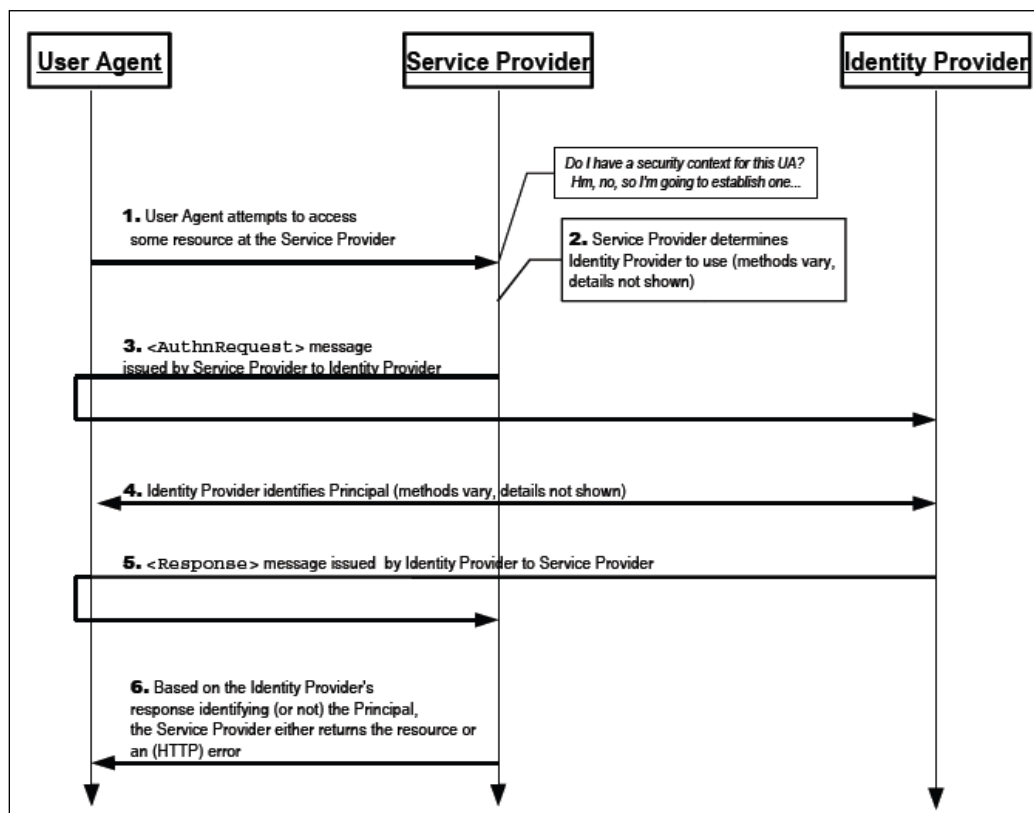


Figure 66: CSP to VAAFI Interface Flow

7.1.2 Master Veteran Index

The AcS activities will integrate with the Master Veteran Index (MVI) by making calls to the MVI web service as defined in the MVI Service Design document. Web service calls consist of SOAP messages submitted over HTTPS. Communication between MVI and IP occurs via VAAFI as a web service proxy. Permit/deny decisions based on application requests are implemented as a set of pre-built, properly-formatted SOAP/XML statements. The following diagram describes the high level interface structure.

The Provisioning activity integrates with MVI for the following functions:

- Add PersonUpdate Person
- Search Person by Traits
- Retrieve Person by Source ID
- Get Corresponding IDs by Source ID

The IP activity integrates with MVI for the following functions:

- Get Corresponding IDs by ICN
- Update Person (correlation)

- Add Correlation

The following diagram depicts the high-level integration of MVI with AcS activities.

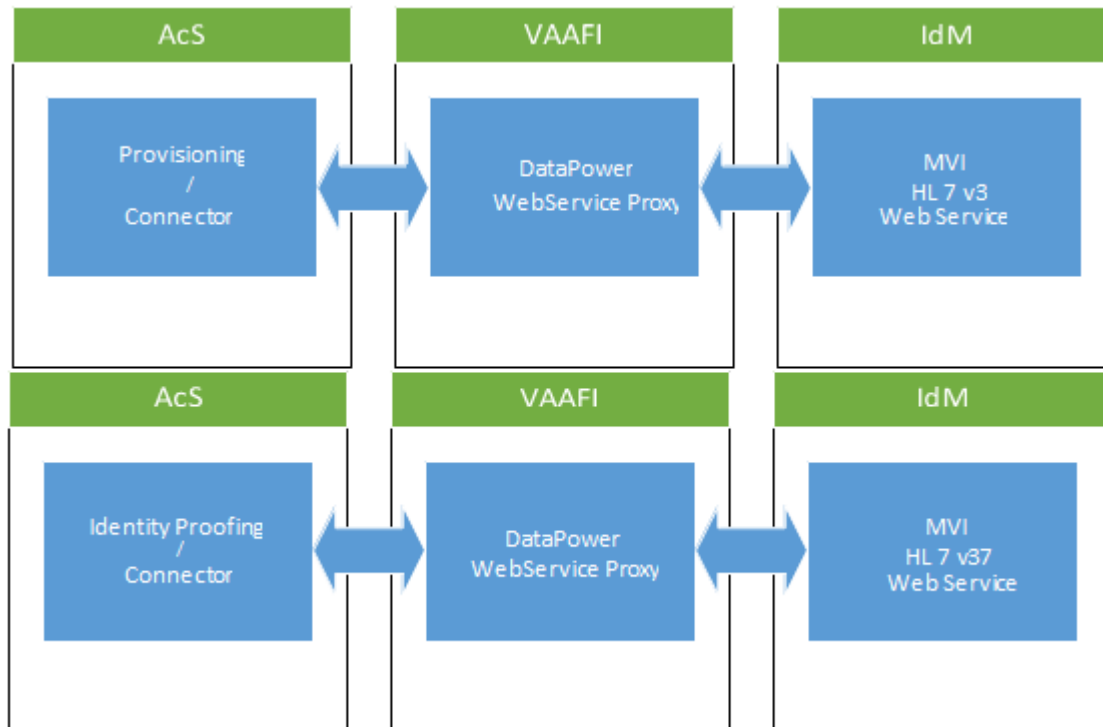


Figure 67: MVI Interface Flow with Provisioning and IP

7.1.3 VA Active Directory

The integration between the Provisioning activity and VA Active Directory (AD) is mandated by several contract documents, including the AcS Increment 2 and Increment 3 RSDs, Provisioning Integration to Active Directory (AD) and Personal Identity Verification (PIV) System iRSD, version 1.2 from May 2013, and 2013 IAM VRM Business Requirements Document (BRD). The integration structure follows the process models (specific to AD) identified in the CRISP ProPath Onboarding and Offboarding sequences. The following diagram depicts the high-level interface structure.

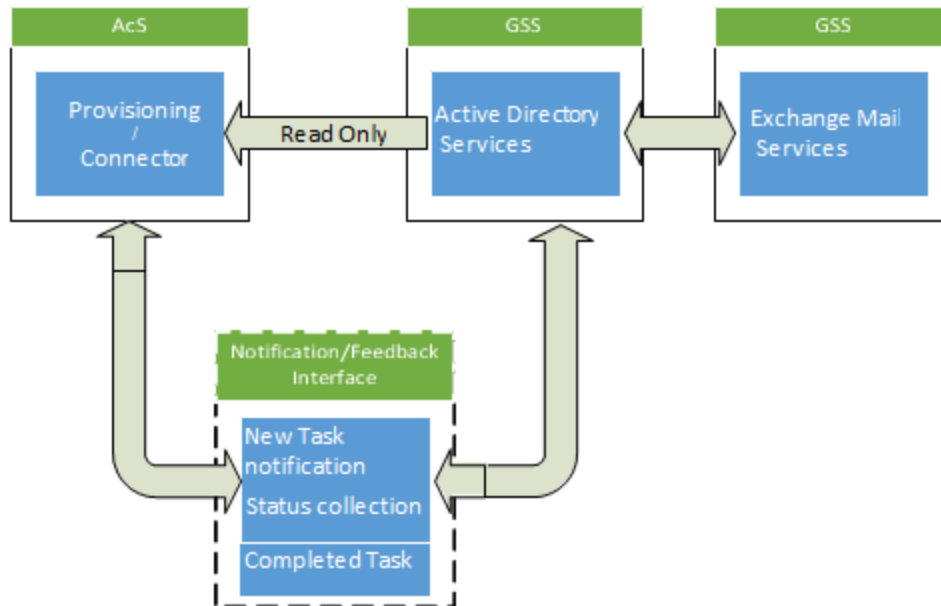


Figure 68: Provisioning – Active Directory Interface Architecture

7.2 Interface Detailed Design

7.2.1 VA CSP Federation with VAAFI

CSP integrates with the VAAFI solution to provide federated authentication of both Level 1 and Level 2 credentials to VA application using Security Assertion Markup Language (SAML) mechanisms. The VAAFI solution is responsible for integrating VA applications to utilize the CSP credential. CSP solution uses SiteMinder federation option pack to construct the SAML, encrypt the content, sign and post it to VAAFI over secure channel.

SSOi is also integrates with VAAFI as service provider method through which VAAFI acts as authentication broker for external users who needs to have access to SSOi resources. VAAFI will authenticate the user and reassert the user attributes in SAML assertion mechanism and present to SSOi proxy layer through which it will consume the assertion and provide the seamless access to the user. The details of the flow are described in section 6.2.2.2.

VA CSP (as CSP/IdP) sending SAML to VAAFI

| | |
|-------------------------------------|---------------------|
| SPID: | [REDACTED] |
| SiteMinder Affiliate Domain: | CSPFederationDomain |
| NameID: | UID |
| Authn Director: | CSP User Directory |
| Encryption Algorithm: | [REDACTED] |
| SLO: | NA |
| Attribute Details: | givenName |

| | |
|-----------------------------|--|
| | sn UID [REDACTED] |
| Signature Algorithm: | [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] |

7.2.2 Master Veteran Index

Section 6.2.1 and section 6.2.6 describe the communication flow with the Master Veteran Index (MVI) for the Provisioning and IP activities.

7.2.3 VA Active Directory

Active Directory: The user details from VA Active Directory are provided to Provisioning service using a daily feed file update. The task is configured on Provisioning to consume the feed file provided at a scheduled time. The user accounts will be correlated to the Provisioning CA IdentityMinder global user based on samAccountName. Additionally, email-based provisioning is setup as part of user onboarding to onboard users to VA Active directory manually. The details of the flow are described in section 6.2.1.

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>
- IBM support site: <https://www.ibm.com/support>
- Radiant Logic site: <http://www.radiantlogic.com>
- Axiomatics site: <http://www.axiomatics.com>
- SailPoint site: <http://www.sailpoint.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 AcS 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.
- SSOi error codes
 - Regular Siteminder Integration /Proxy Based Integration
 - OnAuthAttempt (User not found) – Redirect to failedlogin.aspx
 - OnAuthReject (User enters invalid credentials) – Redirect to failedlogin.aspx
 - OnAccessReject (User not Authorized to access resource) – Redirect to failedlogin.aspx
 - Server Error (500,401,403) – Graceful handling not implemented currently
 - IdleTimeout – Forward to Login Page
 - Federation: As Service Provider
 - User Not Found – Redirect to failedlogin.aspx
 - Invalid SSO Message – Redirect to failedlogin.aspx
 - Unaccepted User Credential (SSO Message) – Redirect to failedlogin.aspx
 - Server Error – Graceful handling not implemented currently
 - Invalid Request – Graceful handling not implemented currently
 - Unauthorized Access – Redirect to failedlogin.aspx
 - Federation: As Identity Provider
 - Server Error – Graceful handling not implemented currently
 - Invalid Request – Redirect to login page
 - Unauthorized Access – Redirect to failedlogin.aspx

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 8.4 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 AcS:

- PDF

- Comma Separated File (CSF)
- Excel

8.4 Navigation Hierarchy

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

8.4.1 CSP

CSP supports credential management, self-service, and administrator functions. The following diagram depicts the flow for CSP.

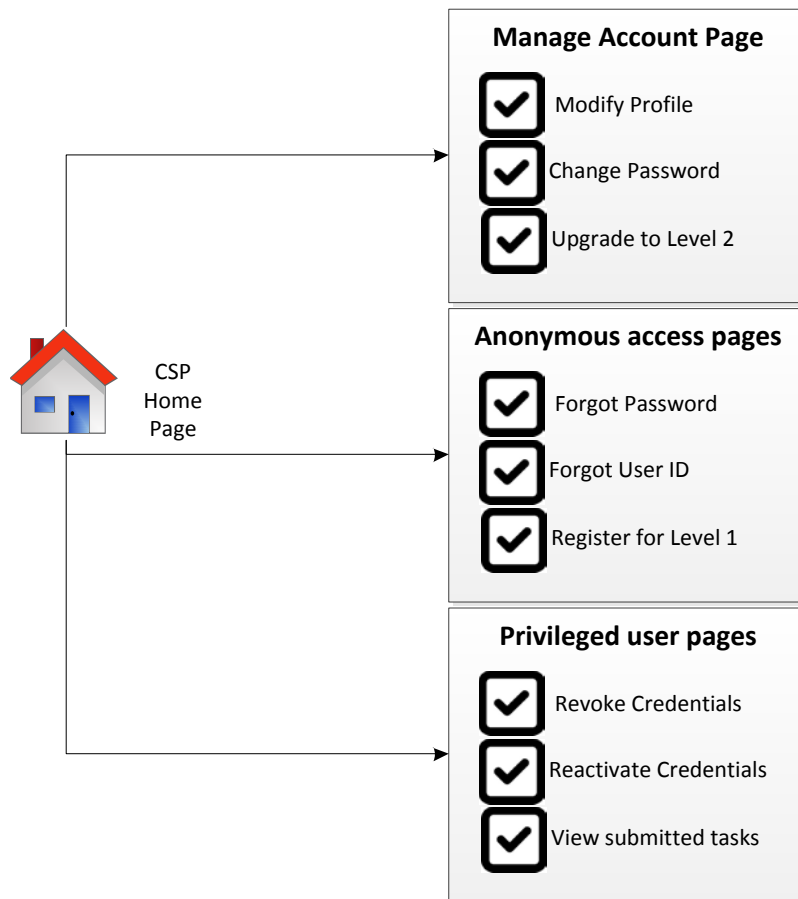


Figure 69: CSP Navigation Hierarchy

The CSP application enables users to login to CSP, register for accounts, modify credential information, and retrieve forgotten User ID/password information. The CSP console displays a login screen for registered users, an icon for new users to register, and icons to retrieve forgotten User IDs or to reset forgotten passwords. The CSP console can be accessed directly by input of the URL or by a redirect from either VAAFI or from a business application. The CSP application is externally facing.

8.4.2 IP

IP supports IP and administrator functions. The following diagram depicts the flow for IP.

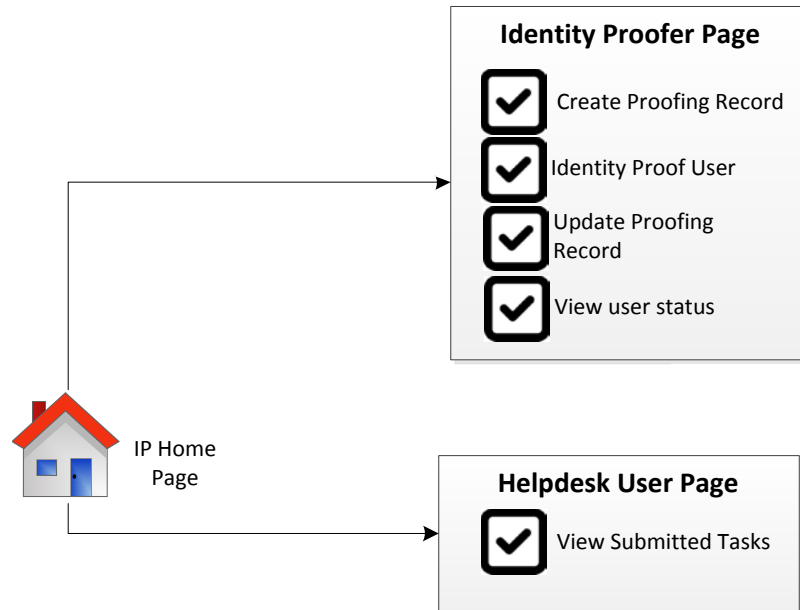


Figure 70: IP Navigation Hierarchy

8.4.3 Provisioning

The navigation hierarchy for Provisioning is depicted in the following diagram. The Provisioning pages require authentication and authorization to access them. Provisioning allows users to perform self-service for application account access and provides administration functions.

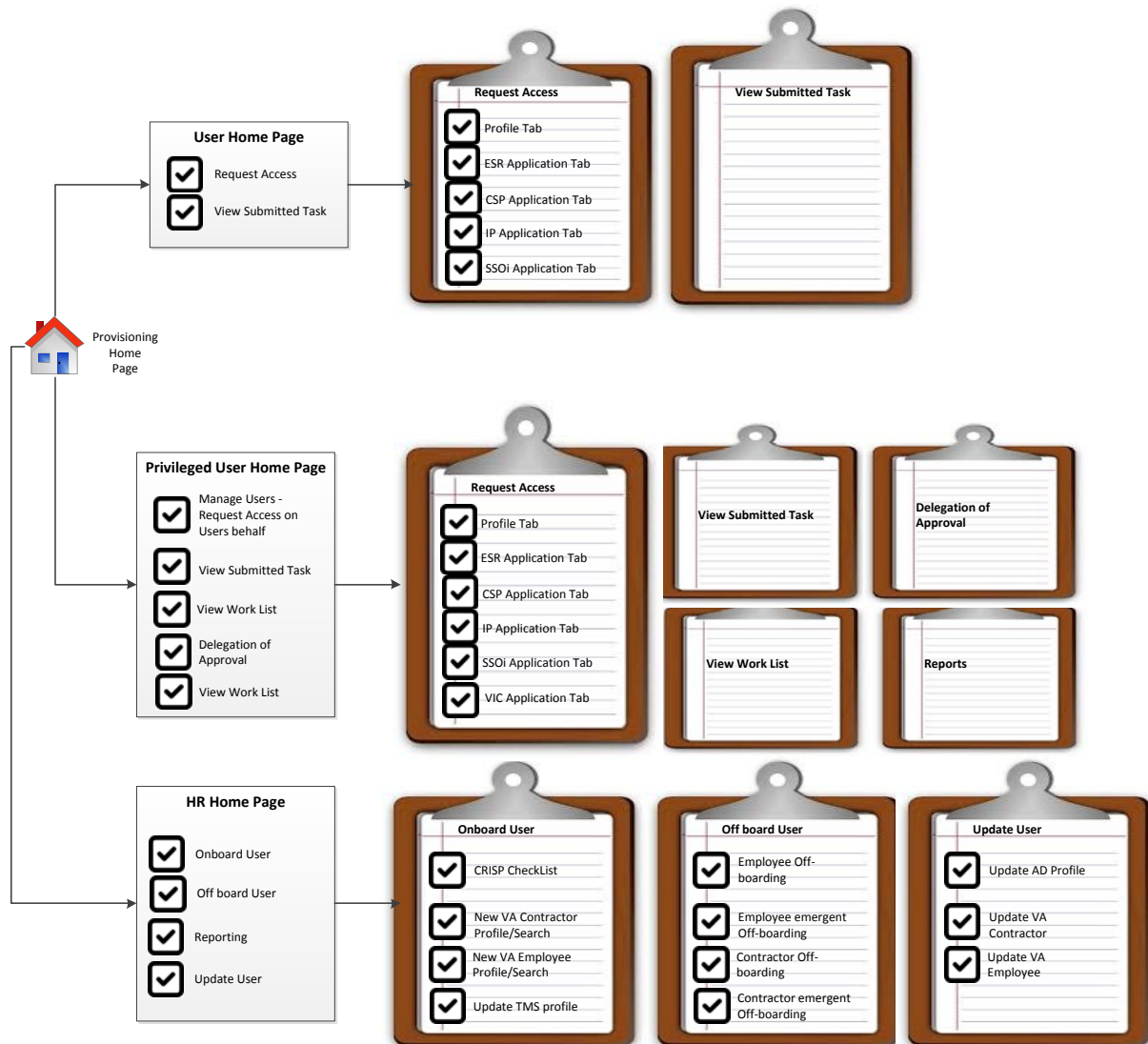


Figure 71: Provisioning Navigation Hierarchy

Upon successful authentication, a customized home page is displayed that restricts the view of information and functionality specific to the user's role.

Privileged Users may view a link to request access to submit provisioning requests. The Request access page has different tabs for each of the application requests and for the user's profile. The Privileged User may view a links to view submitted requests as well as requests pending for approval. The 'Delegation of Approval' link allows the privileged user to delegate approval to other individuals. Privileged users also have the ability to select a link to run and view reports.

9 System Integrity Controls

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 solution, 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 which 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.

Data at Rest:

The following table explains the “data at rest” points.

Table 32: Data Points and Security

| Data Points | Data Type | Explanation |
|--------------------|-----------------------------|--|
| Oracle | Sensitive | <ul style="list-style-type: none">• Stores the IdentityMinder objects- sensitive user attributes.• Stores the audit log for SiteMinder and needs to be secured, but not encrypted as there is no PII.• Stores the audit log for CA IDM and must be encrypted and secured for PII.• See vendor documentation for additional information regarding actual encryption algorithms used. |
| Directory | Sensitive | <ul style="list-style-type: none">• Stores encrypted SiteMinder policy data.• Stores SiteMinder/IdentityMinder user data. Only sensitive user attributes will be encrypted.• Provisioning server related objects and sensitive user attributes are encrypted.• See vendor documentation for additional information regarding actual encryption algorithms used. |
| File Store | Non-Sensitive/ Sensitive | <ul style="list-style-type: none">• IM is stored in a JMS data in file system and contains transactional data. It does not contain any sensitive information.• A FIPS encryption key file is stored in the file system. Access to the file should be restricted and enforced by setting the directory/file access permissions for specific groups and/or users. |

| Data Points | Data Type | Explanation |
|-------------|-----------|--|
| VDS | Sensitive | <ul style="list-style-type: none"> Stores PII data and other user data in clear text. VDS will store PII data in the format that the source system transmits. Both Provisioning and MVI will have to encrypt / one-way hash the data and VAAFI will have to decrypt the data upon receipt. Vendor does not support encryption/de-encryption of data. |

The security controls for the data at reset are managed through the encryption of sensitive attributes at the directory level for the AcS solution. The FIPS 140-2 encryption is applied on the identified PII and sensitive attributes stored in the AcS solution directory attributes. The following table provides the data types (refer to [section A.1](#) below for data type groupings) and who can make updates accordingly.

Table 33: Data Type and Updates

| Type | Provisioning System | CSP System | IP System |
|---------------------------|---------------------------------------|--------------------------------|--------------------------------|
| Identity Information | VA Authorized System (e.g., HRIS, AD) | End User | Privileged Users CSP System |
| User Information | VA Authorized System (e.g., HRIS, AD) | End User | Privileged Users CSP System |
| Provisioning Information | Privileged Users End Users | N/A | N/A |
| CRISP Checklist | Privileged Users | N/A | N/A |
| Access Control Attributes | N/A | Privileged Users | Privileged Users |
| CSP Information | N/A | Privileged Users CSP System | N/A |
| IP Information | N/A | N/A | Privileged Users IP System |

9.1 CSP and IP

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 CSP solution stores user record information required for Level 1 & Level 2 credentials whereas IP stores it 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. The user information is secured to require a valid CSP-recognized credential. 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 CSP and 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 CSP and 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 CSP/IP solution does not allow duplicate identification values. Users are required to confirm their accounts by following instructions emailed to them. Therefore, a CSP/IP user has their e-mail address verified prior to getting a Level 1 or Level 2 credential. CSP/IP has definitive roles established to fulfill each business process. 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.

9.2 eSig

The eSig service operates in a federated environment and requires that the user credentials that are being passed to it belong to an authenticated Level 2 or above user.

9.2.1 Confidentiality of Sensitive Information

The eSig service does not affect the user credential information stored within VA. No passwords are passed between user sessions. The reporting piece of eSig only records the events that occurred and does not affect any VA data.

9.2.2 Privacy of Personal Information

The eSig service does not store any sensitive PII of the user apart from the user id that is passed.

9.2.3 Process Integrity

The eSig service only allows for machine to machine sessions. The machine sessions are authenticated using the DataPower devices. The WebLogic servers only accept requests that are received through DataPower. The CoSign device is located within the internal VA network and is only accessible via the web service calls from the WebLogic servers.

9.2.4 System Availability

The eSig solution implementation is highly available and provides controls to minimize system failures, and access control to minimize man-made failures. The eSig service has software

failover capability available within the CoSign product configuration, and shall also be supported by the DR environment.

9.3 SAC

The SAC service interface is a web service running behind the DataPower appliance which is a hardened hardware appliance used for XML protection. For the purpose of SAC, system integrity controls have been established with simplicity as a core element. SAC only allows access to those with valid VA certificates and over SSL/TLS for encryption.

9.3.1 Confidentiality of Sensitive Information

Mutual authentication has been enabled that limits requestors to those that hold valid VA issued certificates. This requires that both parties identify with one another and provides for nonrepudiation, where neither party can deny communicating with one another. SAC leverages existing VA verification and approval processes for issuing certificates and the certificate that SAC uses for SSL communication is issued from VA certificate authority.

The interface is configured to only use SSL v3.0 and TLS 1.0 and later. It will reject requests that use SSL v2.0 or older, or attempt access with an unrecognized version of SSL.

9.3.2 Privacy of Personal Information

The SAC service does not store any sensitive PII of the users.

9.3.3 Process Integrity

The system is designed to provide authorization services. The DataPower appliance performs schema validations on incoming XML requests and other XML threat reduction capabilities before passing the requests to the Axiomatics PDPs. Only two responses permit or deny, are sent back to the client.

9.3.4 System Availability

The SAC service is highly available and provides controls to minimize system failures, and access control to minimize man-made failures. The SAC service shall have failover capability supported by the DR environment.

9.4 Provisioning

The Provisioning service only allows access to authenticated and authorized users. Provisioning configures user authentication according to federal and VA security policies. Provisioning integrates with the CAR service for auditing and reporting. The auditing data is compiled and made available via the reporting servers. Provisioning implements integrity controls align with VA and Federal security standards.

9.4.1 Confidentiality of Sensitive Information

The Provisioning service stores user profile and authentication information required for authentication and authorization. Additionally, provisioning stores Personally Identifiable

Information (PII) such as Social Security Number, date of birth, and other personal identifiers. This information is stored encrypted. Provisioning stores the user password in an encrypted format in CA Directory. The transmission of information occurs over an SSL channel.

9.4.2 Privacy of Personal Information

The AcS Provisioning service collects and stores a wide range of identity data within its identity store(s) and manages several user account endpoints (e.g., ESR, CSP, TMS). PII is collected by Provisioning during a person's participation in the CRISP onboarding processes. The PII is then stored within the Provisioning user stores and the applicable endpoints. Provisioning provides security controls, such as data at rest (database and directory store encryption services), communication confidentiality and integrity controls (data in motion) when exchanging data as part of its operations as well as authorization/access control to specific data components, to enforce only authorized individuals with a need to know and proper access are granted rights to view/modify users' identity record (including PII).

9.4.3 Process Integrity

The Provisioning service is designed to provide authentication and authorization services. The user authentication credentials are collected and validated. The user is only granted access to data and functionality that the user is authorized to access. The solution also provides user management capabilities. The user management workflows and authorizations are only accessible to authenticated and authorized user administrators.

9.4.4 System Availability

The Provisioning service implementation is highly available and provides controls to minimize system failures, and access control to minimize man-made failures.

9.5 SSOi

The SSOi service only allows access to authenticated users. SSOi configures user authentication according to federal and VA security policies. The SSOi service integrates with the CAR framework for auditing and reporting. The system stores authentication information only, no additional sensitive and PII is stored. SSOi implements proper access control to secure the user information.

9.5.1 Confidentiality of Sensitive Information

The SSOi Service CA SSO toolset stores user profile and authentication information required for authentication only, and does not store any additional sensitive PII in CA Directory. The user password is stored in an Advanced Encryption Standard (AES) 256 encrypted/hashed format in CA Directory. The transmission of information occurs only over an SSL channel. The user information is secured using proper access control implementation. CA SiteMinder does not store user information; it connects to the appropriate user store to fetch the information.

9.5.2 Privacy of Personal Information

The SSOi service does not store any Personally Identifiable Information (PII) of the user.

9.5.3 Process Integrity

The SSOi service is designed to provide authentication services. The user authentication credentials are collected and validated. The user is only granted access to data and functionality that they are authorized to access.

9.5.4 System Availability

The SSOi service implementation is highly available and provides controls to minimize system failures, and access control to minimize man-made failures.

9.6 CAR

The CAR service does not have the permission to alter any information contained in other components of the IAM solution. Rather, it has a read only access and therefore the risk is very low. The CAR service will come pre-equipped with a car admin account already created. The credentials will be provided to VA staff acting as the CAR admin that will then create further users (privileged and regular) as necessary. The access by these users is monitored as well. Moreover, UARM self-monitors its own activity and logs are stored in secure and non-repudiated fashion.

9.6.1 Confidentiality of Sensitive Information

The CAR service is not exposed to any external network and the transmission of information occurs on SSL channel. The user information is secured using proper access control implemented.

9.6.2 Privacy of Personal Information

The system for the CAR solution does not intentionally store Personally Identifiable Information (PII). However, it could process PII data if it is contained in the collected logs/events. In this scenario, PII of the user is stored. Data in transit is FIPS mode encrypted. UARM admin users are stored internal directory and password for them is encrypted and maintained by COTS product.

9.6.3 Process Integrity

The system is designed to provide validation for input forms before submission and storing the information for the user record. No information is entered by the end user other than the user credentials when the administrators are creating new accounts. The CAR service provides proper processing controls such as making sure same user ID is not issued to two users and maintaining the uniqueness of IDs. Additionally, with the full auditing of transactions, any misuse of authority is discernible and traceable in the audit logs/reports.

9.6.4 System Availability

The CAR solution implementation for system is highly available with UARM supporting HA and does provide controls to minimize system failures, access control to minimize man-made failures. VA IAM System Design contains detailed description of the HA architecture for the CAR solution.

The UARM supports HA in virtual environment through VMware High Availability (VMware HA). UARM supports the VMware HA features except Fault Tolerance for EEM. The following are the advantages of enabling UARM HA:

- Physical failure of an ESX server does not affect the installation and configuration of the ESX server, as the failed ESX server is automatically restarted on other ESX servers in the virtual environment cluster.
- Data loss is minimal allowing CA User Activity Reporting Module to seamlessly collect most of the generated events.

In addition to the above measures, the CAR service has also been designed to meet the Federal Government standards and VA security policies. The internal communications between various UARM components are FIPS compliant.

9.7 Virtual Directory Service (VDS)

The VDS grants access to authenticated and authorized users. VDS configures authentication according to federal and VA security policies. VDS integrates with the CAR service for auditing and reporting. The auditing data is compiled and made available via the reporting servers. Provisioning implements integrity controls align with VA and Federal security standards.

9.7.1 Confidentiality of Sensitive Information

The VDS stores consumer authentication information required for authentication and authorization. Consumer password information is stored encrypted in a local VDS data store with an ACI that prevents unauthorized access. The transmission of information occurs over an SSL channel. VDS DSML Web Service is protected by DataPower, which provides the System-to-System authentication and coarse grained authorization through inspection of the client certificate provided during the initial client –to –service handshake. Additionally, a user ID and Password type credential is passed as part of the SOAP / HTTP headers during the client payload request submission. The UserID/Password is used for fine-grained authorization and access control, enforced by the Radiant Logic product. The combined connection channel security approach ensures confidentiality of the connection and enforces the necessary access / authorization controls to ensure only authorized clients are provided access and only to the information they are authorized to view

9.7.2 Privacy of Personal Information

The VDS does not collect nor does it maintain any persistent (disk based) stores of PII data. VDS provides communication confidentiality and integrity controls (data in motion) when exchanging data as part of its operations as well as authorization/access control to specific data components.

9.7.3 Process Integrity

The VDS is designed to provide an attribute exchange of authoritative person attributes to authenticated and authorized consumers. The consumer authentication credentials are collected and validated. The consumer is only granted access to data for which the user is authorized to access. VDS does not support users (persons) directly, VDS consumers are other systems or applications in proxy for users.

9.7.4 System Availability

The VDS implementation is highly available in the production environment and provides controls to minimize system failures, and access control to minimize man-made failures.

9.8 Role Manager

Role Manager service only allows access to authenticated and authorized users to be able to use the tool to perform access governance activities. The Role Manager service does not have the permission to alter any information contained in other components of the IAM solution. Rather, it has a read only access to a VA application, CA LDAP and therefore the risk is low.

9.8.1 Confidentiality of Sensitive Information

The Role Manager service stores user profile from the CA LDAP repository required for authentication and authorization. No Personally Identifiable Information (PII) such as Social Security Number, date of birth, and other personal identifiers are stored in the database. The authoritative user information such as name, title, location etc. is stored encrypted in the Role Manager database. The transmission of information also occurs over an SSL channel.

9.8.2 Privacy of Personal Information

The Role Manager service does not store any Personally Identifiable Information (PII) of the user.

9.8.3 Process Integrity

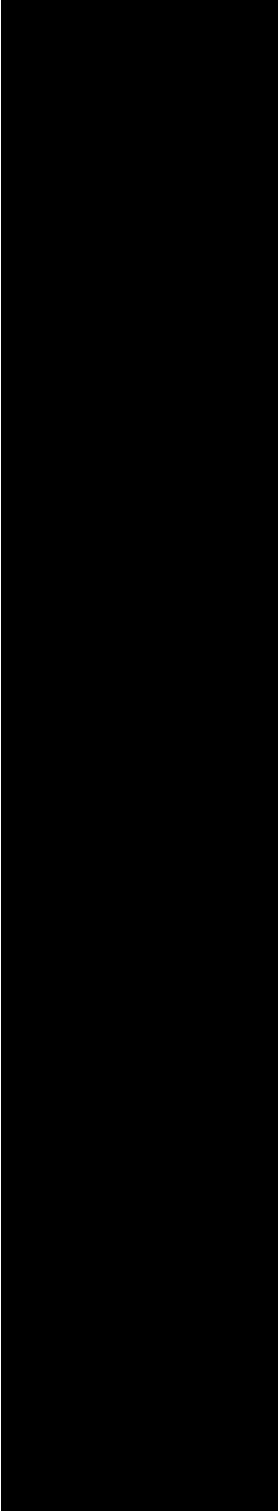
The Role Manager service is designed to provide authenticated users access to governance services. The user is only granted access to data and functionality with the capability that they are authorized to access. These custom capabilities are assigned to end users within the tool. The solution also provides management capabilities such as configurations of access reviews, role mining, auditing and reporting services. The management services are only accessible to system administrators.

9.8.4 System Availability

The Role Manager service implementation is highly available and provides controls to minimize system failures, and access control to minimize man-made failures. The Role Manager service is an independent service with minimal impact on any other ACS services.

10 Approval Signatures

The signature below is an acknowledgement that the signatory understands the purpose and content of this document.



04/29/2014

grated Project Team Chair and Business Sponsor

Date

04/18/2014

Business Sponsor

Date

04/17/2014

M Program Manager

Date

04/17/2014

AcS Program Manager

Date

05/30/2014

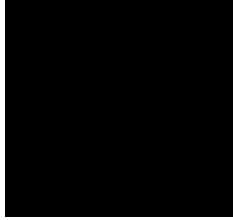
Chief Architect

Date

04/17/2014

Enterprise Architecture

Date



SDE

05/12/2014

Date

A. Additional Information

Additional information that supplements the design specification is provided in the following sections.

A.1. Data Dictionary

The following spreadsheet provides detailed data model for Provisioning, CSP, and IP activities:



ACS Data
Elements.xlsx

A.2. CRISP Onboarding/Offboarding Attributes

The following list provides the required/optional attributes for employees/contractors/HP trainees/volunteers:



Emp Cont HPT Vol
Attributes.docx

A.3. RTM

Refer to section 1.4 for a complete list of requirements documents that are applicable to the AcS solution.

A.4. 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.5. Design Metrics

The design for IAM services is calculated based on requirements from PWS, BRD and CSP population estimates provided by VA. The CSP population estimate spreadsheet is attached below.



VA CSP User
Population Estimates.

A.6. Acronym List and Glossary

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

A.7. Required Technical Documents

Refer to the CA vendor support/web site for detailed product documentation.

A.8. CSP Class Diagram

The CSP.NET wrapper class diagram is shown below.

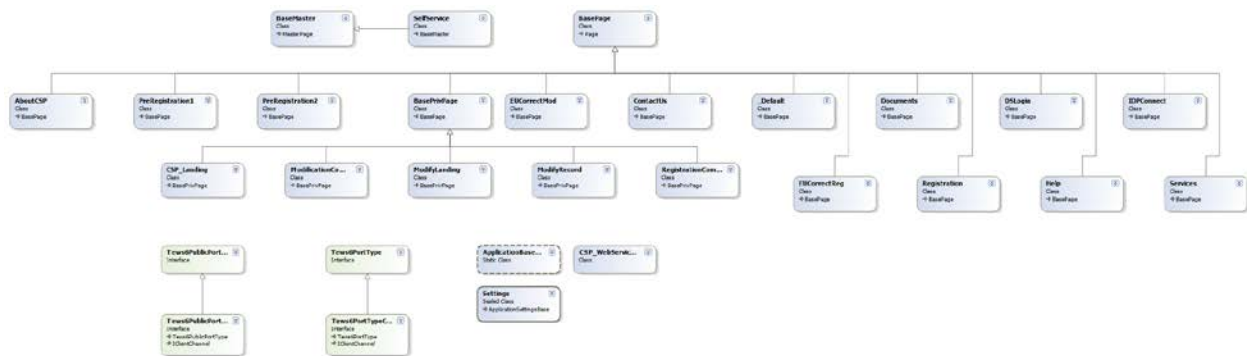


Figure 72: CSP Class Diagram

A.9. IP Class Diagram

The IP.NET wrapper class diagram is shown below.

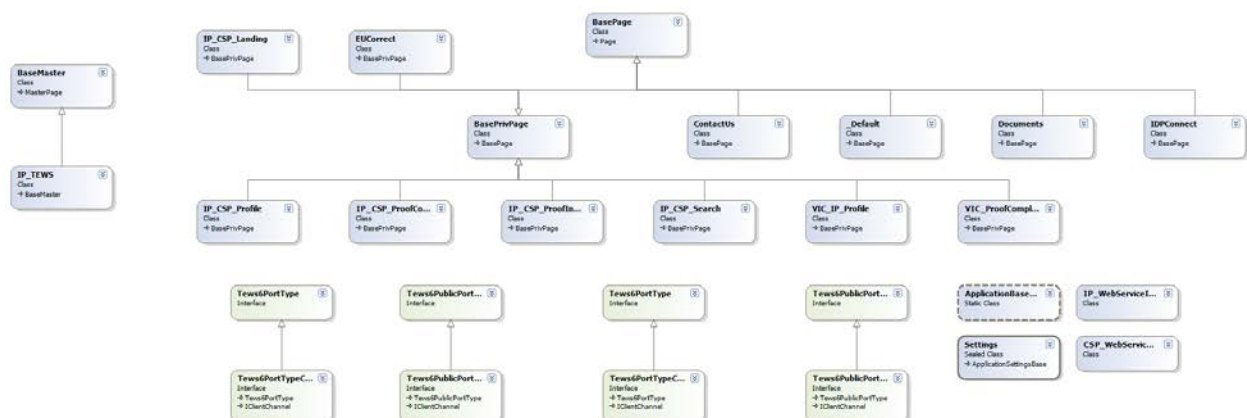


Figure 73: IP Class Diagram

A.10. Responses to Produce WS-Security Headers

| Field | Description |
|------------------|--|
| Use Case Name | Responses to Produce WS-Security Headers |
| Description | This use case describes the process by exchanges which SiteMinder generates and manages WS security headers. |
| Actors | <ol style="list-style-type: none"> 1. Users 2. Client 3. Web Service |
| Pre-Conditions | A valid attribute service end point from VDS which provides a response with set of attributes for a request sent by SiteMinder |
| Trigger | Client access web service endpoint protected by SOA agent |
| Actions | <ol style="list-style-type: none"> 1. Client sends WS SOAP request to web service end point 2. SOA agent intercepts WS SOAP request check for user credentials 3. Extracts the SOAP header 4. Sends the SOAP request to WSS Component 5. WSS Component evaluates the policy and extracts the user information 6. Sends Policy Server validation request 7. Policy server validates the credentials from the input message and add the session token in to WS-header 8. Sends the validation status 9. Password Digest/X509/SAML Profile generated 10. Update the SOAP header with Security token 11. Client gets access to the web service. <p>Alternate Flow</p> <ol style="list-style-type: none"> 1. Client sends WS SOAP request to web service end point 2. SOA agent intercepts WS SOAP request check for session token 3. Policy server validates the token and update WS-Security header 4. Client gets access to the web service. |
| Sequence Diagram | <pre> sequenceDiagram participant Client participant Web Service participant SOA Agent participant WSS Component participant Policy Server participant User Directory Client->>Web Service: 1. Client request access Web service activate Web Service Web Service->>SOA Agent: 2. Extracts the SOAP header from the request deactivate Web Service activate SOA Agent SOA Agent->>WSS Component: 3. Sends the SOAP request to WSS Component deactivate SOA Agent activate WSS Component WSS Component->>Policy Server: 4. Evaluates the policy and extract the user information deactivate WSS Component activate Policy Server Policy Server->>User Directory: 5. Credential validation request deactivate Policy Server activate User Directory User Directory->>Policy Server: 6. Authenticate the user deactivate User Directory Policy Server->>WSS Component: 7. Send the status deactivate Policy Server activate WSS Component WSS Component->>SOA Agent: 8. Generate Password Digest/X509/SAML Profile deactivate WSS Component activate SOA Agent SOA Agent->>Web Service: 9. Update the SOAP header with Security token deactivate SOA Agent activate Web Service Web Service->>Client: 10. Client Get access to the web service deactivate Web Service deactivate Client </pre> |

| Field | Description |
|------------------------|---|
| Main Success Scenarios | User is authenticated and Application is presented to the user |
| Main Failure Scenarios | SOAP fault with authentication failure message returned to client in case of validation of user credential fail |

A.11. Responses to XML Encryptions, Decryptions, and Digital Signature

| Field | Description |
|----------------|---|
| Use Case Name | Responses to XML Encryptions, Decryptions, and Digital Signature |
| Description | This use case describes the process by exchanges which SiteMinder generates and manages WS security headers. |
| Actors | <ol style="list-style-type: none"> 1. Users 2. Client 3. Web Service |
| Pre-Conditions | A X509 certificate signer should be available to digitally sign a complete XML document |
| Trigger | Client access web service endpoint protected by SOA agent |
| Actions | <ol style="list-style-type: none"> 1. A web service consumer application places it in XML format 2. Wraps it with SOAP headers, placing destination's X.509 certificate in a WS-Security header 3. Sends the SOAP request to the WSS component 4. The web service is protected by the SSOi WS-Security authentication scheme and an authorization policy configured to do the following: 5. Obtain the intended recipient's public key certificate from the message headers 6. Authenticate the user 7. Receive the Status of the Authentication 8. Encrypt the required header and message elements. 9. SOA agent then forwards the encrypted message to a destination web service. <p>SSOi Responses to XML Digital Signatures</p> <ol style="list-style-type: none"> 1. A web service consumer application places a digitally signed XML document using its PIV certificate containing (Signature, KeyInfo, KeyName) 2. SOA agent intercepts Web service authentication requests and validates the certificate and compare a certificate UPN with AD 3. SOA agent forwards message to a destination protected web service |

| Field | Description |
|------------------------|--|
| Sequence Diagram | <pre> sequenceDiagram participant Client participant Web Service participant SOA Agent participant WSS Component participant Policy Server participant AD Client->>Web Service: 1. Client request access Web service Web Service->>SOA Agent: 2. SOA Agent intercepts the SOAP request with signed XML document SOA Agent->>SOA Agent: 3. Extracts the SOAP header from the request SOA Agent->>WSS Component: 4. Sends the SOAP request to WSS Component WSS Component->>WSS Component: 5. Evaluates the policy and extract the user information WSS Component->>Policy Server: 6. Provide information to policy server for user validation Policy Server->>AD: 7. Authenticate user against AD AD-->>Policy Server: 8. Send the status Policy Server-->>WSS Component: 9. XML Encryption/response attributes WSS Component->>SOA Agent: 10. Update the SOAP header with Security token SOA Agent->>Web Service: 11. Client Get access to the web service </pre> |
| Main Success Scenarios | User is authenticated and Application is presented to the user. |
| Main Failure Scenarios | SOAP fault with authentication failure message returned to client in case of validation of user credential fail |