

Department of Veterans Affairs

Identity and Access Management Access Services Solution 2.0 Increment 4

System Design Document



August 2014

Version 2.4

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
9/22/2014	2.4	Updated document to address feedback	[REDACTED]
08/22/2014	2.3	Updated design sections for increment 3 for SSOi, SAC, Provisioning, Role Engineering and Compliance, and the Maintenance Screen	[REDACTED]
05/08/2014	2.2	Embedded email approval signatures to the PDF version to post on the [REDACTED] TSPR. Completed a quality review.	[REDACTED] HPTi/DRC
04/14/2014	2.2	Updated based on formal review	[REDACTED]
04/04/2014	2.2	Updated based on additional comments	[REDACTED]
04/01/2014	2.2	Updated document based on peer review feedback	[REDACTED]
03/14/2014	2.2	Updated design sections for increment 3 for SSOi, CAR, IP, VDS, CSP, and Provisioning	[REDACTED]
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 [REDACTED] TSPR.	[REDACTED] HPTi/DRC
12/18/2013	2.1	Minor update to BRD reference after Formal Review	[REDACTED] Tech Leads
11/22/2013	2.0	Updates to include new functionality; de-coupling of CSP and IP, Mobility for SSOi, CRISP Onboarding, and removal of application specific data	[REDACTED]
09/12/2013	1.9	Design elements to address RSD 2.0	[REDACTED]
07/02/2013	1.8	Updates from peer review feedback.	[REDACTED]
06/24/2013	1.7	Updates from peer review feedback.	[REDACTED]
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	[REDACTED]
05/25/2013	1.5	Baselined for Increment 4	[REDACTED]
02/11/2013	1.4	Updates to VIP and VM tables, additional diagram updates, and additional technical clarifications following formal review	[REDACTED] K. [REDACTED]

Date	Version	Description	Author
01/14/2012	1.3	Additional Updates from consolidated peer review feedback. Updated diagrams, tables and text to reflect Terremark environments; added technical clarifications.	[REDACTED]; K. [REDACTED]
12/12/2012	1.2	Updates from peer review feedback. Modification of location from AITC to Terremark and Modification of patch levels.	[REDACTED]
11/30/2012	1.1	Modification of Increment 2 SDD as base document to combine increment 2 and increment 3 into a single document	[REDACTED]
05/11/2012	1.0	Final- Addressed WP R comments.	[REDACTED]
04/20/2012	0.1	Initial Draft	[REDACTED]


Artifact Rationale

The System Design Document (SDD) is a dual-use document that provides the conceptual design as well as the as-built design. This document will be updated as the product is built, to reflect the as-built product. Per the Project Management Accountability System (PMAS) Guide, the SDD 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	7
1.6	Constraining Policies, Directives and Procedures.....	7
1.7	Constraints	9
1.8	Design Trade-offs	12
1.9	User Characteristics.....	12
1.10	User Problem Statement.....	12
2	Background	13
2.1	Overview of the System	13
2.2	Overview of the Business Process	13
2.3	Assumptions.....	13
2.4	Legacy System Retirement.....	17
3	Conceptual Design.....	17
3.1	Conceptual Application Design.....	17
3.1.1	Application Context.....	18
3.1.2	High-Level Application Design	31
3.1.3	Application Locations	33
3.1.4	Application Users	36
3.2	Conceptual Data Design	38
3.2.1	Project Conceptual Data Model	38
3.2.2	Database Information	42
3.2.3	User Interface Data Mapping	43
3.3	Conceptual Infrastructure Design.....	78
3.3.1	System Criticality and High Availability.....	78
3.3.2	Special Technology	79
3.3.3	Technology Locations.....	79
3.3.4	Conceptual Infrastructure Diagram.....	79
4	System Architecture	82
4.1	Hardware Architecture	83
4.2	Software Architecture	95
4.3	Communications Architecture	111
4.4	Communication Channel Security	112

4.5	 Inter-component Communications	112
4.5.1	Production Server PKI Certificate List	126
5	Data Design	133
5.1	DBMS Files.....	133
5.2	Non-DBMS Files.....	134
6	Detailed Design	134
6.1	Hardware Detailed Design	134
6.2	Software Detailed Design	135
6.2.1	Provisioning Design	135
6.2.2	Role Manager (SailPoint IdentityIQ) Design	163
6.2.3	VDS – Attribute Exchange Service Design	172
6.2.4	SSOi Design	179
6.2.5	CSP Design	215
6.2.6	IP Design	221
6.2.7	SAC Design	226
6.2.8	eSig Design	235
6.2.9	CAR Design	241
6.2.10	Product Perspective	243
6.2.11	Specific Requirements	245
6.3	Communications Detailed Design.....	245
6.4	System Maintenance Design	246
6.4.1	Maintenance pages.....	246
7	External Interface Design	248
7.1	Interface Architecture	248
7.1.1	VA CSP Federation with VAAFI	248
7.1.2	Master Veteran Index.....	248
7.1.3	VA Active Directory	249
7.1.4	Provisioning – VistA.....	250
7.2	Interface Detailed Design.....	251
7.2.1	VA CSP Federation with VAAFI	251
7.2.2	Master Veteran Index.....	252
7.2.3	VA Active Directory	252
7.2.4	Provisioning – VistA.....	252
8	Human-Machine Interface	252
8.1	Interface Design Rules	253
8.2	Inputs.....	253
8.3	Outputs.....	254
8.4	Navigation Hierarchy.....	254

8.4.1	CSP	254
8.4.2	IP	255
8.4.3	Provisioning	255
9	System Integrity Controls	256
9.1	CSP and IP	258
9.1.1	Confidentiality of Sensitive Information	258
9.1.2	Privacy of Personal Information	259
9.1.3	Process Integrity.....	259
9.2	eSig.....	259
9.2.1	Confidentiality of Sensitive Information	259
9.2.2	Privacy of Personal Information	259
9.2.3	Process Integrity.....	259
9.2.4	System Availability	259
9.3	SAC.....	260
9.3.1	Confidentiality of Sensitive Information	260
9.3.2	Privacy of Personal Information	260
9.3.3	Process Integrity.....	260
9.3.4	System Availability	260
9.4	Provisioning.....	260
9.4.1	Confidentiality of Sensitive Information	260
9.4.2	Privacy of Personal Information	261
9.4.3	Process Integrity.....	261
9.4.4	System Availability	261
9.5	SSOi.....	261
9.5.1	Confidentiality of Sensitive Information	261
9.5.2	Privacy of Personal Information	261
9.5.3	Process Integrity.....	262
9.5.4	System Availability	262
9.6	CAR.....	262
9.6.1	Confidentiality of Sensitive Information	262
9.6.2	Privacy of Personal Information	262
9.6.3	Process Integrity.....	262
9.6.4	System Availability	262
9.7	Virtual Directory Service (VDS)	263
9.7.1	Confidentiality of Sensitive Information	263
9.7.2	Privacy of Personal Information	263
9.7.3	Process Integrity.....	263
9.7.4	System Availability	264

9.8	Role Manager	264
9.8.1	Confidentiality of Sensitive Information	264
9.8.2	Privacy of Personal Information	264
9.8.3	Process Integrity	264
9.8.4	System Availability	264
10	Approval Signatures	265
A.	Additional Information	266
A.1.	Data Dictionary	266
A.2.	CRISP Onboarding/Offboarding Attributes	266
A.3.	RTM.....	266
A.4.	Packaging and Installation	266
A.5.	Design Metrics	266
A.6.	Acronym List and Glossary	267
A.7.	Required Technical Documents	267
A.8.	CSP Class Diagram	267
A.9.	IP Class Diagram	267
A.10.	Responses to Produce WS-Security Headers.....	268
A.11.	Responses to XML Encryptions, Decryptions, and Digital Signature ...	269

List of Figures




Figure 1:	 Solution Overview	19
Figure 2:	CSP Context Diagram	20
Figure 3:	IP Context Diagram	22
Figure 4:	eSig Context Diagram	23
Figure 5:	SAC Context Diagram	24
Figure 6:	PROV Context Diagram	26
Figure 7:	SSOi Context Diagram	28
Figure 8:	CAR Context Diagram.....	30
Figure 9:	 Solution Application Design	32
Figure 10:	 Solution Conceptual Data Mode	39
Figure 11:	New VA Employee Profile Information	44
Figure 12:	New VA Contractor Profile Information.....	45
Figure 13:	New HP Trainee Profile Information	45
Figure 14:	New Volunteer Profile Information	46
Figure 15:	New VA Employee Work/Home Location Information.....	46
Figure 16:	New VA Contractor Work/Home Location Information	47
Figure 17:	New HP Trainee Work/Home Location Information.....	47
Figure 18:	New Volunteer Work/Home Location Information.....	48




Figure 19: New VA Employee Organization and Employment Information.....	48
Figure 20: New VA Contractor Organization and Employment Information	49
Figure 21: New HP Trainee Organization and Employment Information.....	50
Figure 22: New Volunteer Organization and Employment Information	51
Figure 23: New VA Employee Miscellaneous Information.....	52
Figure 24: New VA Contractor Miscellaneous Information	53
Figure 25: New HP Trainee Miscellaneous Information	54
Figure 26: New Volunteer Miscellaneous Information	55
Figure 27: CRISP Checklist Screen	56
Figure 28: Modify Account: Step 1 User Profile	62
Figure 29: Modify Account: Step 2 Security Questions.....	62
Figure 30: Change Password.....	63
Figure 31: Upgrade to Level 2: Step 1 User Profile	64
Figure 32: Upgrade to Level 2: Step 2 Security Questions.....	65
Figure 33: Self-Registration: Step 1 User Profile	66
Figure 34: Self-Registration: Step 2 Security Questions	67
Figure 35: Identity Proof User: Step 1 User Profile	68
Figure 36: Identity Proof User: Step 2 Address Verification	69
Figure 37: Identity Proof User: Step 3 Primary Verification	70
Figure 38: Identity Proof User: Step 4 Secondary Identification.....	70
Figure 39: Update a User: Step 1 User Profile	71
Figure 40: Update a User: Step 2 Address Verification	72
Figure 41: Update a User: Step 3 Primary Identification.....	73
Figure 42: Update a User: Step 4 Secondary Identification.....	73
Figure 43: SSOi Centralized Login Page.....	74
Figure 44: SSOi PIV Only Login Page.....	75
Figure 45: Mobile Login Page	76
Figure 46: SAC PAP Landing Page.....	77
Figure 47: SAC PAP Landing Page.....	77
Figure 48:  Production Environments	80
Figure 49: Logical Network String Diagram.....	82
Figure 50: Network Communication Architecture.....	83
Figure 51: Software Architecture.....	96
Figure 52:  Network Security Topology.....	112
Figure 53: Provisioning Detail Design.....	136
Figure 54: Provisioning User Onboarding Sequence Diagram	138
Figure 55: Provisioning: Third-Party / DoD Onboarding Sequence Diagram	140

Figure 56: Provisioning: Update Provisioning Record from MVI Sequence Diagram.....	143
Figure 57: Provisioning: User Offboarding Sequence Diagram.....	144
Figure 58: Provisioning: User Provisioning Sequence Diagram.....	146
Figure 59: User De-Provisioning Sequence Diagram.....	147
Figure 60: Explore and Correlate from Endpoints Sequence Diagram	148
Figure 61: Request New VistA User Account (Prov(SPML(add)) VistA VSA).....	150
Figure 62: Correlate an Existing VistA User Account with Provisioning User's Identity Record (VistA VSA (SPML(add))	151
Figure 63: Correlate an Existing VistA User Account with Provisioning User's Identity Record (VistA VSA (SPML(add))	151
Figure 64: Modify VistA User Account (Prov(SPML(modify))	152
Figure 65: Update Provisioning User's Identity Record Correlated VistA User Account Data	153
Figure 66: Search for VistA User Account(s) (Prov (SPML(search))	154
Figure 67: Get VistA Instances (Prov(SPML(listTargets))	155
Figure 68: Retrieve Vista User Account (Prov(SPML (lookup))	156
Figure 69: Deprovision VistA Account (Prov(SPML(delete))→VistA VSA).....	157
Figure 70: Suspend VistA User Account (Prov (SPML(suspend))→VistA VSA) ..	158
Figure 71: Update Provisioning User's Identity Record Correlated VistA User Account Status to "Suspended" (VistA VSA(SPML(suspend))→Prov)	159
Figure 72: Reactivate VistA User Account (Prov (SPML(resume))→VistA VSA) .	160
Figure 73: Update Provisioning User's Identity Record Correlated VistA User Account Status to "Active" (VistA VSA(SPML(resume))→Prov).....	161
Figure 74: Get VistA User Account State (Prov (SPML (active))→VistA VSA)	162
Figure 75: Bind a Provisioned User to a VistA Account	163
Figure 76: Role Manager Detailed Design	164
Figure 77: Authoritative Source – VA Repository Sequence Diagram	165
Figure 78: Role Mining – VA Application Sequence Diagram	167
Figure 79: Access Re-certification – Role Composition Sequence Diagram	169
Figure 80: Create Provisioning Role(s) in Provisioning IdM	171
Figure 81: Retrieve User by CSPID Sequence Diagram.....	173
Figure 82: VDS Detailed Design	175
Figure 83: PROV-VDS-MVI Design	176
Figure 84: SSOi Detailed Design.....	180
Figure 85: SSOi STS Architecture Diagram	182

Figure 86: SSOi Centralized Logon Page with Windows Authentication Sequence Diagram.....	182
Figure 87: Centralized Log on Page with UserID/Password Authentication Sequence Diagram	183
Figure 88: Centralized Log on Page with PIV Authentication Sequence Diagram	183
Figure 89: Centralized PIV Only Log on with PIV Authentication Sequence Diagram.....	184
Figure 90: SSOi Support for LOA 2/3 External Users Sequence Diagram	187
Figure 91: SSOi Mobility Support Sequence Diagram	190
Figure 92: Access Mobile Application Using Native Apps Sequence Diagram ...	191
Figure 93: Federation IdP and SP for Internal Users.....	193
Figure 94: Application Protected by Separate IdP (Other than SSOi) Sequence Diagram.....	194
Figure 95: WS Federation for Internal Users Sequence Diagram	197
Figure 96: SSOi Support for Attribute Service Sequence Diagram	199
Figure 97: SSOi Proxy Authentication Request Sequence Diagram	201
Figure 98: Session Management Sequence Diagram	202
Figure 99: SSOi STS Architecture Flow Sequence Diagram	204
Figure 100: Centralized Logon Page Flow	207
Figure 101: Centralized Logon Page Error Handling Flow	209
Figure 102: Centralized Login Page Supported Partial and Complete Logoff Capabilities	210
Figure 103: Centralized Logon Page - Logoff Flows	211
Figure 104 SSOi Authenticated Landing Page Mock-up.....	212
Figure 105 IAM Logged Off Page Mock-up	214
Figure 106: SiteMinder Policy Architecture for Core Centralized Authentication Flows	215
Figure 107: CSP Detailed Design	216
Figure 108: Credential Issuance Sequence Diagram	217
Figure 109: Revoke/Reissue Credential Sequence Diagram	219
Figure 110: Federation with Consuming Application Sequence Diagram	220
Figure 111: IP Detailed Design.....	222
Figure 112: Identity Proof a User Sequence Diagram.....	223
Figure 113: Create Proofing Record Sequence Diagram.....	225
Figure 114: SAC Detailed Design.....	227
Figure 115: Enforce Access Control Decision Sequence Diagram.....	229

Figure 116: Security Policy Authoring Sequence Diagram	230
Figure 117: Manage Access Control Policies	232
Figure 118: Make Access Control Decisions Sequence Diagram	233
Figure 119: Make Access Control Decisions (XACML 2.0) Sequence Diagram...	234
Figure 120: eSig Detailed Design.....	236
Figure 121: Example Visible Signature	238
Figure 122: User Management – Sign Document Sequence Diagram.....	238
Figure 123: User Management – Verify Document Sequence Diagram.....	240
Figure 124: CAR Detailed Design.....	241
Figure 125: Process Activity Logs to Generate Reports Sequence Diagram	242
Figure 126: Maintenance Page for  Component	246
Figure 127: CSP to VAAAFI Interface Flow	248
Figure 128: MVI Interface Flow with Provisioning and IP	249
Figure 129: Provisioning – Active Directory Interface Architecture	250
Figure 130: CSP Navigation Hierarchy	254
Figure 131: IP Navigation Hierarchy	255
Figure 132: Provisioning Navigation Hierarchy.....	256
Figure 133: CSP Class Diagram	267
Figure 134: IP Class Diagram.....	267
Figure 135: Responses to Produce WS Security Headers Sequence Diagram ...	268
Figure 136: Responses to XML Encryptions, Decryptions and Digital Signature Sequence Diagram	269

List of Tables

Table 1: System Identification.....	3
Table 2: Scope Inclusions	3
Table 3: Scope Exclusion	5
Table 4: Project Documents	5
Table 5: Policies, Directives, and Procedures	7
Table 6: Assumptions and Constraints.....	14
Table 7: CSP Application Context Description	20
Table 8: IP Application Context Description	22
Table 9: eSig Application Context Description.....	23
Table 10: SAC Application Context Description.....	24
Table 11: PROV Application Context Description	26
Table 12: SSOi Application Context Description.....	28
Table 13: CAR Application Context Description.....	30
Table 14: Activities in the High-Level Application Design.....	32





Table 15:	 Solution Application Locations	34
Table 16:	 Solution Users	36
Table 17:	Database Inventory	40
Table 18:	Database Inventory	42
Table 19:	Special Technology Requirements	79
Table 20:	Hardware Appliance	84
Table 21:	Virtual Machines and Appliances	85
Table 22:	 Products and Versions	97
Table 23:	Software Components	100
Table 24:	Programming Languages	110
Table 25:	Operating Systems	110
Table 26:	Port Communications and Protocols	112
Table 27:	Pre-Production PKI Certificate List	119
Table 28:	Production Cert List	126
Table 29:	Database File System	133
Table 30:	Provisioning User Onboarding	138
Table 31:	Provisioning: Third-Party / DoD Onboarding	140
Table 32:	Provisioning: Update Provisioning Record from MVI	143
Table 33:	Provisioning Web Service Function	Error! Bookmark not defined.
Table 34:	Provisioning: User Offboarding	144
Table 35:	Provisioning: User Provisioning	146
Table 36:	User De-Provisioning	147
Table 37:	Explore and Correlate from Endpoints	148
Table 38:	Authoritative Source – VA Repository Sequence	165
Table 39:	Role Mining – VA Application	167
Table 40:	Access Re-certification – Role Composition	169
Table 41:	Retrieve User by CSPID	173
Table 42:	MVI Webservice	178
Table 43:	Centralized PIV Only Log on with PIV Authentication	184
Table 44:	SSOi Support for LOA 2/3 External Users	187
Table 45:	VAAFI IdP SAML Integration	188
Table 46:	Access Mobile Application Using Native Apps	191
Table 47:	Application Protected by Separate IdP (Other than SSOi)	194
Table 48:	WS Federation for Internal Users	197
Table 49:	SSOi Support for Attribute Service	199
Table 50:	SSOi Proxy Authentication Request	201
Table 51:	Session Management	202

Table 52: SSOi STS Architecture	204
Table 53: Credential Issuance	217
Table 54: Revoke/Reissue Credential	219
Table 55: Federation with Consuming Application	220
Table 56: Potential Impact Categories for Authentication Errors	222
Table 57: Identity Proof a User	224
Table 58: Create Proofing Record.....	226
Table 59: Enforce Access Control Decision	229
Table 60: Security Policy Authoring	231
Table 61: Manage Access Control Policies.....	232
Table 62: Make Access Control Decisions.....	233
Table 63: Make Access Control Decisions Using XACML 2.0 Request/Response	234
Table 64: User Management – Sign Document.....	238
Table 65: User Management – Verify Document	240
Table 66: Process Activity Logs	242
Table 67:  Solution Products	244
Table 68: VA CSP (as CSP/IdP) sending SAML to VAAFI	251
Table 69: Responses to Produce WS Security Headers	268
Table 70: Responses to XML Encryptions, Decryptions and Digital Signature...	269

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 () 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 () solution, which includes the applicable subcomponents. The individual subcomponents or groups are referred to as a VA () activity or the VA () activities. The VA () 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 () activities, commercial off-the-shelf (COTS) products are used to enable the specific capabilities of the () 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 () solution's primary customers are both internal and external user communities who need logical access to VA business applications. The primary subsystems for the () 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 [REDACTED] 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 [REDACTED] 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
- [REDACTED] Solution Architects
- [REDACTED] 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 [REDACTED] 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 [REDACTED] 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 [REDACTED] solution. This document applies to the following systems and software:

Table 1: System Identification

Name	Description	Abbreviation	Version	Release
VA [REDACTED] 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	[REDACTED]	V 2.0.0	Release 4 (Increment 4)

1.3 Scope

This document focuses on the technical system design to provide the foundation for the [REDACTED] 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 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

Includes
<p>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)</p> <ul style="list-style-type: none"> • Provides functionality to delete user access
<p>IP:</p> <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)
<p>PROV:</p> <ul style="list-style-type: none"> • Provides user account provisioning along with pre-defined roles for VA application • 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) • Role manager is integrated with the Provisioning service for the purpose of performing management and enforcement of the mined or manually created roles within the SailPoint tool itself • The SailPoint tool is integrated with SSOi (CA SiteMinder) for seamless authentication and improved user experience when using the SailPoint tool.
<p>SAC:</p> <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

Includes
<ul style="list-style-type: none"> 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 [REDACTED] 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.
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"> N/A

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
[REDACTED] 2.0_i4_RSD.PD	Requirement Specification Document for VA IAM [REDACTED] Release 2, Increment 4

Document Name	Description
I3 Requirements Specification Document: AcS 2.0 i3 RSD	Provides requirements for [REDACTED] Increment 3.
VA [REDACTED] 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 [REDACTED] Increment 2.
I3 Requirements Specification Document: AcS Requirements Specification Document I3 v2	Provides updated requirements for [REDACTED] Increment 3
I4 Requirements Specification Document: [REDACTED] Requirements Specification Document I4 V6	Provides updated requirements for [REDACTED] Increment 4
I3 Use Cases: VA AcS Solution Use Case Model i3 rev 2.2AC	Provides use cases for [REDACTED] solution
I4 Use Cases: VA [REDACTED] Solution UC Model i4 AC	Provides use cases for [REDACTED] solution
I3 Requirements Traceability Matrix: VA AcS Solution i3 RTM	Provides the requirements traceability matrix for the [REDACTED] solution
I4 Requirements Traceability Matrix: VA [REDACTED] Solution i4 RTM	Provides the requirements traceability matrix for the [REDACTED] 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 [\[REDACTED\]pmas/Documents/PMAS_Guide.pdf](#).

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.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
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.
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.

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
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 [REDACTED] 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.

[REDACTED] 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 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 [REDACTED] solution does not have a common single unique identifier throughout the [REDACTED] activities, increasing the complexity of the integration between activities. SECID will be used by [REDACTED] 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.
- **Oracle Database:** 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.

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.
- **SSOi integrations:** The CAR product (UARM) does not support integration with the current integration patterns offered by SSOi. Therefore, SSO with CAR at this point is not supported.


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).

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 identity 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  solution design:

- The user store and policy store have read-intensive operations. Based on the projected usage demands, the policy store and user store should be created in their own CA Directory Servers instances. Alternatively, if the stores are consolidated on common servers with failover topology, system's performance may degrade between the read and write transactions. Additionally, if the read intensive operations are occurring in the same place where the data is being written then it is likely that data mismatch may occur at time of the reading transaction.
- 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's support for signing of web forms is indirect. It requires converting the web-based form, snippet of code or UI component to a standard, supported document type (e.g. Adobe PDF, MS Word, etc..) before being able to sign it.

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 [REDACTED] with standards and enforcement of appropriate secure access practices.

It will be necessary for VA to standardize on enterprise [REDACTED] 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 [REDACTED] Development Support task is to design, develop, implement, integrate, operationalize, and sustain an enterprise-wide VA [REDACTED] solution for VA VRM. In order to coordinate [REDACTED] 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 [REDACTED] 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 [REDACTED] 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 [REDACTED] activities. The system design is based on a Service Oriented Architecture (SOA) approach. The solution architecture uses accepted COTS products for each of VA [REDACTED] 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 [REDACTED] 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 [REDACTED] 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 [REDACTED] solution.

Table 6: Assumptions and Constraints

Component	Assumption / 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 [REDACTED] 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 A.4).• 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.

Component	Assumption / 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 provides indirect ability to sign web forms through conversion of the general "web form" to a supported for signing format (Adobe PDF, Microsoft Word, etc.). • 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 Proofers 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

Component	Assumption / Constraints
	<p>support higher LOA proofing records.</p> <ul style="list-style-type: none"> One or more Identity Proofing records may be associated with each VA enterprise identity record, allowing versatile Identity information to be collected and used as part of user certification process.
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 runtime transaction analysis for enforcing other potential SOD violations if specific logic is not programmed directly in the solution. 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  will be through 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.

Component	Assumption / Constraints
	<ul style="list-style-type: none"> UARM is currently nearing its end of life. Any future enhancements of the product will be limited. UARM does not support PIV authentication. Since it is a flash based application it also cannot be 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 [REDACTED] infrastructure will be integrated in the appropriate VA Active Directory domain for each environment. The [REDACTED] 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 [REDACTED] solution such as VAAFI and Terremark, which only support 99.6% and 99.9% availability, respectively. Therefore, if the solution components support 99.9% availability, this may not be achieved due to external dependencies which may be limited to the VAAFI 99.6% figure. 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 [REDACTED] 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 [REDACTED] 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 [REDACTED] solution.

3.1.1 Application Context

This section provides context for each of the activities developed for VA [REDACTED] solution. The aim of [REDACTED] solution is to deploy a cohesive and consistent foundational [REDACTED] architecture that is flexible, modular, extensible, and scalable in VA's infrastructure. VA [REDACTED] foundation infrastructure enables internal users, external users and VA business partners to access various [REDACTED] 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 Service (CAR)

Figure 1 below depicts the high-level interactions between the various activities, including interactions between [REDACTED] with other VA applications, and to internal/external business partner applications.

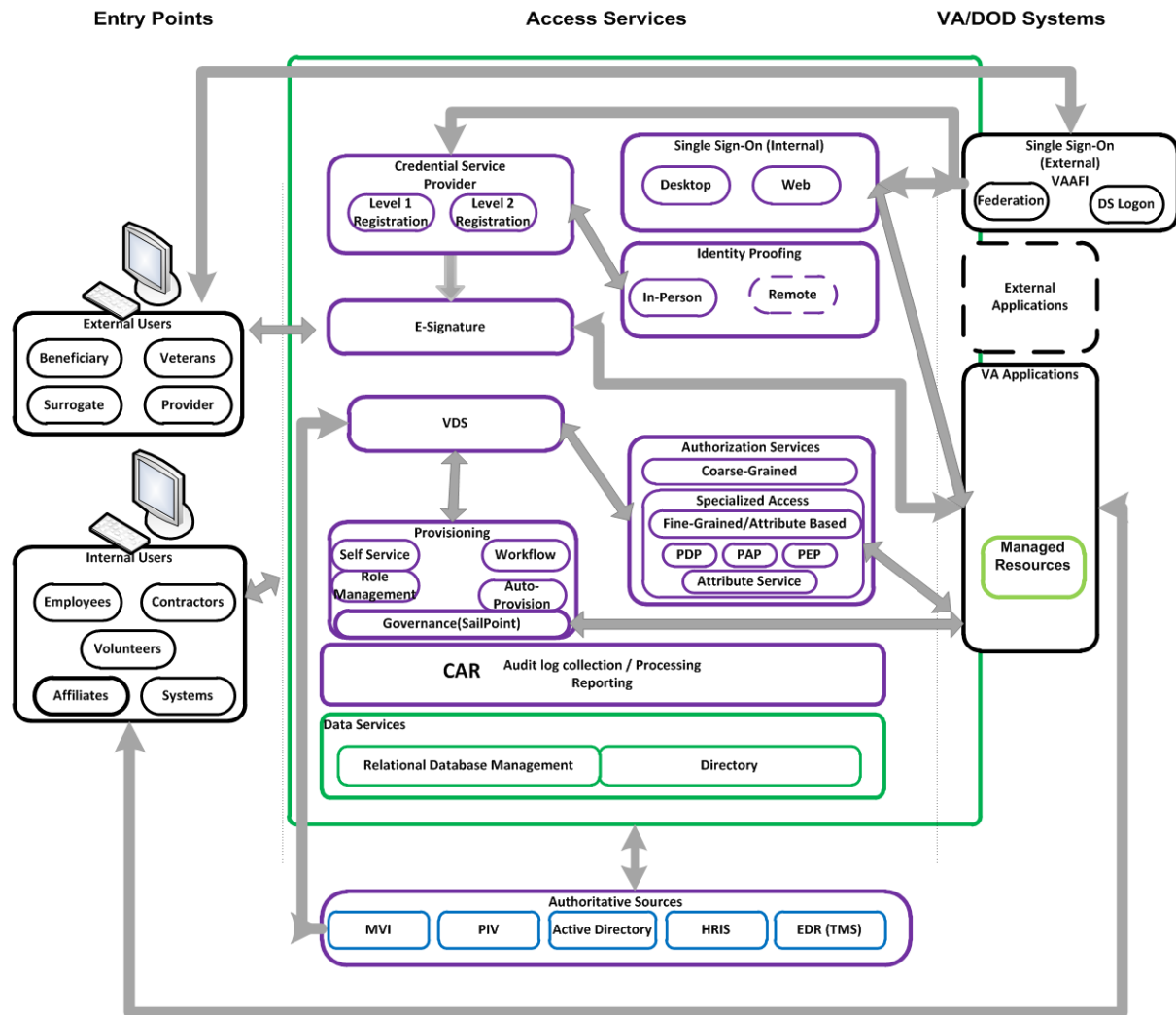


Figure 1: [REDACTED] Solution Overview

Each of the [REDACTED] 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 [REDACTED] 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.

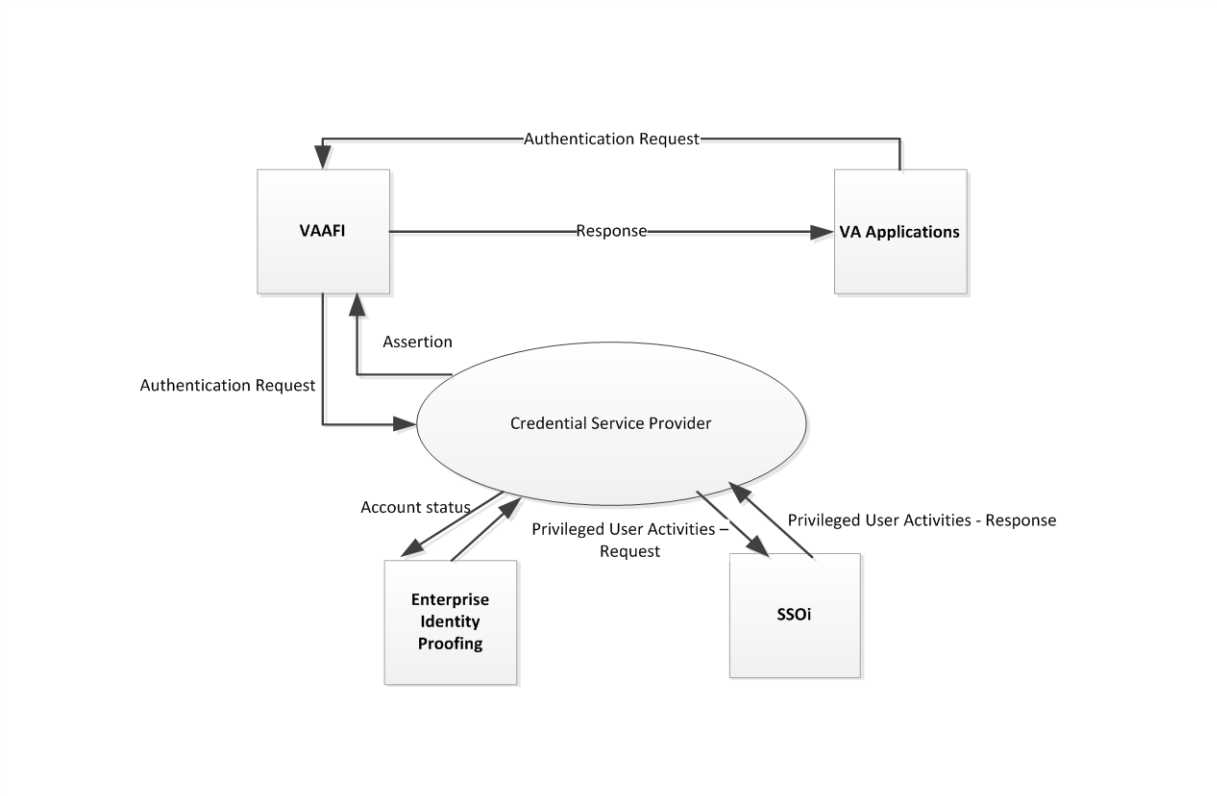


Figure 2: CSP Context Diagram

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

ID	Interface Name	Input Messages	Output Messages	External Party
2	Identity Proofing -CSP	SOAP over HTTPs	SOAP over HTTPs	VA Applications (e.g., VIC)
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 a 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.

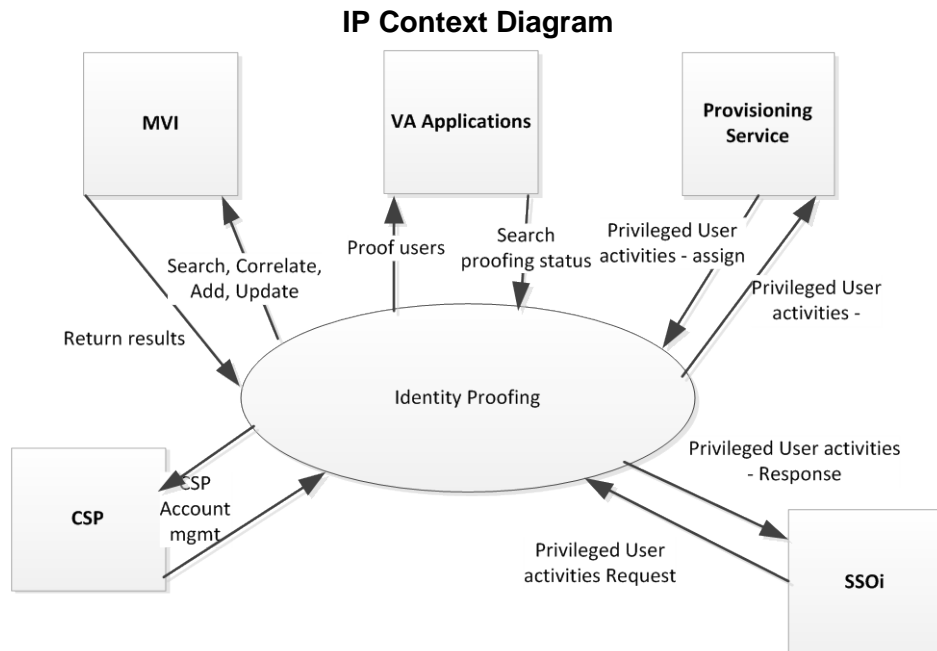


Figure 3: IP Context Diagram

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 relies for authentication of the end user to its partner applications/clients. eSig, on behalf of its clients, uses the signer's submitted identity data, intent, and file data to apply digital signature and provide the means for validating the integrity and non-repudiation of 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 custom application. The eSig custom code is a java/J2EE Web 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.

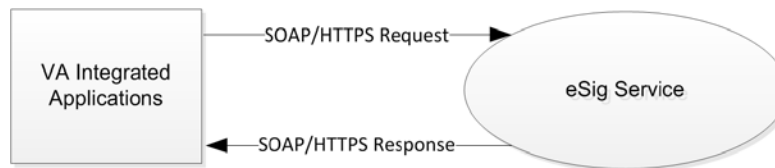


Figure 4: eSig Context Diagram

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.

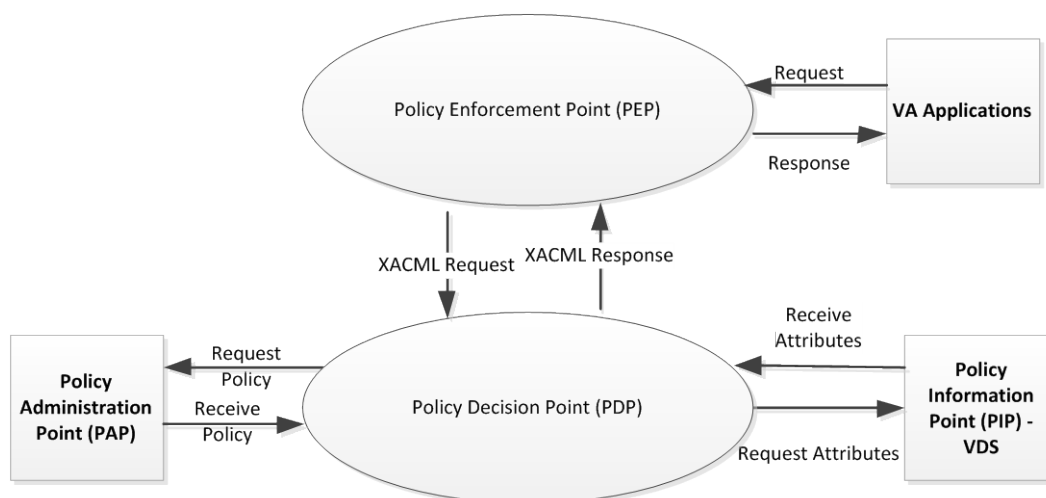


Figure 5: SAC Context Diagram

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)

ID	Interface Name	Relegated Object	Input Messages	Output Messages
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.

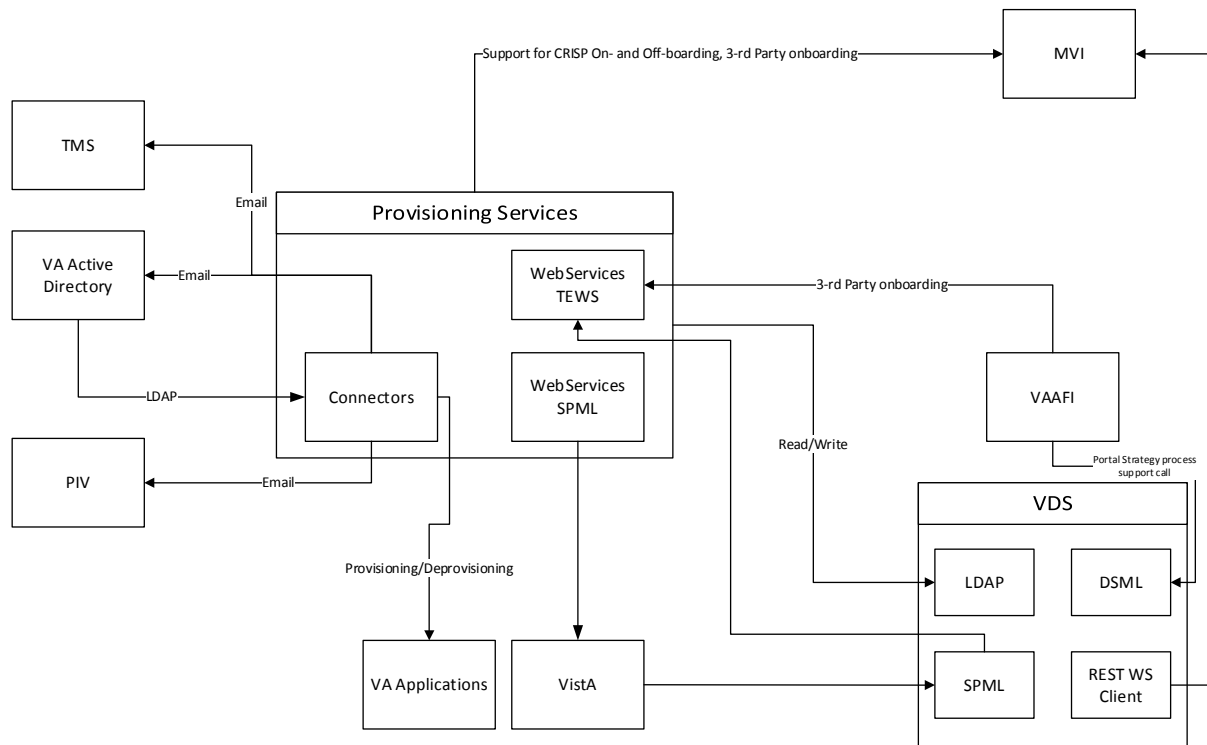


Figure 6: PROV Context Diagram

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 as Create User Task and Modify User Task.

ID	Interface Name	Relegated Object	Input Messages	Output Messages	External Party
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 that 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.

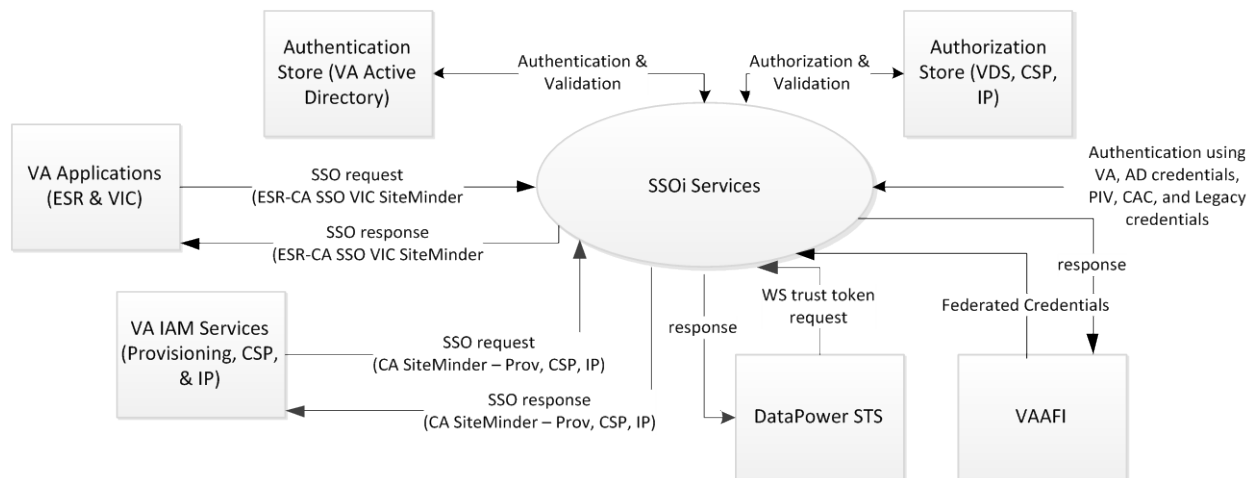


Figure 7: SSOi Context Diagram


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.

ID	Interface Name	Relegated object	Input Messages	Output Messages	External Party
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/HTTP S	HTTP/HTT PS	The SSOi hosted application like centralized logon pages are consumed by SSOI integrated applications
5	VA Applications-SSOi	SSOi Service	HTTP/HTTP S	HTTP/HTT PS	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/res ponce	SAML request /response	VAAFI interacts with SSOi service for federation as service provider or identity provider
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  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.

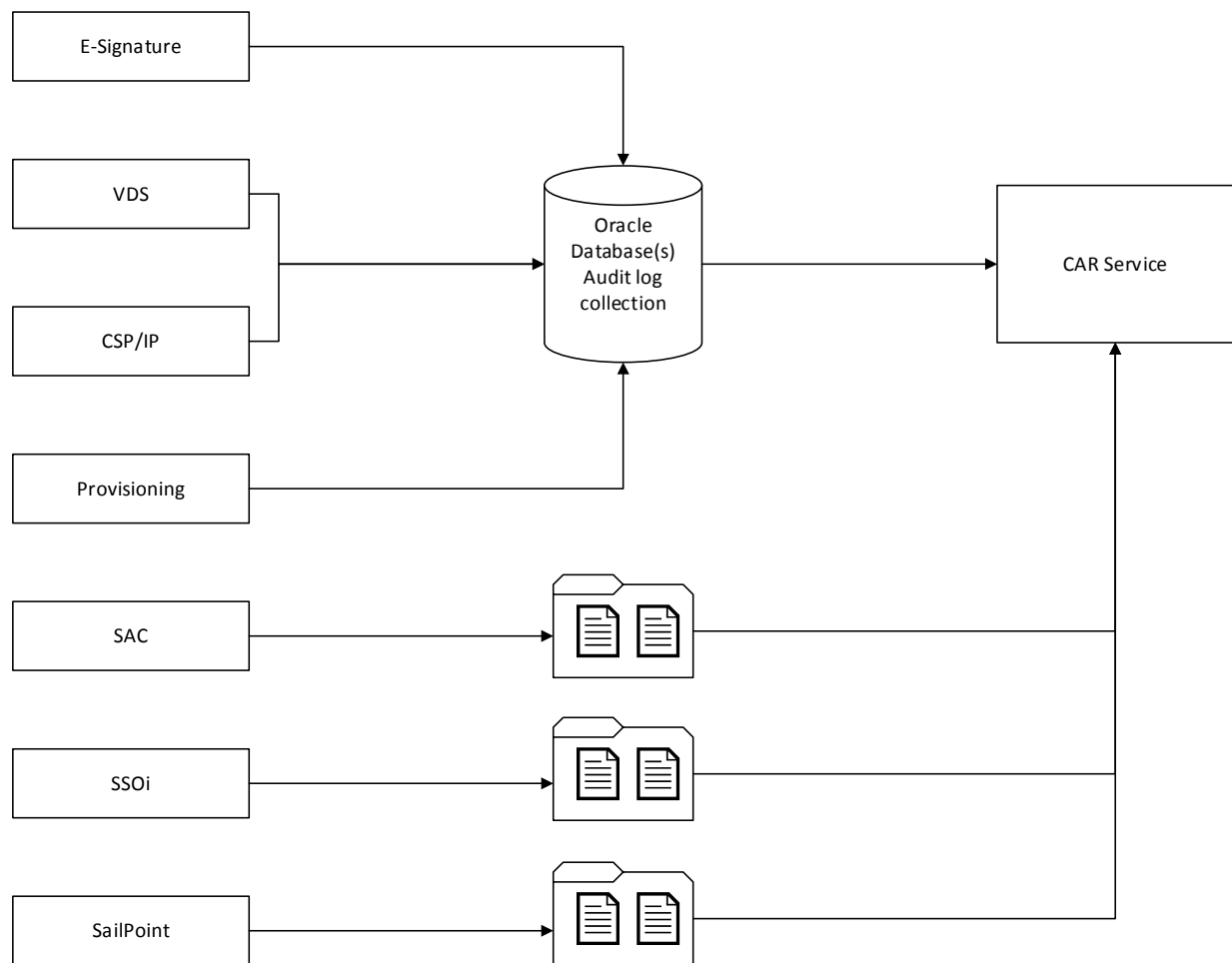


Figure 8: CAR Context Diagram

Table 13: CAR Application Context Description

ID	Interface Name	Related object	Input Messages	Output Messages	External Party
1	eSig	Digital Signatures	SQL queries	ODBC Response	ODBC interface is queried by CAR agent connector to collect the audit logs from the eSig Audit Source
2	VDS	LDAP Queries, DSML queries	SQL queries	ODBC Response	ODBC interface is queried by CAR agent connector to collect to the VDS audit source
3	CSP and IP	SSOi Service	SQL queries	ODBC Response	ODBC interface is queried by CAR agent connector to collect the CA IDM audit source

ID	Interface Name	Related object	Input Messages	Output Messages	External Party
4	Provisioning	SSOi Service	SQL queries	ODBC Response	ODBC interface is queried by CAR agent connector to collect the CA IDM audit source
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
7	SailPoint	SSOi Service	File Reader Queries	File Reader Response	File base Reader is used by CAR agent to collect the SailPoint text based audit logs

CAR interacts with each of the [REDACTED] 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 [REDACTED] solution and identifies the major [REDACTED] activities and/or relationships with VA applications.

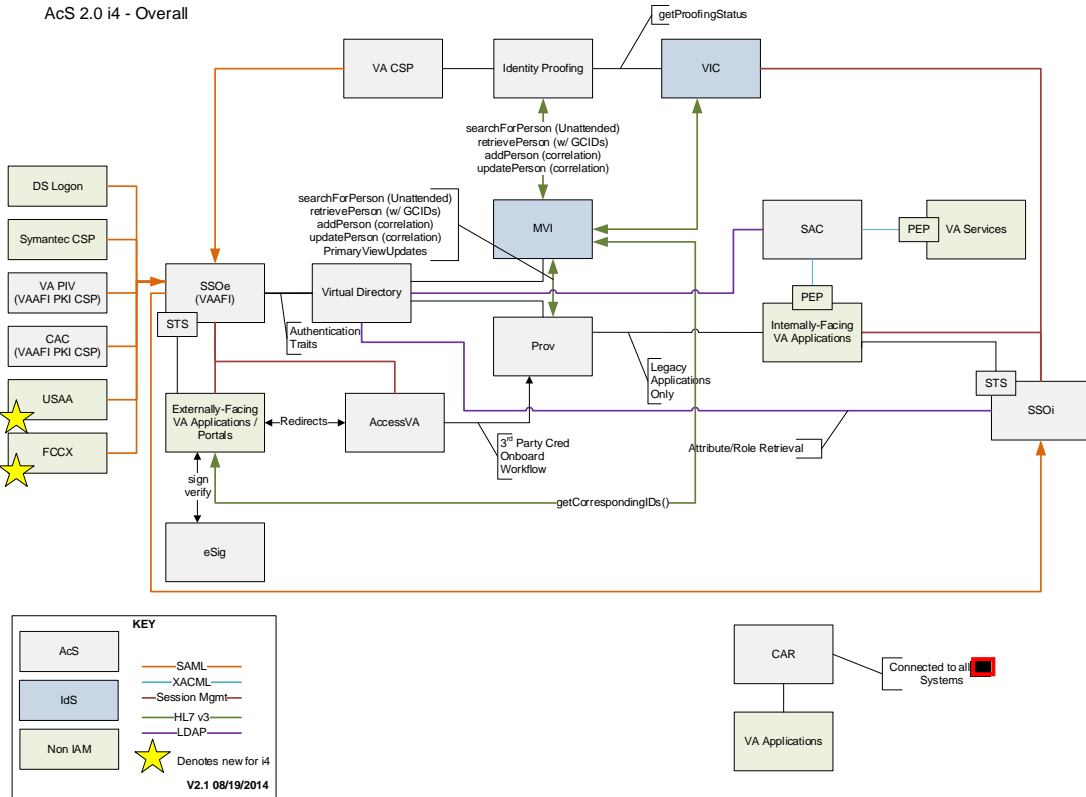


Figure 9: Solution Application Design

The following table provides high-level description for each of the 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 6.2.2.4.

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


ID	Name	Description	Service or Legacy Code	External Interface Name	Internal Interface Name
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: [REDACTED] Solution Application Locations

Application Component	[REDACTED] 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. Servlet Exec is used in conjunction with CA SiteMinder Federation Option pack. All appropriate JVMs on all [REDACTED] environments were updated as part of the OIG audit findings resolution. The NewAtlanta ServletExec v6.0 from 11/30/2007 product supports a minimum of Java 1.5, as listed in the release notes, but has no specific references to restrictions about newer versions of Java. As ServletExec needs to have a waiver per TRM, this process will be initiated. Waiver approval will be reflected in the SDD	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 IdentityMind er	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)

Application Component	 Service	Description	Location at Which Component is Run
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)
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)

Application Component	Service	Description	Location at Which Component is Run
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)
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 solution activities:

Table 16: Solution Users

Application Component	Description	User
CSP	Performs administrative functions including controlling Identity Minder related configurations and tasks	CSP Administrator
CSP	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
CSP	A user (Veteran, beneficiary, or other VA stakeholder) requesting or having a user credential of any level	End User

Application Component	Description	User
IP	Performs administrative functions including controlling Identity Minder related configurations and tasks and managing the proofing registration interfaces	IP Administrator
IP	Responsible for Identity Proofing users confirming identity of applicant to comply with SP 800-63 and VA 6501	Identity 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
SAC	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
eSig	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
Provisioning	Performs administrative functions in Identity Minder including management of end users, workflows, connections to end points as well as configurations objects	Provisioning Administrator
Provisioning	Responsible for registering, approving, and managing user provisioning and de-provisioning lifecycle	Provisioning Privileged User
Provisioning	A user who uses provisioning to self-register, manage user profile, and check request status to gain access to integrated applications	End User
Provisioning	A system that is authorized to use the provisioning web service functions for creating SECID and Add User.	Authorized Systems
Provisioning	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
Provisioning	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

Application Component	Description	User
SSOi	A user interacts with SSOi for initial logon to facilitate the integrated application logon	End User
CAR	Performs administrative functions including management of UARM reports dashboard, generation of reports, and creating other users in UARM	CAR Administrator
CAR	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 [REDACTED] 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 [REDACTED] 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 [REDACTED] activities, refer to [section A.1](#).

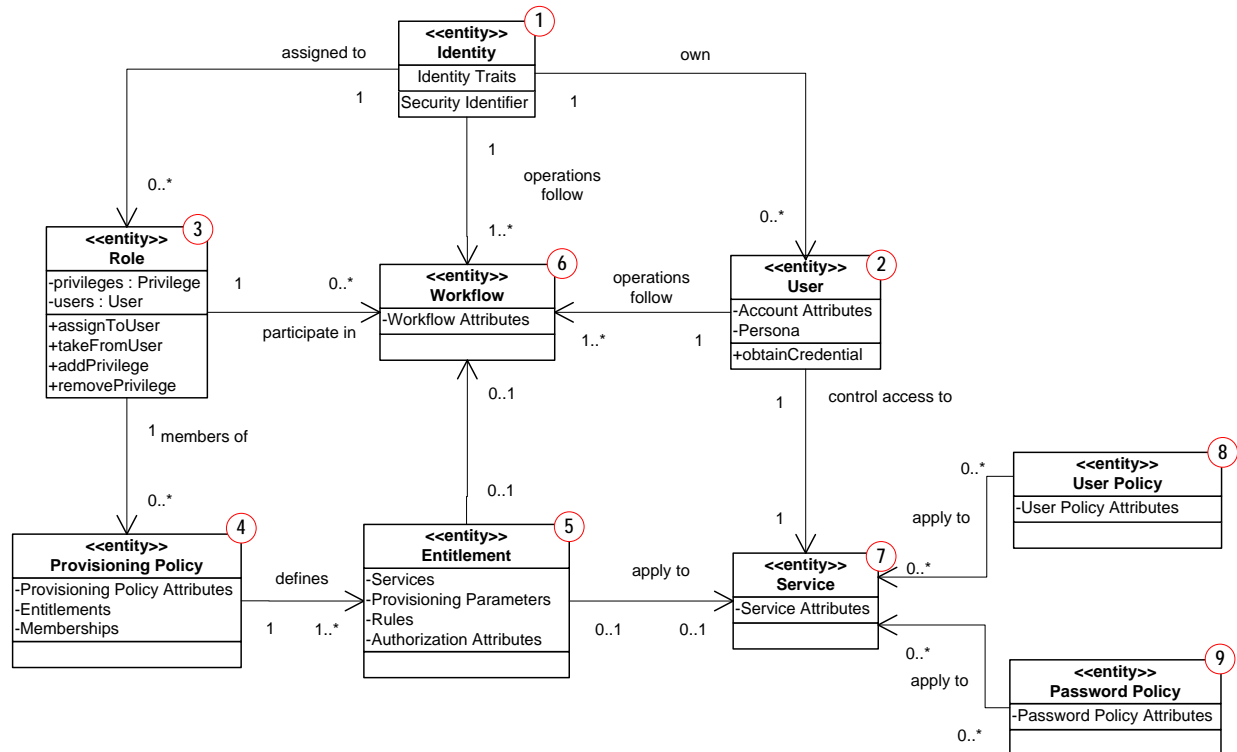


Figure 10: Solution Conceptual Data Mode

The VA 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 following table describes the 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.	<ul style="list-style-type: none"> - One Identity 	<ul style="list-style-type: none"> - One Identity can be assigned to 0 or more Roles - One Identity can own 0 or more Accounts - One Identity has only one security identifier for the lifetime of the identity.
②	User (Account)	The User (Account) attributes 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.

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

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

3.2.2 Database Information












As part of the  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  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  Solution

Database Name	Description	Type	Steward
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  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  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  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  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  Solution
eSig Audit	eSig Audit data collection store where auditable transaction logs are collected for reporting purposes.	Create / Replace / Interface / Modify	VRM  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 any) are encrypted. The database is used by Provisioning service for role manager component.	Create / Replace / Interface / Modify	VRM  Solution

3.2.3 User Interface Data Mapping

This section describes and defines the data that will be available for users of the  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 [REDACTED] 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, Figure 11 through Figure 14, initiate the onboarding process for new VA employees and contractors, HP trainees, and volunteers.

The screenshot displays the 'New VA Employee: Profile' interface. At the top, a breadcrumb trail reads 'New VA Employee Profile/Search: Select User > New VA Employee: Profile'. Below this is a four-step process bar: 1. Profile (highlighted with an orange arrow), 2. Profile Work Home (blue arrow), 3. Profile Org (grey arrow), and 4. Profile Misc (grey arrow). A legend indicates that a red dot next to a field name signifies a required field. The main section is titled 'Personal Information' and contains the following fields:

- First Name: Text input, (required)
- Last Name: Text input, (required)
- Middle Initial/Name: Text input, (optional)
- Suffix: Text input, (optional)
- External Email: Text input, (e.g.: name@email.com)(required)
- Date of Birth (required): Text input with a calendar icon
- SSN: Text input, (e.g.: 123456789)(required)
- Gender: Dropdown menu with 'Choose One' selected, (required)
- Height: Text input, (inches)(required)
- Eye Color: Dropdown menu with 'Choose One' selected, (required)
- Hair Color: Dropdown menu with 'Choose One' selected, (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 Choose One (required)

• Height (inches)(required)

• Eye Color Choose One (required)

• Hair Color Choose One (required)

Figure 12: New VA Contractor Profile Information

VA Provisioning Service

Skip to main content

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 Choose One (required)

• Height (inches)(required)

• Eye Color Choose One (required)

• Hair Color Choose One (required)

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 through Figure 18.

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 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 System

• = 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 through Figure 22.

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

[Skip to main content](#)
[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

Required

Organizational and Employment Information

- Supervisor ID SEC ID (required) [Browse](#)
- VA OIT PD Project (required)
- VA Project Manager (required) [Browse](#)
- Occupation Code (required)
- Employment Status (required)
- Department (required)
- Title (required)
- Sponsor (required) [Browse](#)
- Office Location (required)
- Cost Center (required)
- Special Security Access Required (required)
- Emergency Responder (required)
- Critical Employee (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

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) jmadmin [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, Figure 23 through Figure 26.

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

[Skip to main content](#)
[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 Registrat
Update TMS Profile
Reporting
Manage Users
Update User

[Users](#)
[Groups](#)
[Roles and Tasks](#)
[Endpoints](#)
[Provisioning Endpoints](#)
[Policies](#)
[Reports](#)
[System](#)

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)

VA Provisioning Service

[Skip to main content](#)
[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 Registrat
Update TMS Profile
Reporting
Manage Users
Update User

[Users](#)
[Groups](#)
[Roles and Tasks](#)
[Endpoints](#)
[Provisioning Endpoints](#)
[Policies](#)
[Reports](#)
[System](#)

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 VA. All rights reserved.

About VA Provisioning Service

Figure 25: New HP Trainee 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 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

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

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, Figure 27, is used to capture the data against the checklist.

VA Provisioning Service

Skip to main content

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"/>		

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.

3.2.3.1.6 Provisioning – VistA Binding application screens

3.2.3.1.6.1 Binding application home screen

At invocation of the resource “Bind VistA Account” (link in the IdM GUI), Provisioning will perform series of operations in the background to determine a list of VistA instances, available for the user for which he/she can perform Provisioning identity record to VistA account mapping. A user with no VistA accounts registered with provisioning will be shown the full list of available VistA instances returned by the “listTargets” operation. If Provisioning determines that there are VistA instances available for the user to perform the binding action on, the home screen will provide the user the ability to select through a pull down menu an available VistA instance for which he/she can perform the binding of their Provisioning identity record to the specific VistA account. A button to continue the binding process will advance the user to the next screen.

Bind VistA account to Provisioning identity record

1 Select VistA instance 2 Validate Access/Verify codes 3 Bind VistA account

* = Required

Select an available VistA instance

* VistA instance name Choose One (required)

Next Cancel

[Above]Initial screen, for a user who has not been bound or been provisioned through Provisioning to any VistA instance.

A table with all VistA instances the user has been provisioned access to along with their current availability status and user binding status will be displayed.

Bind VistA account to Provisioning identity record

1 Select VistA instance 2 Validate Access/Verify codes 3 Bind VistA account

Select an available VistA instance

Instance #	VistA instance name	Binding status	Availability status
1.	IFCAP	Bound	Available
2.	VistA2	Bound	Unavailable

* Select additional VistA instance Choose One (required)

Next Cancel

[Above]Initial screen, for a user who has been bound or been provisioned through Provisioning to several VistA instances with the remainder of VistA instances available for selection to complete the binding process.

If a user tries to click on “Next” without selecting an instance entry from the pull-down list, an error message informing the user of the problem is displayed and the user is provided with another attempt to select an entry from the available for binding VistA instances.

Bind VistA account to Provisioning identity record

1 Select VistA instance 2 Validate Access/Verify codes 3 Bind VistA account

Select an available VistA instance

* A VistA instance selection from the pull-down selection box is mandatory before proceeding to next step.

Instance #	VistA instance name	Binding status	Availability status
1.	IFCAP	Bound	Available
2.	VistA2	Bound	Unavailable

* Select additional VistA instance Choose One (required)

Next Cancel

[Above]Initial screen, for a user who has been bound or been provisioned through Provisioning to several VistA instances with the remainder of VistA instances available for selection to complete the binding process.

If there are VistA instances, unavailable at the moment, a message informing the user that they can try to initiate the binding process later will be provided as well.

[Above]Initial screen, for a user who has not been bound or been provisioned through Provisioning to any VistA instance, but not all VistA instances are available.

Instance #	VistA instance name	Binding status	Availability status
1.	IFCAP	Bound	Available
2.	VistA2	Bound	Unavailable
3.	VistA3	Bound	Available

[Above]Initial screen, for a user who has been bound or been provisioned through Provisioning to all VistA instances.

If Provisioning determines that there are currently no available VistA instances¹ for the user, but some may become available soon, the home screen will display a message, informing the user that at this time there are no available VistA instances.

¹ Filtered list of instances from the complete list received by using listTargets and the ones the Provisioning user has already been bound with

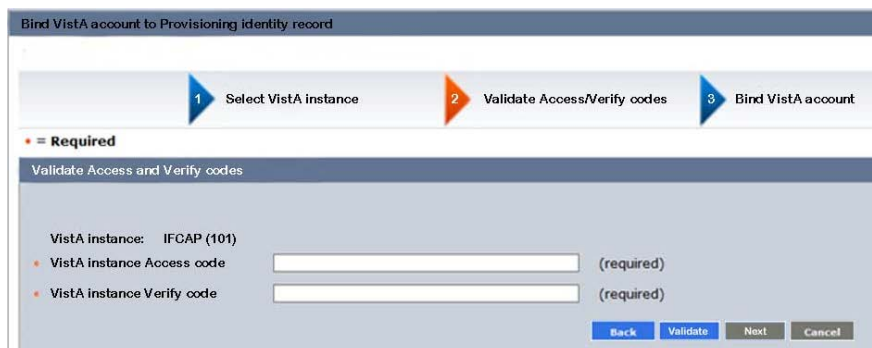


Instance #	VistA instance name	Binding status	Availability status
1.	IFCAP	Bound	Available
2.	VistA2	Bound	Unavailable
3.	VistA3	Bound	Available

[Above]Initial screen, for a user who has been bound or been provisioned through Provisioning to all currently available VistA instances. Additional VistA instances may be accessible shortly.

3.2.3.1.6.2 Access/Verify code input screen

No additional processing will be made between the clicking of the button to continue on the home screen and the display of the “Validate Access/Verify codes” screen.



The Access/Verify code input screen will provide VistA instance information text as well as two password-type (cloaked typing) fields labeled for Access and Verify codes respectively to allow the user to enter the data. A “Validate” button will allow the user to initiate the validation phase of the binding process and receive account profile data².

² This step is necessary to accommodate product restriction on navigational and action buttons. Validation of Access/Verify codes cannot be provided in the same step as navigation to the next screen. If Access/verify codes were to fail, there is no way to force the user to return to the same screen and display the error message and allow the user to retry their validation attempt per [REDACTED] Rel2 i4 RSD requirement.

If Access/Verify codes are validated, a “Next” button is activated, allowing the user to go to the binding process.

If Access/Verify codes are validated, a “Next” button is activated, allowing the user to go to the binding process.

3.2.3.1.6.3 Binding process completion/feedback screen

At the “Bind VistA Account” step, a summary of the pre-binding task of validating the Access/verify codes along with the VistA instance info is displayed. The user then submits (“Finish”) the binding task and the Binding processing sequence correlates the newly-bound VistA account information with the Provisioning User identity record and displays appropriate notification message back to the user. If additional VistA instances, available to the user remain for Binding, the user is provided with an option to go back to the Home screen with pull down selection, otherwise to the home screen with VistA instances status.

VistA accounts data and associated Provisioning server GlobalUser mapping use Provisioning Manager's native functionality to store the data and make the appropriate correlation. Additional requirements, necessary to determine the rules for updates to Provisioning Identity record using at provisioning endpoints data changes (made using VistA instance's native toolset). For more information on the native attribute mapping in the Provisioning server LDAP store, see Appendix A.1, "[REDACTED] Data Elements.xlsx", Prov-Vista tab.

3.2.3.2 CSP Screen Interface

This section shows the screens to which the [REDACTED] 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, Figure 28, 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, Figure 29, 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, Figure 30, 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

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

copyright © 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, Figure 31, 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

* Phone Number
###-###-####

* Street Address

* City

* State

* Country

* 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, Figure 32, 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, Figure 33, 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

* Country

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, Figure 34, 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
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 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  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, Figure 35, 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 
[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, Figure 36, 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 [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 Person being proofed: Rajesh Radhakrishnan

* Address Validation Type Phone bill from local phone service provider

* Postmark Date: Month MM Postmark Day DD Postmark Year YYYY N/A

Street Address 123

City city

State MO

Country UNITED STATES

Postal Code 63368
#####-####

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, Figure 37, 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 Logout

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

* = Required Person being proofed: Amy Ehm

* ID Type United States (U.S.) Passport (unexpired)

* Country of Issuance UNITED STATES

* State of Issuance Choose One:

* Identification Number

* Expiration Date: Month MM Exp Day DD Exp Year YYYY ☐ N/A

* Information Provided/Verified By Choose One:

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, Figure 38, 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: Logout

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

* = Required Person being proofed: Amy Ehm

* ID Type State-Issued Drivers License

* Country of Issuance Choose One:

* State of Issuance Choose One:

* Identification Number

* Expiration Date: Month MM Exp Day DD Exp Year YYYY ☐ N/A

* Information Provided/Verified By Choose One:

Back Next Cancel

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, Figure 39, 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 DOB Month MM DOB Day DD DOB Year YYYY

* User ID

* Phone Number
###-###-####

* Street Address

* City

* State

* Country

* Postal Code
#####-####

* Email

* Affiliation

** Proofing Station # Filter (Not Required)

* 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, Figure 40, 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'. The main form area has a light yellow background. It starts with a note '* = Required' and 'Person being proofed: FIRST TESTER TWO'. The first field is '* Address Validation Type' with a dropdown menu showing 'Choose One:'. Below this is '* Postmark Date' with three dropdowns for 'Month MM', 'Postmark Day DD', and 'Postmark Year YYYY', followed by a checkbox for 'N/A'. The address fields are: 'Street Address' (PO BOX 111112), 'City' (ROUND HILL), 'State' (VA), 'Country' (USA), and 'Postal Code' (20141) with a format hint '####-####'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

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, Figure 41, 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 [redacted] Logout

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

* = Required Person being proofed: Amy Ehm

* ID Type United States (U.S.) Passport (unexpired)

* Country of Issuance UNITED STATES

* State of Issuance Choose One:

* Identification Number

* Expiration Date: Month MM Exp Day DD Exp Year YYYY ☐ N/A

* Information Provided/Verified By Choose One:

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, Figure 42, 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 Person being proofed: Amy Ehm

* ID Type State-Issued Drivers License

* Country of Issuance Choose One:

* State of Issuance Choose One:

* Identification Number

* Expiration Date: Month MM Exp Day DD Exp Year YYYY ☐ N/A

* Information Provided/Verified By Choose One:

Back Next Cancel

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 [REDACTED] 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, Figure 43, 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	Windows Authentication
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.	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.
<input type="text"/> User ID <input type="password"/> Password <input type="button" value="Login"/>	 <input type="button" value="Login"/>	 <input type="button" value="Login"/>
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:	If you experience issues trying to use Windows Authentication, please contact the National Service Desk Support, VBA (Philadelphia):

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, Figure 44, is accessed by end users to authenticate to integrated VA applications with SSOi using only a PIV card.

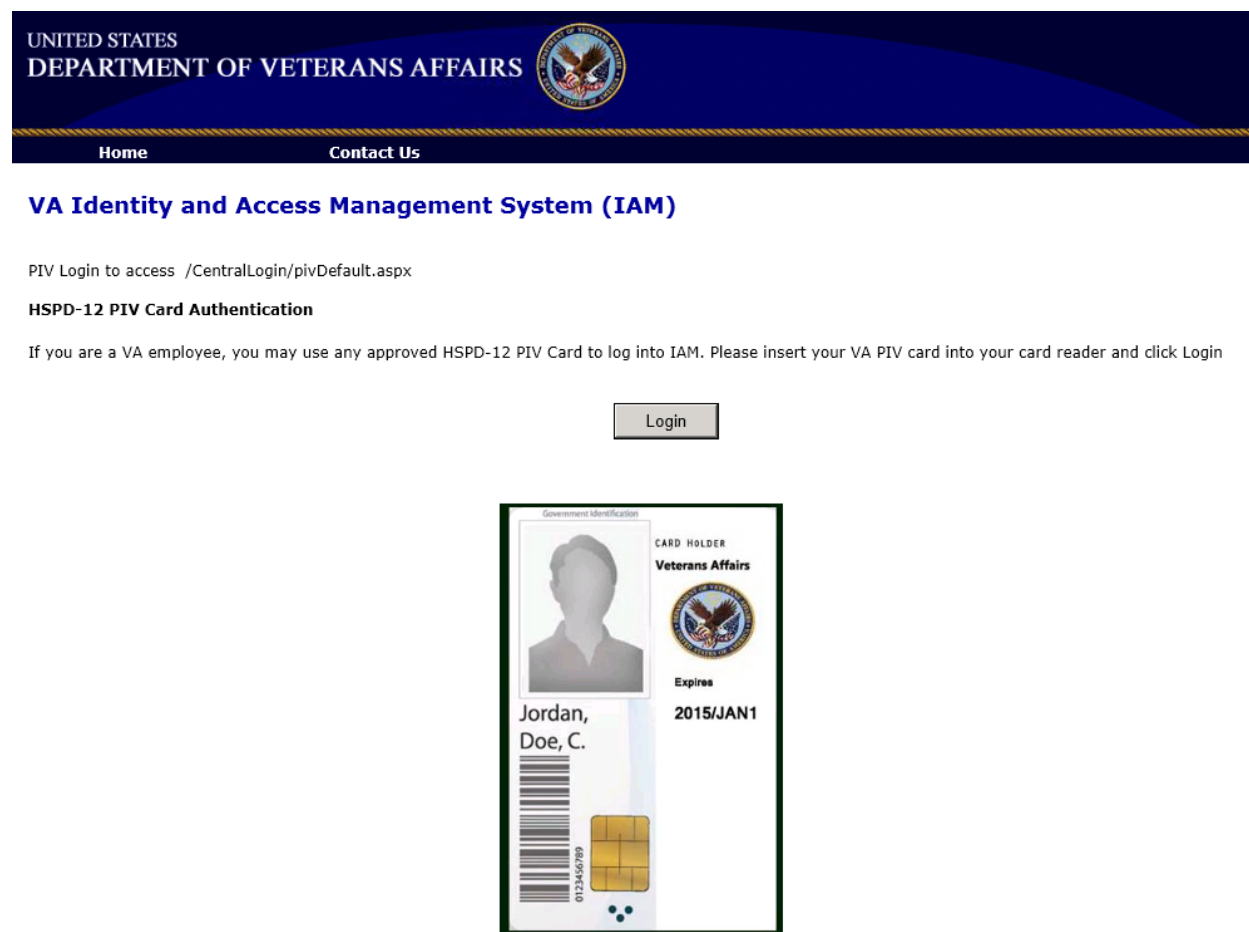


Figure 44: SSOi PIV Only Login Page

3.2.3.4.3 Mobile Login Page

The following screen, Figure 45, 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.

The current release of the Mobile Login page at this time does not have any automation built in for Mobile device or Mobile OS platform recognition. It relies on the device's browser capability to display a relatively lightweight desktop HTML page and scale down/up the resolution of the login page depending on the specific mobile device's capabilities.

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

Enter your VA Active Directory (AD) user ID (i.e. vhaismsmithj) and password below, then click Login.

User ID

Password

Login

If you do not remember your VA Network user ID and password, please contact the National Service Desk Support:

PIV Card

Insert your PIV card into your card reader and click Login. Please enter your PIN when prompted.

Login

If you do not remember your PIN or experience other issues with your PIV card, please contact the National Service Desk Support:

Philadelphia, at 855-675-4557 (Option 5)

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 45: Mobile Login Page

3.2.3.5 SAC Screen Interface

This section shows the screens to which the [REDACTED] users have access to administer the SAC service.

3.2.3.5.1 PAP Landing Page

The following screen, Figure 46, is accessible to SAC privileged users once they initiate the Axiomatics thick client to create or open workspaces for policy authoring.

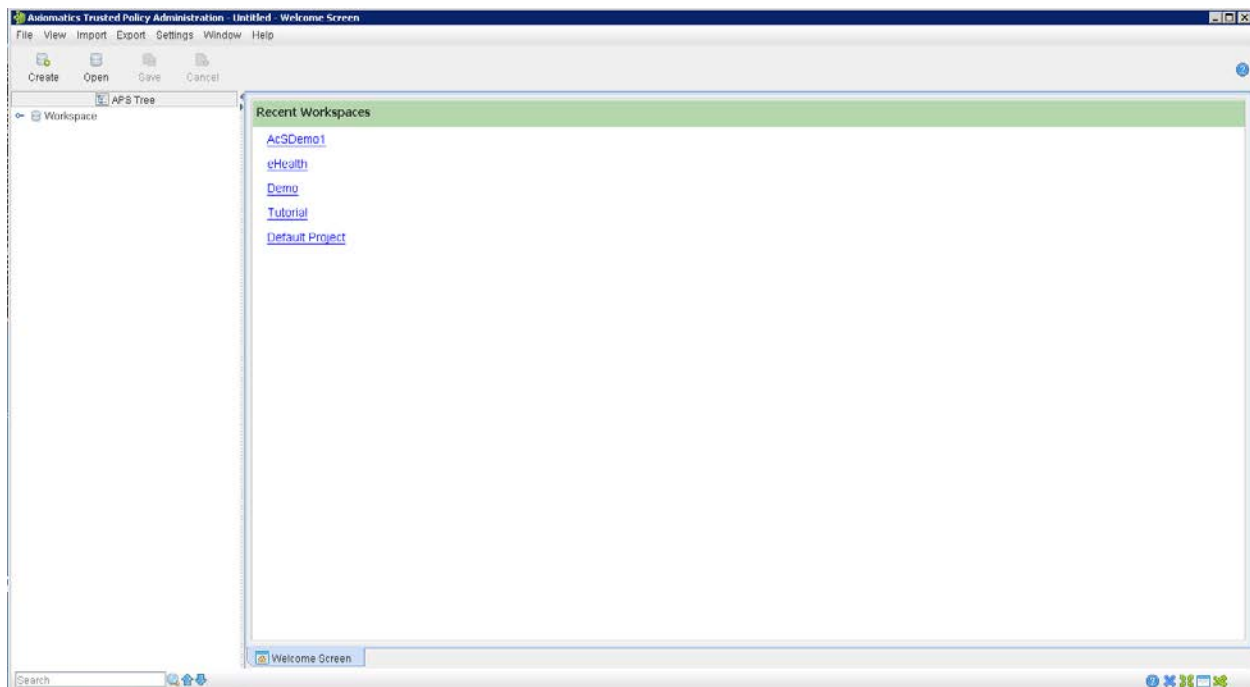


Figure 46: SAC PAP Landing Page

3.2.3.5.2 PAP Authoring Page

Once a workspace is opened or created by the privileged user, the following screen, Figure 47, displays in which the SAC privileged user creates/edits XACML 3.0 policies.

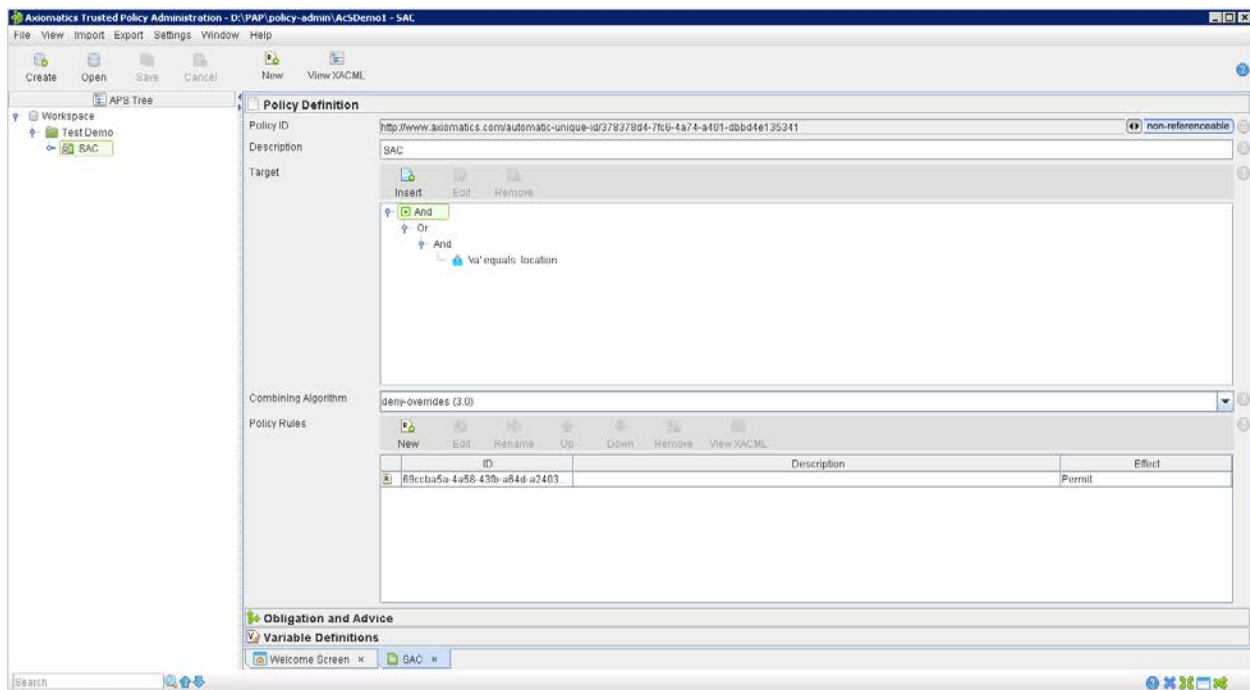


Figure 47: SAC PAP Landing Page

3.2.3.6 [REDACTED] Solution Report Interface

The reporting interface for the [REDACTED] 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 [REDACTED] solution. The section focuses on the primary environments and locations where the [REDACTED] activities are installed. The information is provided as 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 [REDACTED] 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 [REDACTED] 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 [REDACTED] 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 [REDACTED]	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 [REDACTED] 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 [REDACTED] 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 [REDACTED] infrastructure environment is set up at the Terremark data center in Culpeper, Virginia. The alternate site or disaster recovery site for VA [REDACTED] operations is the Terremark data center in Miami, Florida.

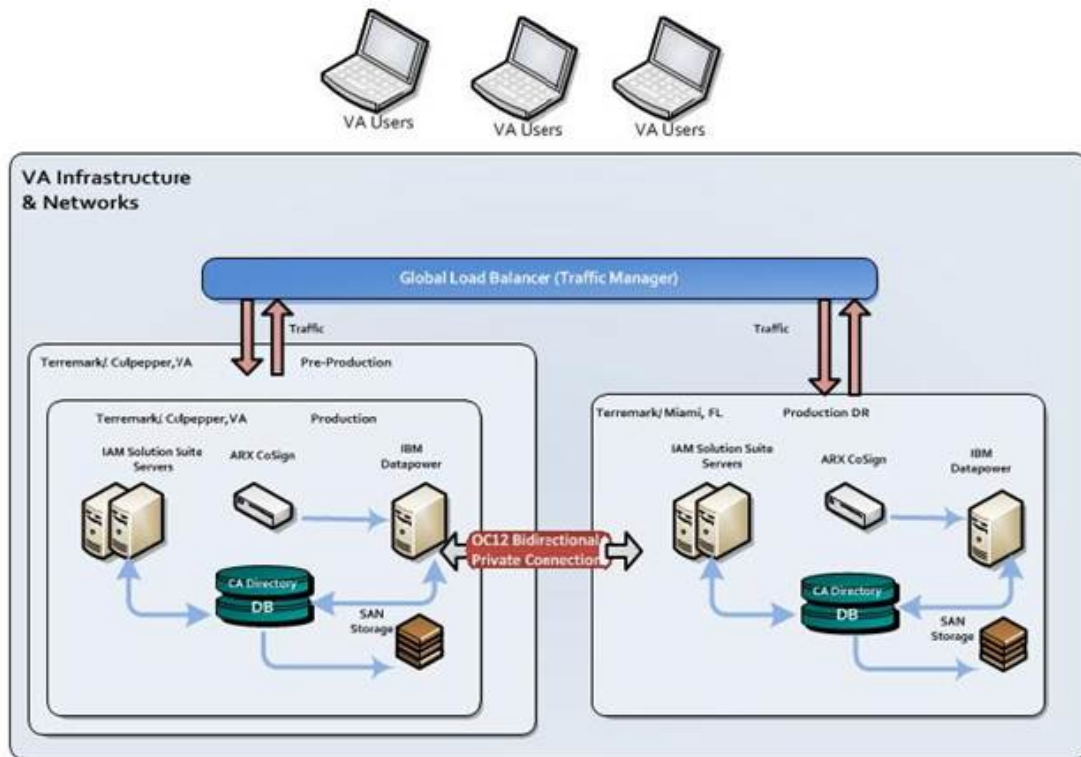


Figure 48: [REDACTED] Production Environments

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 [REDACTED] 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 [REDACTED] 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, Figure 49, provides a logical view of the [REDACTED] solution components.

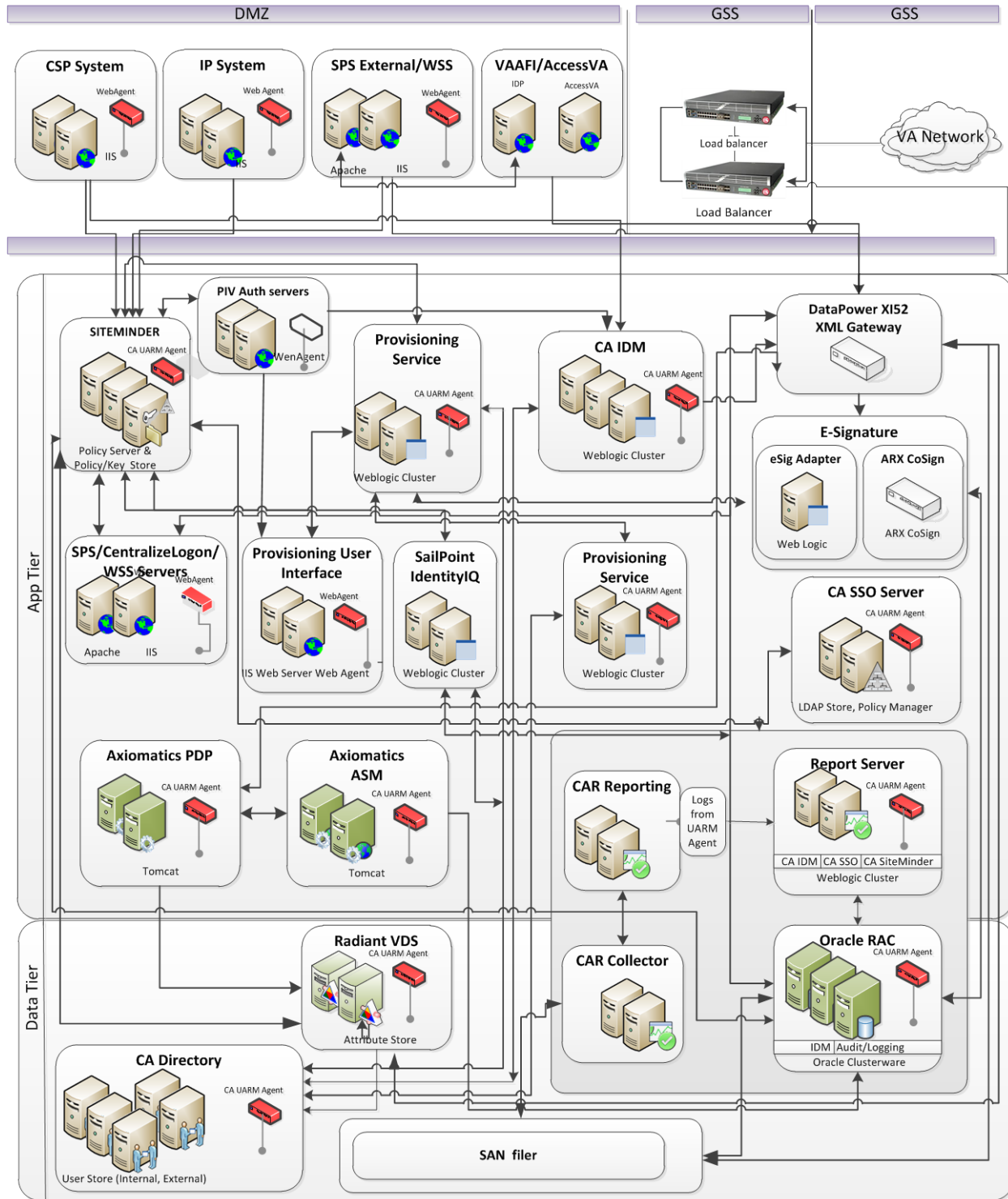


Figure 49: Logical Network String Diagram

4 System Architecture

The 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 [REDACTED] solution. The communication architecture describes the connection and security requirements needed between the hardware components.

4.1 Hardware Architecture

The following diagram, Figure 50, shows the [REDACTED] solution hardware architecture and network topology.

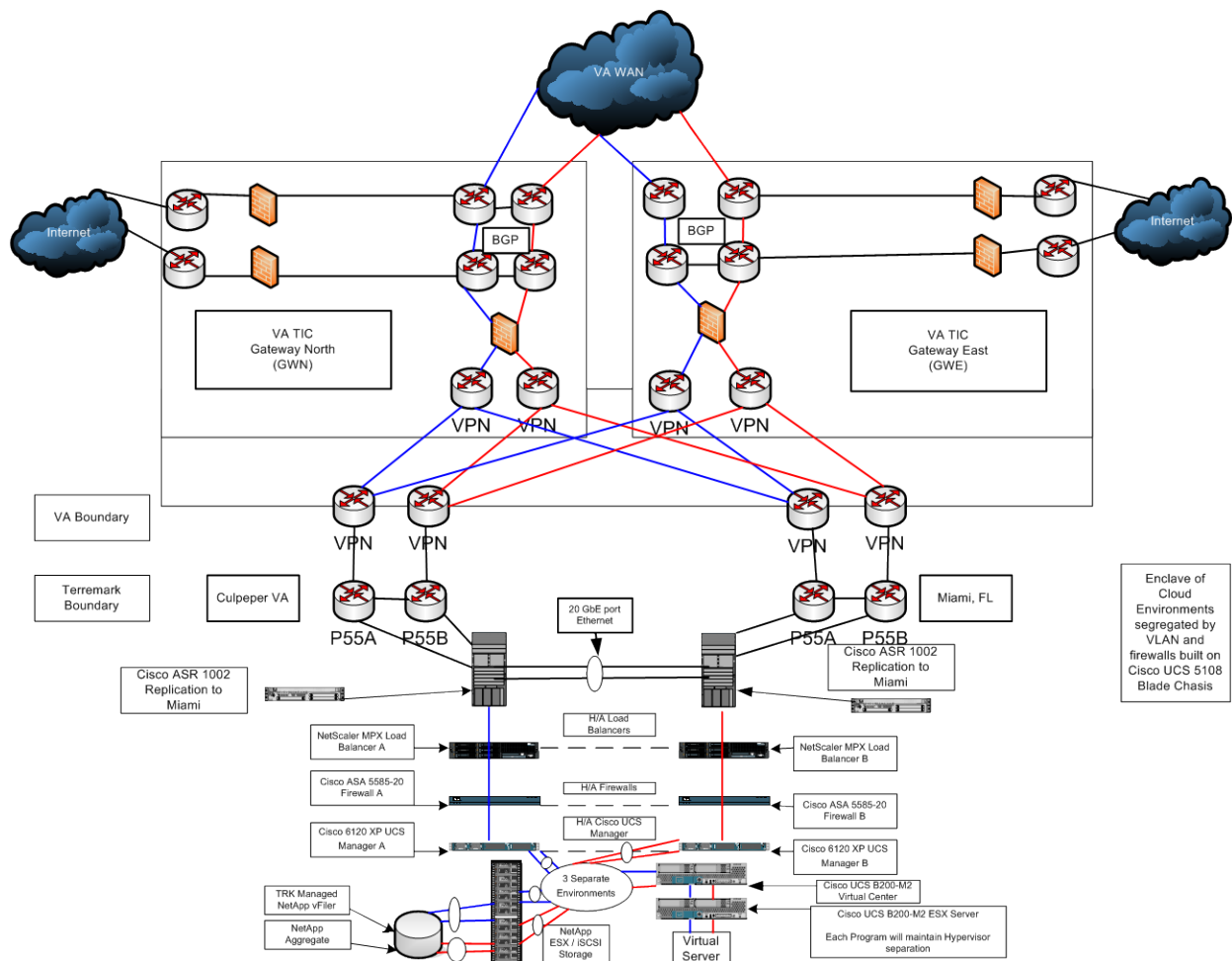


Figure 50: Network Communication Architecture

The following table provides information for the hardware appliances used for the VA [REDACTED] 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)	<p>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.</p>	<p>The ARX CoSign device has a built-in mechanism to provide High Availability configuration. eSig's HA setup uses two CoSign appliances. One is defined as the primary and the other is designated as the secondary cluster member. All information processed by the primary appliance is replicated securely to the secondary appliance using IPSEC protocol. In case of a replication failure, up to ten retries are made and if still unsuccessful, an alert is sent to the designated eSig administrator point of contact as configured on the appliance. The custom eSig webApplication under normal circumstances always communicates with the primary CoSign device. The communication is configurable through a property file. In case of hardware problems and/or maintenance periods when the secondary appliance needs to be made the primary and vice-versa, a change in the eSig WebApplication property file is not necessary as the switching of the roles of the appliances, swaps their network configuration as well. Currently there is no replication between the eSig cluster information across physical sites - e.g. Production appliances in Terremark's Culpeper, VA Production site do not share information with their counterparts in the Miami, FL Disaster recovery site. Additional backup/restore procedures will be necessary to switch eSig to use a different physical site in case of emergency or actual disaster recovery.</p>

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

The uniform resource locators (URLs) for CSP, IP, CAR, Provisioning, SAC, SSOi, VDS, and eSig for production, pre-production and SQA are provided in the table below. The [REDACTED] 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 [REDACTED] application components, will reside in the GSS. The following table provides details on the [REDACTED] solution machines such as ports, URLs, protocols hostnames for each application in every environment.

**Table 21: Virtual Machines and Appliances
SQA (AITC)**

Application	Number of VMs	Number of Physical Servers	Hostname
CSP, IP, Federation Services WebUI, SPS, WSS (IIS- Single instance on each, Tomcat)	5	N/A	[REDACTED]
IdentityMinder supporting (Credential Service Provider and Identity Proofing) WebLogic cluster Admin service on primary node	3	N/A	
Centralized Logon page, SPS, WSS (IIS- Single instance on each)	1	N/A	

Application	Number of VMs	Number of Physical Servers	Hostname
PIV Authentication Handler (IIS) Single instance on each No OCSP responder or CRL configuration	1	N/A	
IdentityMinder support (Provisioning Service) (WebLogic) Admin service on primary node	2	N/A	
Provisioning WebUI (IIS) Single instance on each	2	N/A	
Provisioning Server	2	N/A	
CA Directory (CSP and IP)	3	N/A	
CA Directory (Provisioning)	2	N/A	
CA SSO Server	2	N/A	
CA SSO	2	N/A	
CA UARM (Tomcat)	4	N/A	
CA Report Server (Weblogic)	2	N/A	

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	
Axiomatics PDP (Tomcat)	1	N/A	
Axiomatics ASM/PAP (Tomcat)	1	N/A	
Axiomatics Policy Auditor	1	N/A	
Radiant Logic VDS	Not Applicable	1	
Oracle RAC	Not Applicable	2	
DataPower XI50 (Appliance)	Not Applicable	2	
ARX CoSign (Appliance)	Not Applicable	1	
eSig Weblogic Servers Admin service on primary node	2	N/A	
Role manager (SailPoint) servers (WebLogic) Admin service on primary node	2	NA	

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	
Centralized Logon page, SPS, WSS (IIS) Single IIS instance on each Web403/404 will replace 413/414	2	N/A	
PIV Authentication Handler (IIS) Single IIS instance on each	2	N/A	
IdentityMinder supporting (Credential Service Provider and Identity Proofing) (Weblogic) Admin service on primary node	2	N/A	
IdentityMinder support (Provisioning Service) (Weblogic) Admin service on primary node	3	N/A	
Provisioning WebUI (IIS) Single IIS instance on each	2	N/A	

Application	Number of VMs	Number of Physical Servers	Hostname
Provisioning Server	2	N/A	
CA Directory (CSP and IP)	2	N/A	
CA Directory (Provisioning)	2	N/A	
CA SSO Server	2	N/A	
CA UARM	3	N/A	
CA Report Server	1	N/A	
CA SiteMinder (Weblogic) includes CA Directory instance for SiteMinder Admin service on primary node Admin UI on primary node	3	N/A	
Axiomatics PDP (Tomcat)	2	N/A	
Axiomatics ASM/PAP (Tomcat)	1	N/A	

Application	Number of VMs	Number of Physical Servers	Hostname
Radiant Logic VDS	N/A	1	
Oracle Database	N/A	2	
DataPower XI52 (Appliance)	Not Applicable	N/A	
ARX CoSign (Appliance)	Not Applicable	N/A	
eSig WebLogic Servers Admin service on primary node	2	N/A	
Role manager (SailPoint) servers (WebLogic) Admin service on primary node	2	N/A	

Production (Terremark Culpeper, VA)

Application	Number of VMs	Number of Physical Servers	Hostname
CSP,IP,Federation Services WebUI,SPS,WSS (IIS) Single IIS instance on each	4	N/A	
Centralized Logon page, SPS, WSS (IIS , Tomcat) Single IIS instance on each	2	N/A	

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	
IdentityMinder (CSP and IP) (Weblogic) Admin service on primary node	2	N/A	
IdentityMinder (Provisioning) (Weblogic) Admin service on primary node	3	N/A	
Provisioning WebUI (IIS) Single IIS instance on each	2	N/A	
Provisioning Server	2	N/A	
CA Directory (CSP,IP)	2	N/A	
CA Directory (Provisioning)	2	N/A	
CA SSO Server	2	N/A	
CA UARM	3	N/A	

Application	Number of VMs	Number of Physical Servers	Hostname
CA Report Server (WebLogic)	1	N/A	
CA SiteMinder (WebLogic) includes CA Directory instance for SiteMinder Admin service on primary node Admin UI on primary node	3	N/A	
Axiomatics PDP (Tomcat)	2	N/A	
Axiomatics ASM/PAP (Tomcat)	1	N/A	
Radiant Logic VDS	N/A	2	
Oracle Database	N/A	2	
DataPower XI52	Not Applicable	N/A	
ARX CoSign	Not Applicable	N/A	
eSig WebLogic Servers	2	N/A	
Role manager (SailPoint) servers (WebLogic)	2	N/A	


DR (Terremark Miami, FL)

Application	Number of VMs	Number of Physical Servers	Hostname
CSP,IP,Federation Services WebUI (IIS)	4	N/A	
Centralized Logon page, SPS, WSS (IIS, Tomcat)	2	N/A	
PIV Authentication Handler (IIS)	2	N/A	
IdentityMinder (CSP) (WebLogic)	2	N/A	
IdentityMinder (Provisioning) (WebLogic)	3	N/A	
Provisioning WebUI (IIS)	2	N/A	
Provisioning Server	2	N/A	
CA Directory (CSP and IP)	2	N/A	

Application	Number of VMs	Number of Physical Servers	Hostname
CA Directory (Provisioning)	2	N/A	
CA SSO Server	2	N/A	
CA UARM	3	N/A	
CA Report Server (WebLogic)	1	N/A	
CA SiteMinder (WebLogic) includes CA Directory instance for SiteMinder	2	N/A	
Axiomatics PDP (Tomcat)	2	N/A	
Axiomatics ASM/PAP (Tomcat)	1	N/A	
Radiant Logic VDS	N/A	2	
Oracle Database	N/A	2	
DataPower XI52 (Appliance)	N/A	N/A	

Application	Number of VMs	Number of Physical Servers	Hostname
ARX CoSign (Appliance)	N/A	N/A	
eSig WebLogic Servers	2	N/A	

4.2 Software Architecture

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

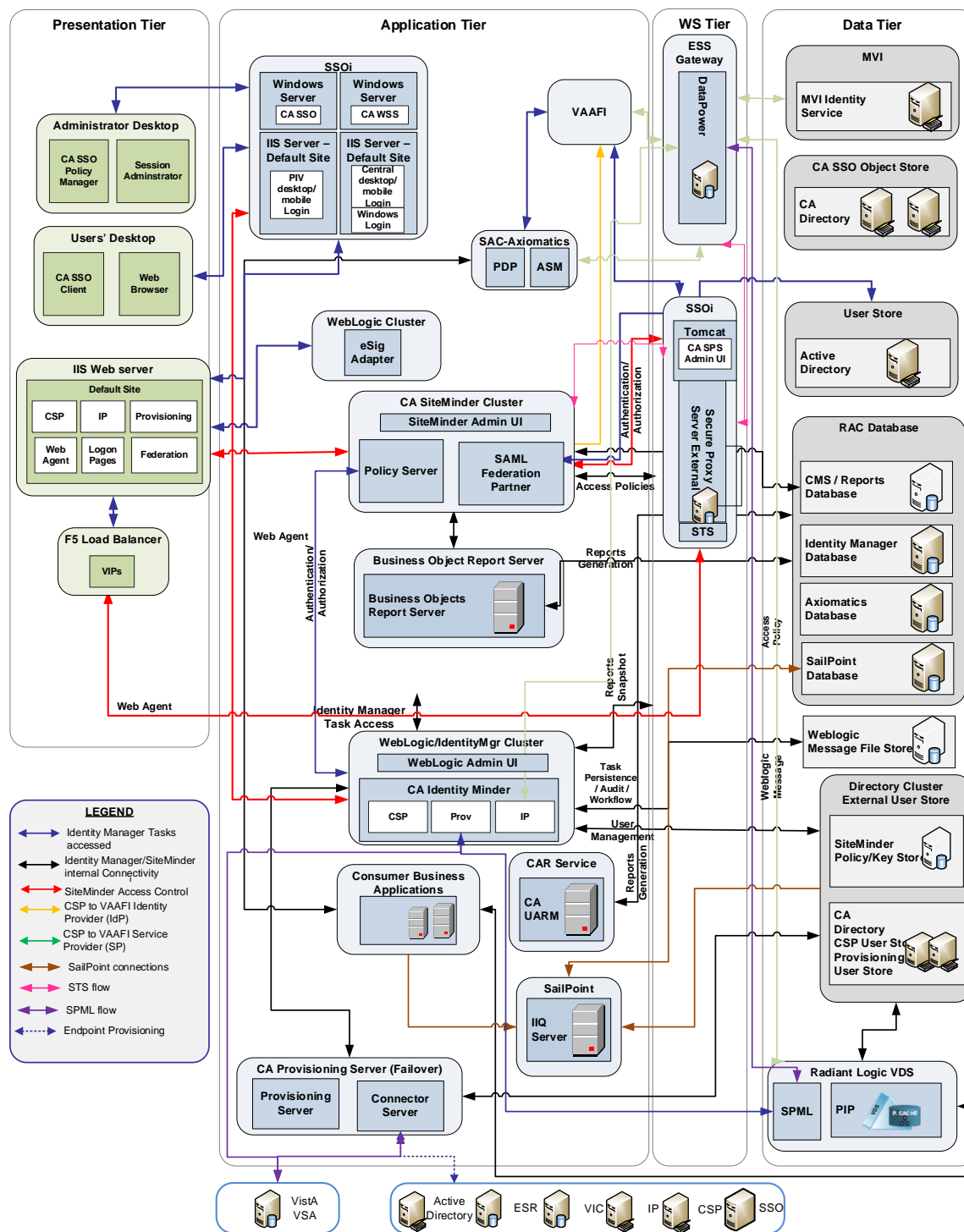


Figure 51: Software Architecture

The following table describes the [REDACTED] solution products for each of the [REDACTED] services and versions.

**Table 22:  Products and Versions
Credential Service Provider (CSP)**

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

Single Sign-On – Internal (SSOi)

Products	Abbreviation	Product Version/Release
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)

Products	Abbreviation	Product Version/Release
CA IdentityMinder	CA IdentityMinder	R12.6 SP3
IIS Web Sever	-	7.5
CA Web Agent	-	SM r12.51/12.0SP3
WebLogic	-	10.3.6(TRM Compliant till Q3-2016) Planned upgrade to 12c Q1-2015
Oracle Database	-	11gR2
CA Directory	LDAP directory	12.0 SP7
CA SiteMinder	CA SM 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
Radiant Logic VDS	Attribute Service & Policy Information Point	6.2.2
SailPoint Unified Governance Platform	SailPoint IdentityIQ Access Governance Manager	v6.1p2
SPML	Service Provisioning Markup Language	SPML v2.0

Specialized Access Control (SAC)

Products	Abbreviation	Product Version/Release
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)

Products	Abbreviation	Product Version/Release
CA User Activity Reporting Module ³	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)

Products	Abbreviation	Product Version/Release
ARX Co-Sign	Digital Signature	v6.3
WebLogic	-	10.3.6(TRM Compliant till Q3-2016) Planned upgrade to 12c Q1-2015

Identity Proofing (IP)

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

The following table provides information about the software components.

Table 23: Software Components
Oracle Database 11gR2

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

Characteristic	Description
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	<p>For the [REDACTED] 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.</p>

CA Directory

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

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

Characteristic	Description
Directory Instances	User store CA IdentityMinder for CSP solution and Provisioning services, Policy and Key store for CA

Characteristic	Description
	SiteMinder for CSP service Object/policy store for CA SSO for SSOi services.
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 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 that provide reverse proxy and federation to the applications.

Characteristic	Description
IIS Web Server Instances	CA IdentityMinder Registration / user profile management/admin UI for CSP service
High Availability	<p>IIS Web Servers are used by the CSP, centralized logon, PIV Auth and Federation servers to support multiple services. They will be CSP Login / Registration, Provisioning, and protected by the SiteMinder Option Pack (Federation), PIV Authentication Servers, and Centralized Logon Server Page.</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</p>

Characteristic	Description
	<p>maintain the session for the entirety of each user transaction. In the event that all of the IIS web servers fail on Terremark Culpeper, VA site, the Citrix NetScaler load balancer will be configured to route the traffic to Terremark Miami, FL site.</p> <p>There are two IIS web servers required by CA IdentityMinder, which are load balanced by the Citrix NetScaler load balancer. The IIS web servers for provisioning service reside in Terremark.</p> <p>There are two IIS web servers required for PIV, Federation, and Centralized logon.</p>


Application Tier – WebLogic Application Server

The application tier for the Provisioning service is made up of a cluster of WebLogic application servers. The Application Tier is a shared environment for hosting application components. The  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.

Characteristic	Description
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</p>

Characteristic	Description
	failover. Therefore, when the instances in a Clusternode fail, they will failover to the alternate cluster node.

Application Tier –Tomcat Application Server

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  related applications hosted are listed below. The Axiomatics PDP and ASM components are hosted on the Tomcat application servers.

Characteristic	Description
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.

Characteristic	Description
Subcomponents	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.

Characteristic	Description
	<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> <p>Policy Auditor: Simplifies the analysis and validation process of XACML policies. Provides a user-friendly web-based graphical interface.</p>
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.

Characteristic	Description
Subcomponents	<p>IdentityMinder Server: Executes workflows within IdentityMinder. It includes the Management Console and the User Console deployed on a WebLogic cluster.</p> <p>Provisioning Server: Manages the lifecycle of user accounts on endpoint systems. This server is required, as the CA IdentityMinder installation will support account provisioning.</p> <p>User store: The IdentityMinder user store is maintained by CA IdentityMinder. This is an existing store that contains the user identities that a company needs to manage. The user store for VA  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.

Characteristic	Description
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 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

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.

Characteristic	Description
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>
High Availability	<p>A number of components for CA SSO that 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

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.

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. Additionally, according to CA vendor, UARM is near its End-Of-Life, and attempting to migrate from the CentOS linux to RedHat Enterprise linux platform in order bring CAR in compliance with TRM is not going to be vendor supported.

Characteristic	Description
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> <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 Web Application

The eSig custom WebApplication is the isolation layer for the core eSig appliance, providing the client/partner exposed eSig functionality. eSig uses the CoSign appliance as a building block and provides the capability to digitally sign documents to applications within VA. All events, associated with each digital signing, verification or user deletion operations, are recorded and made available to the CAR service for reporting.

Characteristic	Description
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>Java Web Application</p> <p>The eSig Web Application is a standard J2EE application utilizing a combination of MVC and Façade design patterns. The eSig servlet, part of the abbreviated MVC pattern, currently accepts only SOAP WebService calls but can be extended with a Web UI if required. The Façade pattern component carries out the following categories of operations:</p> <ul style="list-style-type: none"> ○ User Management: The user management function allows the service to add or remove an eSig 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 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 eSig uses run on separate VMs (systems). The eSig WebApplication runs within an application server cluster 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 High availability feature within the ARX CoSign appliances requires a minimum of two CoSign appliances is configured for manual failover through switching of the roles of the current primary and secondary appliances. In case of failure of the primary CoSign appliance, the secondary is promoted to a primary and it takes over the eSig tasks. Active-Active load balancing of the requests among the two devices is not supported. Replication of the configuration and user data is ensured between the two devices, thus allowing for manually initiated failover with</p>

Characteristic	Description
	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.

Radiant Logic VDS

Radiant Logic VDS acts as an abstraction layer, extracting identity and context information from various (in-scope) applications and data silos.

Characteristic	Description
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)

Role manager (SailPoint) is the centralized tool that 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.

Characteristic	Description
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

Characteristic	Description
	<p>data</p> <p>3- Configure access re-certifications</p> <p>SailPoint Unified Governance Platform (SP UGP): The SP UGP centralizes identity data, captures business policy, models roles, and approaches managing identity data on a risk-based, approach.</p> <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  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  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 components and protocols used.

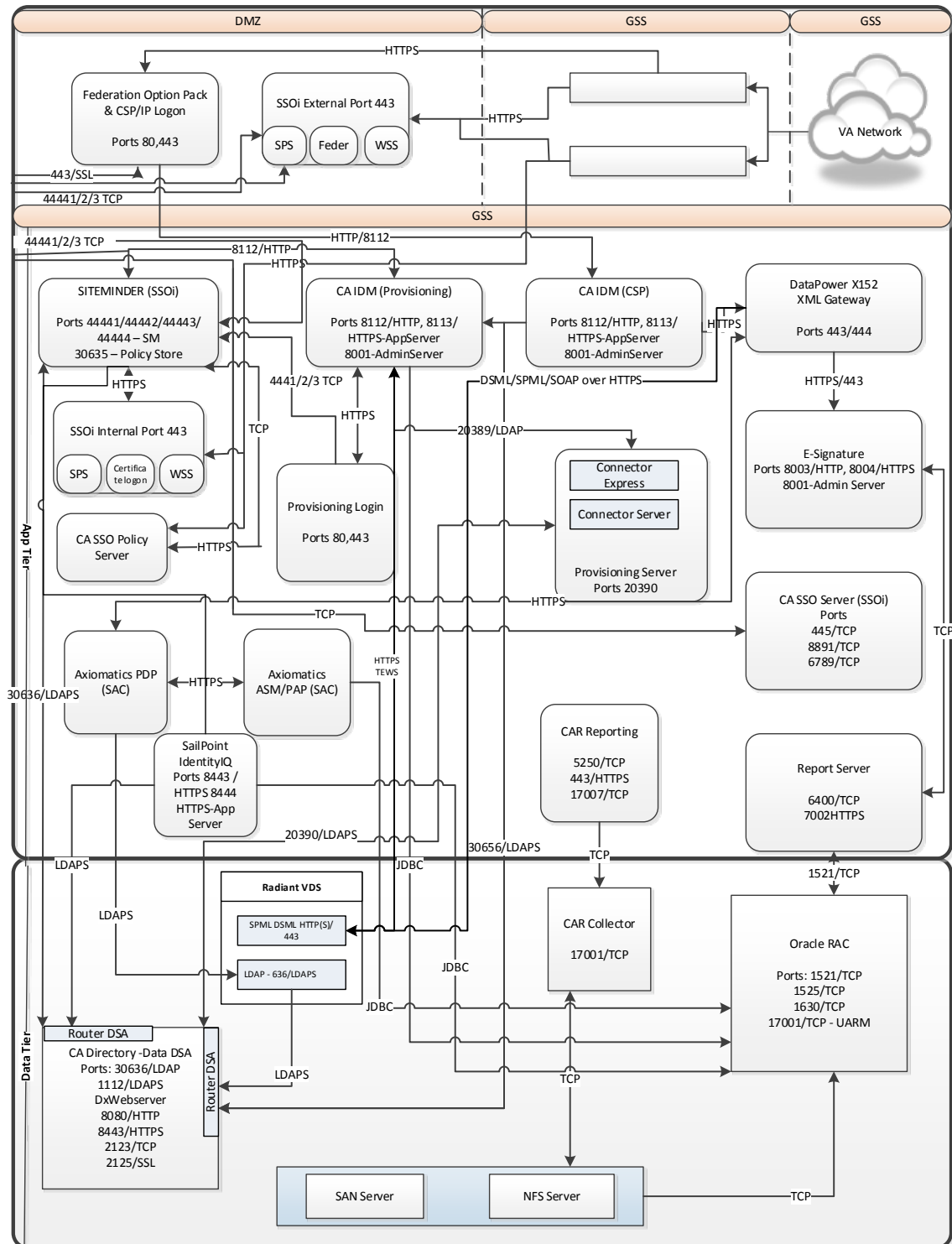


Figure 52: [REDACTED] Network Security Topology

4.4 Communication Channel Security

In order for [REDACTED] system components to communicate internally (within the boundaries of [REDACTED] 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 [REDACTED] 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 [REDACTED] 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 <http://vaww.pki.va.gov/ssltls/>. The following lists the server certificates for the [REDACTED] components:

- The publicly accessible [REDACTED] 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 [REDACTED] DMZ component.
- The SSL/TLS certificates assigned to the [REDACTED] external access URLs were requested from and issued by VAs commercial (publicly trusted) certificate authority - GTE Cybertrust
- The [REDACTED] native components communicating TCP/IP layer secured FIPS mode of encryption.
- VA Internal User Access
- [REDACTED] Infrastructure Security

4.5 [REDACTED] 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 [REDACTED] 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)
Oracle Database	Internal		DataGuard	TCP
Oracle Database	Internal		Connection Manager	TCP
Oracle Database	Internal		Oracle Management Agent	TCP
Oracle Database	Internal		Oracle Enterprise Database Console (HTTP Port)	HTTP

Application	Network	Port(s)	Reason	Protocol(s)
Oracle Database	Internal		Oracle Enterprise Database Console (RMI Port)	TCP
Oracle Database	Internal		Oracle Enterprise Database Console (JMS Port)	TCP
Oracle Database	Internal		Agent command and control listening port	TCP
Oracle Database	Internal		CA UARM collection server	TCP
Oracle Database	Internal		SAILPT – Role manager internal database	TCP
CA Directory (CSP,IP, Provisioning)	Internal		Provisioning router dsa	TCP
CA Directory (CSP,IP, Provisioning)	Internal		Provisioning main dsa	TCP
CA Directory (CSP,IP, Provisioning)	Internal		Provisioning common objects dsa	TCP
CA Directory (CSP,IP, Provisioning)	Internal		Provisioning inclusions dsa	TCP
CA Directory (CSP,IP, Provisioning)	Internal		Provisioning notify dsa	TCP
CA Directory (CSP,IP, Provisioning)	Internal		DXWebserver Listener (SSL)	HTTPS
CA Directory (CSP,IP, Provisioning)	Internal		DXWebserver Listener for shutdown command	TCP
CA Directory (CSP,IP, Provisioning)	Internal		Dxmanager-DXadmin communication	TCP
CA Directory (CSP,IP, Provisioning)	Internal		CSP/PROV/SMPS Router DSA	LDAPS
CA Directory (CSP,IP, Provisioning)	Internal		CSP Data DSA	LDAPS

Application	Network	Port(s)	Reason	Protocol(s)
CA Directory (CSP,IP, Provisioning)	Internal		SMPS Data DSA	LDAPS
CA Directory (CSP,IP, Provisioning)	Internal		PROV Data DSA	LDAPS
CA Directory (CSP,IP, Provisioning)	Internal		DXadmin Secure LDAP	TCP
CA Directory (CSP,IP, Provisioning)	Internal		Agent command and control listening port	TCP
CA Directory (CSP,IP, Provisioning)	Internal		CA UARM Collection Server	TCP
Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI)	DMZ		Accounting port	TCP
Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI)	DMZ		Authentication port	TCP
Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI)	DMZ		Authorization port	TCP
Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI)	DMZ		Auditing Port	TCP

Application	Network	Port(s)	Reason	Protocol(s)
Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI)	DMZ		SSL port for reverse proxy	HTTPS
Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI)	DMZ		Agent command and control listening port	TCP
Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI)	DMZ		CA UARM Collection Server	TCP
CA Report Server	Internal		WebLogic Port for Report Server	HTTPS
CA Report Server	Internal		Central Management Console Server Port	TCP
CA Report Server	Internal		Agent command and control listening port	TCP
CA Report Server	Internal		CA UARM Collection Server	TCP
Federation Option Pack	DMZ		ServletExec port for listening incoming requests from IIS	TCP
Federation Option Pack	DMZ		Agent command and control listening port	TCP
Federation Option Pack	DMZ		CA UARM Collection Server	TCP
CA Identity Manager (CSP,IP, Provisioning)	Internal		Administration Port	HTTPS
CA Identity Manager (CSP,IP, Provisioning)	Internal		Manage Server Port	TCP

Application	Network	Port(s)	Reason	Protocol(s)
CA Identity Manager (CSP,IP, Provisioning)	Internal		Node Manager	TCP
CA Identity Manager (CSP,IP, Provisioning)	Internal		Agent command and control listening port	TCP
CA Identity Manager (CSP,IP, Provisioning)	Internal		CA UARM Collection Server	TCP
Provisioning Server	Internal		Provisioning Server	TCP
Provisioning Server	Internal		Agent command and control listening port	TCP
Provisioning Server	Internal		CA UARM Collection Server	TCP
CA SiteMinder	Internal		Accounting port	TCP
CA SiteMinder	Internal		Authentication port	TCP
CA SiteMinder	Internal		Authorization port	TCP
CA SiteMinder	Internal		Auditing Port	TCP
CA SiteMinder	Internal		SSL port for reverse proxy	HTTPS
CA SiteMinder	Internal		WebLogic port for SiteMinder Admin UI	TCP
CA SiteMinder	Internal		Agent command and control listening port	TCP
CA SiteMinder	Internal		CA UARM Collection Server	TCP
CA SiteMinder SPS	DMZ/Internal		Apache HTTP Port	HTTP
CA SiteMinder SPS	DMZ/Internal		Apache SSL port	HTTPS
CA SiteMinder SPS	DMZ/Internal		Tomcat/ SPS HTTP Port	HTTP
CA SiteMinder SPS	DMZ/Internal		Tomcat/SPS SSL Port	HTTPS
CA UARM	Internal		Administration Port for CA UARM	TCP

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

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


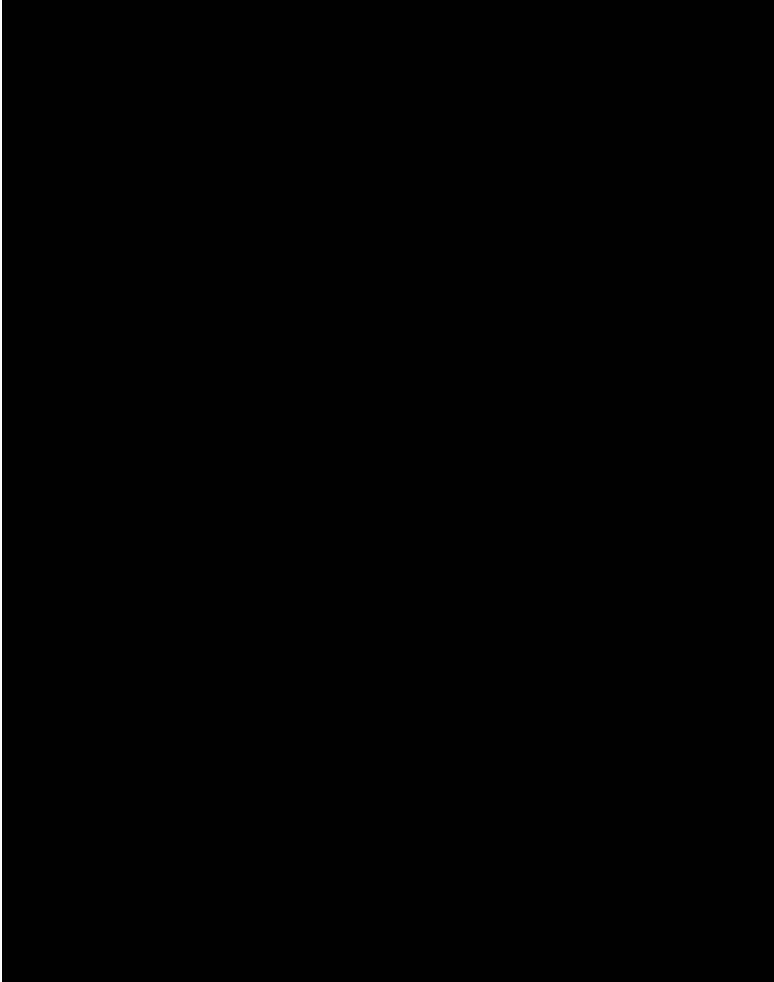
Table 27 and Figure 28 provide the  solution inter-component communications details.

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)	

Computer Name (Hostname)	Common Name (CN)	FQDN	Cert Type	Issuer	Cert Function	Description	Comments
			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	
			Internal	VA	Web URL	PIV authentication	
			External	VA	Web URL	SiteMinder SPS	

Computer Name (Hostname)	Common Name (CN)	FQDN	Cert Type	Issuer	Cert Function	Description	Comments
			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
			Internal	VA	SSL	CA Directory	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 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

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

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

4.5.1 Production Server PKI Certificate List

Table 28: Production Cert List

Computer Name (Hostname)	Common Name (CN)	FQDN	Cert 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
			External	External CA	Web URL	FQDNs for Citrix NetScaler Load balancer N/A

Computer Name (Hostname)	Common Name (CN)	FQDN	Cert Type	Issuer	Cert Function	Comments
			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
			Internal	VA	Web URL	FQDNs for Citrix NetScaler Load balancer N/A

Computer Name (Hostname)	Common Name (CN)	FQDN	Cert 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	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
			Internal	VA	SSL	Management
			Internal	VA	SSL	Management


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


Computer Name (Hostname)	Common Name (CN)	FQDN	Cert Type	Issuer	Cert Function	Comments
			Internal	VA	Server	
			Internal	VA	SSL	Management interface
			Internal	VA	Web Service	Dispatcher Service
			Internal	VA	URL	
			Internal	VA	Server	
			Internal	VA	SSL	Management interface
			Internal	VA	Web Service	Dispatcher Service
			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	Server	Also serve as auditing cert
			Internal	VA	SSL	Management
			Internal	VA	SSL	WebLogic port

Computer Name (Hostname)	Common Name (CN)	FQDN	Cert Type	Issuer	Cert Function	Comments
			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  solution as well as the data security implementation.

5.1 DBMS Files

The  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/cspidm_data
CPIPIDM_INDX	+ORADATA/acsdbs/datafile/cspidm_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 [REDACTED] 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 [REDACTED] 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 [REDACTED] solution and its activities in detail.

6.1 Hardware Detailed Design

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

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



20131108 - [REDACTED] IAM
TerreMark PreProd ar

6.2 Software Detailed Design

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

6.2.1 Provisioning Design

The Provisioning service is an integral component of the [REDACTED] 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.

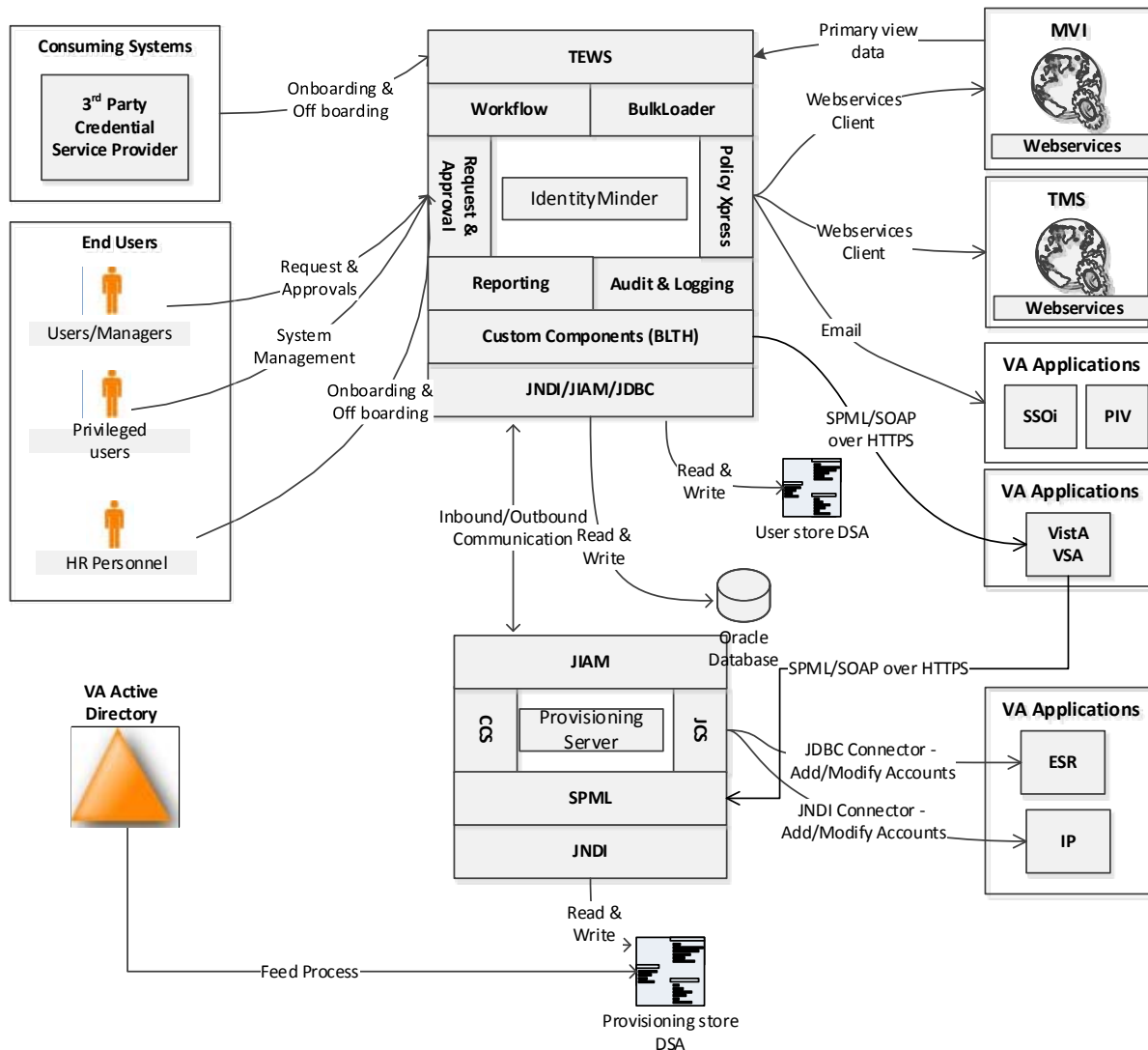


Figure 53: Provisioning Detail Design

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 [REDACTED] 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

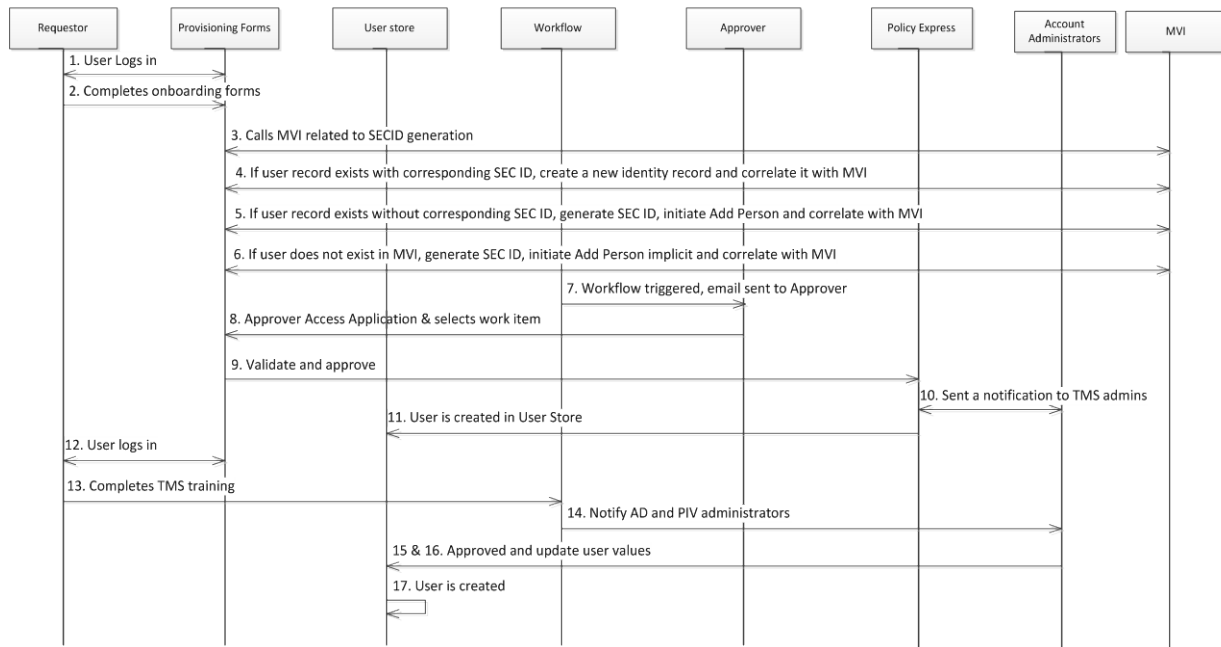


Figure 54: Provisioning User Onboarding Sequence Diagram

Table 30: 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	<ol style="list-style-type: none"> 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 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

Field	Description
	<p>to be on boarded and submit the IdentityMinder task</p> <ol style="list-style-type: none"> IdentityMinder makes a call to MVI, to check the existence of the record If the user record exists with corresponding Sec ID, then the CA IdentityMinder validates the identity record with the SEC ID returned from MVI exists in Provisioning, otherwise returns an error. 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. 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 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 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 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 The user will be created in the user store of provisioning system HR/Sponsor/COR: with required privileges login to CA IdentityMinder, the system which implements the provisioning system HR/Sponsor/COR access the CRISP checklist select the “TMS training completed” checkbox Workflow associated with the task gets triggered and sends notification to Active Directory administrators and PIV system administrators 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 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 The user will be created in the user store of provisioning system
Main Success Scenarios	<ol style="list-style-type: none"> Successful generation of SEC ID for VA employee/contractor/HP Trainees/Volunteers 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"> SEC ID creation process error out Failure in creation of user in provisioning system

6.2.1.2 Provisioning: Third-Party / DoD Onboarding

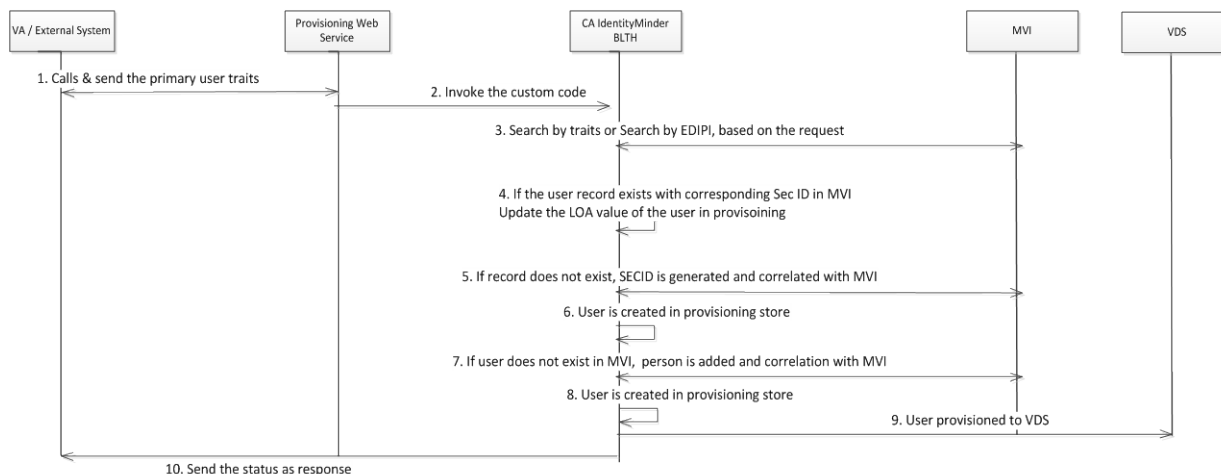


Figure 55: Provisioning: Third-Party / DoD Onboarding Sequence Diagram

Table 31: 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	1. Provisioning Service – web service 2. VA / External System 3. Provisioning Service – CA IdentityMinder 4. MVI 5. VDS
Pre-Conditions	1. The VA system have appropriate access privileges to access provisioning service to onboard user
Trigger	1. The VA / External System calls Provisioning service for onboarding
Actions	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 (US and foreign(3-letter country code, Province/Region and Postal Code)), Date of Birth, Email(optional), Gender , EDIPI(optional), CSP ID and LOA. Along with the attributes, a self-asserted Boolean value will be passed, to inform whether the attribute value is self-asserted or CSP provided 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

Field	Description
	<p>as traits to search the user.</p> <ol style="list-style-type: none"> 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"> 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. 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 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 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 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. The user will be created in the user store of provisioning system, with all the attributes including MVI_ attributes returned from the search. 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. The user will be created in the user store of provisioning system, with all MVI attribute values The provisioning record is provisioned to VDS system The provisioning system sends a response to the VA system on the status of the operation
Main Success Scenarios	<ol style="list-style-type: none"> Successful generation of Sec ID for third-party user 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"> Sec ID creation process error out Failure in creation of user in provisioning system or VDS

The Provisioning 3-rd party user onboarding web service function description is provided in the following table.


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

Table 32: Provisioning Web Service Function

Method /Function	Description of Method/Function	Input	Output
VAThirdPartyOnboardUser Profile()	Onboard a third party user into	<ol style="list-style-type: none"> First Name (Required) FNSelfAssert (Required) 	SECID (10 digits)

Method /Function	Description of Method/Function	Input	Output
	provisioning store	- 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)	– string)

6.2.1.3 Provisioning: Update Provisioning Record from MVI

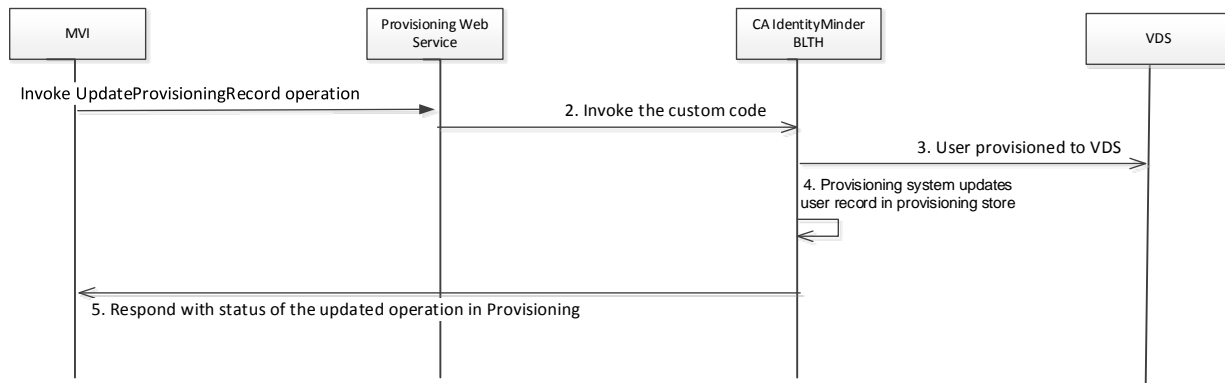


Figure 56: Provisioning: Update Provisioning Record from MVI Sequence Diagram

Table 33: 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	<ol style="list-style-type: none"> 1. MVI system have appropriate access privileges to access provisioning service to update the user
Trigger	<ol style="list-style-type: none"> 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 UpdateProvisioningRecord() 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 and Address (US and foreign(3-letter country code, Province/Region and Postal Code)). 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
Main Success	Successful update of user record in provisioning and VDS

Field	Description
Scenarios	
Main Failure Scenarios	Failure in update of user in provisioning system or VDS

6.2.1.4 Provisioning: User Offboarding

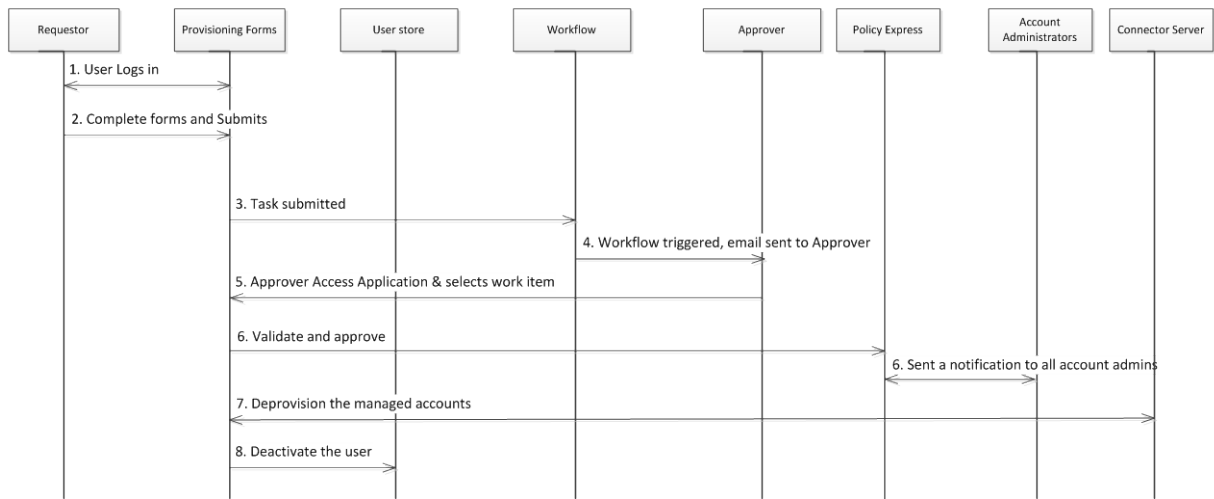


Figure 57: Provisioning: User Offboarding Sequence Diagram

Table 34: 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"> Provisioning Service (CA Identity Minder) (Provisioning forms, workflow, policy express, Connector Server) HR/Sponsor/COR (Requestor) VA Manager (Approver) User Store Account Administrators
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 provides notice for separating from employment to VA Manager. VA Manager/Sponsor is notified of breach of rules by VA Employee
Actions	<ol style="list-style-type: none"> Requester with proper privileges login to CA IdentityMinder to initiate user off boarding process Requestor access the appropriate form to submit a request for off boarding

Field	Description
	<p>a user</p> <ol style="list-style-type: none"> Workflow associated with the task gets triggered and appends a work item to the HR/Sponsor/COR queue. Workflow sends an email to the HR/Sponsor/COR to Approve/Reject the off boarding of user to the provisioning system 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 user 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 system Provisioning system will de provision accounts for managed endpoints via connector server User is deactivated in the user store and roles / group membership are updated accordingly
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	<p>Error during deactivation of VA Employee/Contractor/HP Trainees/Volunteers in the provisioning system</p>

6.2.1.5 Provisioning: User Provisioning

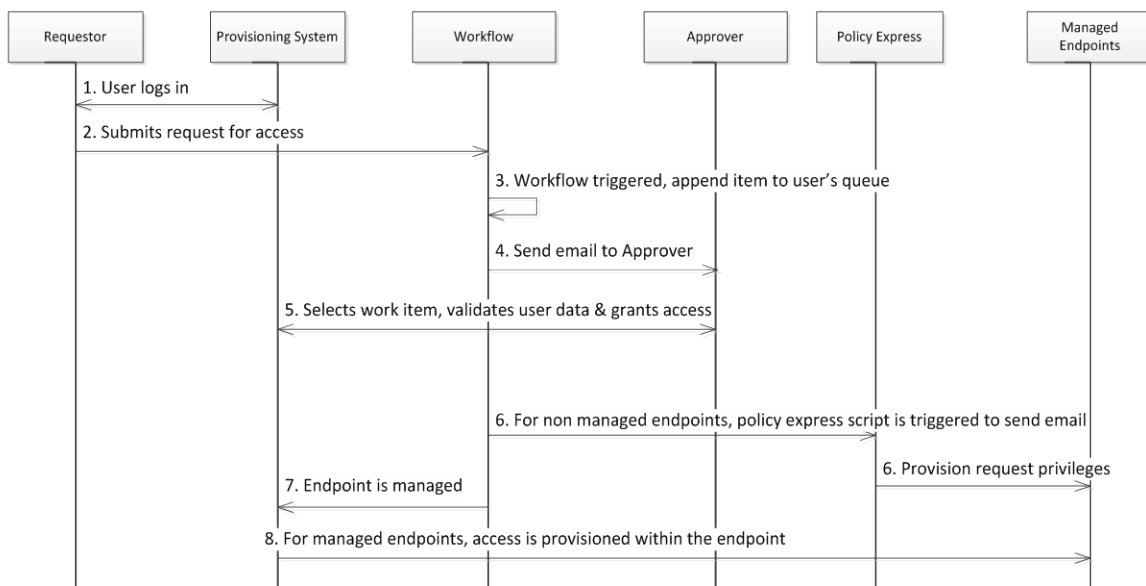


Figure 58: Provisioning: User Provisioning Sequence Diagram**Table 35: Provisioning: User Provisioning**

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"> 1. Provisioning Service (Provisioning system, workflow, policy express) 2. Employee/Contractor (Requestor) 3. VA Manager (Approver) 4. Managed Endpoints (via Account Administrators for non-managed endpoints)
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 requires access to VA application to perform their job function
Actions	<ol style="list-style-type: none"> 1. Requester with proper privileges login to CA IdentityMinder to request access to a managed endpoint 2. Requestor accesses the access request form and submits a request for access to an endpoint 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 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 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 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 provision the access. 8. Provisioning Server connects with the appropriate connector server and provision the request privileges at the endpoint
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

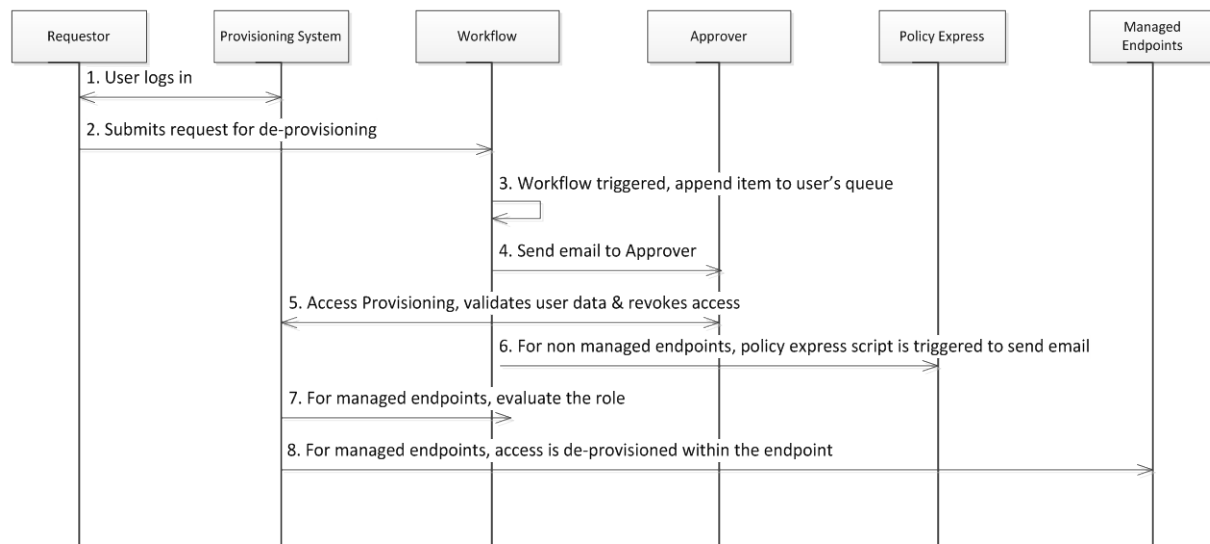


Figure 59: User De-Provisioning Sequence Diagram

Table 36: 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"> 1. Provisioning Service (Provisioning system, workflow, policy express) 2. Employee/Contractor (Requestor) 3. VA Manager (Approver) 4. Managed Endpoints (via Account Administrators for non-managed endpoints)
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 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

Field	Description
	<p>request</p> <ol style="list-style-type: none"> 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 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 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. Provisioning Server connects with the appropriate connector server and connects to the endpoint and de-provision the request privileges
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

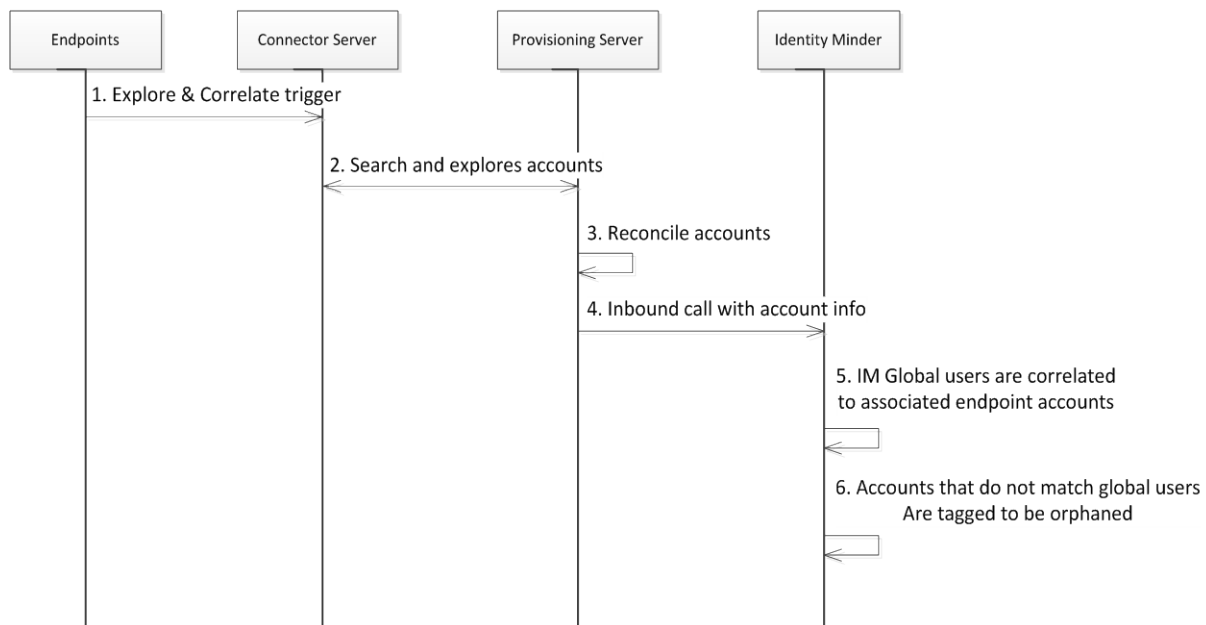


Figure 60: Explore and Correlate from Endpoints Sequence Diagram

Table 37: Explore and Correlate from Endpoints

Field	Description
Use Case	Explore and Correlate from Endpoints

Field	Description
Name	
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 gets 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 operation 2. Connector Server searches the endpoint and explores the account and pass it to the provisioning server 3. Provisioning server reconciles the explored accounts with the existing global user for correlation 4. Provision server does the inbound call to the IdentityMinder on the explored and correlate accounts 5. 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 account 6. The accounts that do not match global users are tagged to be orphaned
Main Success Scenarios	The identities from the VA application are explored and correlated successfully

Field	Description
Main Failure Scenarios	Failure to run the explore and correlate job

6.2.1.8 Provisioning: VistA VSA use cases

This section contains the use cases for the integration between Provisioning and VistA VSA. Those use cases have been represented as Rational Rose process flow (activity) diagrams.

6.2.1.8.1 Request New VistA User Account (Prov(SPML(add))→VistA VSA)

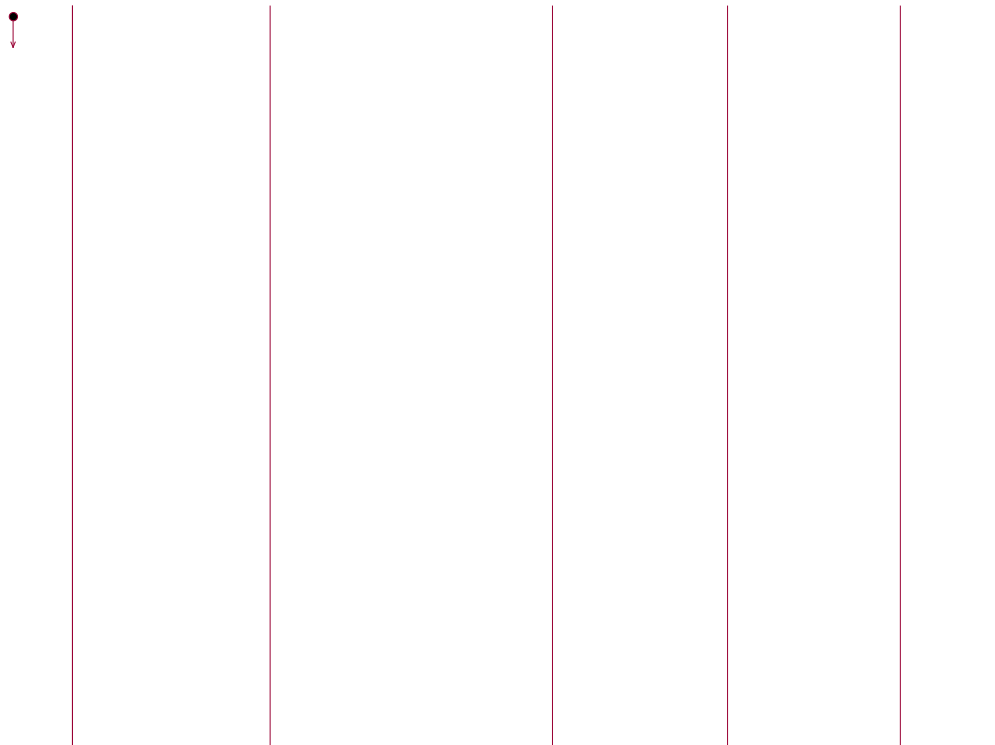


Figure 61: Request New VistA User Account (Prov(SPML(add)) VistA VSA)

Note: Access/Verify codes requirements are addressed as part of the “binding” process after the user is provisioned in a particular VistA instance

6.2.1.8.2 Correlate an Existing VistA User Account with Provisioning User's Identity Record (VistA VSA (SPML(add))→Prov)

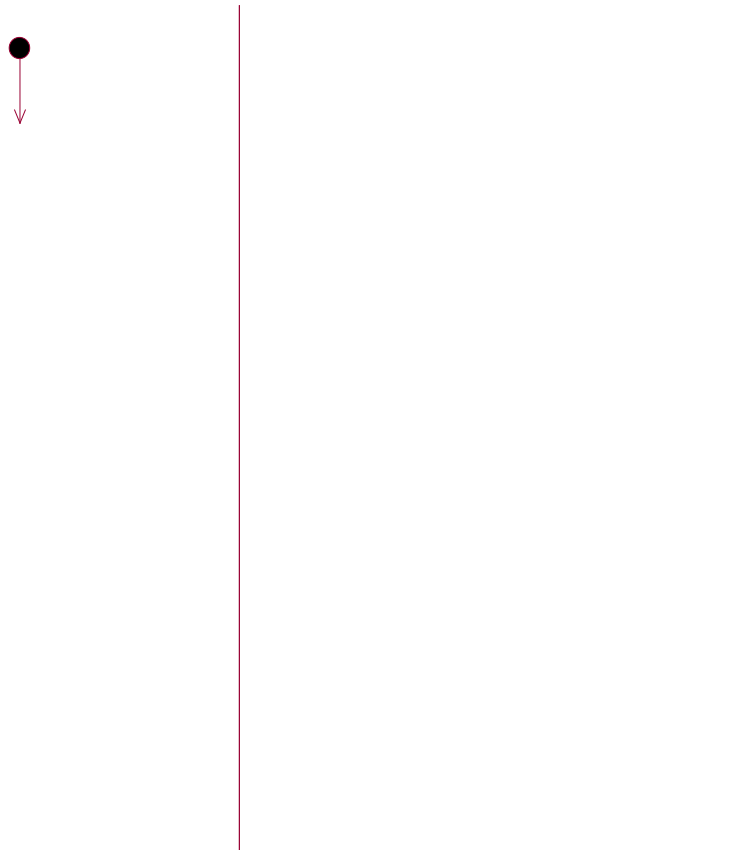


Figure 62: Correlate an Existing VistA User Account with Provisioning User's Identity Record (VistA VSA (SPML(add))→Prov)

6.2.1.8.3 Modify VistA User Account (Prov(SPML(modify))→VistA VSA)

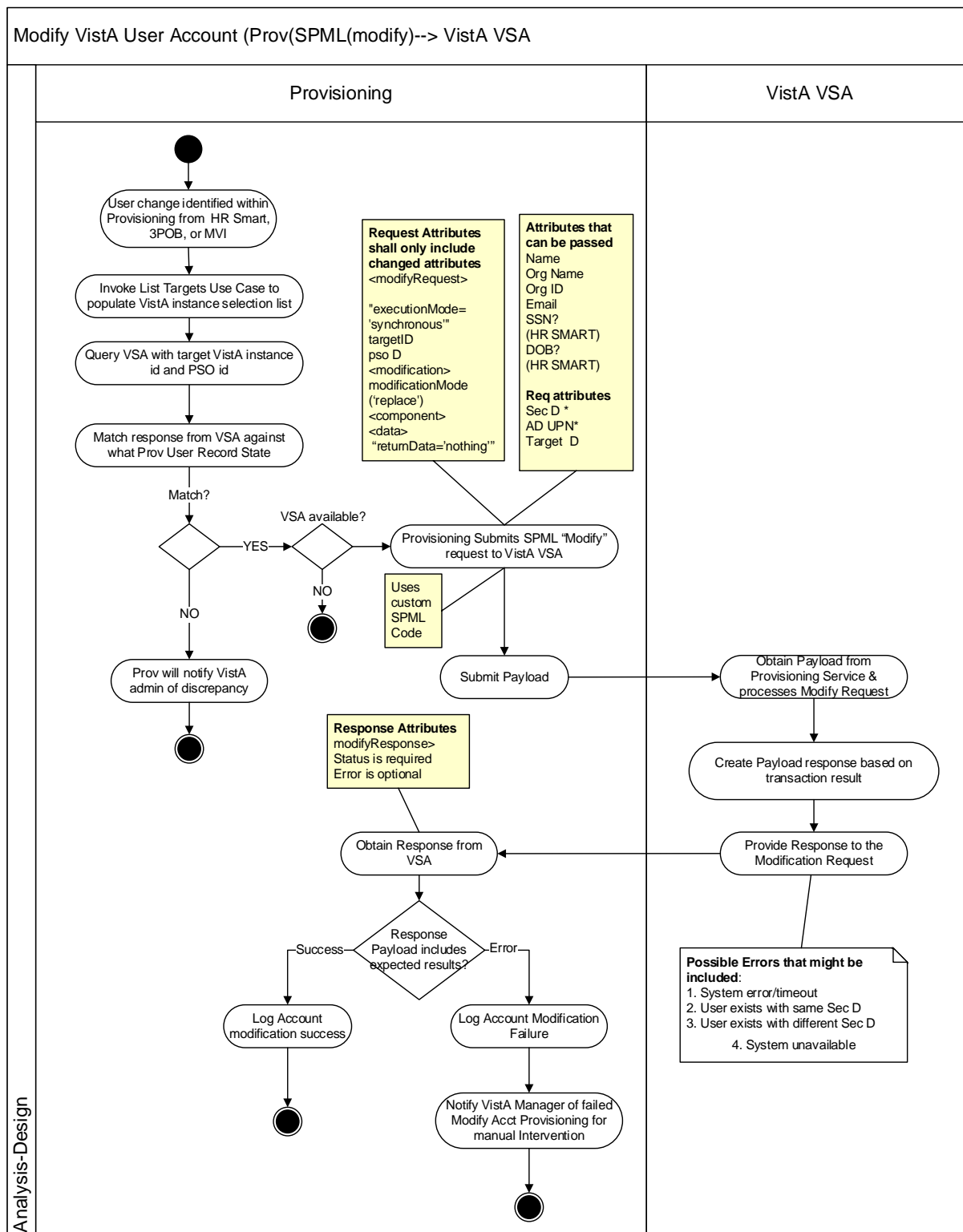


Figure 63: Modify VistA User Account (Prov(SPML(modify)))

□ VistA VSA)

6.2.1.8.4 Update Provisioning User's Identity Record Correlated VistA User Account Data (VistA VSA(SPML(modify))→Prov)

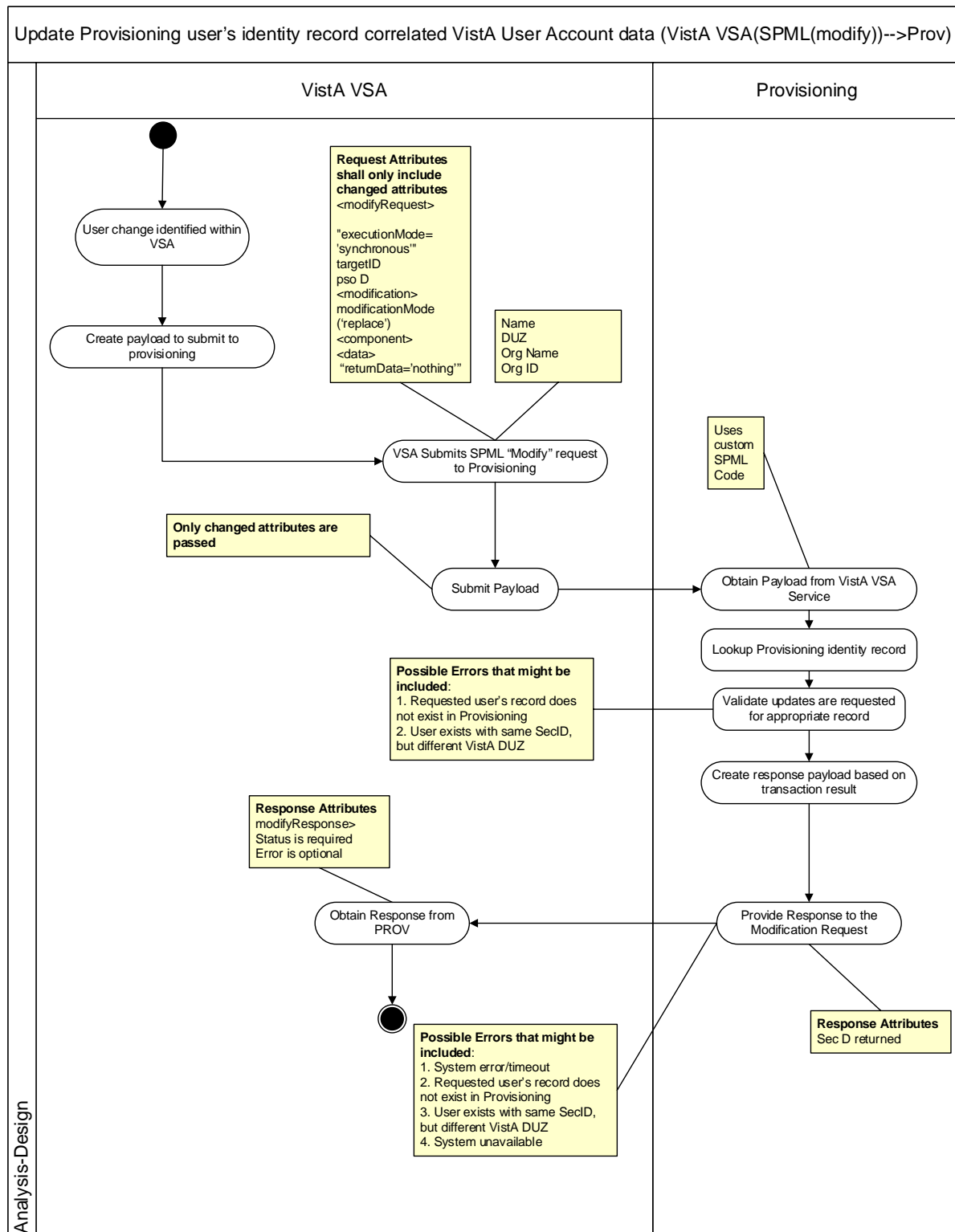


Figure 64: Update Provisioning User's Identity Record Correlated VistA User Account Data

6.2.1.8.5 Search for VistA User Account(s) (Prov (SPML(search))→VistA VSA)

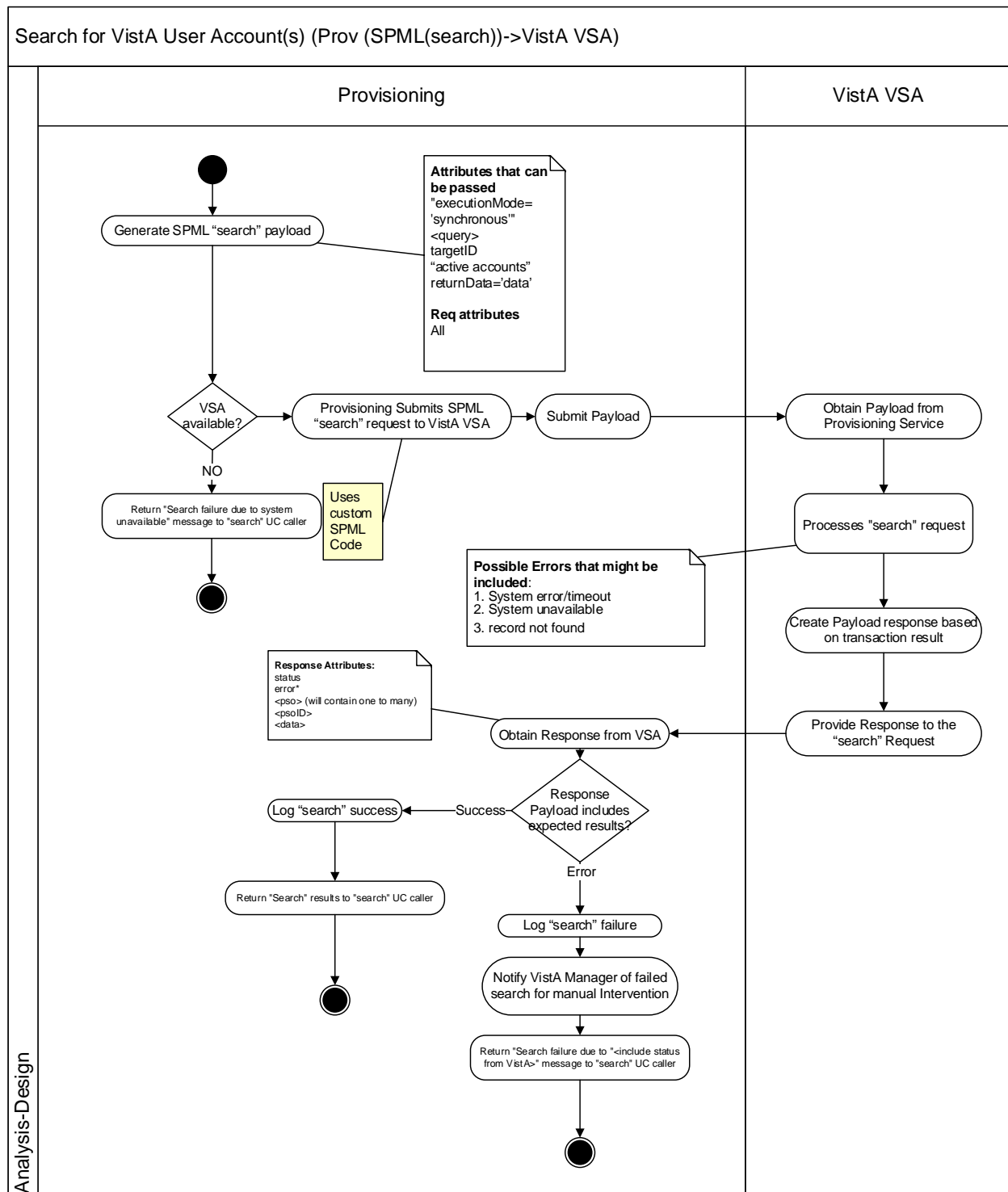


Figure 65: Search for VistA User Account(s) (Prov (SPML(search)))

□ VistA VSA)

6.2.1.8.6 Get VistA Instances (Prov(SPML(listTargets))→VistA VSA)

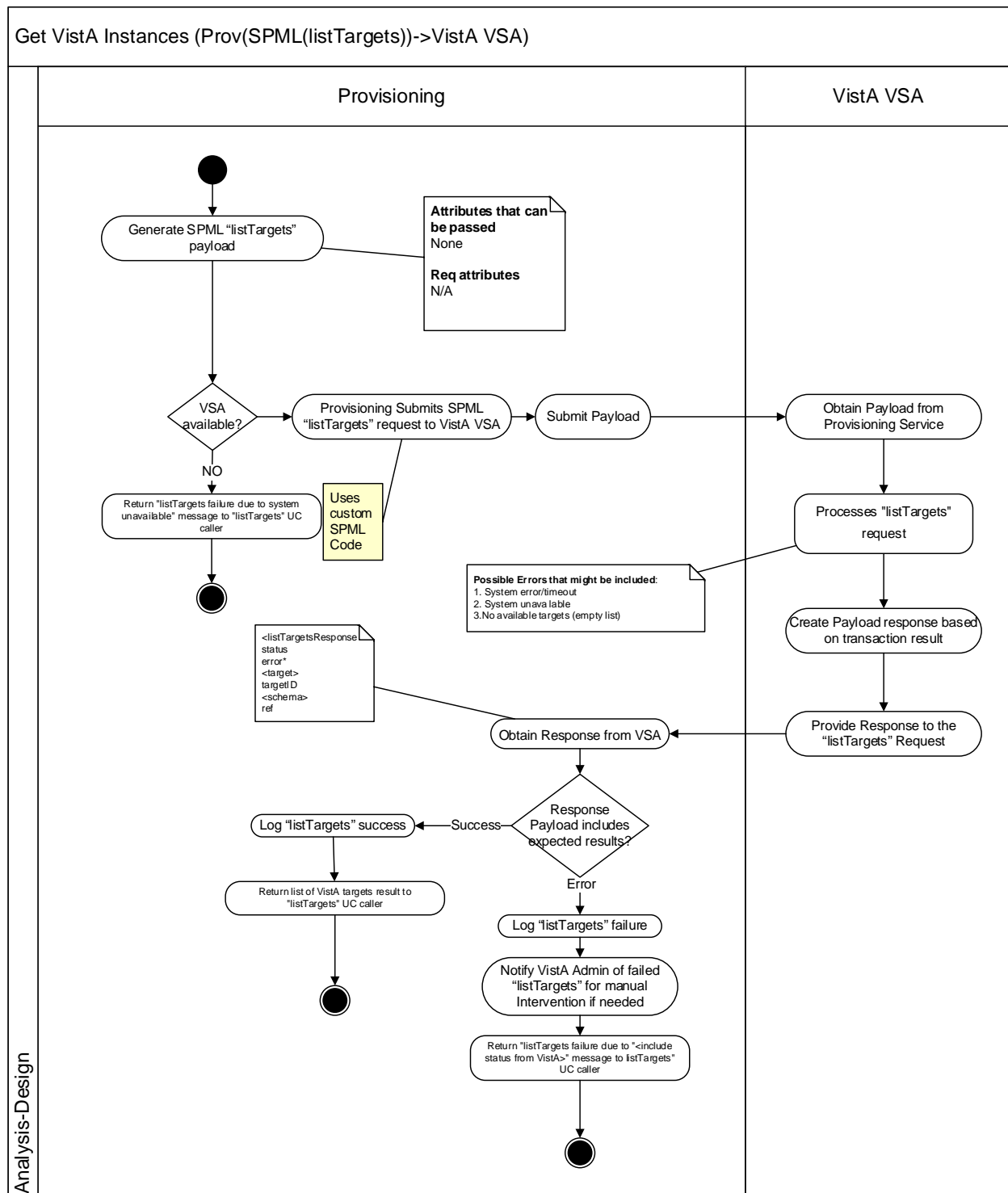


Figure 66: Get VistA Instances (Prov(SPML(listTargets))

□ VistA VSA)

6.2.1.8.7 Retrieve Vista User Account (Prov(SPML (lookup))→VistA VSA)

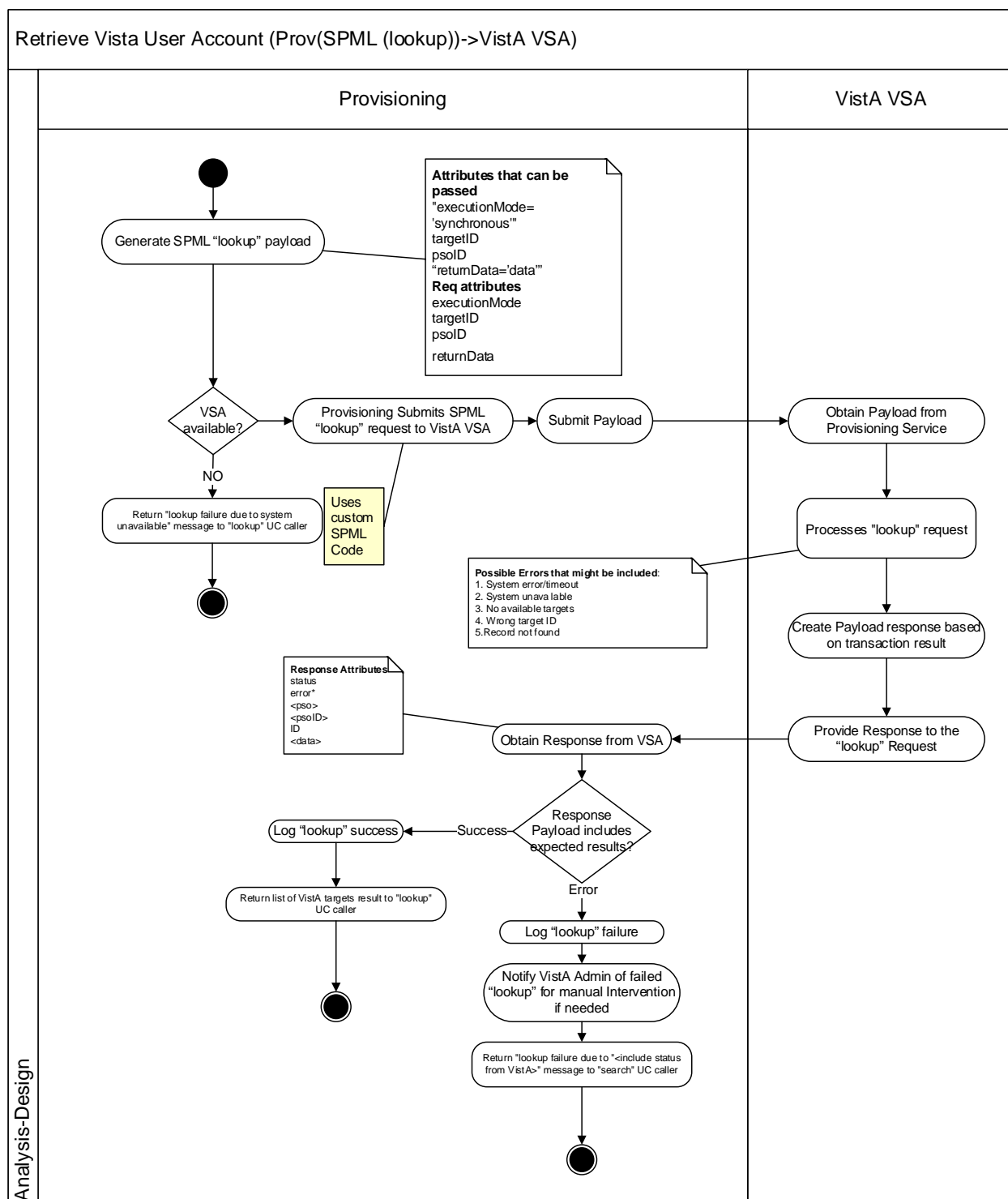


Figure 67: Retrieve Vista User Account (Prov(SPML (lookup))

□ VistA VSA)

6.2.1.8.8 Deprovision VistA Account (Prov(SPML(delete))→VistA VSA)

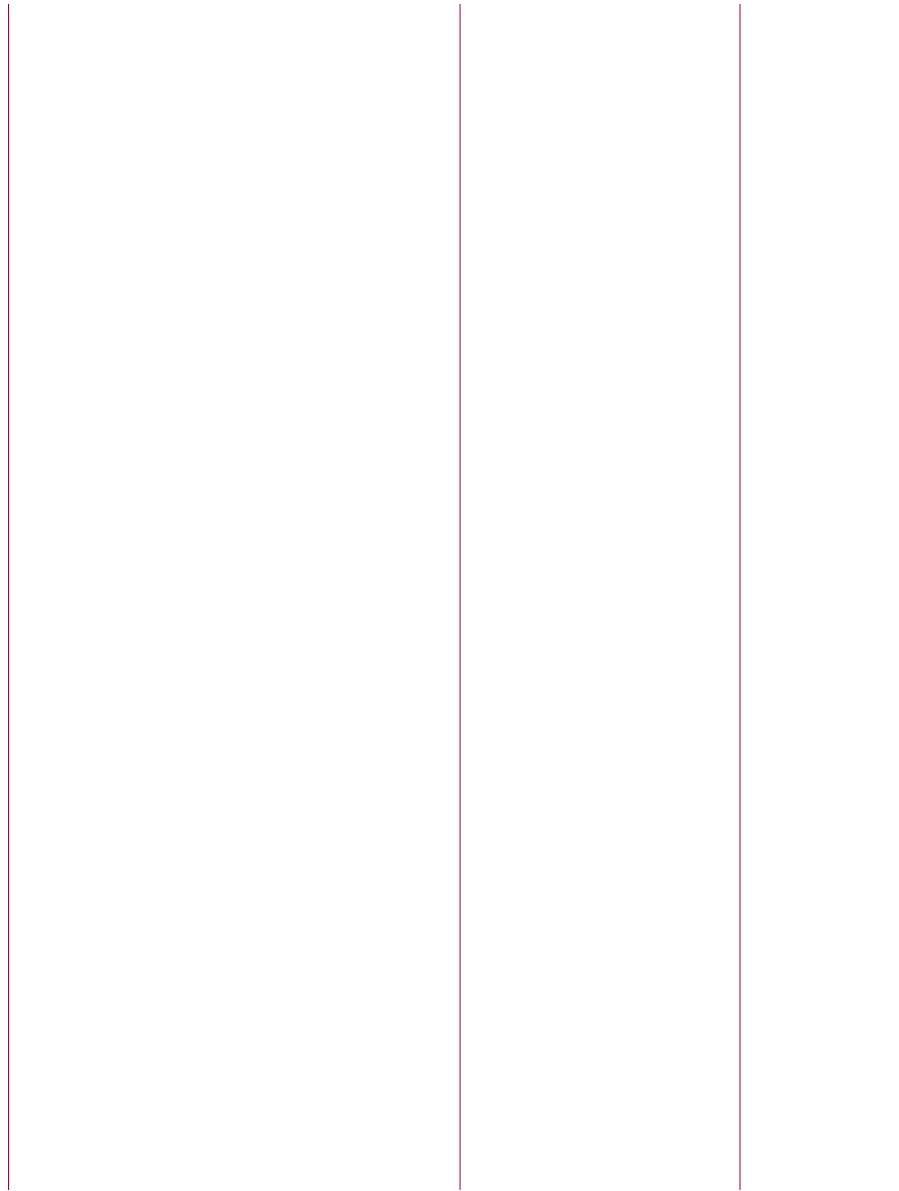


Figure 68: Deprovision VistA Account (Prov(SPML(delete))→VistA VSA)

6.2.1.8.9 Suspend VistA User Account (Prov (SPML(suspend))→VistA VSA)

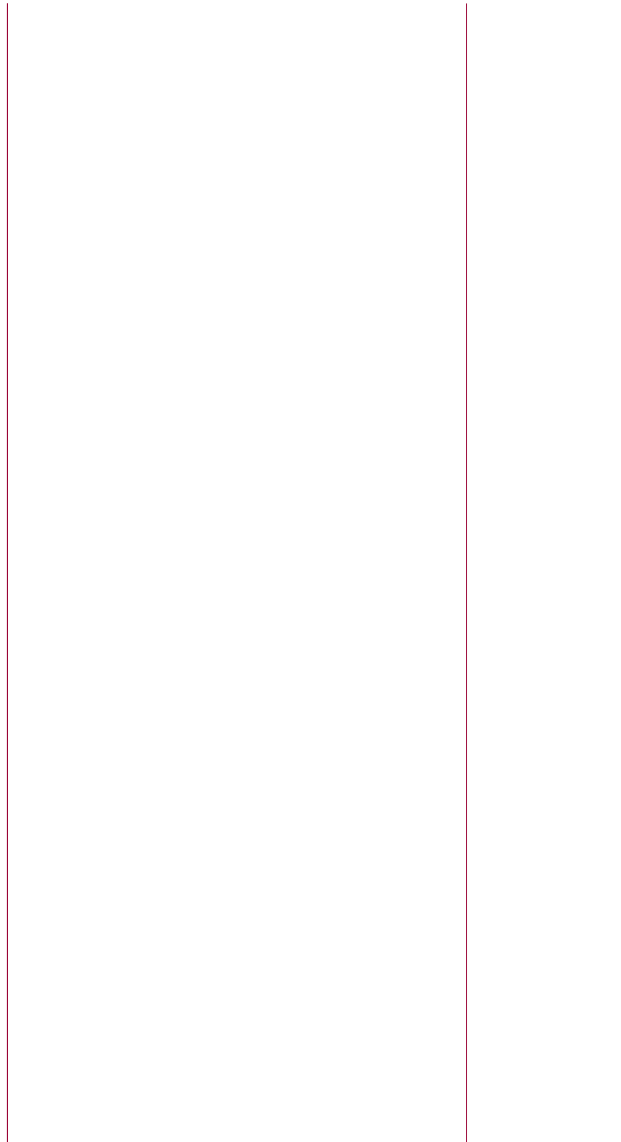


Figure 69: Suspend VistA User Account (Prov (SPML(suspend))→VistA VSA)

6.2.1.8.10 Update Provisioning User's Identity Record Correlated VistA User Account Status to "Suspended" (VistA VSA(SPML(suspend))→Prov)

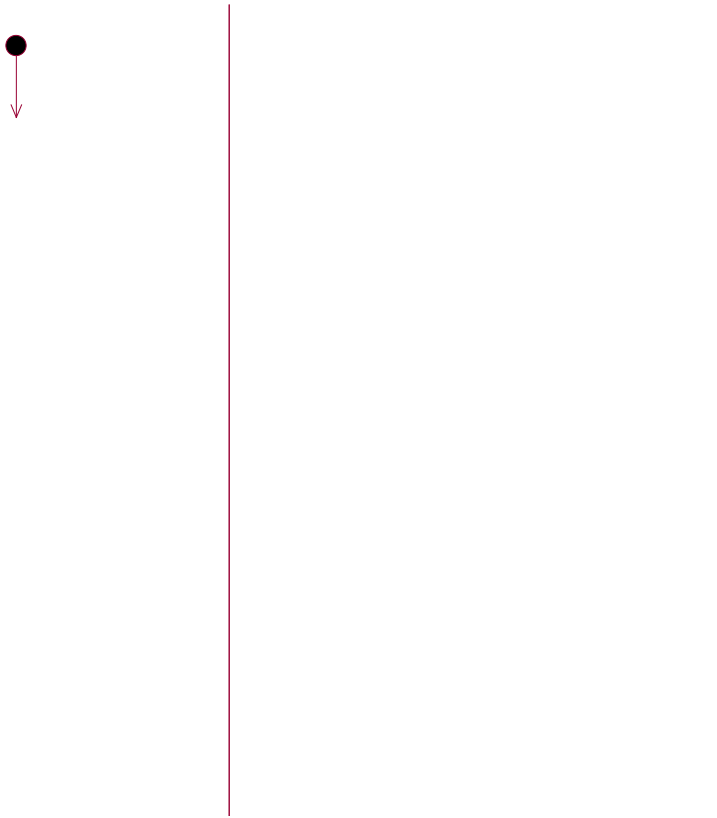


Figure 70: Update Provisioning User's Identity Record Correlated VistA User Account Status to "Suspended" (VistA VSA(SPML(suspend))→Prov)

6.2.1.8.11 Reactivate VistA User Account (Prov (SPML(resume))→VistA VSA)

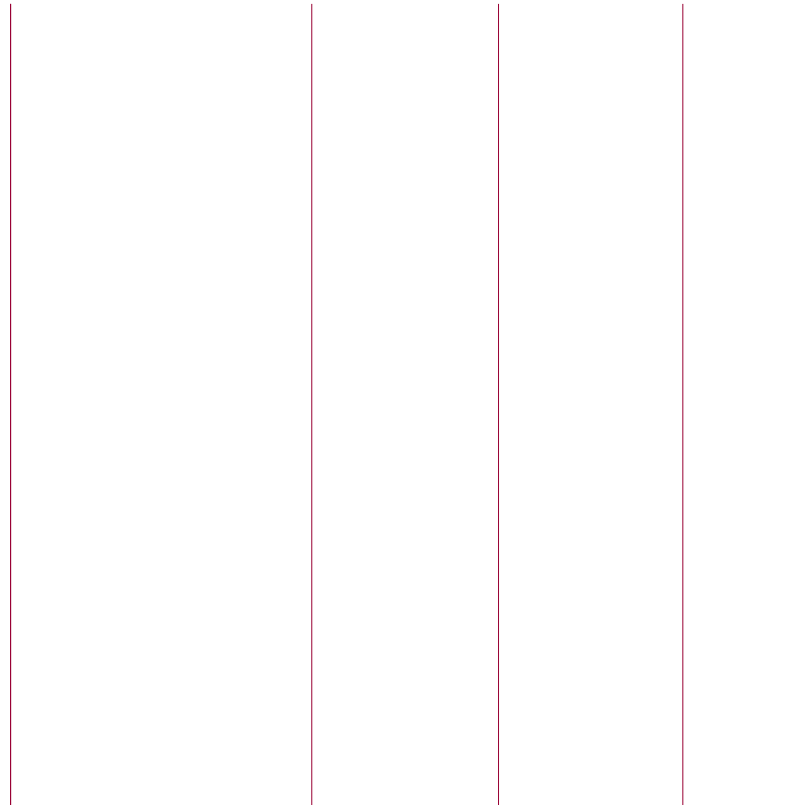


Figure 71: Reactivate VistA User Account (Prov (SPML(resume))→VistA VSA)

6.2.1.8.12 Update Provisioning User's Identity Record Correlated VistA User Account Status to "Active" (VistA VSA(SPML(resume))→Prov)



Figure 72: Update Provisioning User's Identity Record Correlated VistA User Account Status to "Active" (VistA VSA(SPML(resume))→Prov)

6.2.1.8.13 Get VistA User Account State (Prov (SPML (active))→VistA VSA)

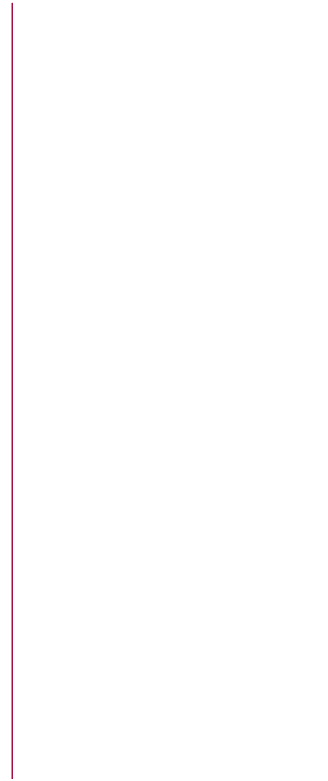


Figure 73: Get VistA User Account State (Prov (SPML (active))→VistA VSA)

6.2.1.8.14 Bind a Provisioned User to a VistA Account

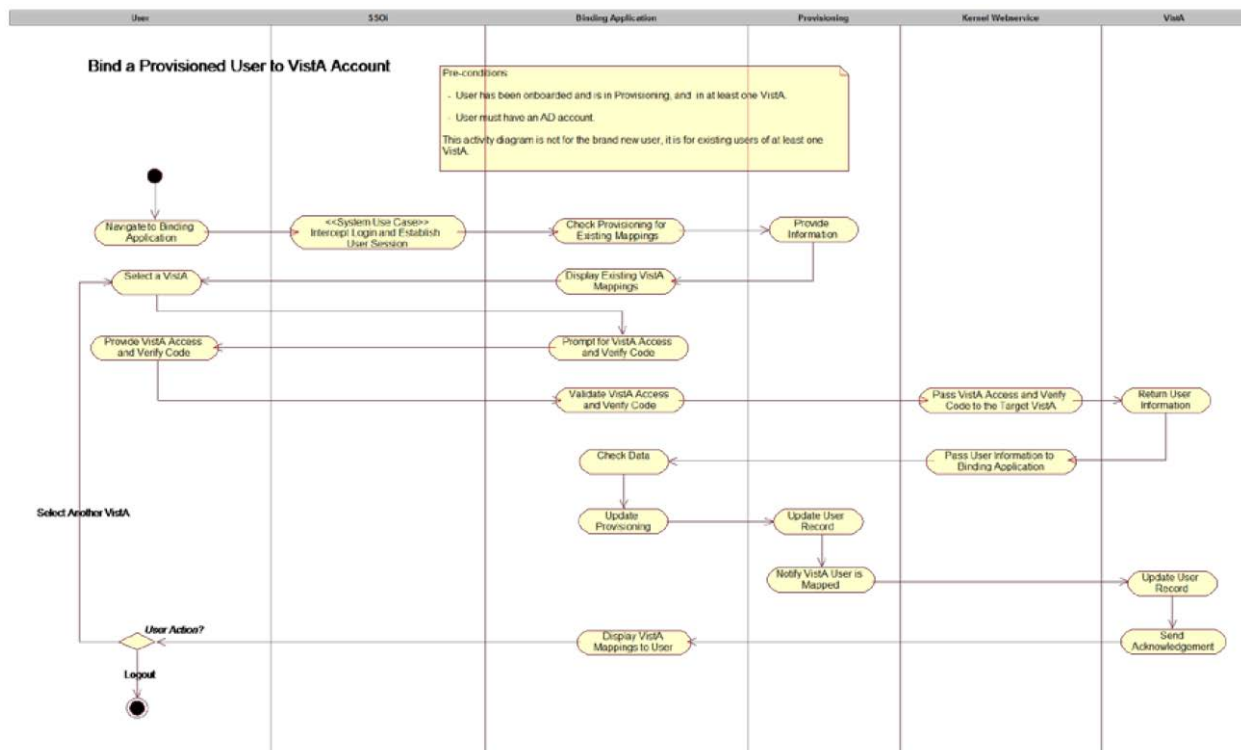


Figure 74: Bind a Provisioned User to a VistA Account

6.2.2 Role Manager Design

The role manager tool is an integral component of the [REDACTED] 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.

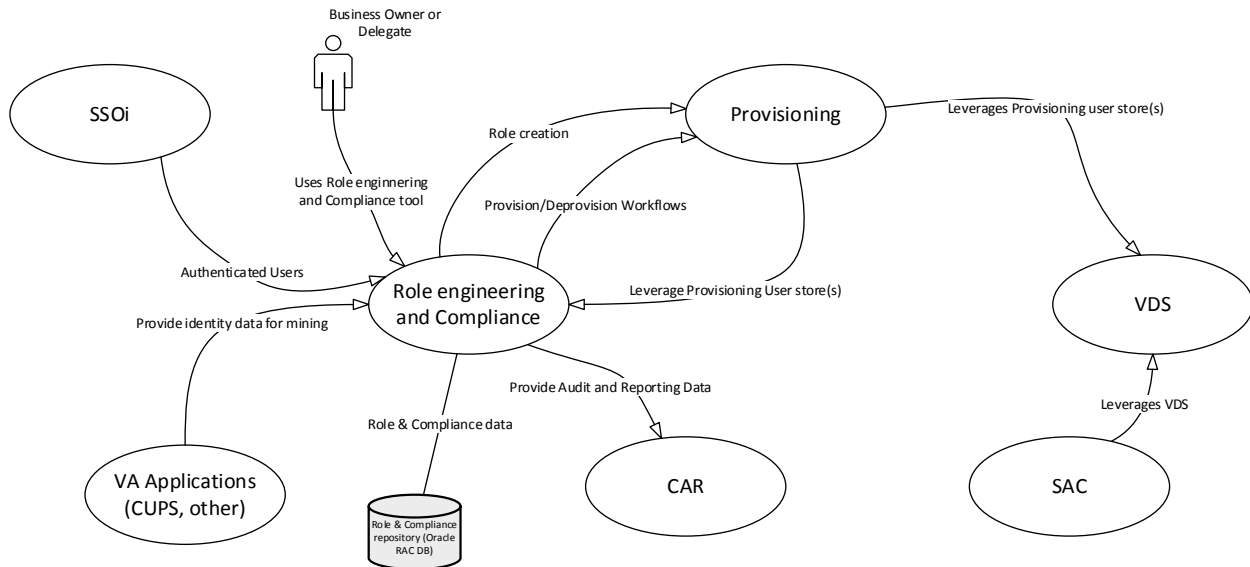


Figure 75: Role Manager Detailed Design

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.

The integration of the SailPoint Role engineering and compliance tool with SSOi will be handled using one of the existing and well-established integration patterns – through Siteminder WebAgent.

Integration of the SailPoint tool with the [REDACTED] CAR component will be handled through flat file log management and ingestion. Further analysis and potentially prototyping may be necessary to integrate CAR directly with the SailPoint RDBMS. Per Vendor statement, upgrades to the SailPoint tool may cause schema changes to be introduced in the underlying role engineering and compliance store. This circumstance may cause integration work done with CAR to be re-done again after each SailPoint Identity IQ product upgrade.

The connection points between the SailPoint role engineering and compliance tool with the [REDACTED] provisioning component will be handled through the development of a custom connector for SailPoint to handle WebService connection to one of Provisioning's exposed WebService interfaces (TEWS or SPML).

Role Manager Components:

- **Unified Governance Platform:** 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

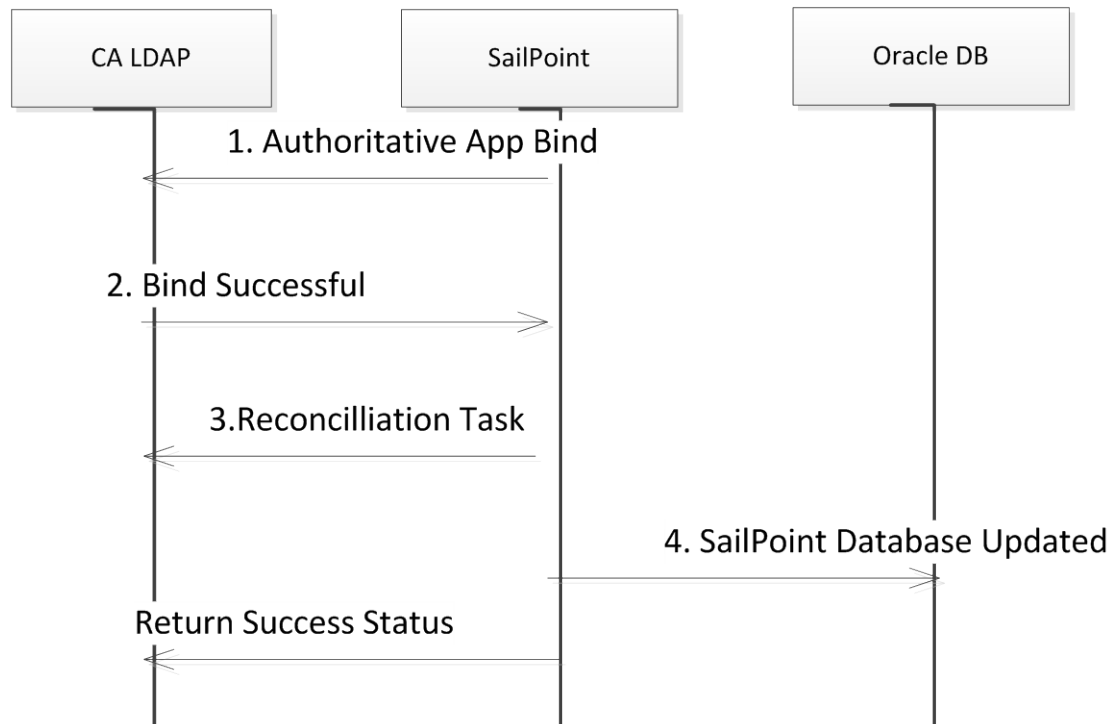


Figure 76: Authoritative Source – VA Repository Sequence Diagram

Table 38: Authoritative Source – VA Repository Sequence

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	1. The authoritative application is configured in Role Manager to connect to

Field	Description
	<p>the target CA LDAP source.</p> <ol style="list-style-type: none"> 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>
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

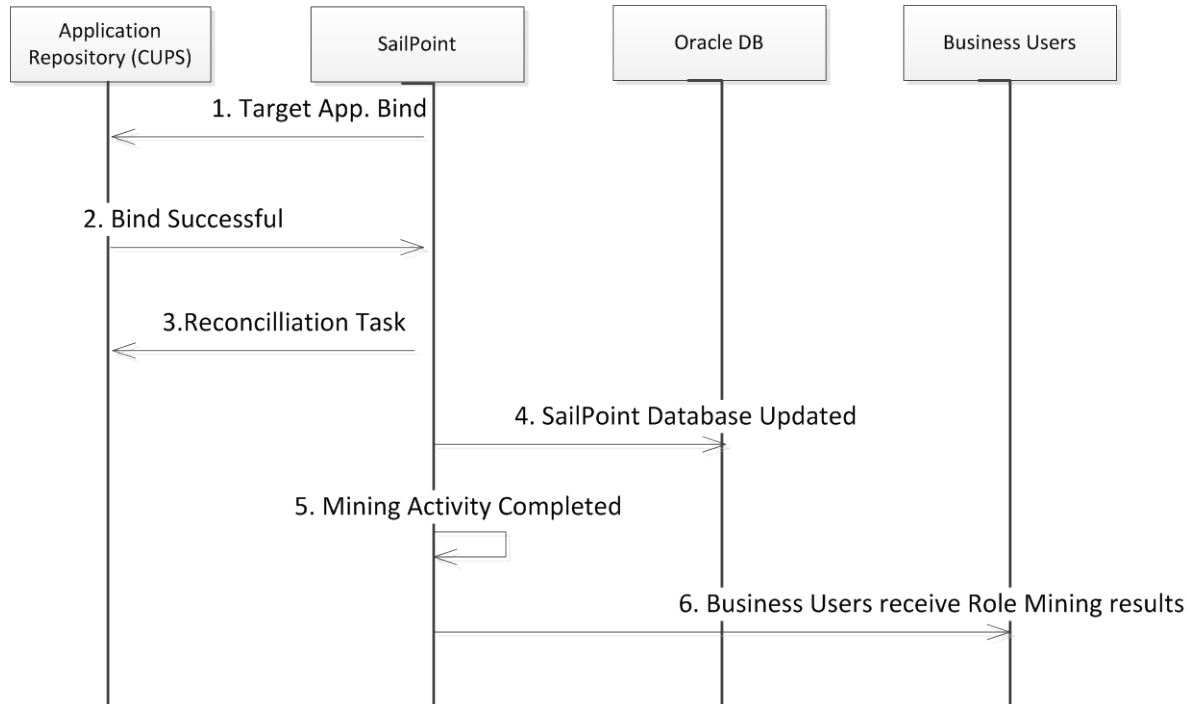


Figure 77: Role Mining – VA Application Sequence Diagram

Table 39: 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	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	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 target repository for pulling in mining data. 4. User information is pulled inside Role Manager and update is made in the

Field	Description
	<p>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 successful reconciliation.</p>
Main	The user data is reconciled inside Role Manager and the role mining results

Field	Description
Success Scenarios	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

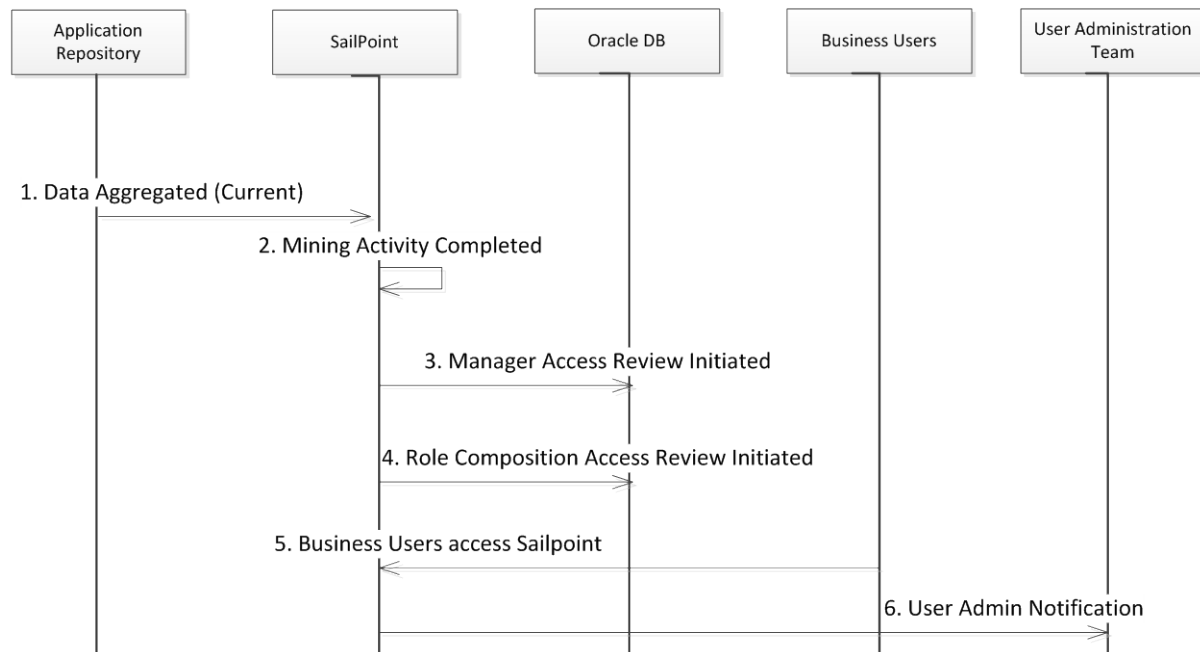


Figure 78: Access Re-certification – Role Composition Sequence Diagram

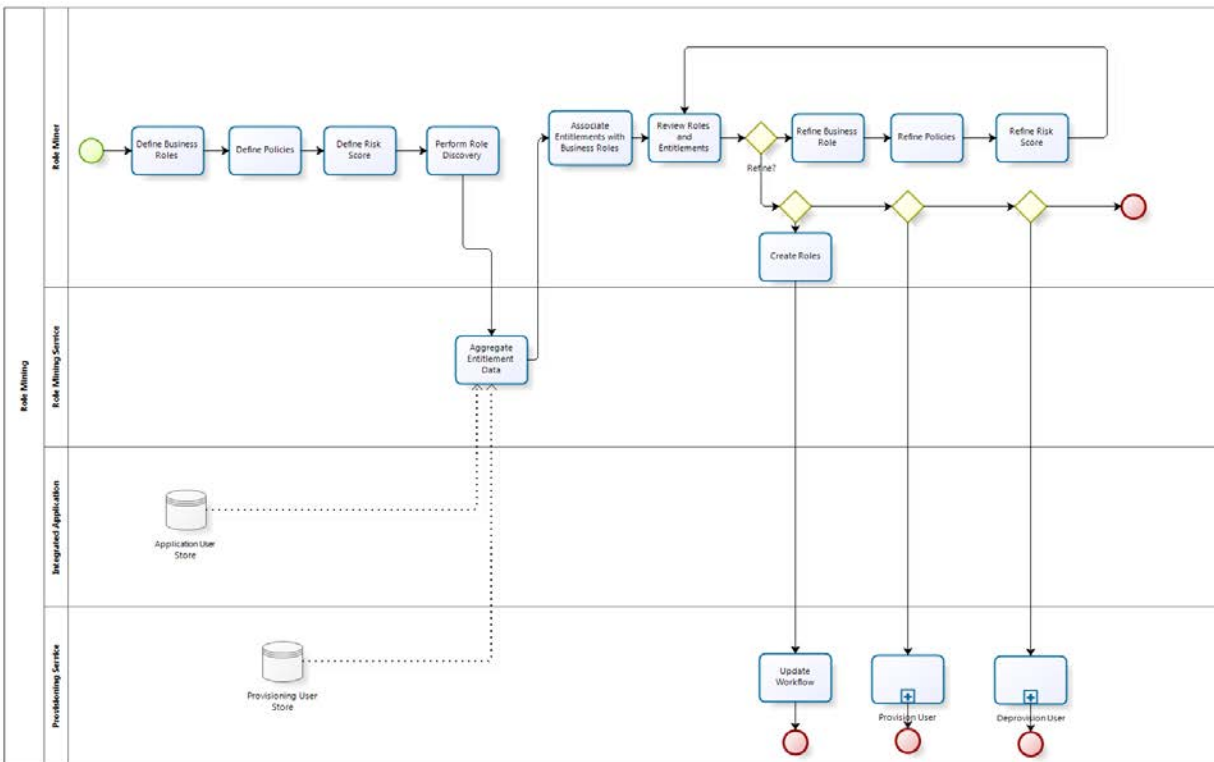
Table 40: Access Re-certification – Role Composition

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	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	1. The application repository has successfully reconciled in Role Manager to aggregate the most up-to-date VA user information (from the target

Field	Description
	<p>source).</p> <ol style="list-style-type: none"> 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 Manager which is hosted on the database by the Role Manager administrator. 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. 5. The application owner can access the Role Manager dashboard and complete the access re-certification staged above to either approve/revoke users’ access. 6. Any revocation request from the access re-certification is communicated to the user administrator team manually.
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.

6.2.2.4 SailPoint – Provisioning integration use cases

6.2.2.4.1 Create Provisioning Role(s) in Provisioning IdM



Powered by
bizagi
BPM

Figure 79: Create Provisioning Role(s) in Provisioning IdM

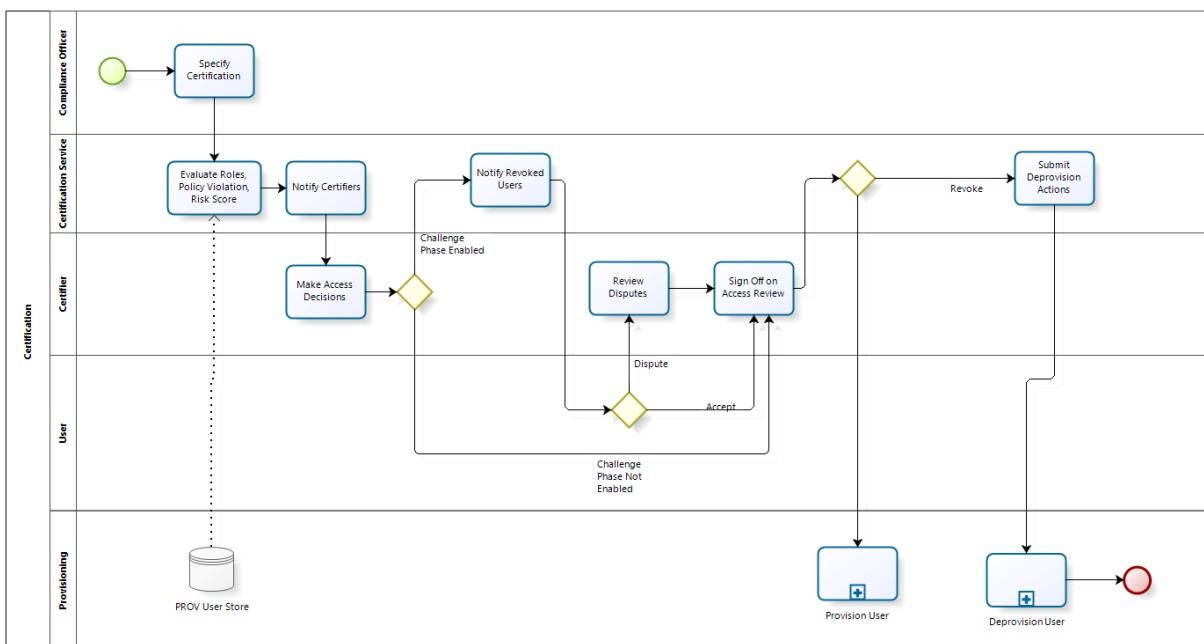
6.2.2.4.2 Update Provisioning Role(s) in Provisioning IdM

See [Create Provisioning Role\(s\) in Provisioning IdM](#)

6.2.2.4.3 Delete Provisioning Role(s) in Provisioning IdM

See [Create Provisioning Role\(s\) in Provisioning IdM](#)

6.2.2.4.4 Add Provisioning Role(s) associated with Provisioning user identity record



Powered by
bizagi
Modeler

6.2.2.4.5 Modify Provisioning Role(s) list associated with Provisioning user identity record

See [Add Provisioning Role\(s\) associated with Provisioning user identity record](#)

6.2.2.4.6 Delete Provisioning Role(s) list associated with Provisioning user identity record

See [Add Provisioning Role\(s\) associated with Provisioning user identity record](#)

6.2.3 VDS – Attribute Exchange Service Design

The VDS is a supporting component of the [redacted] solution that provides authoritative user attributes to other [redacted] 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 Retrieve User by CSPID Use Case

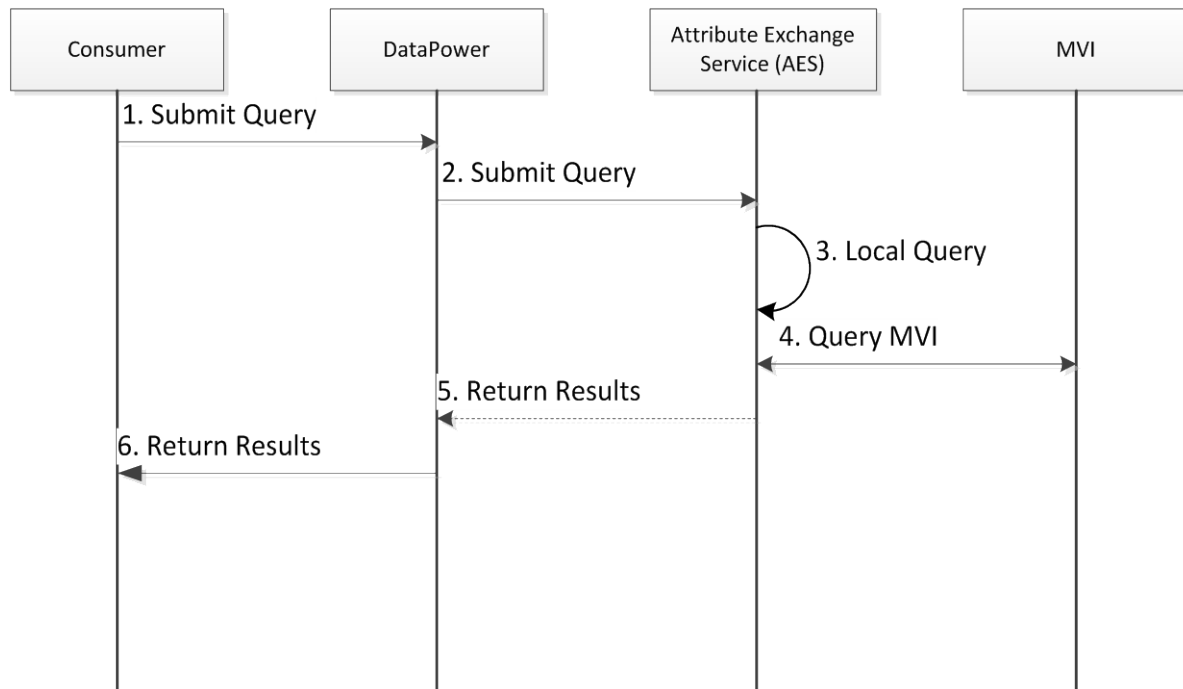


Figure 80: Retrieve User by CSPID Sequence Diagram

Table 41: Retrieve User by CSPID

Field	Description
Use Case	Retrieve User by CSPID
Actors	1. VAAFI (consumer) 2. MVI

Field	Description
	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
Success	1. VDS found CSPID (locally) and SecID (MVI) returning one result 2. VDS did not find CSPID (locally) returning zero results
Failures	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.

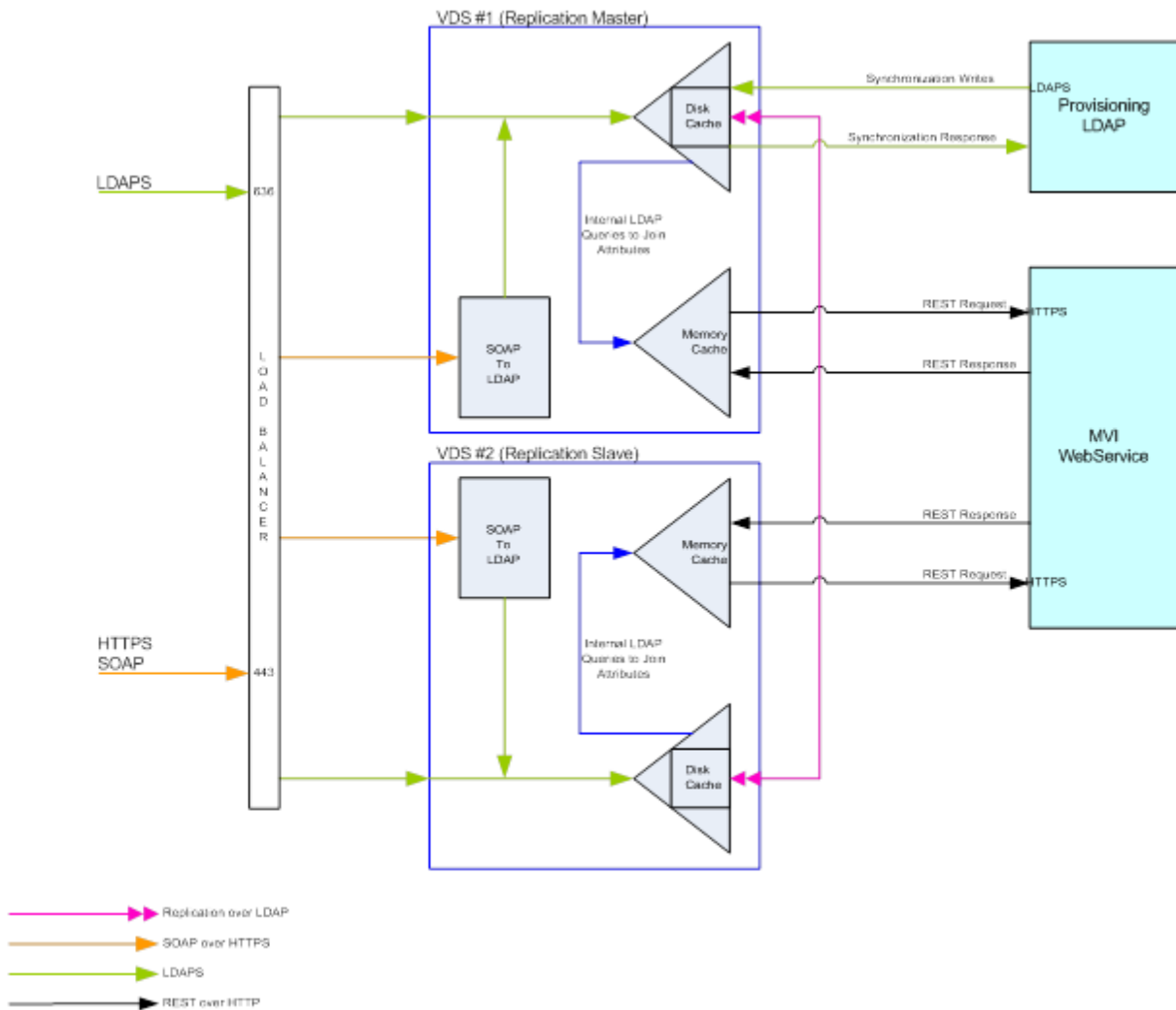


Figure 81: VDS Detailed Design

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 Figure 83 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)

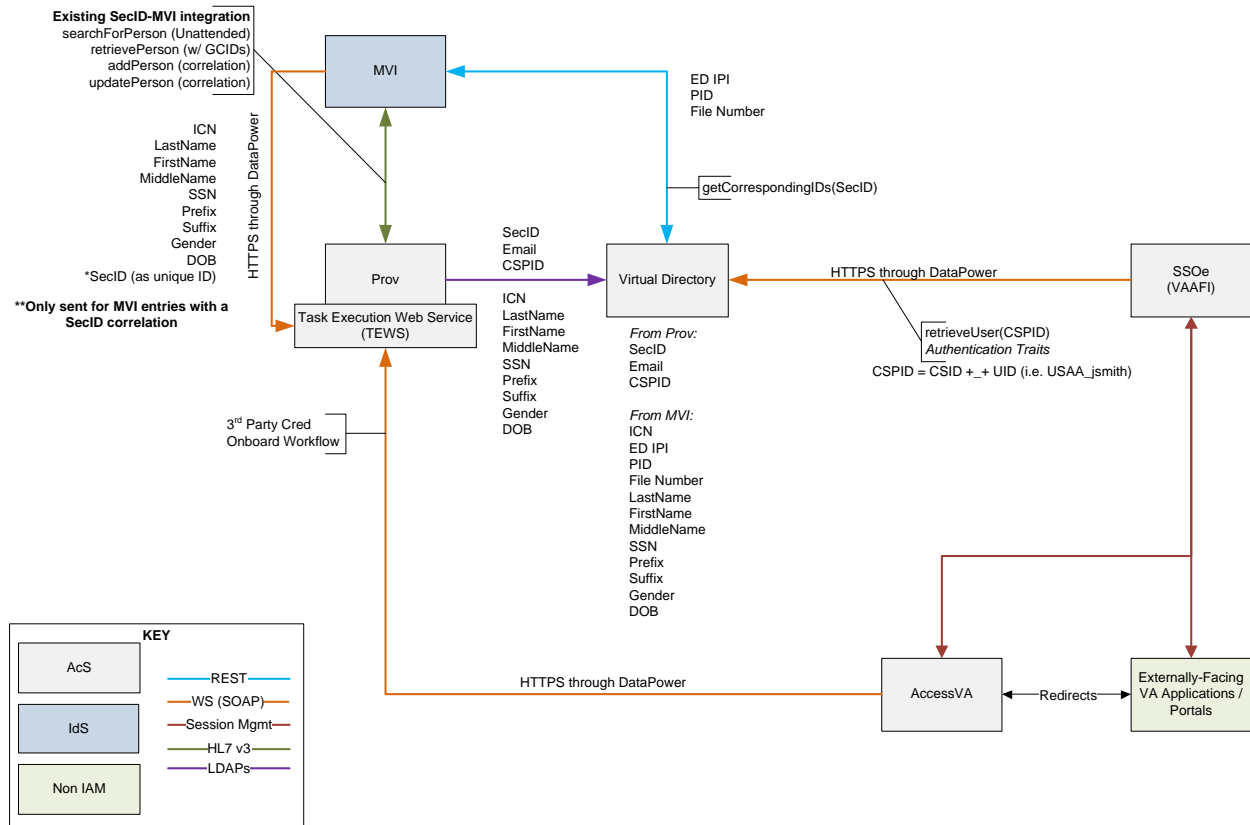


Figure 82: PROV-VDS-MVI Design

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	Multi value	Prov Attribute Name	VDS Attribute name
CSP ID	PROV	Y	VACSPID	cspid
ICN	MVI	N	N/A	icn
PID	MVI	Y	N/A	pid
SEC ID	PROV	N	VASECID	secid
dodedipnid	MVI	Y	VAEDIPI	dodedipnid
LastName	PROV	N	sn, MVILastName	lastname

Attribute	VDS Interface	Multi value	Prov Attribute Name	VDS Attribute name
FirstName	PROV	N	givenName, MVIFirstName	firstname
MiddleName	PROV	N	initials, MVIMiddleName	middlename
SSN	PROV	N	VASSN, MVISSN	ssn
Prefix	PROV	N	VAPrefix, MVIPrefix	prefix
Suffix	PROV	N	VASuffix, MVISuffix	suffix
Gender	PROV	N	VAGender, MVIGender	gender
DOB	PROV	N	VADOB, MVIDOB	dob
Email	PROV	N	mail	email
File Number (BIRLS)	MVI	Y	N/A	filenumber
Date of Death	PROV	N	MVIDateOfDeath	dateofdeath
Identity Theft	PROV	N	MVIIdentityTheft	identitytheft

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  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.

Table 42: MVI Webservice

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:



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.

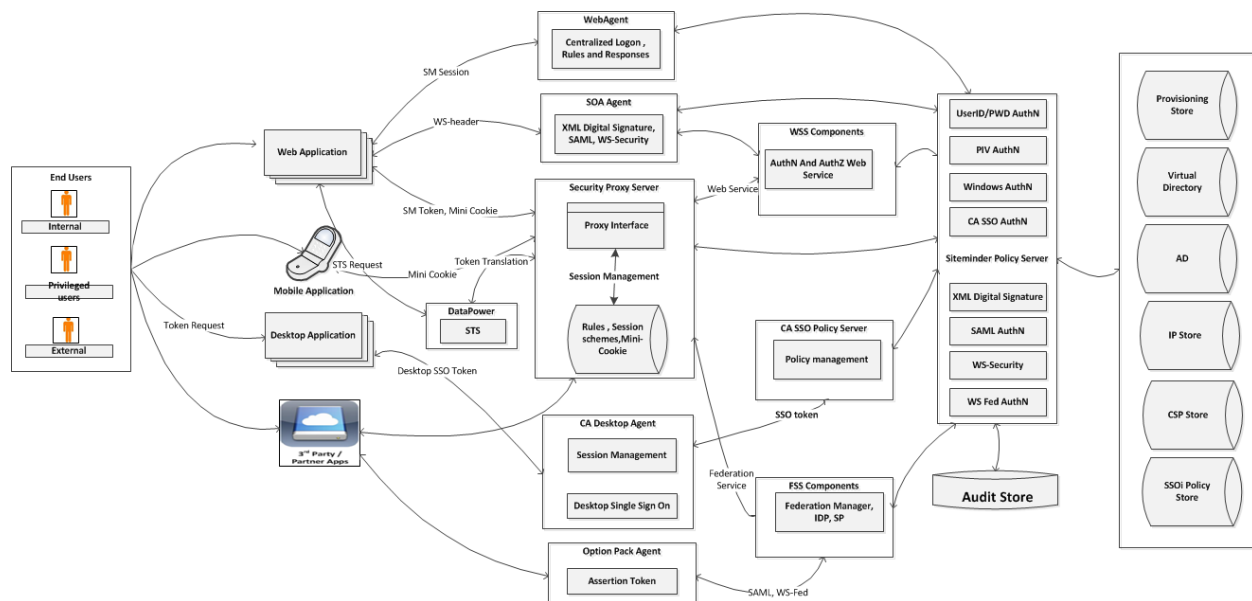


Figure 83: SSOi Detailed Design

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.

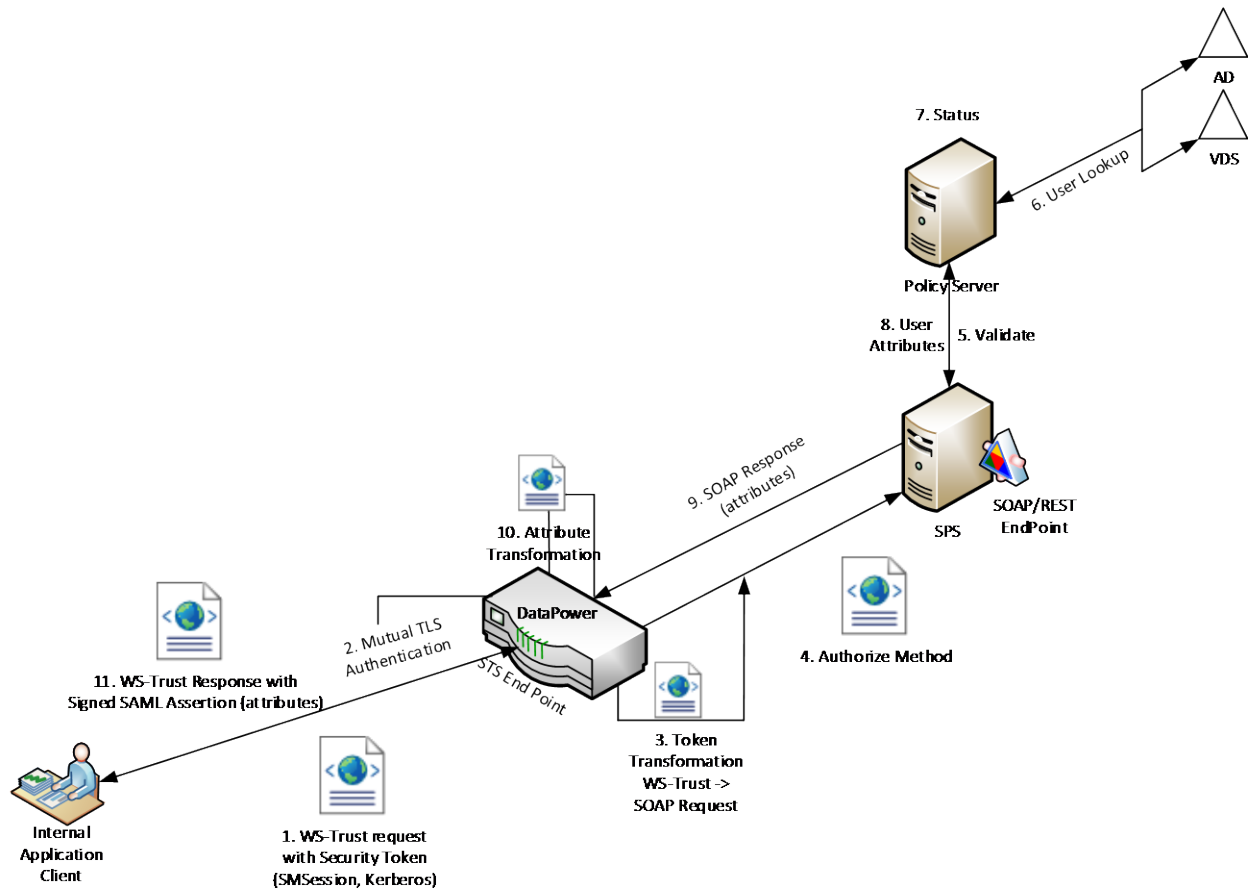


Figure 84: SSOi STS Architecture Diagram

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

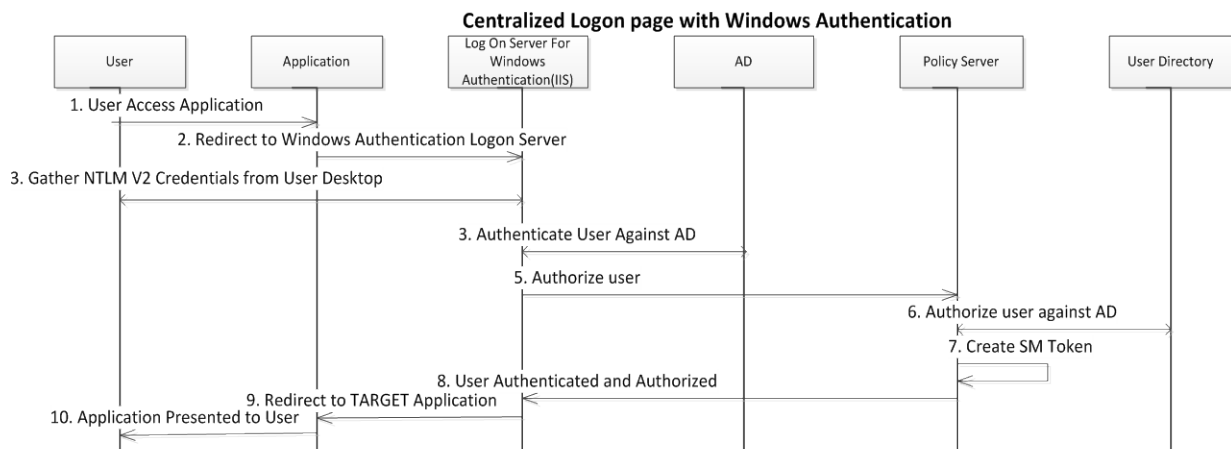


Figure 85: SSOi Centralized Logon Page with Windows Authentication Sequence Diagram

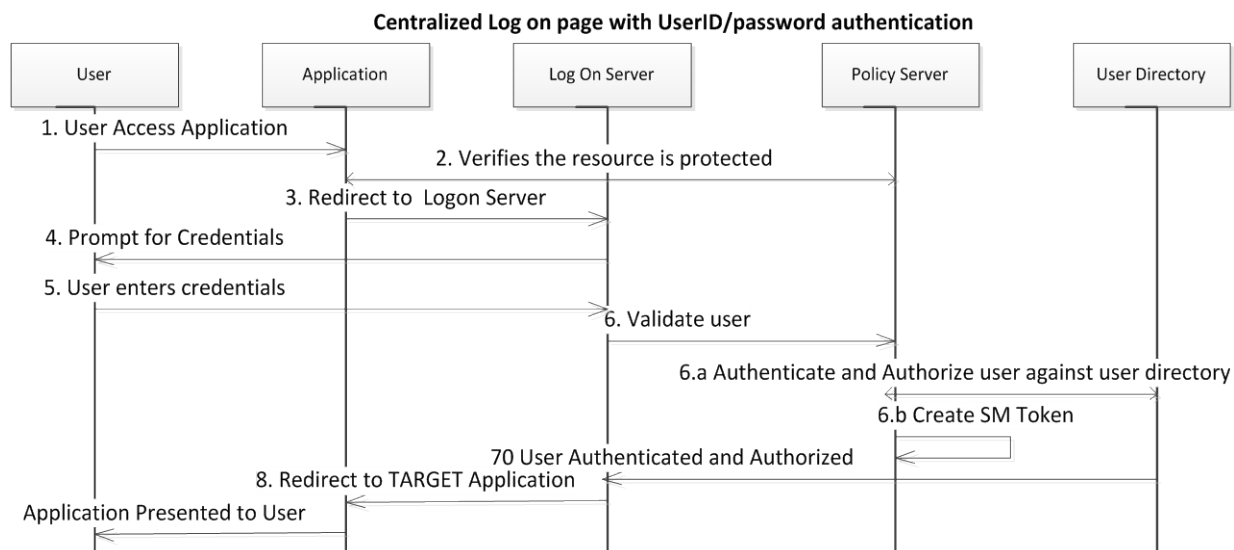


Figure 86: Centralized Log on Page with UserID/Password Authentication Sequence Diagram

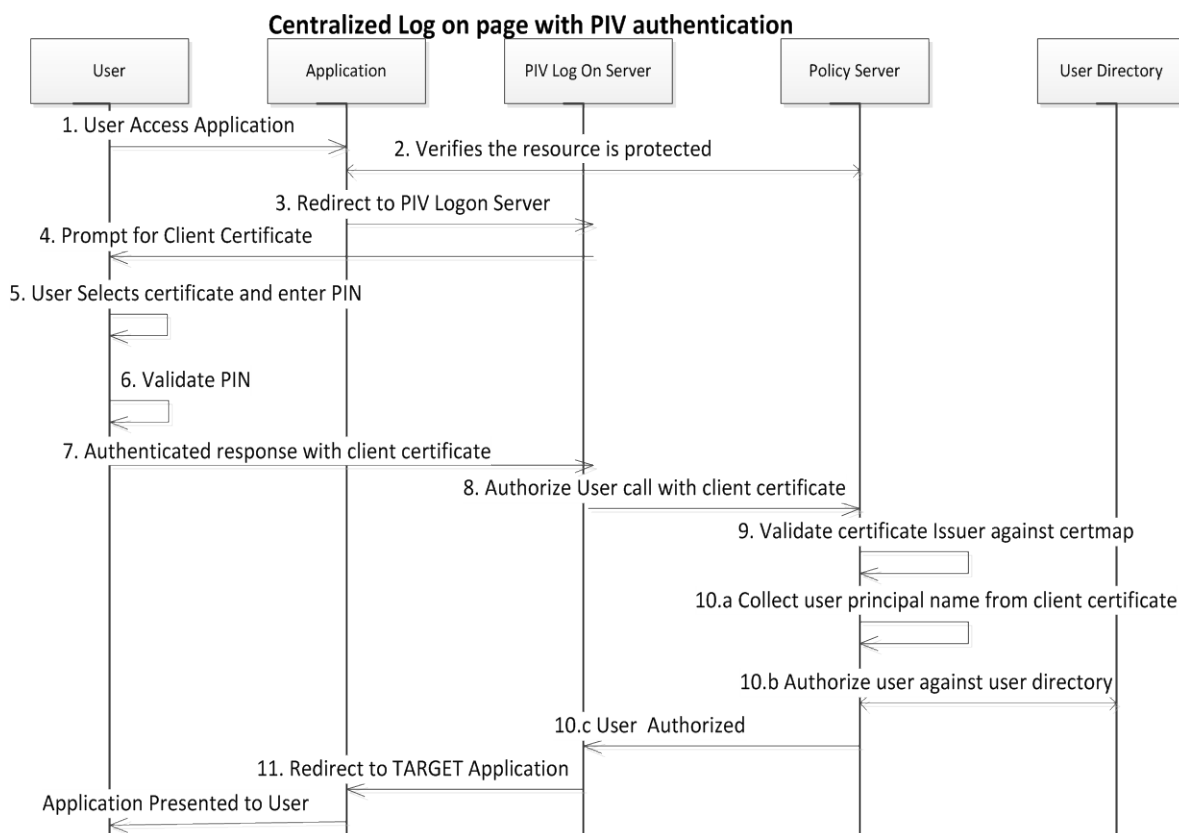


Figure 87: Centralized Log on Page with PIV Authentication Sequence Diagram

Centralized PIV only Log on page with PIV authentication

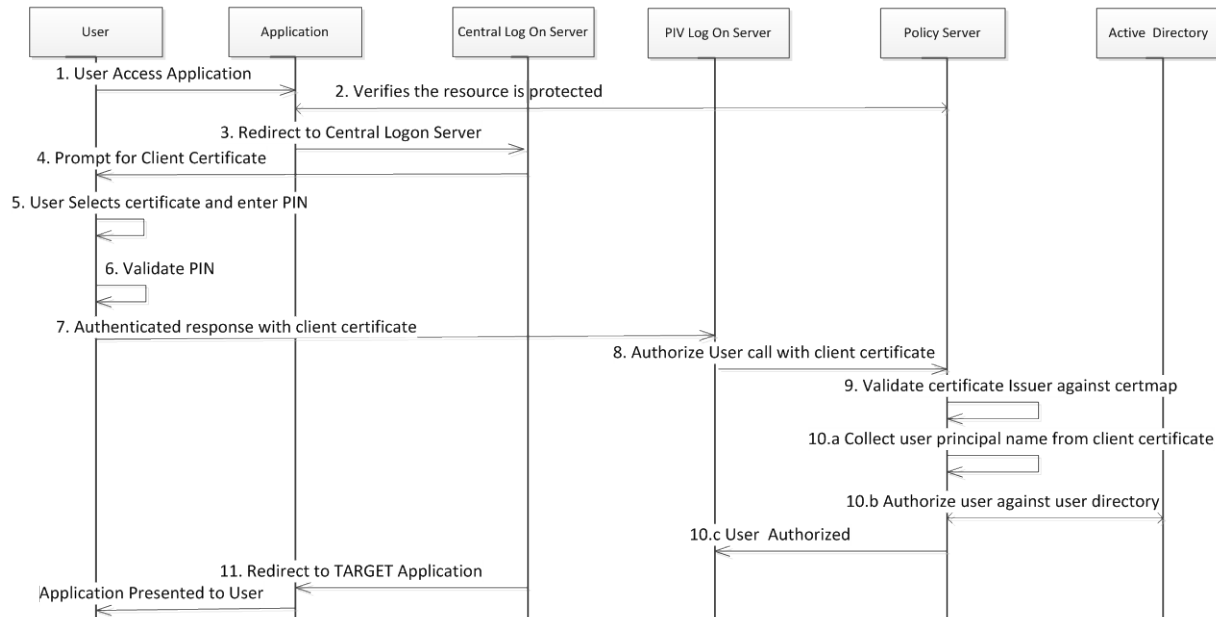


Figure 88: Centralized PIV Only Log on with PIV Authentication Sequence Diagram

Table 43: Centralized PIV Only Log on with PIV Authentication

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 verifies it with policy server 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.

Field	Description
	<ol style="list-style-type: none"> 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. 10. If the user lookup 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.

Field	Description
	<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
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 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

Field	Description
	<p>logon page</p> <ul style="list-style-type: none"> 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

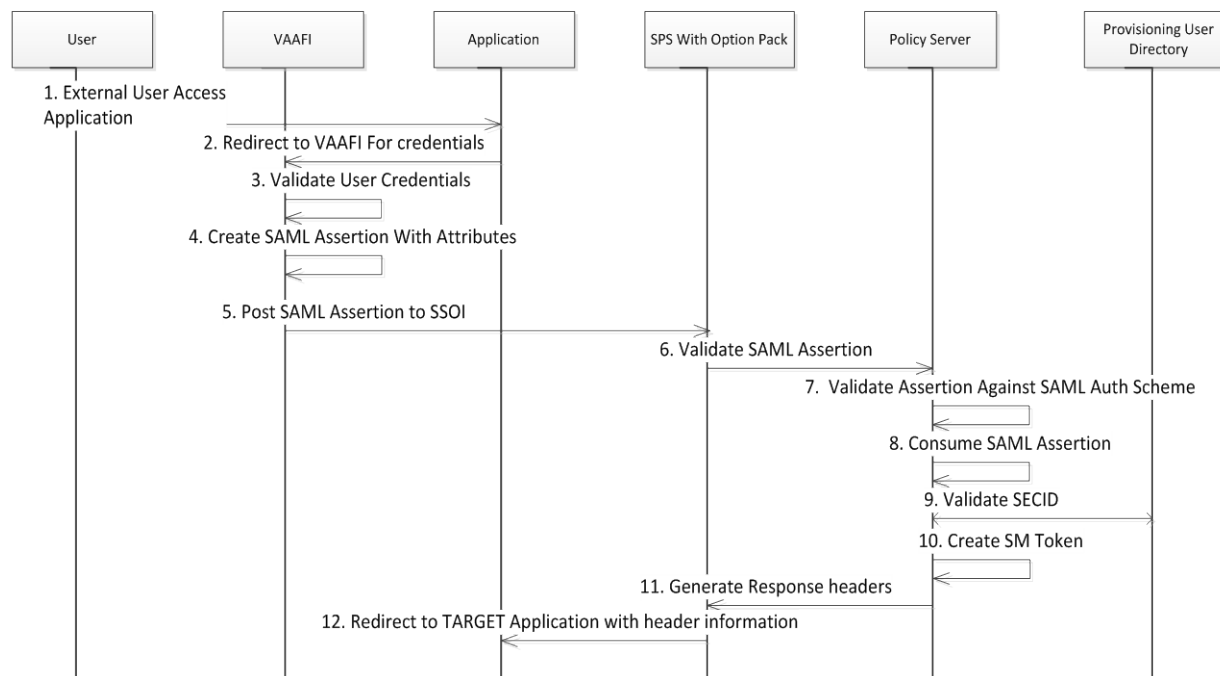


Figure 89: SSOi Support for LOA 2/3 External Users Sequence Diagram

Table 44: SSOi Support for LOA 2/3 External Users

Field	Description
Use Case Name	LOA2/3-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"> External User VAAFI SSOi Integrated Application(s) User Directory
Pre-Conditions	<ol style="list-style-type: none"> The SECID which will be received from VAAFI and will be available as correlated attribute in Provisioning store A valid external card user access the SSOi protected application through Access VA

Field	Description
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. 5. SSOI SAML Consumer server makes a call to the SiteMinder Policy server to validate SAML assertion. 6. 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. 7. SM Policy server validates the user retrieved from SAML assertion against Provisioning User directory by validating SECID 8. 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 9. 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
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>For each integration using SPS, the scenarios for Session timeout, logout and authentication/authorization failures will be implemented in a similar fashion as documented in 6.2.4.10 Centralized Login page</p>

Table 45: VAAFI IdP SAML Integration

Field	Description
IDPID:	
SiteMinder Affiliate Domain	N/A
NameID	SubjectDN

Field	Description
AuthN Director	NA
Encryption Algorithm	AES128
SLO	NA
Attribute Details	va_eauth_secid , va_eauth_csid, va_eauth_birthdate, va_eauth_pnidtype, va_eauth_pnid, va_eauth_credentialassurancelevel, va_eauth_dodedipnid, va_eauth_birlsfilenumber, va_eauth_middlename, va_eauth_lastname, va_eauth_state, va_eauth_icn, va_eauth_suffix
Signature Algorithm	Signing Algorithm: RSA with SHA1 RSA Key Size: 256 SAML Token: Signed Attribute Encryption: AES-128

6.2.4.3 SSOi Mobility Support

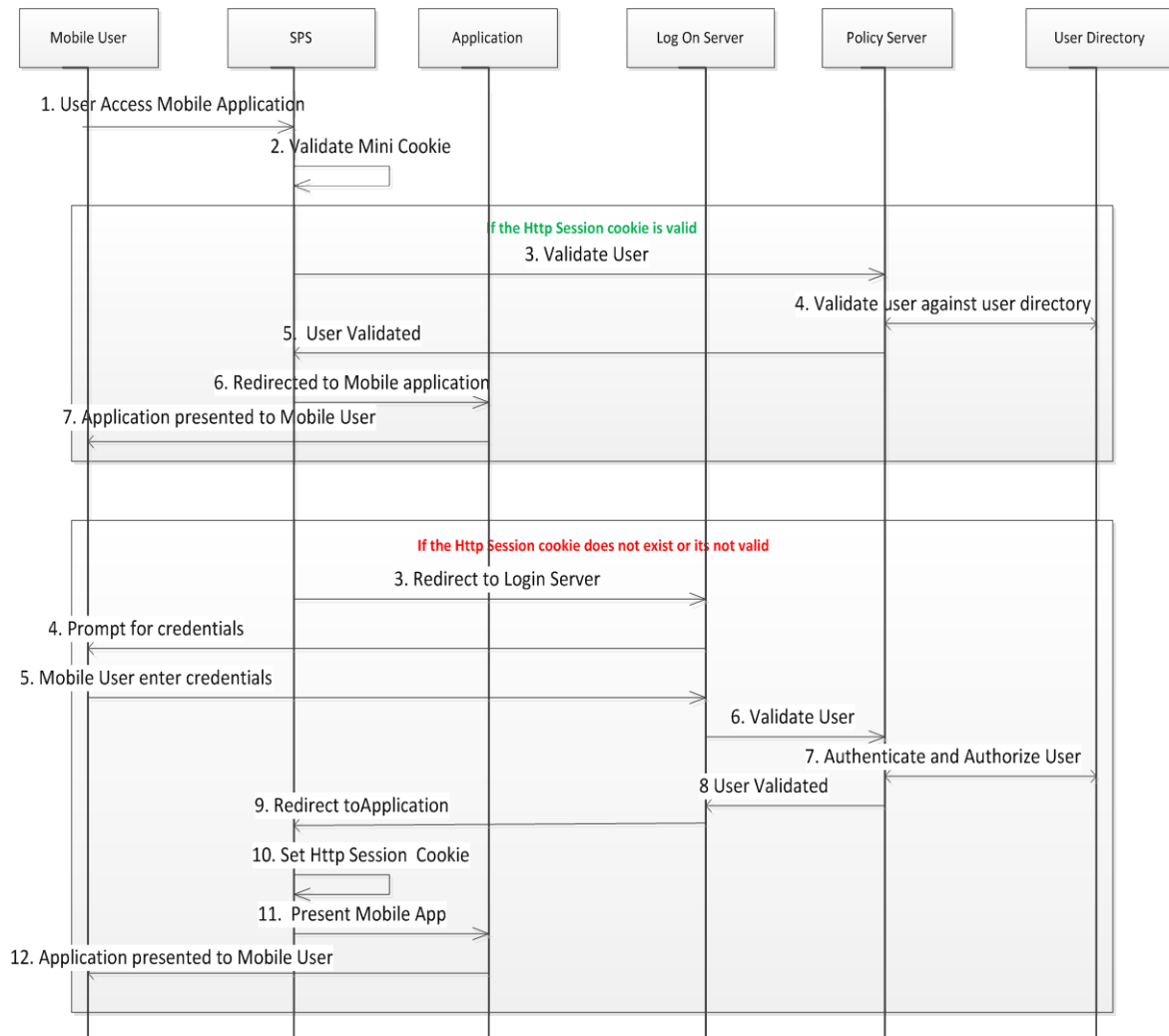


Figure 90: SSOi Mobility Support Sequence Diagram

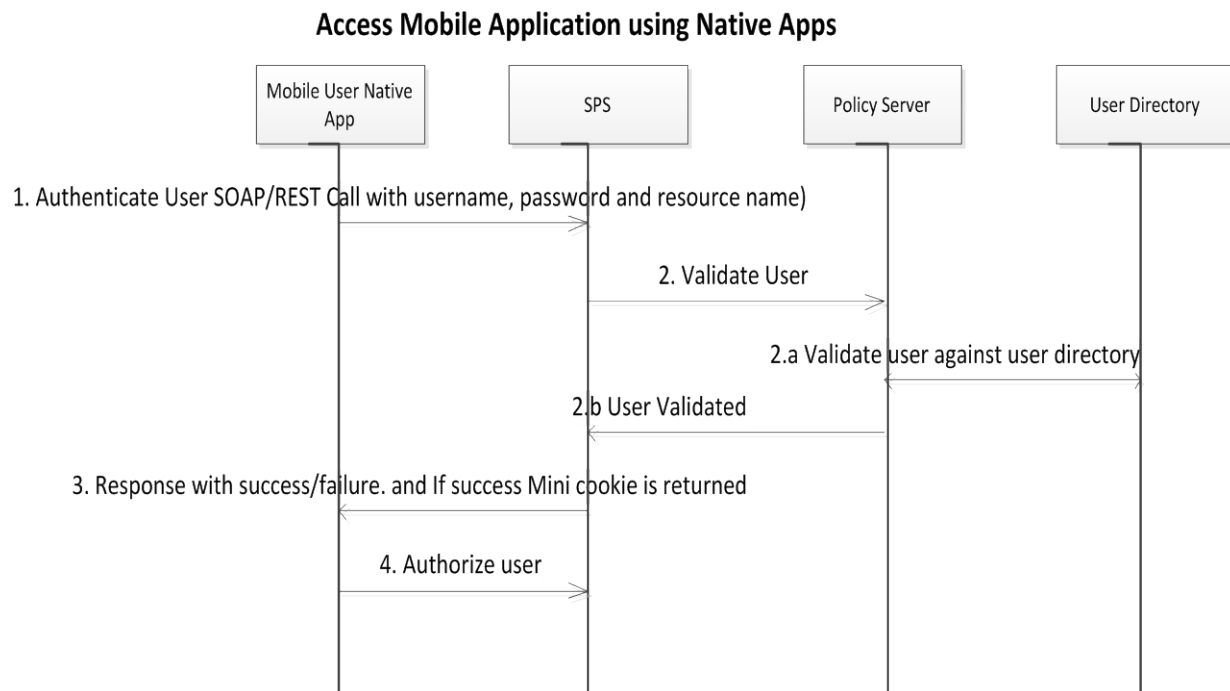


Figure 91: Access Mobile Application Using Native Apps Sequence Diagram

Table 46: Access Mobile Application Using Native Apps

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	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	Http Session Cookie is Valid 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

Field	Description
	<ol style="list-style-type: none"> 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 logon 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) 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
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 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 Session Timeout redirects the users back to the centralize Mobile logon page

Field	Description
	<ul style="list-style-type: none"> 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

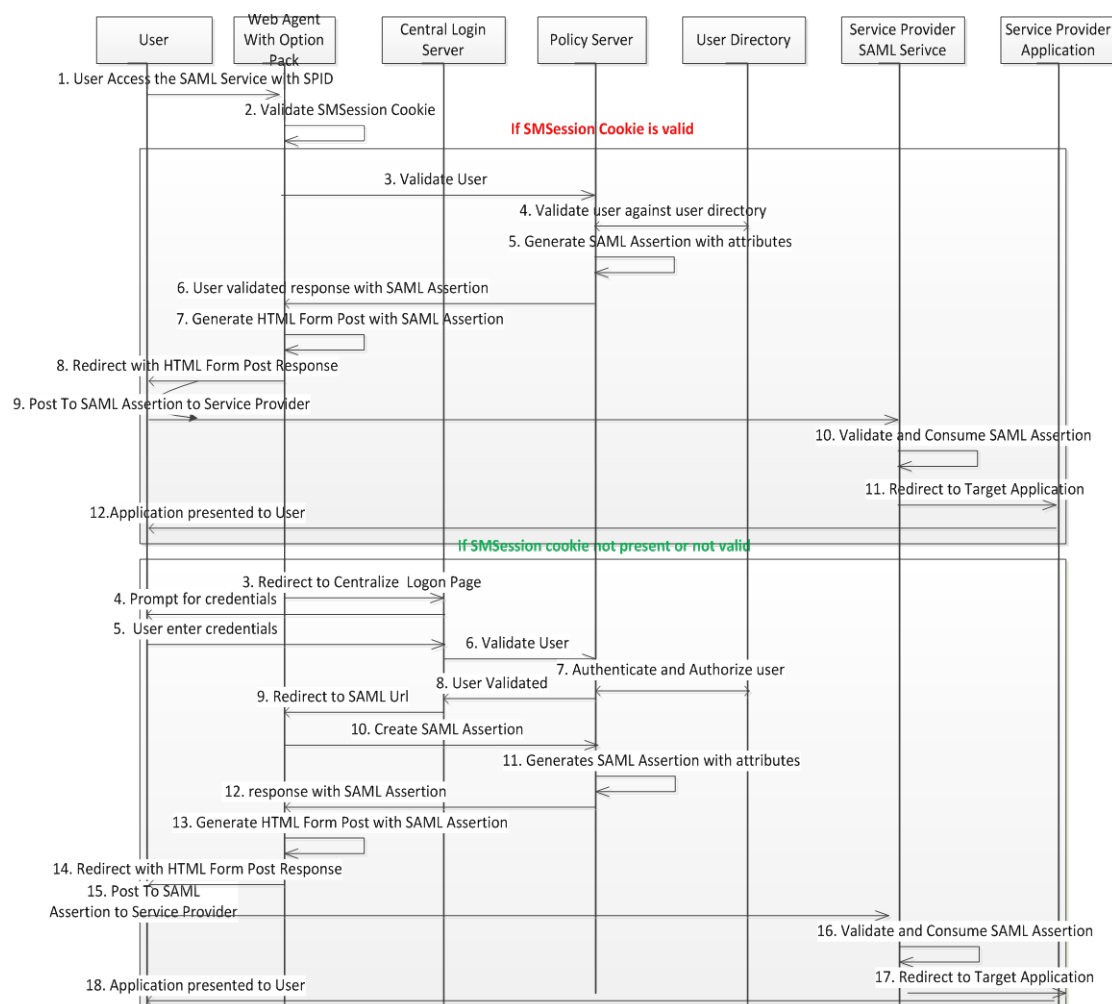


Figure 92: Federation IdP and SP for Internal Users

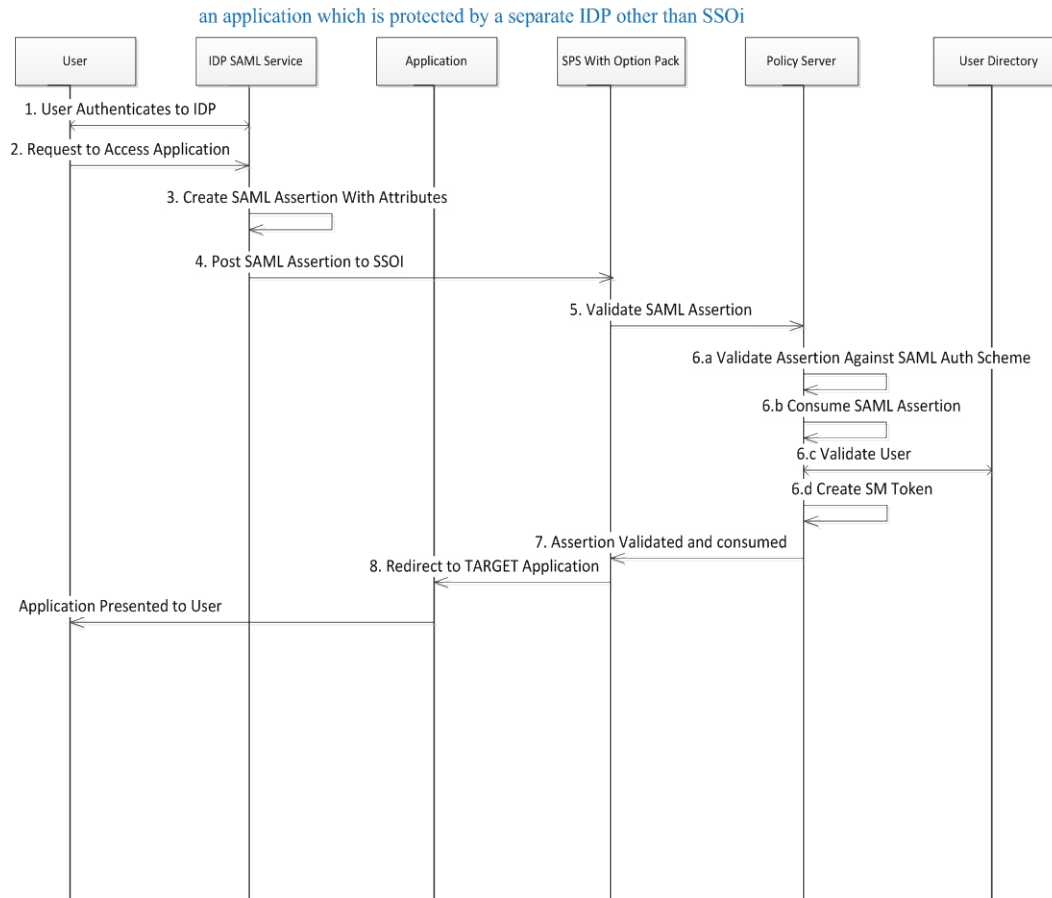


Figure 93: Application Protected by Separate IdP (Other than SSOi) Sequence Diagram

Table 47: Application Protected by Separate IdP (Other than SSOi)

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	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	Identity Provider (IdP) – Without a Valid Session Cookie 1. An internal user accesses an application (IdP-protected URL) which is at

Field	Description
	<p>service provider without a SiteMinder session cookie.</p> <ol style="list-style-type: none"> Web server redirects user to centralize log on page and prompted for authentication credential User enters the credentials SiteMinder Policy server validates against User store. SiteMinder Policy server authenticates and authorizes the user SiteMinder Policy Server creates valid user token SiteMinder Policy server redirects to SAML URL SiteMinder Policy server generates the SAML Assertion by: SiteMinder Policy Server adds the required attributes such as user Principal Name (UPN), email, firstname and lastname IdP posts the SAML assertion to the Service Provider SAML Assertion Consumer service: SiteMinder Policy Server (IdP) generates HTML Form Post with SAML assertion SiteMinder Policy Server (IdP) redirects with HTML form post response SiteMinder Policy Server (IdP) posts SAML assertion to Service Provider Service provide Consumes the SAML assertion generated by SSOi and grants the access to the user Service provider redirect to protected SSOi application with valid SiteMinder session Service provider present application to the end user <p>Identity Provider (IdP) – With a Valid Session Cookie</p> <ol style="list-style-type: none"> An internal user accesses an application (IdP protected URL) which is at service provider with a SiteMinder Session cookie. The user is validated by SiteMinder Policy Server. SiteMinder Policy Server generates the SAML assertion by adding all the required attributes such as user Principal Name (UPN), email, firstname and lastname IdP posts the SAML assertion to the Service Provider SAML Assertion Consumer service: IdP generates HTML form post with SAML Assertion IdP redirects with HTML Form Post Response IdP posts to SAML Assertion to Service Provider Service provider consumes the SAML assertion generated by SSOi and grants the access to the user Service provider redirects to protected SSOi application with valid SiteMinder session Service provider presents application to the end user <p>Service Provider (SP)</p>

Field	Description
	<ol style="list-style-type: none"> 1. An internal user accesses an application that 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 10. User is redirected protected SSOi application with valid SiteMinder session by Service provider
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 • Default Logout will redirect the user back to the centralize logon page <p>VA as SP:</p>

Field	Description
	<ul style="list-style-type: none"> 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

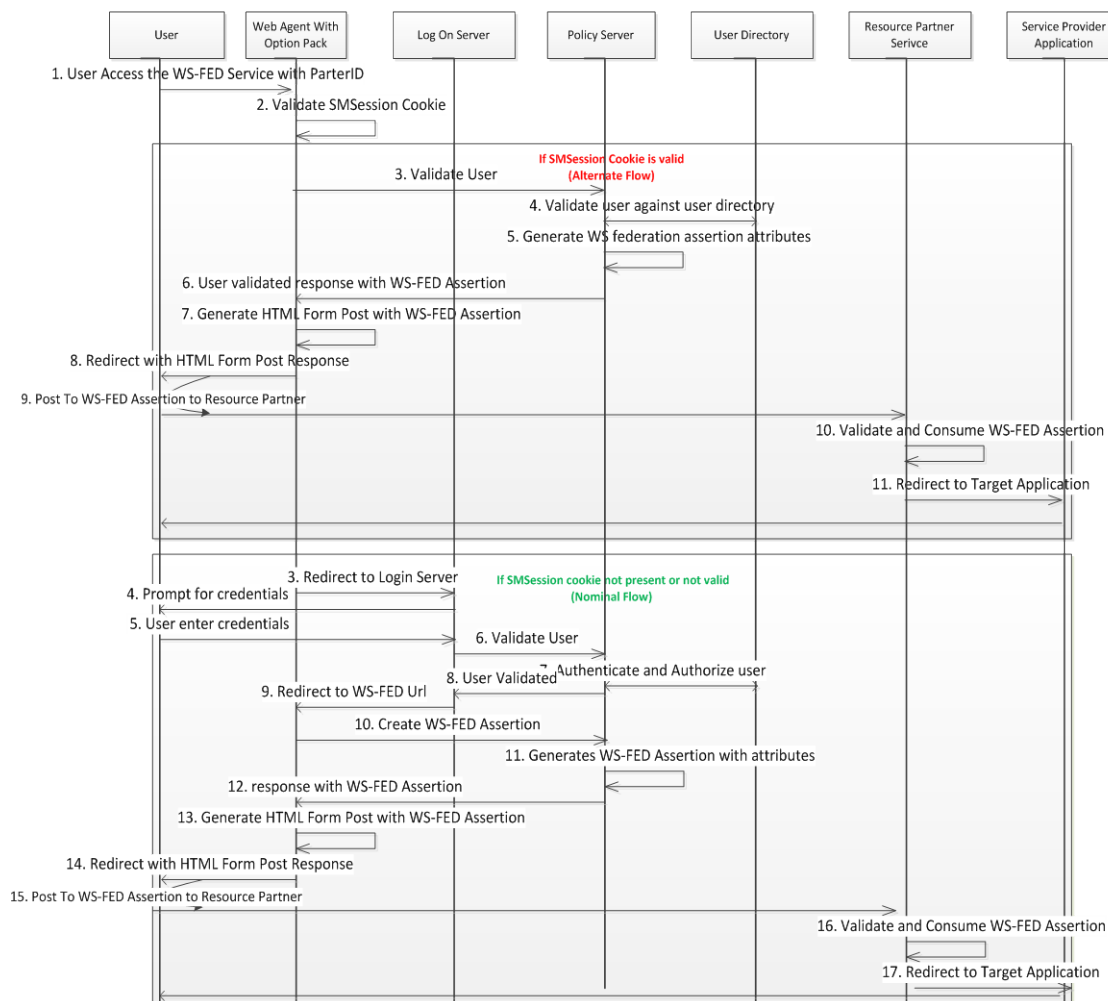


Figure 94: WS Federation for Internal Users Sequence Diagram

Table 48: WS Federation for Internal Users

Field	Description
Use Case Name	WS Federation for Internal Users

Field	Description
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 17. Redirect to Target Application <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

Field	Description
	9. Relying party consumes WS-Federation 10. Redirect to Target Application
Main Success Scenarios	User is authenticated and Application is presented to the user.
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

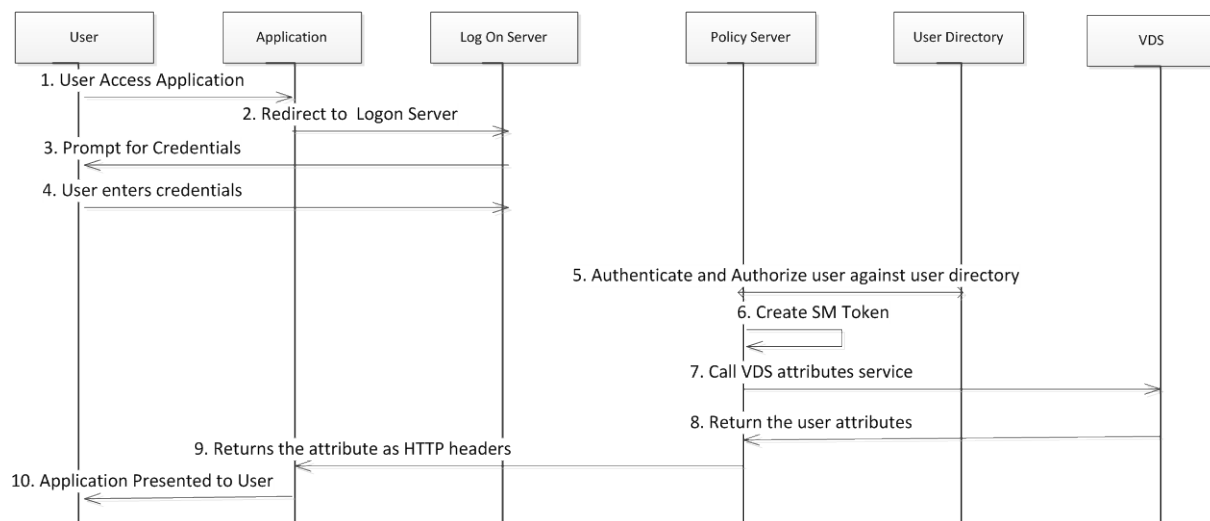


Figure 95: SSOi Support for Attribute Service Sequence Diagram

Table 49: 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	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

Field	Description
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.
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

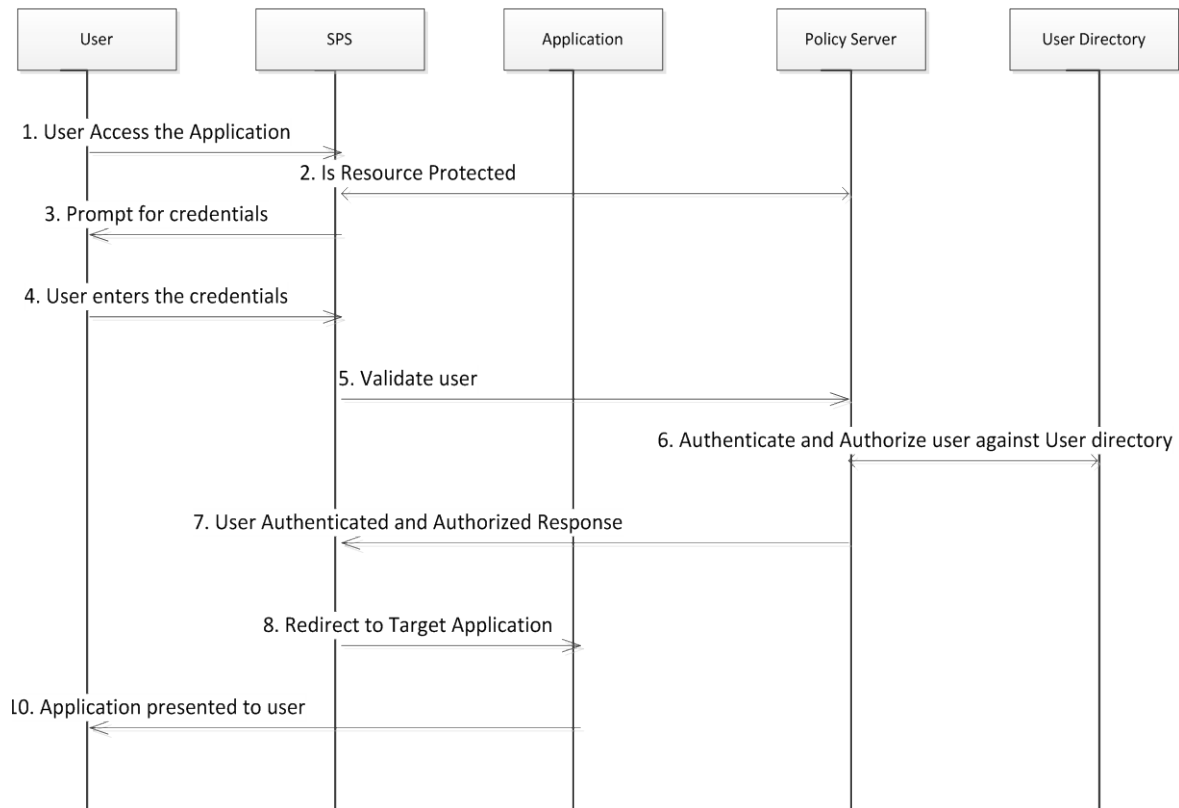


Figure 96: SSOi Proxy Authentication Request Sequence Diagram

Table 50: 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	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	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

Field	Description
	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
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

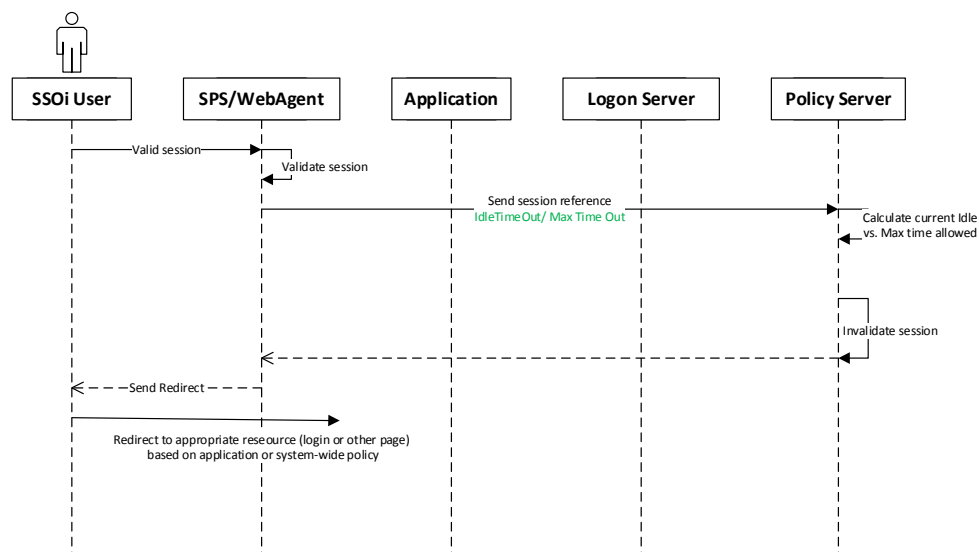


Figure 97: Session Management Sequence Diagram

Table 51: Session Management

Field	Description
Use Case Name	Session Management
Description	This use case describes the process by which SiteMinder manages session tokens.
Actors	1. SSOi User of Web application or STS WebService (User)

Field	Description
	<ol style="list-style-type: none"> 2. Siteminder WebAgent (WebAgent) 3. Siteminder Policy Server (Policy Server) 4. Siteminder WebAgent Protected application (Application) 5. SSOi Central login page (Logon server)
Trigger	<ol style="list-style-type: none"> 1. User stays idle (more than the established maximum idle time) after initial successful authentication and authorization to an Application and attempts to request an Application resource. 2. User's total session lifetime exceeds maximum time set in policy after initial successful authentication and authorization to an Application and attempts to request an Application resource.
Pre-Conditions	A User has a valid single sign-on token
Actions	<p>SSOi Session idle time out and token refresh enforcement</p> <ol style="list-style-type: none"> 1. An already authenticated user requests a resource within a SiteMinder protected application 2. WebAgent intercepts the user's request and evaluates it for presence of SiteMinder session data 3. WebAgent sends session data to Policy Server 4. Policy Server evaluates the session for: <ol style="list-style-type: none"> a. maximum idle time set for resource <ol style="list-style-type: none"> i. If the user idle time is greater than the maximum time out set in SSOi policy, SSOi logs the user out ii. WebAgent sends an appropriate redirect response message (based on application or systemwide policy) to the user's browser. iii. User's browser requests the redirected resource (login page, notification page, etc). b. max session lifetime set for before reauthentication <ol style="list-style-type: none"> i. If the user session lifetime is greater than the max time out set in policy, SSOi invalidates the current session and logs the user out. ii. WebAgent sends an appropriate redirect response message (based on application or systemwide policy) to the user's browser. iii. User's browser requests the redirected resource (login page, notification page, etc).
Main Success Scenarios	Session management policy is enforced
Main Failure Scenarios	Failure scenarios outside of COTS vendor code are not applicable for this part of the functionality

Note: Specific steps invoked after internal product session evaluation are described in section [6.2.4.10 Centralized Login Page](#)

6.2.4.9 SSOi STS Architecture Flow

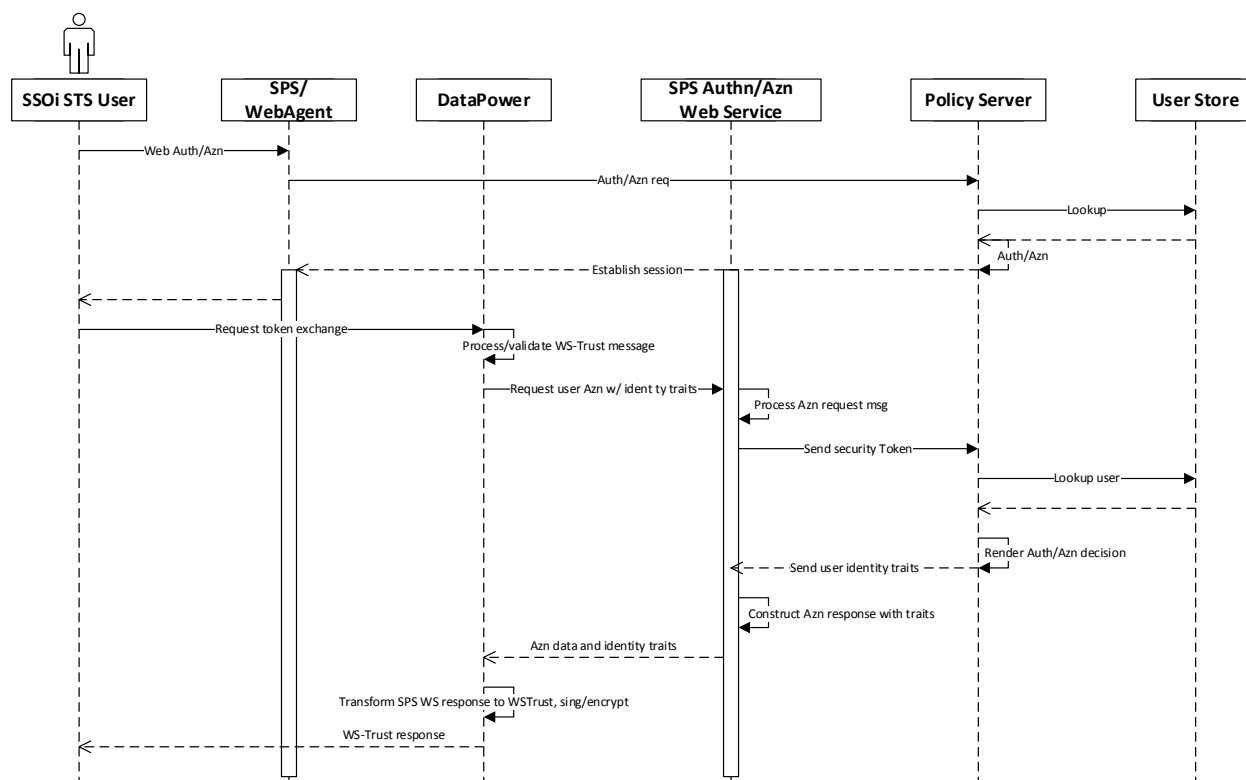


Figure 98: SSOi STS Token exchange sequence diagram

Note: SSO STS architecture implements DataPower in conjunction with Secure Proxy Server (SPS) Web service to provide required functionality.

Table 52: SSOi STS Token exchange

Field	Description
Use Case Name	SSOi STS Token exchange
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. SSOi User 2. Siteminder WebAgent (Web Agent) 3. Secure Proxy Server (SPS) 4. IBM WebSphere DataPower XI5x appliance (DataPower) 5. SPS Authn/Azn Web Service 6. Siteminder Policy Server (Policy Server) 7. User Store
Pre-Conditions	A user has a valid CA SiteMinder single sign-on token or

Field	Description
	A user has a valid VA Active Directory/Kerberos token
Trigger	Client accesses the SSOi STS web service endpoint at DataPower
Actions	<ol style="list-style-type: none"> 1. Internal application creates a WS-Trust request message with a Security Token (SMSession or Kerberos) as part of SOAP body and sends 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 the security token 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 the security token to SiteMinder Policy Server. 6. Policy Server decrypts the security token and validates it. Policy server extracts the user context from the session and performs a lookup in 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-Trust message, containing the WS-Token to the requesting internal application. Application consumes the WS-Token and receives the user attribute sets with the updated SMSession token <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

Field	Description
	10. Client receives updated SOAP response with user session and attributes
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> <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.

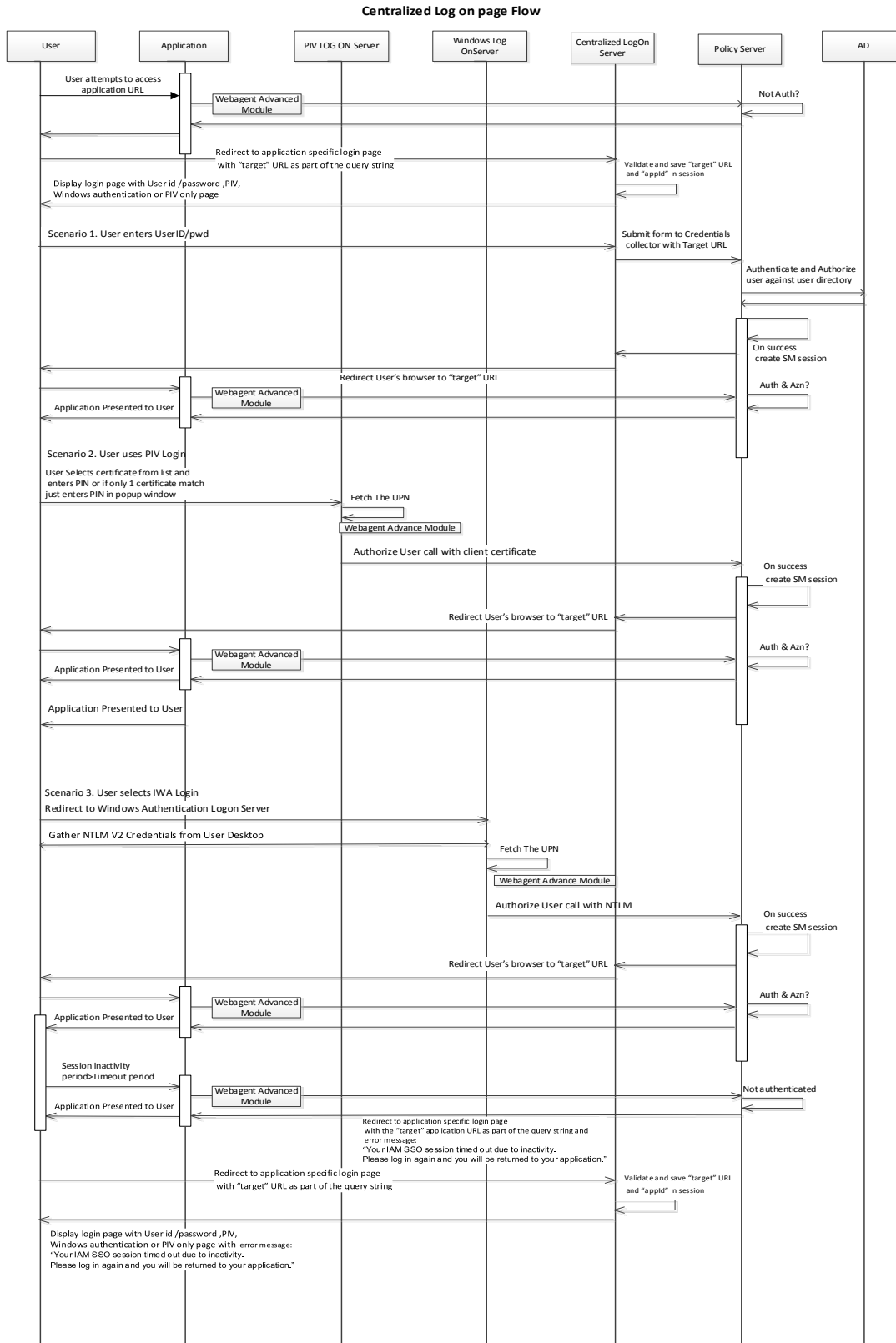


Figure 99: Centralized Logon Page Flow

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 figure represents the error handling capabilities behind the authentication and authorization processes, implemented within the Centralized Login page.

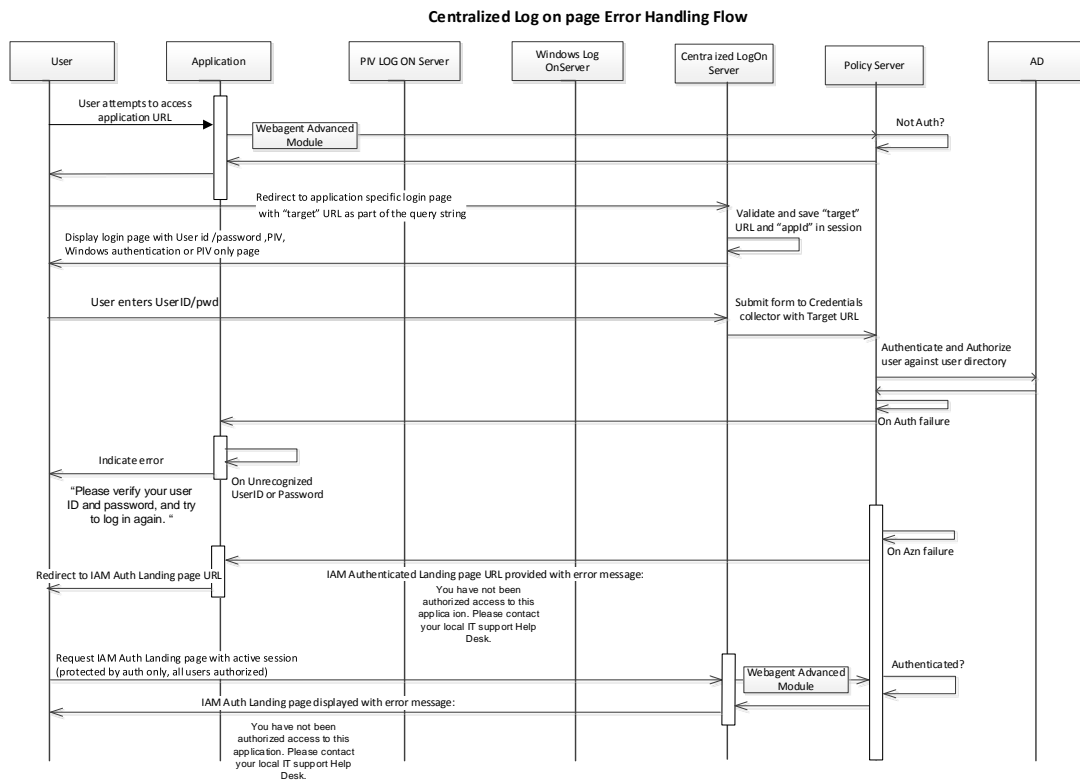


Figure 100: Centralized Logon Page Error Handling Flow

The following figure represents the supported partial and complete logoff capabilities implemented within the Centralized Login page.

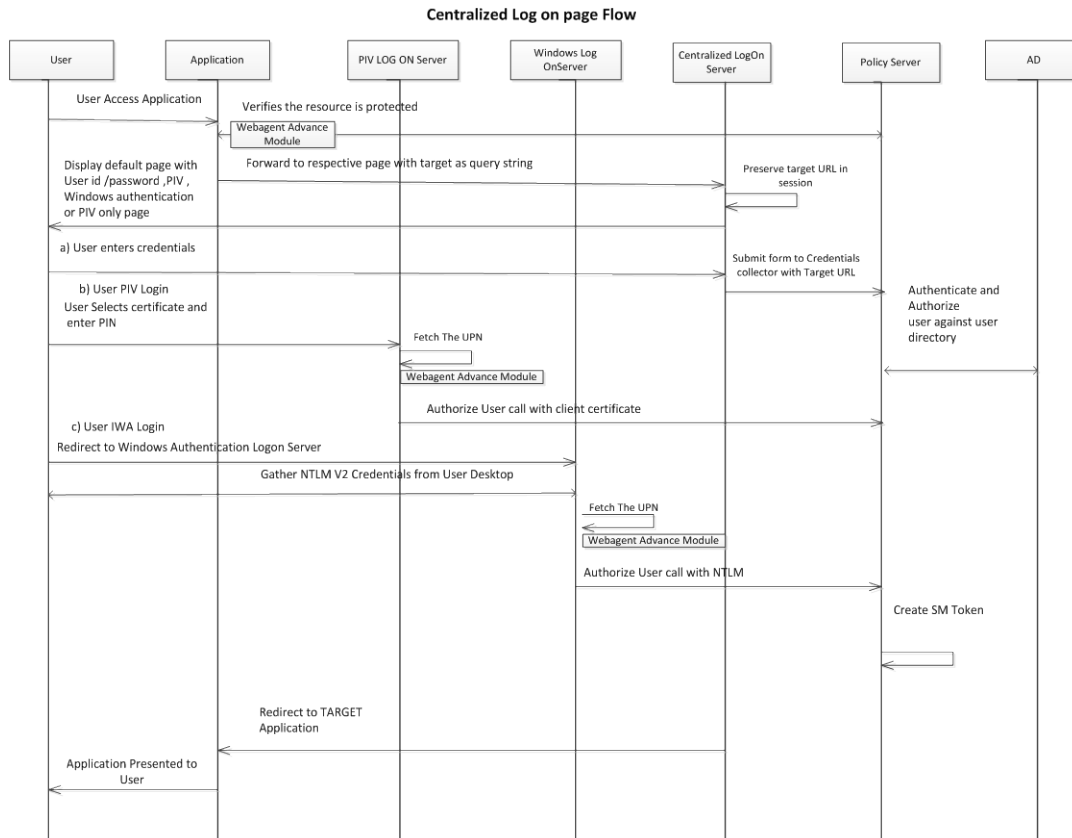


Figure 101: Centralized Login Page Supported Partial and Complete Logoff Capabilities

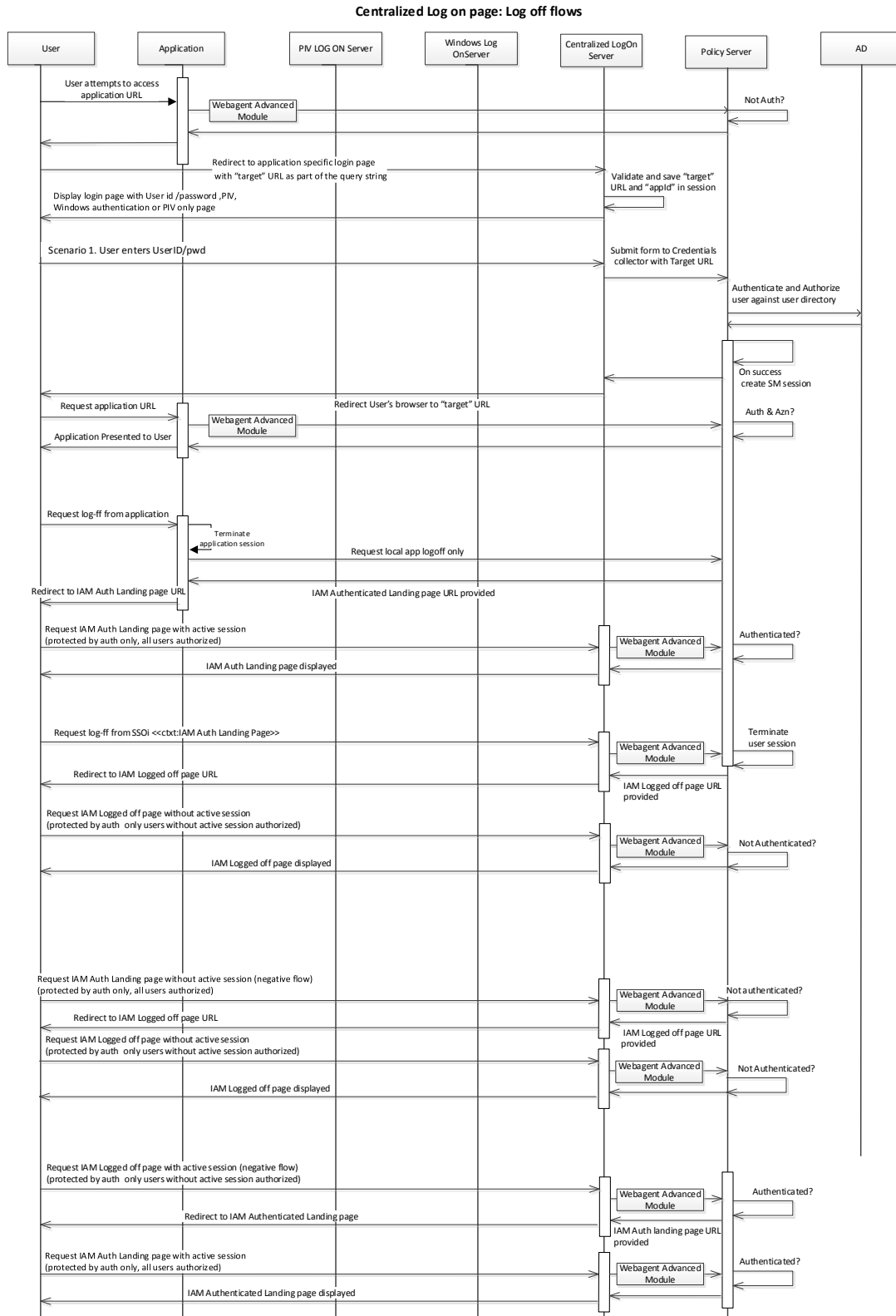


Figure 102: Centralized Logon Page - Logoff Flows

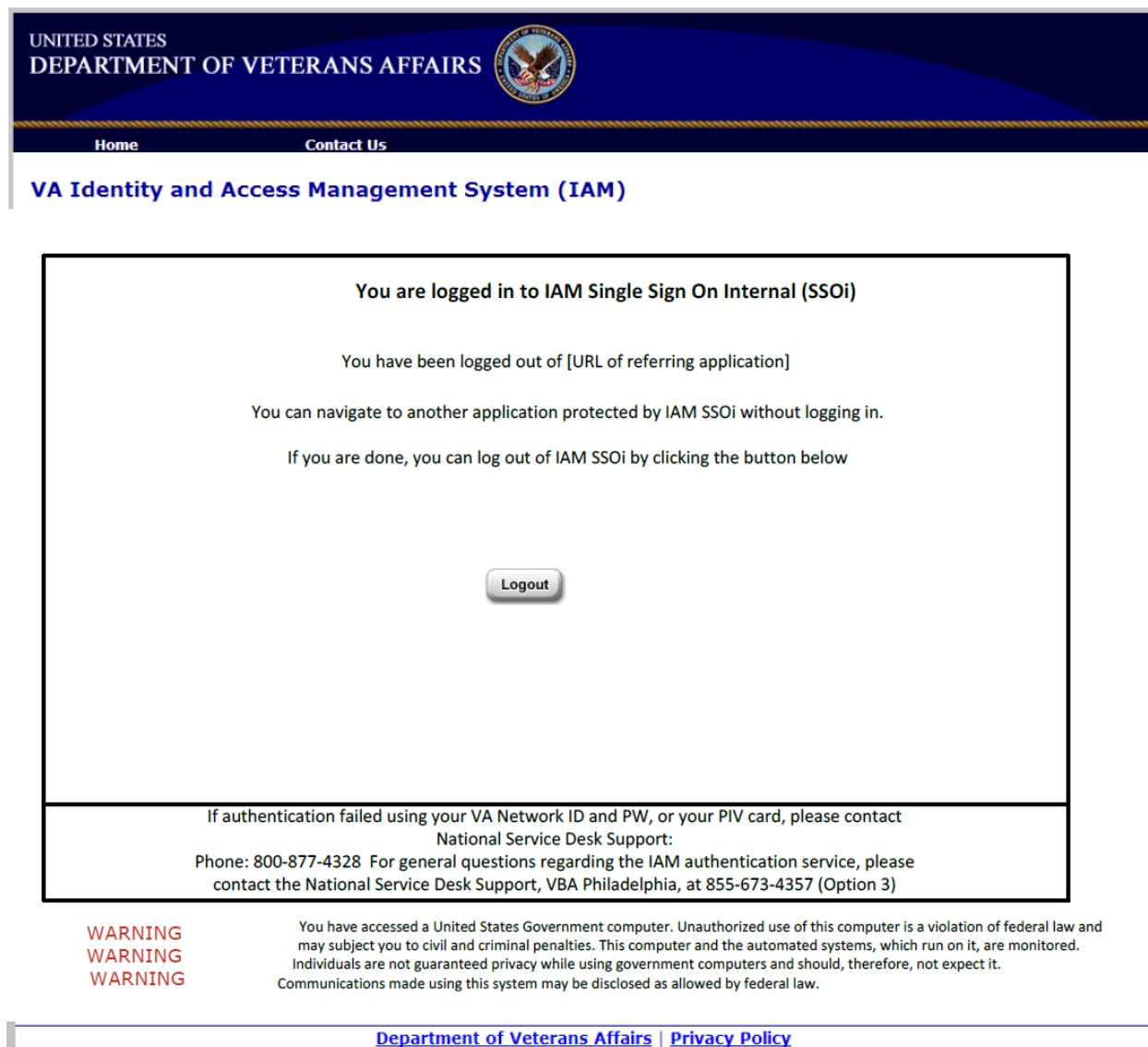


Figure 103 SSOi Authenticated Landing Page Mock-up



VA Identity and Access Management System (IAM)

You are logged out of IAM Single Sign On Internal (SSOi)


If you navigate to an application, you will be asked to log in again.

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.


Figure 104 IAM Logged Off Page Mock-up

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	Windows Authentication
<p>Enter your VA Active Directory (AD) user ID (i.e. vhaismsmithj) and password below, then click Login.</p> <p>Please verify your user ID and password, and try to login again</p> <p>User ID <input type="text"/></p> <p>Password <input type="password"/></p> <p>Login</p> <p>If you do not remember your VA Network user ID and password, please contact the National Service Desk Support:</p>	<p>Insert your PIV card into your card reader and click Login. Please enter your PIN when prompted.</p>  <p>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>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>Login</p> <p>If you experience issues trying to use Windows Authentication, please contact the National Service Desk Support, VBA (Philadelphia):</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)

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 105 IAM Centralized Login page error handling screen Mock-up

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

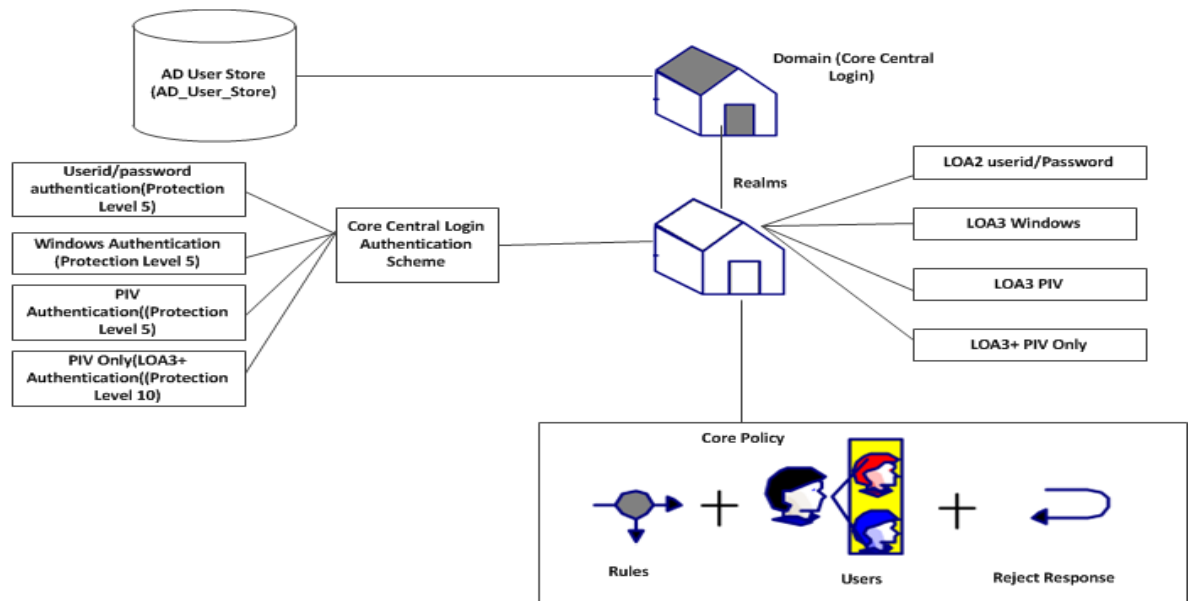


Figure 106: SiteMinder Policy Architecture for Core Centralized Authentication Flows

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.

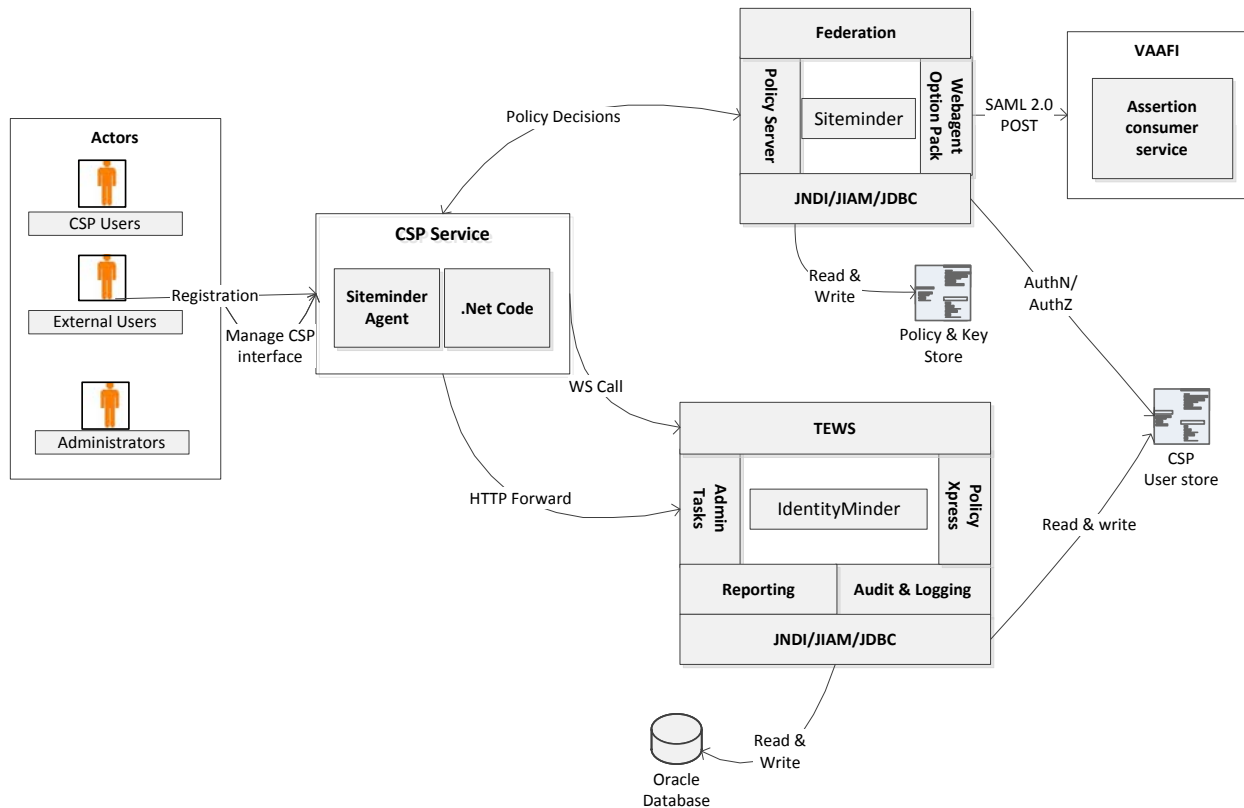


Figure 107: CSP Detailed Design

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

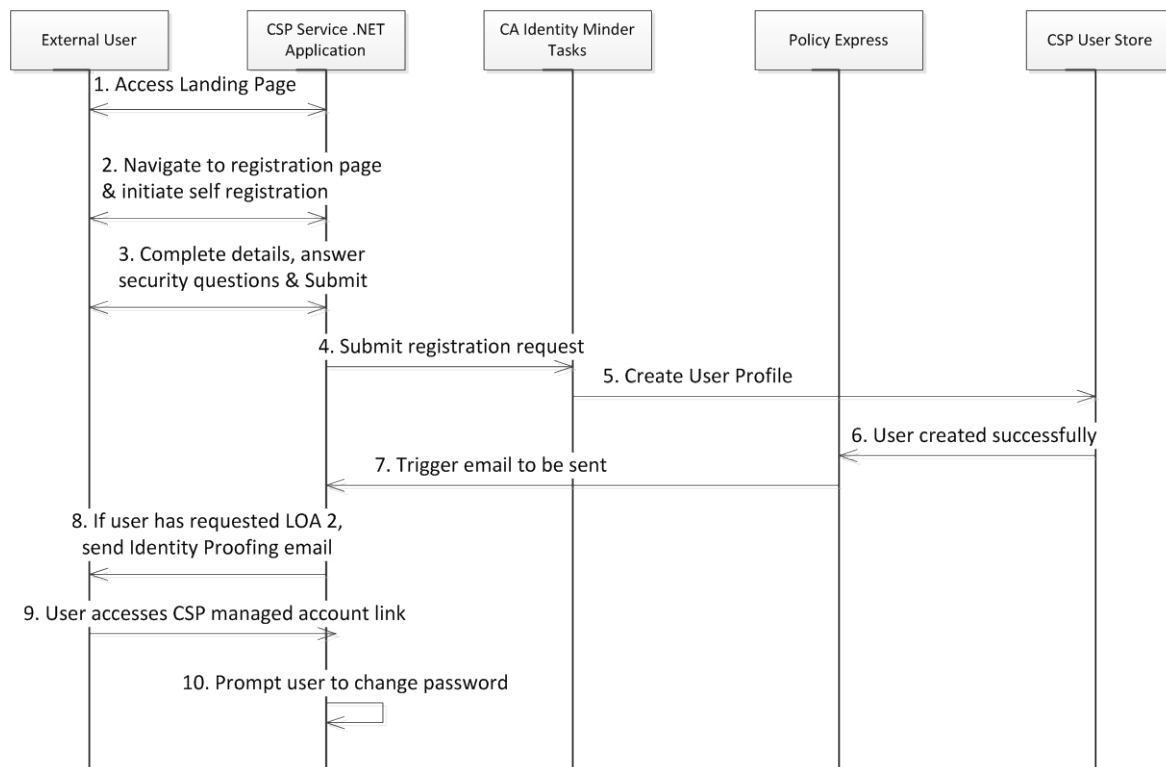


Figure 108: Credential Issuance Sequence Diagram

Table 53: 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

Field	Description
	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
Actions	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

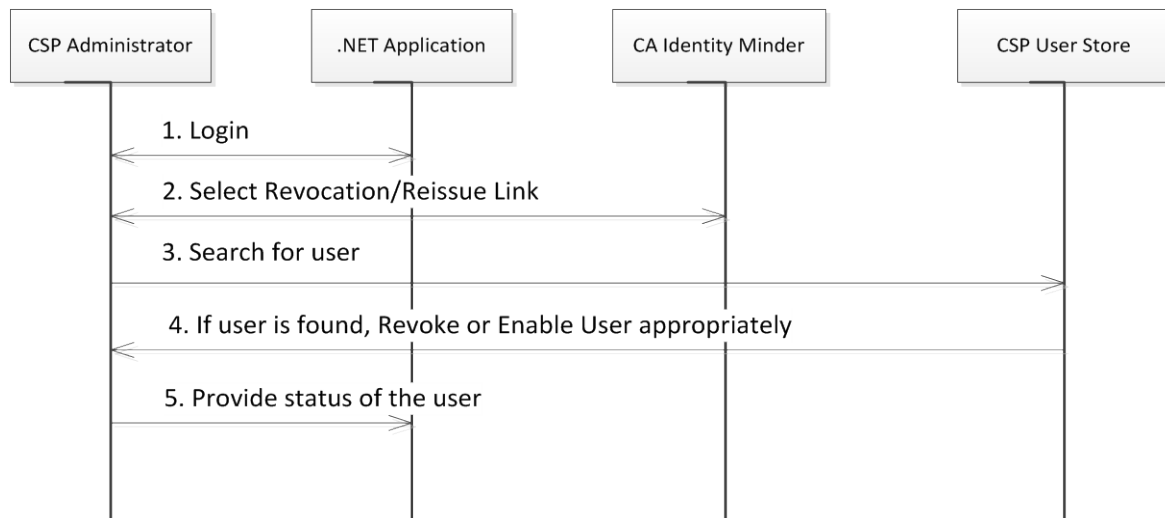


Figure 109: Revoke/Reissue Credential Sequence Diagram

Table 54: 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
Actions	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

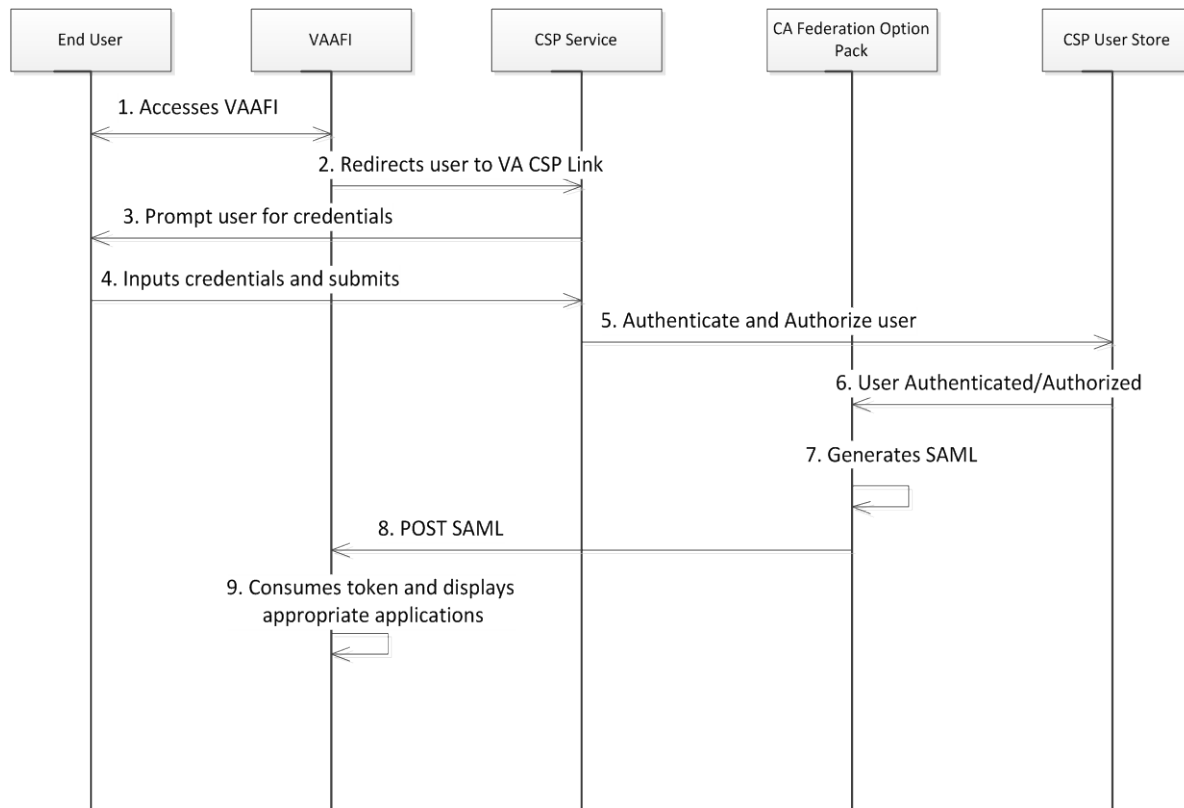


Figure 110: Federation with Consuming Application Sequence Diagram

Table 55: Federation with Consuming Application

Field	Description
Use Case Name	Federation with Consuming Application
Description	This workflow describes the technical activities and associated data exchanges through which a CSP user who poses LOA 1/ 2 credential, federate to VAAFI, to access the application behind VAAFI.
Actors	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
Actions	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

Field	Description
	<p>store is</p> <ol style="list-style-type: none"> 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 201⁴, HSPD-12⁵, OMB A-130, Appendix I⁶, VA Information Security Policies and Directives (e.g. VA Handbook 6500, Appendix F), NIST SP800-63⁷, 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 information⁸. IP services are classified as in-person, remote or hybrid.

Table 56, as defined in OMB M04-04⁹, is referenced to the NIST SP 800-63 Identity proofing processes and drives their scope and extensiveness.

⁴ <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

⁵ <https://www.dhs.gov/homeland-security-presidential-directive-12>

⁶ http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

⁷ <http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>

⁸ <http://www.gartner.com/it-glossary/identity-proofing-services>

⁹ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>

Table 56: Potential Impact Categories for Authentication Errors

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

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

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

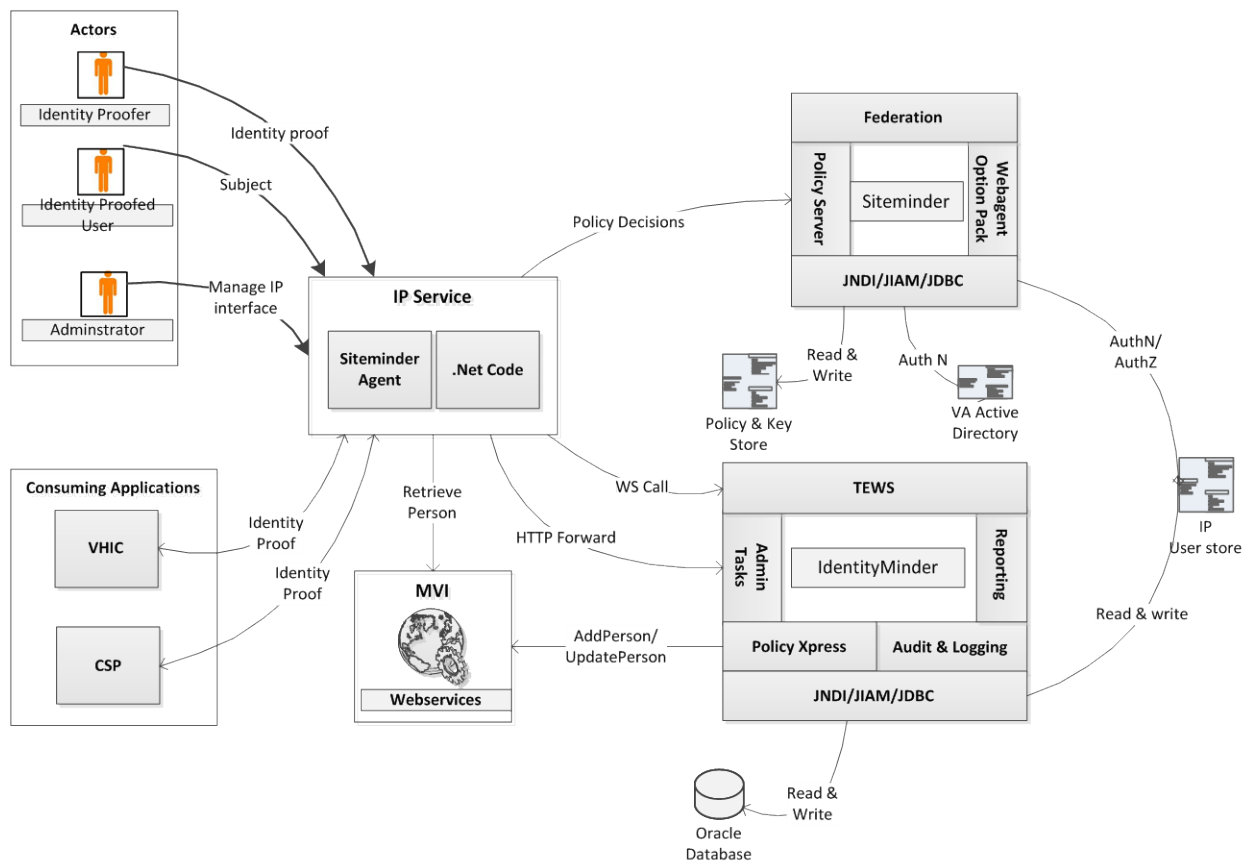


Figure 111: IP Detailed Design

CA IdentityMinder:

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

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

IP Service:

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

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

6.2.6.1 Identity Proof a User

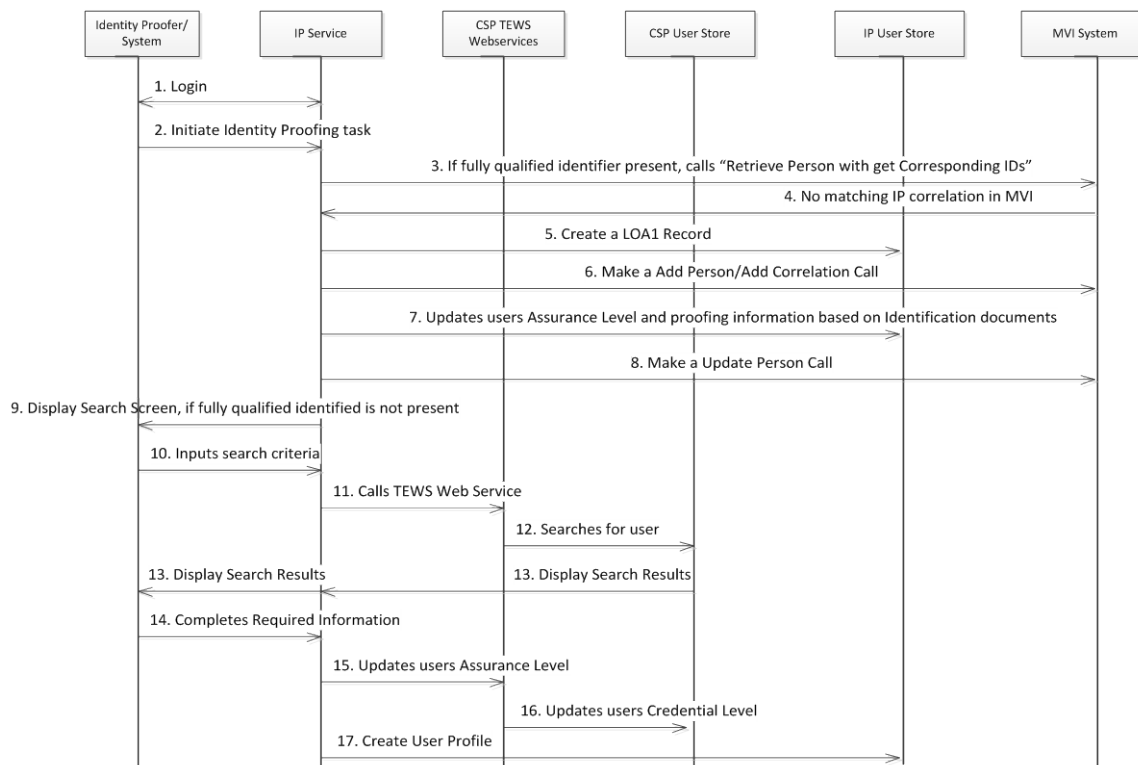


Figure 112: Identity Proof a User Sequence Diagram

Table 57: 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
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

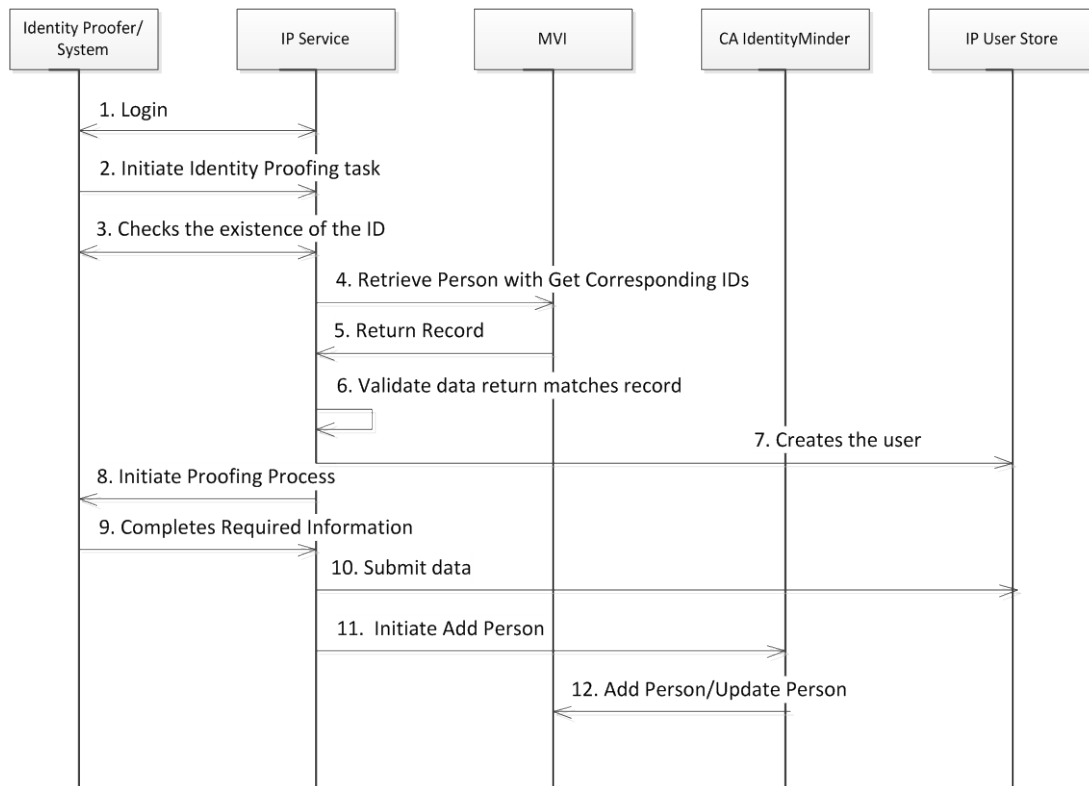


Figure 113: Create Proofing Record Sequence Diagram

Table 58: 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 Service 2. Identity Proofer/System 3. CSP TEWS Web services 4. CA Identity Minder
Pre-Conditions	Identity Proofer/system have the required access to perform the create proofing record function
Trigger	CSP user goes to the proofing station to get identity proofed
Actions	<ol style="list-style-type: none"> 1. Identity Proofer/System logs into IP service 2. Identity proofer/System initiates create identity proof task on the IP service 3. IP services receives the fully qualified identifier and checks the existence of the ID in the IP system 4. IP services get the primary view of the user and make a MVI function call "Retrieve Person with get Corresponding IDs" 5. MVI returns the person record. 6. Validates the primary data matches the retrieved person record 7. Create the user record in IP system, if it is not present already 8. Identity Proofer enters all the necessary information for identity proofing and submits the record to update the IP service 9. IP service make a TEWS call to CA IdentityMinder of the IP system 10. Submit the data to IP store 11. The policy express of IdentityMinder gets triggered and calls the MVI Add person or update person (correlation) function based on existence of user in MVI
Main Success Scenarios	Created of LOA 2 user in Identity Proofing system
Main Failure Scenarios	Error during create proofing record

6.2.7 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.

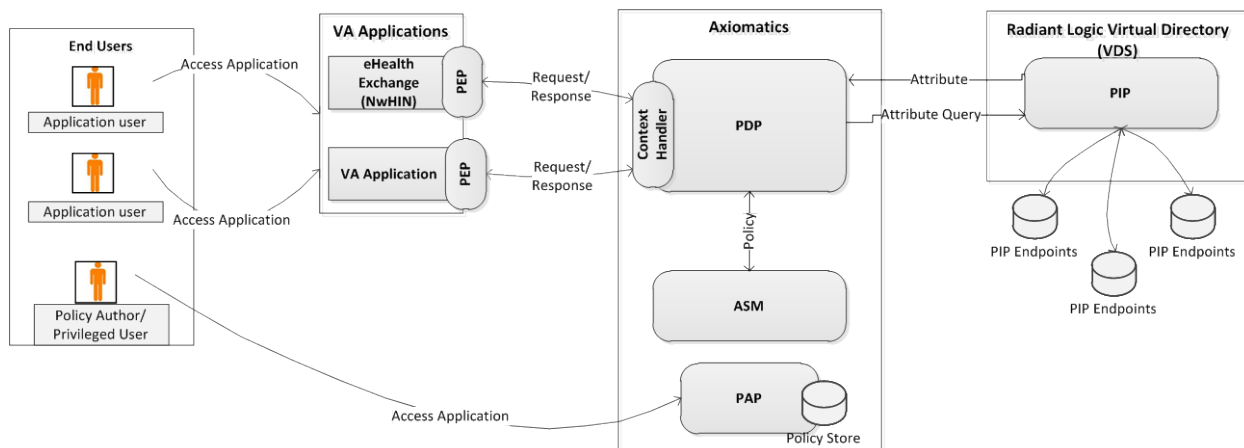


Figure 114: SAC Detailed Design

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.

- **Legacy PDP functionality:** PDP has backwards compatibility with XACML 2.0 standard and currently the SAC implementation has a separate endpoint, configured for handling legacy application requests.**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

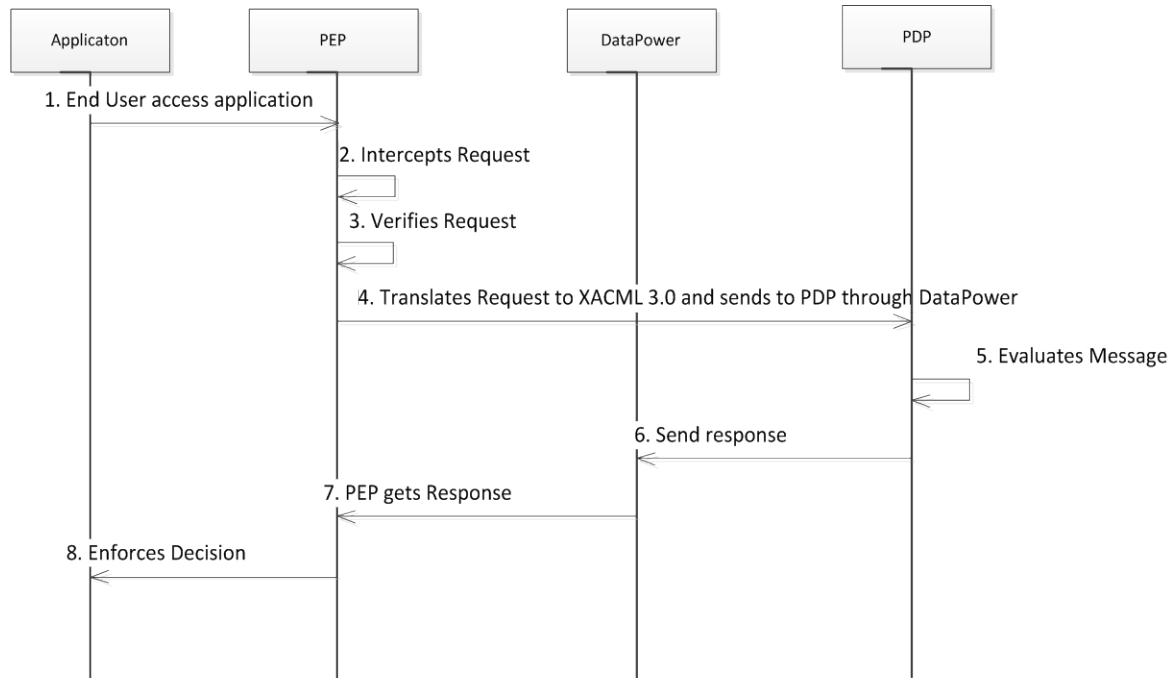


Figure 115: Enforce Access Control Decision Sequence Diagram

Table 59: 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	1. Application 2. PEP 3. DataPower 4. PDP
Pre-Conditions	1. Enter User has authenticated session with Application 2. TLS session is established between the Application and PEP
Trigger	The PEP receive a request for an authorization from an application
Actions	1. End-User attempts to access protected application. 2. PEP intercepts access request 3. The PEP can reside between the end user and the application 4. The PEP can reside within the application itself 5. PEP verifies request is valid and contains authentication attributes that can be

Field	Description
	<p>used to uniquely identify the user</p> <ol style="list-style-type: none"> PEP translates access request to XACML 3.0 Includes authentication attributes (SECID, ICN, unique identifier) May include client preferences, data restrictions, user security, contextual constraints Forwards XACML 3.0 request to DataPower DataPower performs XML threat reduction and forwards request to PDP 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. The PDP response is sent to DataPower DataPower sends PDP response to the PEP. PEP receives XACML 3.0 access control decision response from the PDP. PEP enforces access control that it received from PDP.
Main Success Scenarios	<ol style="list-style-type: none"> If Decision is Permit, access is granted to the user to access the protected resource. If Decision is Deny, access is denied. The user is not allowed to access the protected resource. The processing of Indeterminate or Not Applicable is determined by the application requirements.
Main Failure Scenarios	<ol style="list-style-type: none"> Message format/contents are not valid PDP is non-responsive and decision is not provided to application

6.2.7.2 Security Policy Authoring

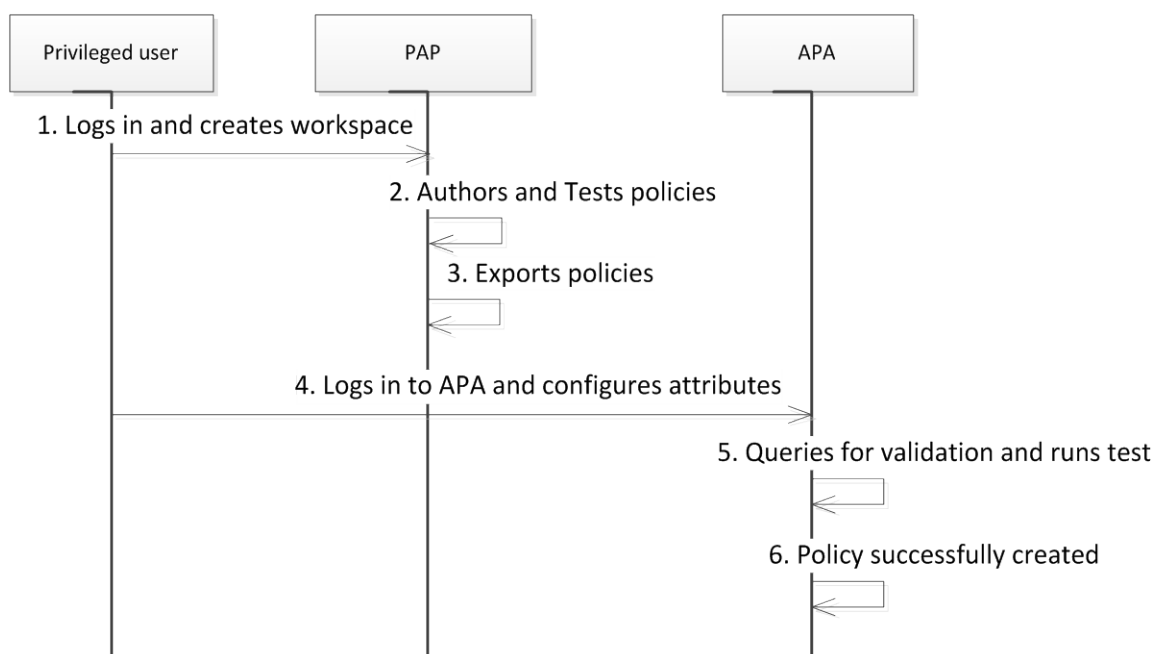


Figure 116: Security Policy Authoring Sequence Diagram

Table 60: 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	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	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 4. Once completed, the privileged user exports policy package to dedicated file location 5. Privileged User logs into APA and configures attributes from the PEP perspective 6. Privileged User creates queries for validation and runs validation tests 7. Policy is authorized successfully upon successful testing
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

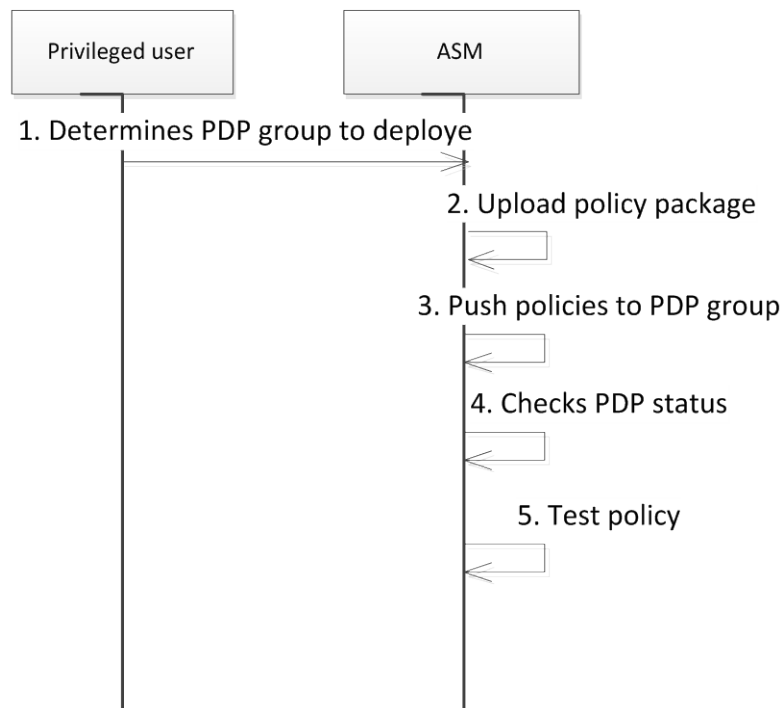


Figure 117: Manage Access Control Policies

Table 61: 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	1. Privileged User 2. 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	1. Privileged User determines proper PDP group to deploy policy package 2. Upload validated policy package 3. Push policies to managed PDP within PDP group 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
Main Success Scenarios	Policy is pushed to PDP successfully
Main Failure	Policy upload fails and user has to start over.

Field	Description
Scenarios	

6.2.7.4 Make Access Control Decisions

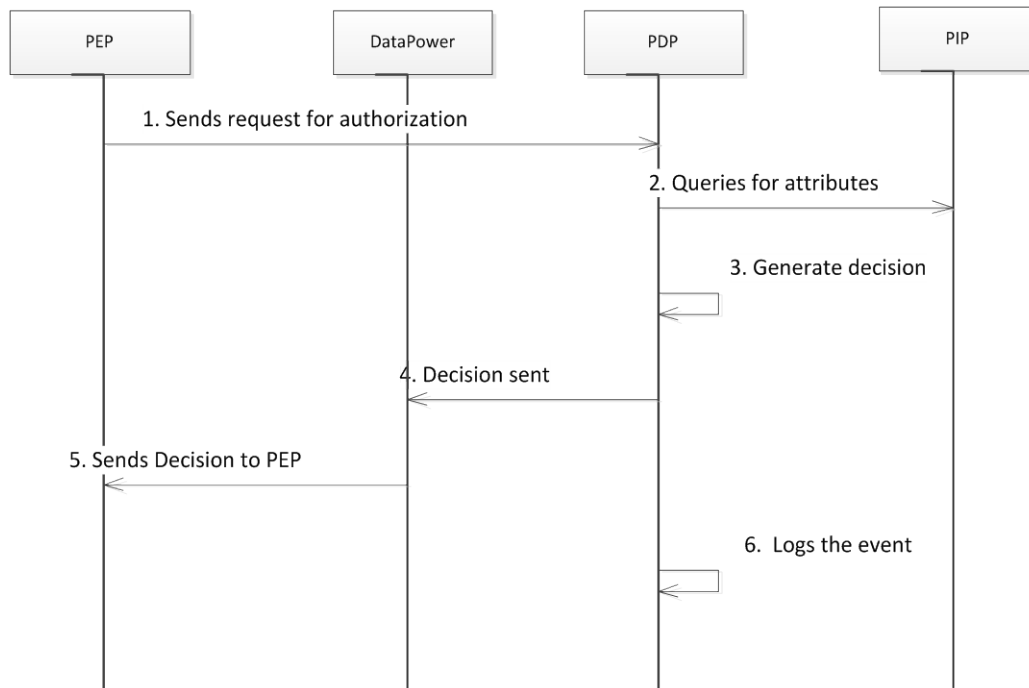


Figure 118: Make Access Control Decisions Sequence Diagram

Table 62: 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
Actions	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

Field	Description
	<p>access control decision</p> <p>4. The XACML 3.0 response/access control decision is sent to DataPower</p> <p>5. DataPower sends the XACML 3.0 response/access control decision to the requested PEP</p> <p>6. PDP logs the access request and response</p>
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

6.2.7.5 Make Access Control Decisions (XACML 2.0)

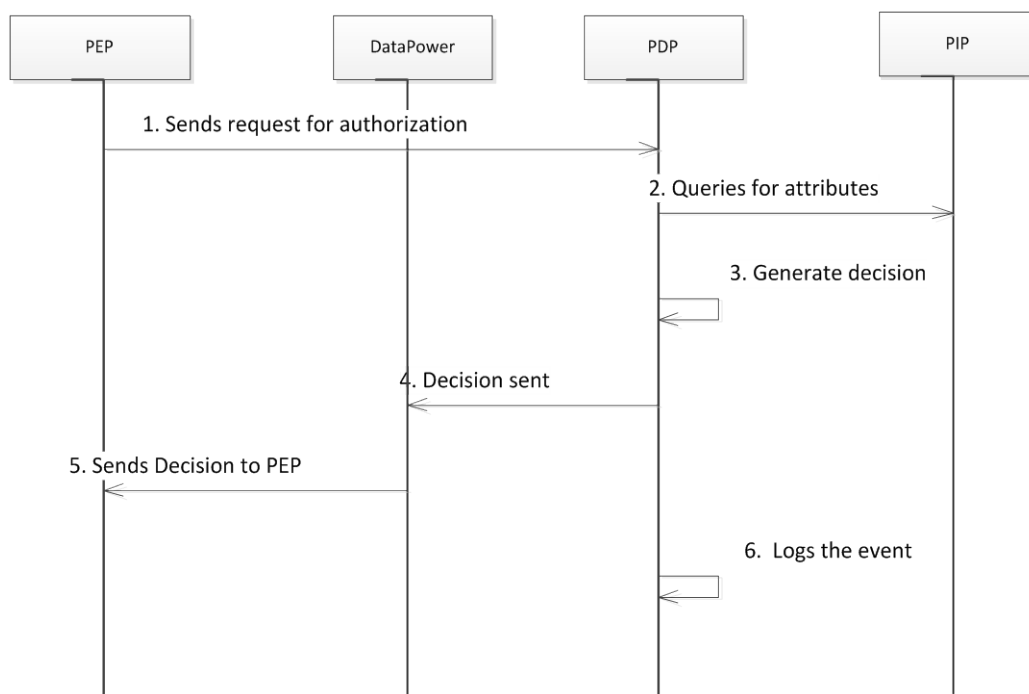


Figure 119: Make Access Control Decisions (XACML 2.0) Sequence Diagram

Table 63: Make Access Control Decisions Using XACML 2.0 Request/Response

Field	Description
Use Case Name	Make Access Control Decisions using XACML 2.0 request/response
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	<p>1. PEP</p> <p>2. DataPower</p> <p>3. PIP</p>

Field	Description
	4. PDP
Pre-Conditions	The application authorization policy and needed attributes exist
Trigger	PDP receives XACML request from PEP via DataPower
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 2.0 request, the attributes retrieved from the PIP, and the XACML 2.0 security policies to generate an access control decision 4. The XACML 2.0 response/access control decision is sent to DataPower 5. DataPower sends the XACML 2.0 response/access control decision to the requested PEP 6. PDP logs the access request and response
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.

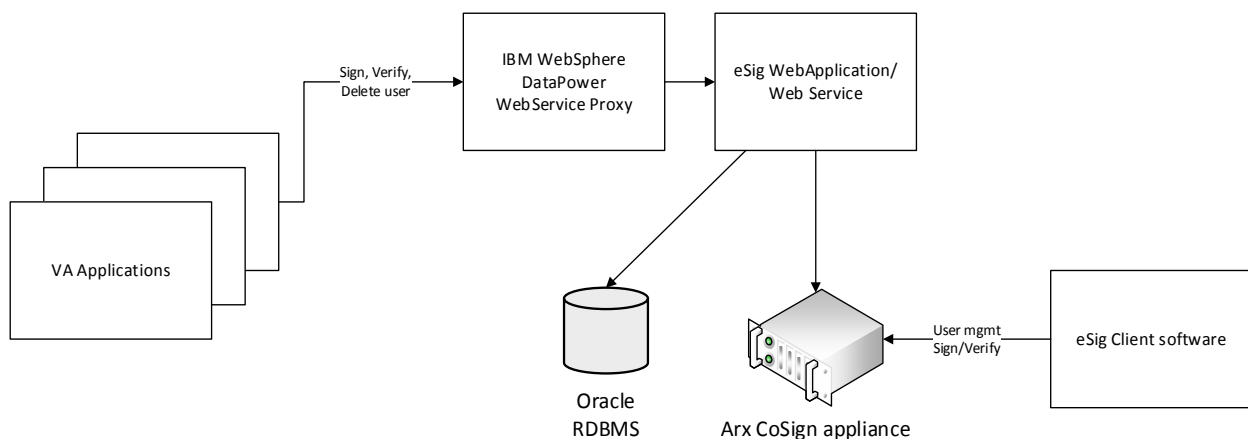


Figure 120: eSig Logical Design

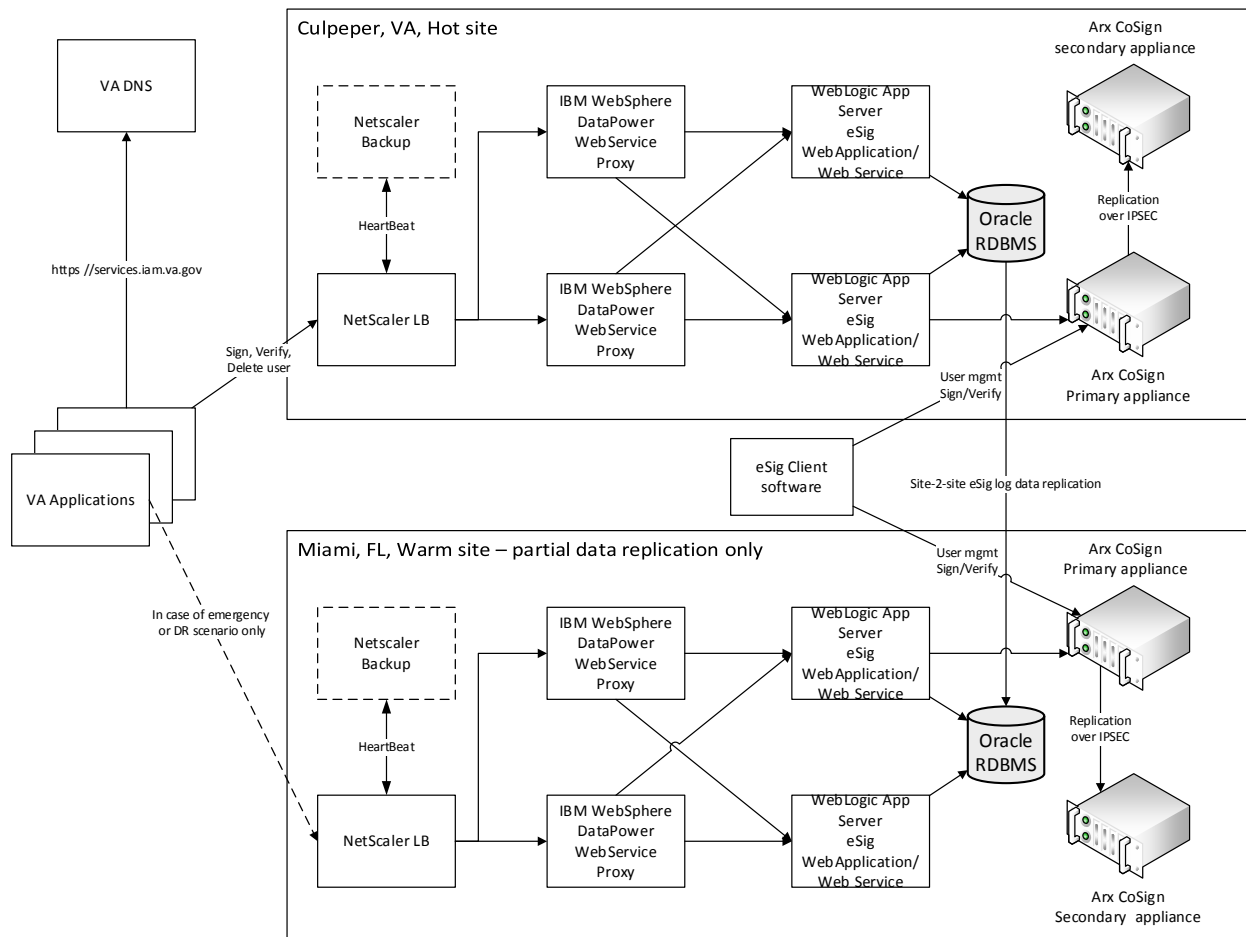


Figure 121 eSig Physical design

The eSig custom code is implemented as Java/J2EE application, exposing a WebService interface. The implementation uses the Java Servlet API v2.3. This configuration allows integration of the eSig services with both web based applications and supports machine to machine SOAP WebService calls. The eSig WebApplication utilizes the façade design pattern, which allows for flexibility in backing interface definitions and abstraction from exposing backend system complexities to the eSig clients/partners. With the façade approach, any changes to the CoSign appliance will most likely not result in any changes on the eSig interface exposed to its clients/partners. The façade pattern allows for flexible manipulation of user roles and can prevent certain function calls based on the eSig request submitter's role. Requests to the eSig WebApplication are stateless. Parallel execution of the façade pattern implementation classes (supported OOB by the underlying Web application server J2EE Web Container) allows for optimized scalability of the custom code.

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). The reason (if supplied) will be under the email address, and the signature date and time with the GMT offset value positioned under the reason on the right side of the signature box, as the following figure illustrates.

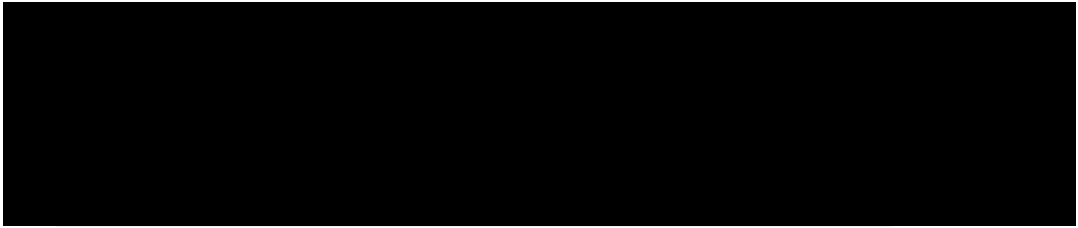


Figure 122: Example Visible Signature

6.2.8.1 Sign a Document

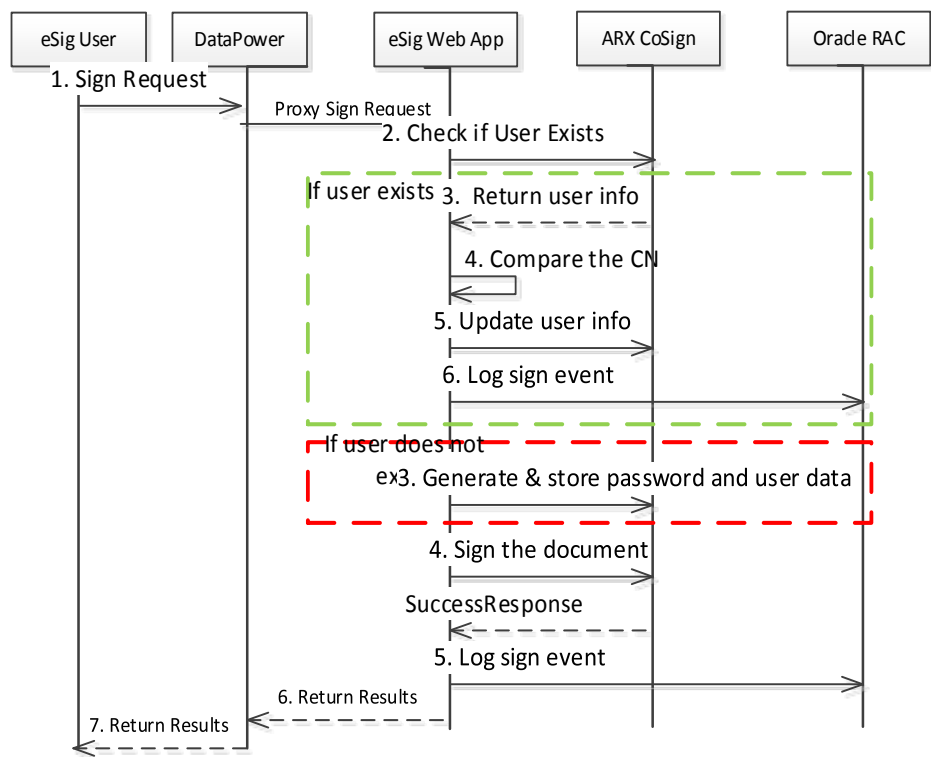


Figure 123: Sign a Document Sequence Diagram

Table 64: Sign a Document

Field	Description
Use Case Name	Sign a Document
Description	This Use Case describes the process through which a User signs a document electronically.

Field	Description
Actors	<ol style="list-style-type: none"> 1. eSig user 2. DataPower 3. eSig Web App (eSig Web Service) 4. ARX CoSign 5. Oracle RAC
Pre-Conditions	<ul style="list-style-type: none"> • The document type to be submitted is one of the supported types by eSig. • End user is authenticated with at least LOA 2 or above credential.
Trigger	A VA application sends a digital signing request to eSig.
Actions	<ol style="list-style-type: none"> 1. DataPower intercepts the signature request from the user and sends it to the eSig Web Service. 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"> 3.1 ARC CoSign returns the user information 3.2 The eSig Web Service compares the CN 3.3 The eSig Web Service updates the user information in the ARX CoSign 3.4 The eSig Web Service logs the sign event with the Oracle RAC 4. If the user does not exist, eSig Web Service generates and stores the encrypted password and user data. 5. The eSig Web Service signs the document and sends the success response to ARX CoSign. 6. The eSig Web Service logs the sign event and returns results to DataPower.
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 Verify Document

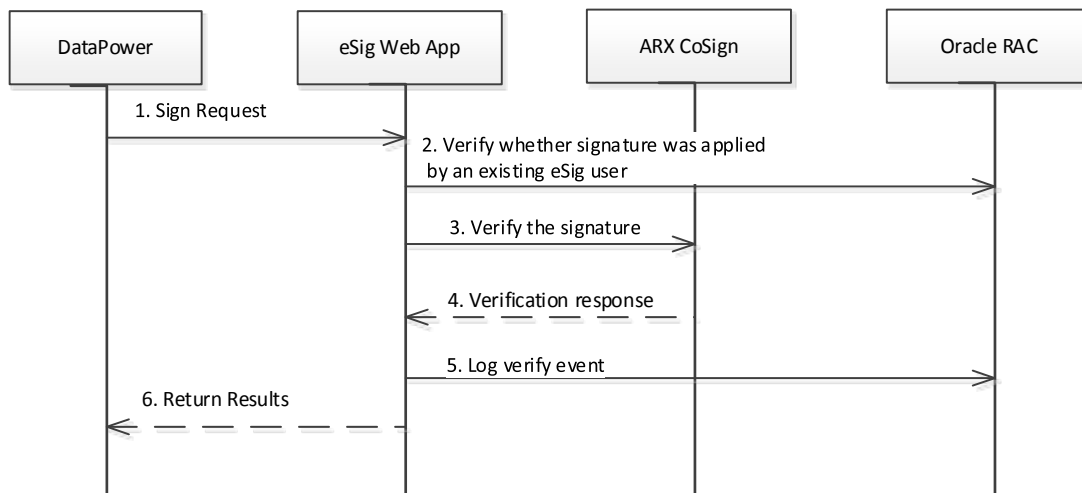


Figure 124: Verify a signed document - sequence diagram

Table 65: Verify a signed document

Field	Description
Use Case Name	Verify a signed document
Description	This Use Case describes the process through which a signed document is verified
Actors	<ol style="list-style-type: none"> 1. eSig user 2. DataPower 3. eSig Web Application (Web Service) 4. ARX CoSign 5. Oracle RAC
Pre-Conditions	The document type to be submitted is one of the supported types by eSig
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 Web Service. 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.
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)

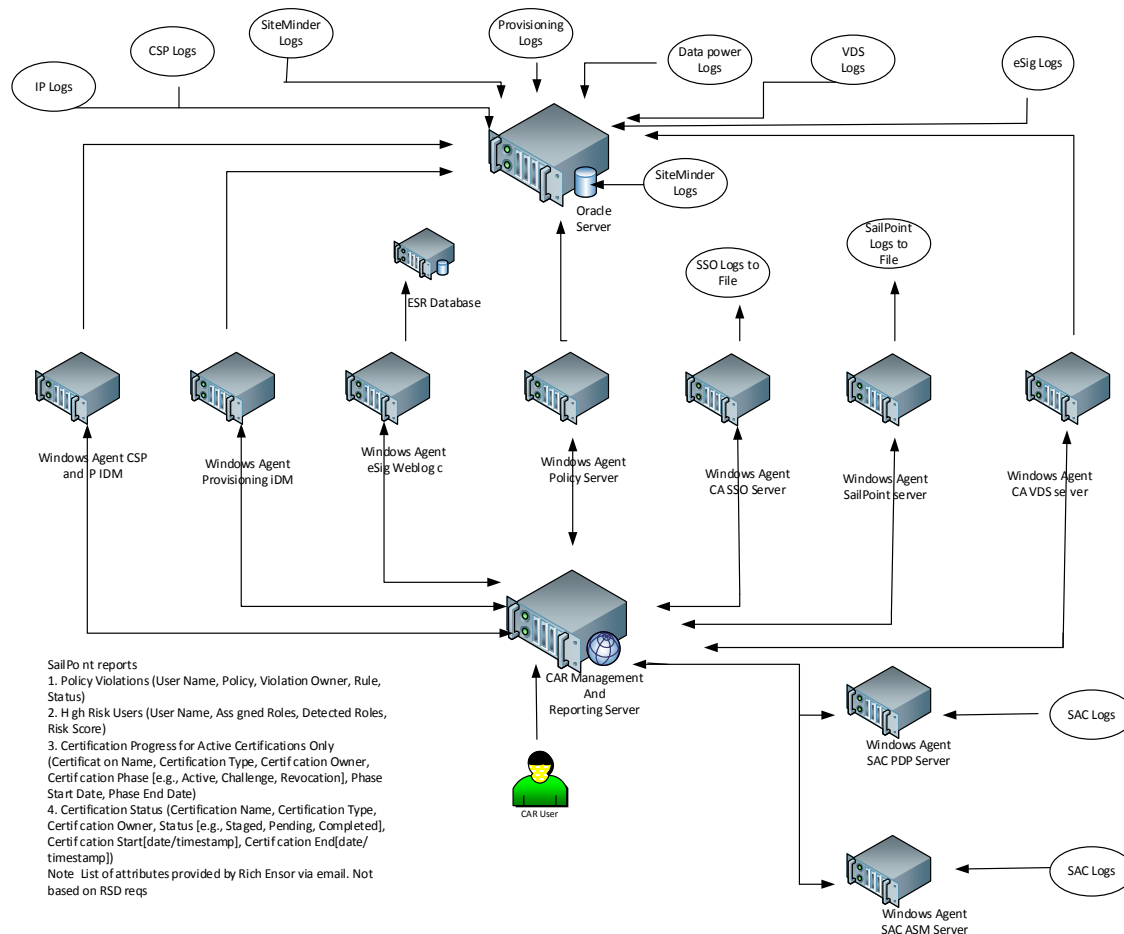


Figure 125: CAR Detailed Design

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

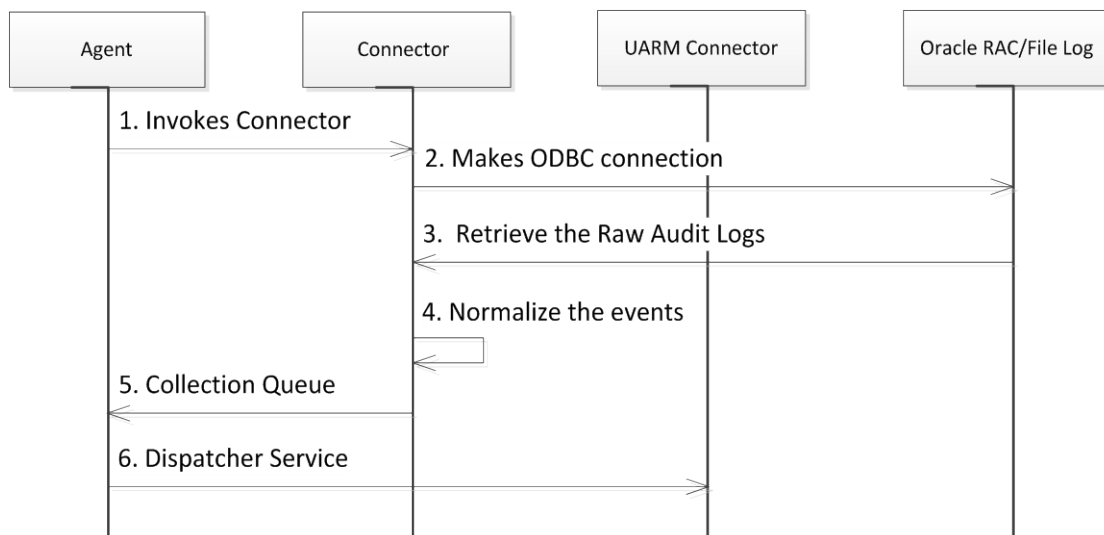


Figure 126: Process Activity Logs to Generate Reports Sequence Diagram

Table 66: Process Activity Logs

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	1. Agent 2. Connector 3. UARM Connector 4. Oracle RAC/File Log
Pre-Conditions	The [REDACTED] 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 [REDACTED] activity agent.

Field	Description
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.
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 [REDACTED] 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 [REDACTED] solution.

6.2.10.1.4 Communications Interfaces

Refer to section 4.3 for the detailed communication design for the [REDACTED] solution.

6.2.10.1.5 Memory Constraints

This section is not applicable to the [REDACTED] solution.

6.2.10.1.6 Special Operations

This section is not applicable to the [REDACTED] solution.

6.2.10.2 Product Features

The [REDACTED] solution is based on the foundation of CA COTS products. The table below describes the [REDACTED] solution products.

Table 67:  Solution Products

#	Software	Description
1	CA IdentityMinder	A scalable, configurable identity management solution that automates onboarding, modification and off-boarding of users, enables self-service requests and automates proactive identity compliance processes.
2	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.
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 HPUX 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_Vet (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.

#	Software	Description
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.
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 [REDACTED] solution constraints and dependencies.

6.2.11 Specific Requirements

This SDD provides the foundational detailed design for [REDACTED] activities under VA Development Support program. VA [REDACTED] 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 [REDACTED] solution.

6.4 System Maintenance Design

During periods of system maintenance or outages, customer/user facing Graphical User Interfaces (GUI) have to be updated to inform the specific [REDACTED] audience of the state of the system, what the expected return to service timeframe is and any additional references - e.g. Help Desk numbers, ANR information that may be needed for the users of the system in order to allow them to either use an out-of-band process or be kept informed of any progress as needed.

6.4.1 Maintenance pages

The following figure reflects the general form of the Maintenance page to be displayed for any [REDACTED] component with customer/user facing GUI during a period of either scheduled or unscheduled maintenance.

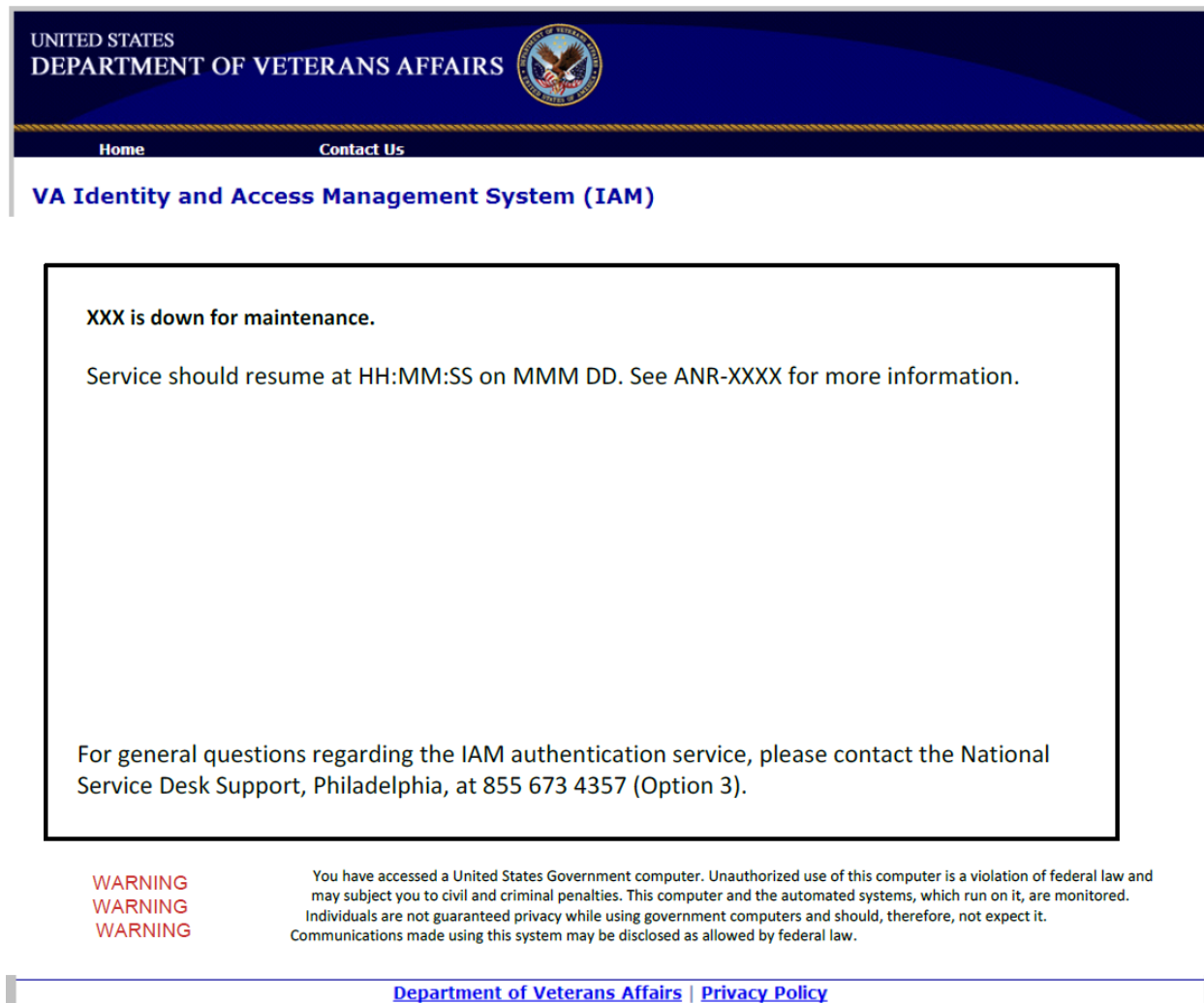


Figure 127: Maintenance Page for [REDACTED] Component

Each of the following [REDACTED] sub-systems (IP, CSP, Prov, SSOi Central Login, CAR, and SailPoint) will be updated to include a customized maintenance page with appropriate system reference on each page.

The [REDACTED] e-Sig, SAC and VDS services do not provide a GUI for users or customers. Any maintenance being performed on those services will have to be communicated to the customers/partners consuming those services so they can display the appropriate notification for partial or full loss of functionality/service on their respective GUIs.

Note: Administrative GUIs for the [REDACTED] COTS products will not have a maintenance page, as they are not exposed to external audience and are necessary for the actual maintenance process.

In order to allow for a centralized control of maintenance page requirements, maintenance page enforcement policies in Siteminder Policy server shall control the redirects to the appropriate maintenance pages for IP, CSP, Provisioning, SSOi Central Login, and SailPoint. Individual policies per [REDACTED] component will ensure each component can be enforced separately or in a group. Policies will be enabled and disabled as dictated by the deployment plans for each production deployment for the above listed components.

CAR maintenance pages will be handled through rules on the Apache servers supporting each of the CAR UI components. Those rules will be enabled and disabled as dictated by the deployment plans for each production deployment of CAR.

Maintenance pages will have two principal locations, dictated by the various circumstances in which a maintenance can occur.

Maintenance pages for all [REDACTED] system components, except CAR will be hosted on the Centralized login page servers as a primary location.

When maintenance requires downtime of all Siteminder Policy servers, all Centralized login page servers or any of the Policy server supporting user stores, which in effect will disallow policy evaluation and enforcement for Maintenance Page policies, a secondary hosting location will be used on each of the forward facing web servers for each [REDACTED] component (CAR falls under this category by the fact that it does not integrate with SSOi).

Local WebServer rules will be configured to enforce the complete bypass of any requests for application resources and redirect to a web server available to host the maintenance pages, with the same business rules as the Siteminder Policies. These web server maintenance page rules will follow the same enforcement by the deployment plan for each production deployment.


Since the individual WebServer rule usage will require multiple server modifications, care needs to be exercised not to omit any of the applicable web servers and not enable rules on a component which should not be under maintenance.

Content of the Maintenance pages will be updated before maintenance period's start in both primary and secondary hosting locations as well as during the maintenance to ensure consistency.

For future implementations, a CMS like TeamSite or similar may be used to provide ease of roll-out of maintenance pages.

As an alternative Maintenance pages can be hosted at LoadBalancer appliance, but this approach will make the control of the maintenance pages outside of the [REDACTED] control and require AIDE involvement at each maintenance period.

7 External Interface Design

This section describes the external interfaces with which the  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 Figure 127: CSP to VAAFI Interface Flow, 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.

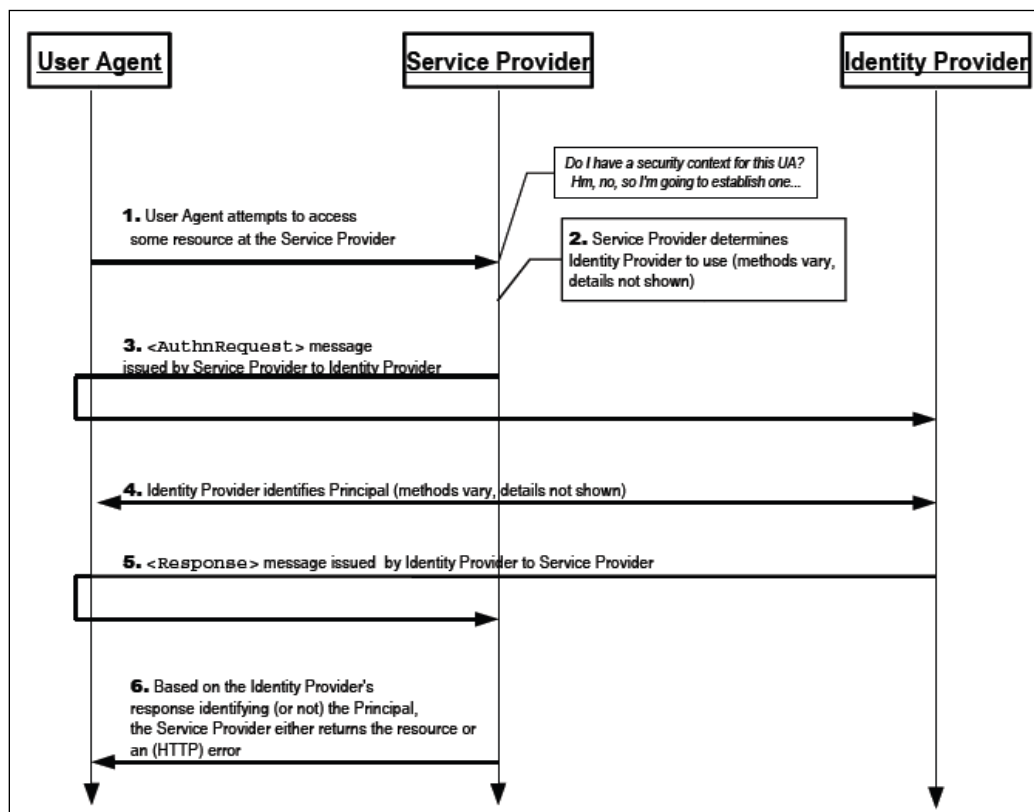


Figure 128: CSP to VAAFI Interface Flow

7.1.2 Master Veteran Index

The  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 Person/Update 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 [REDACTED] activities.

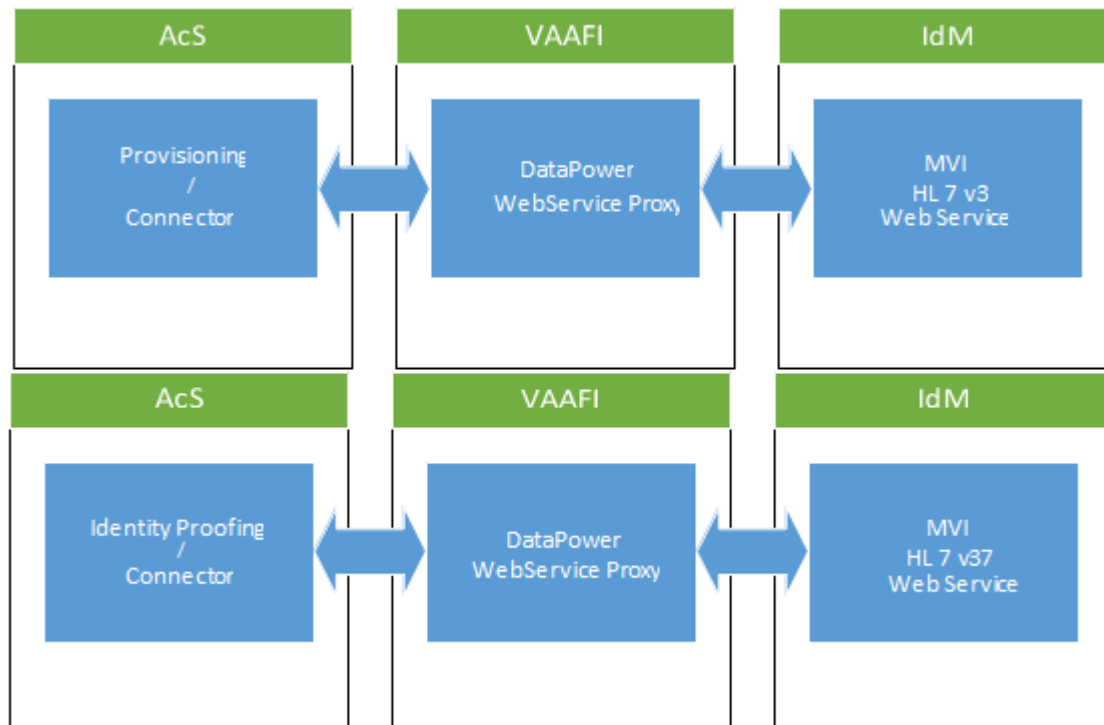


Figure 129: MVI Interface Flow with Provisioning and IP

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 [REDACTED] Increment 2, Increment 3, and Increment 4 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.

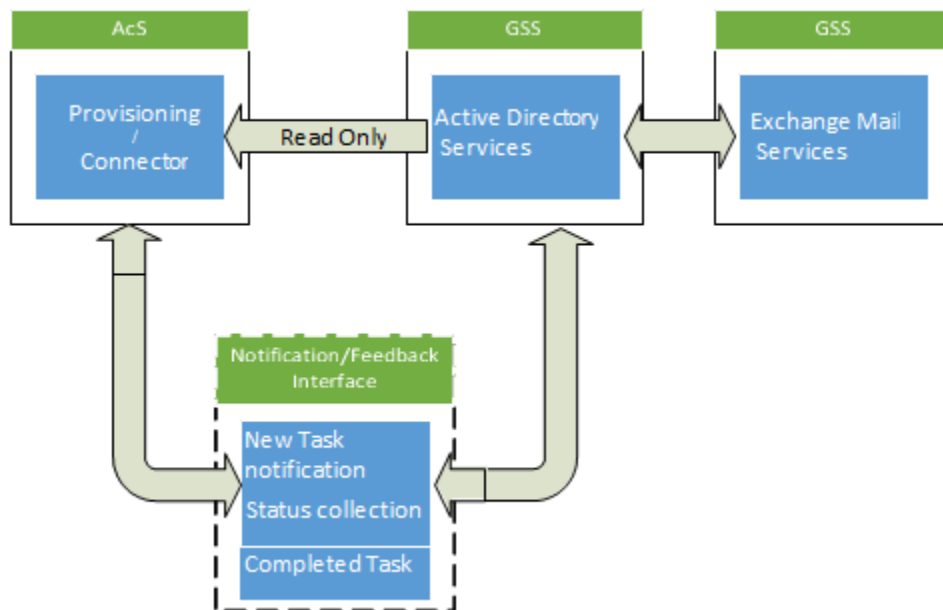


Figure 130: Provisioning – Active Directory Interface Architecture

7.1.4 Provisioning – VistA

The high level integration between Provisioning and VistA systems described in Release 2, Increment 4 is shown in the diagram below.

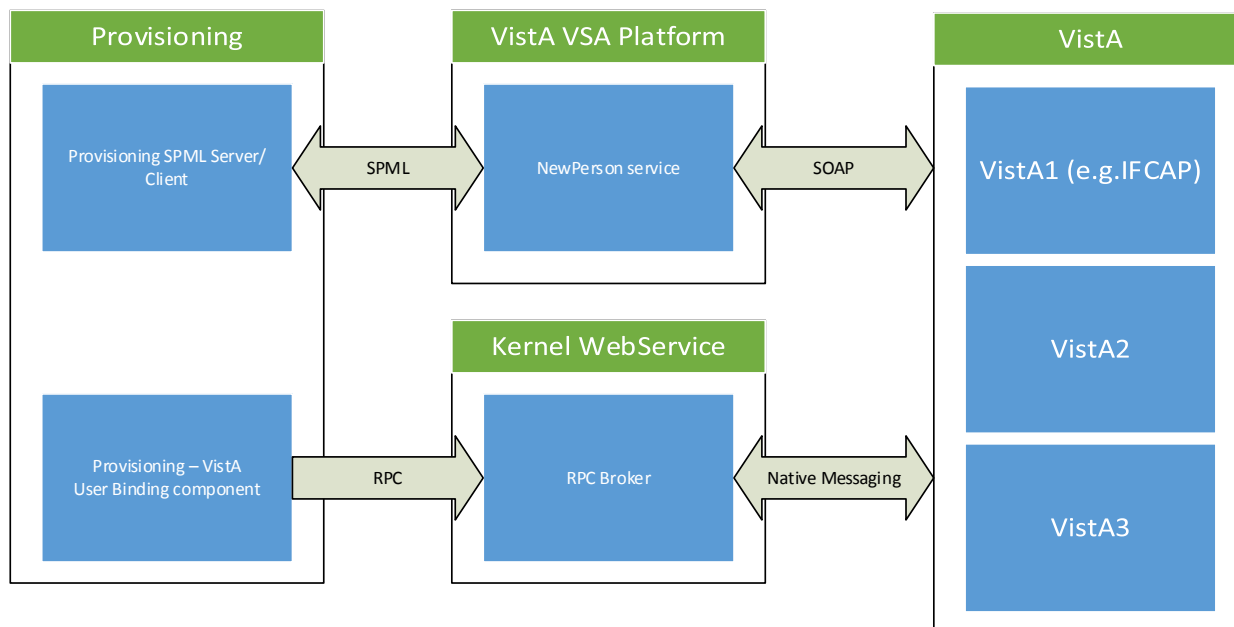


Figure 131 Provisioning – VistA Integration

The Provisioning SPML inbound (Server) and outbound (client) is a combination of Radiant Logic vendor provided SPML server implementation, tied to the existing Provisioning Identity

Minder's TEWS component using VDS custom code and a custom Provisioning connector for the SPML Client side.

The Provisioning – VistA binding application will be built using a combination of CA Identity Minder OOB presentation and workflow capabilities as well as custom Business Logic Task Handler (BLTH) code to satisfy the requirements described in [REDACTED] Rel2 I4 RSD.

The combination of COTS-based and custom component implementation allows the completion of the two way SPML and RPC interfaces with the capabilities described in various supplemental documents to the [REDACTED] Rel2 I3 RSD (e.g. VistA_IAM_White_Paper_v04.docx, Standard Prov SPML Interface.docx, IAM VistA Activity Diagrams 20140801.docx IAM VistA Activity Diagrams 20140801.docx) and subsequent requirements clarification discussions.

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.

Table 68: VA CSP (as CSP/IdP) sending SAML to VAAFI

Field	Description
SPID:	[REDACTED]
SiteMinder Affiliate Domain:	CSPFederationDomain
NameID:	UID
Authn Director:	CSP User Directory
Encryption Algorithm:	Block: aes-128 Key: rsa-v15
SLO:	NA
Attribute Details:	givenName sn UID VAASSURANCELEVEL

Field	Description
Signature Algorithm:	Signing Algorithm: RSAwithSHA1 RSA Key Size: 128 SAML Token : Signed Attribute Encryption: NA Assertion encrypted with certificate CN=ORC ECA SW 4,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US

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.


7.2.4 Provisioning – VistA

Section 6.2.1.8 describe the User-to-system and system-to-system interactions in conjunction with the bidirectional Provisioning to VistA activities.


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  activities as appropriate for the end users.

8.1 Interface Design Rules

The following design rules are applicable to the user interfaces for the  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  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 [REDACTED]

- PDF
- Comma Separated File (CSF)
- Excel

8.4 Navigation Hierarchy

This section documents the navigation hierarchy for [REDACTED] 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.

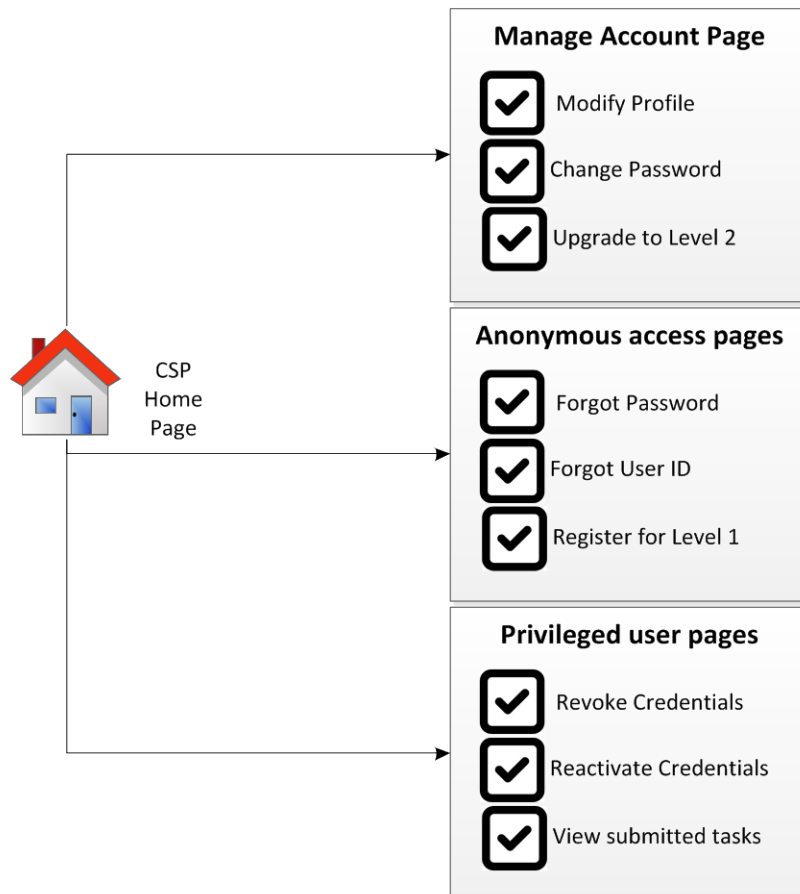


Figure 132: CSP Navigation Hierarchy

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.

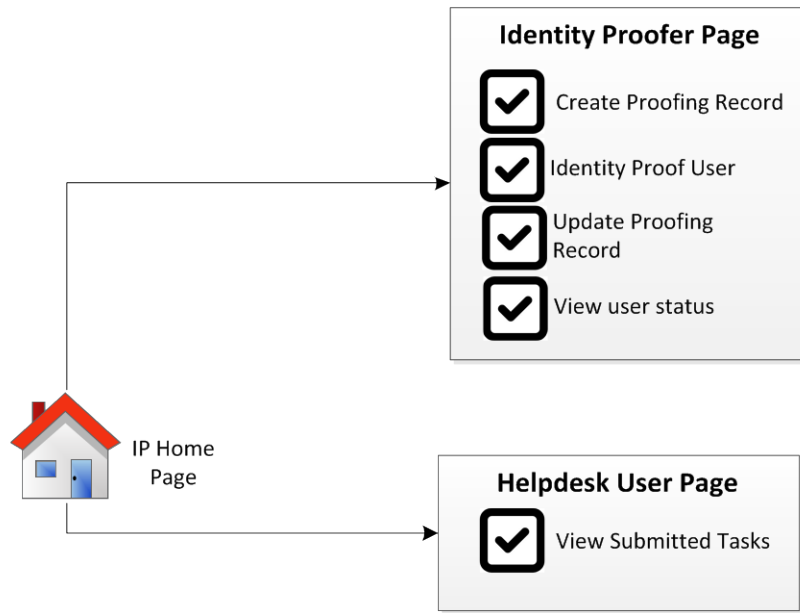


Figure 133: IP Navigation Hierarchy

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.

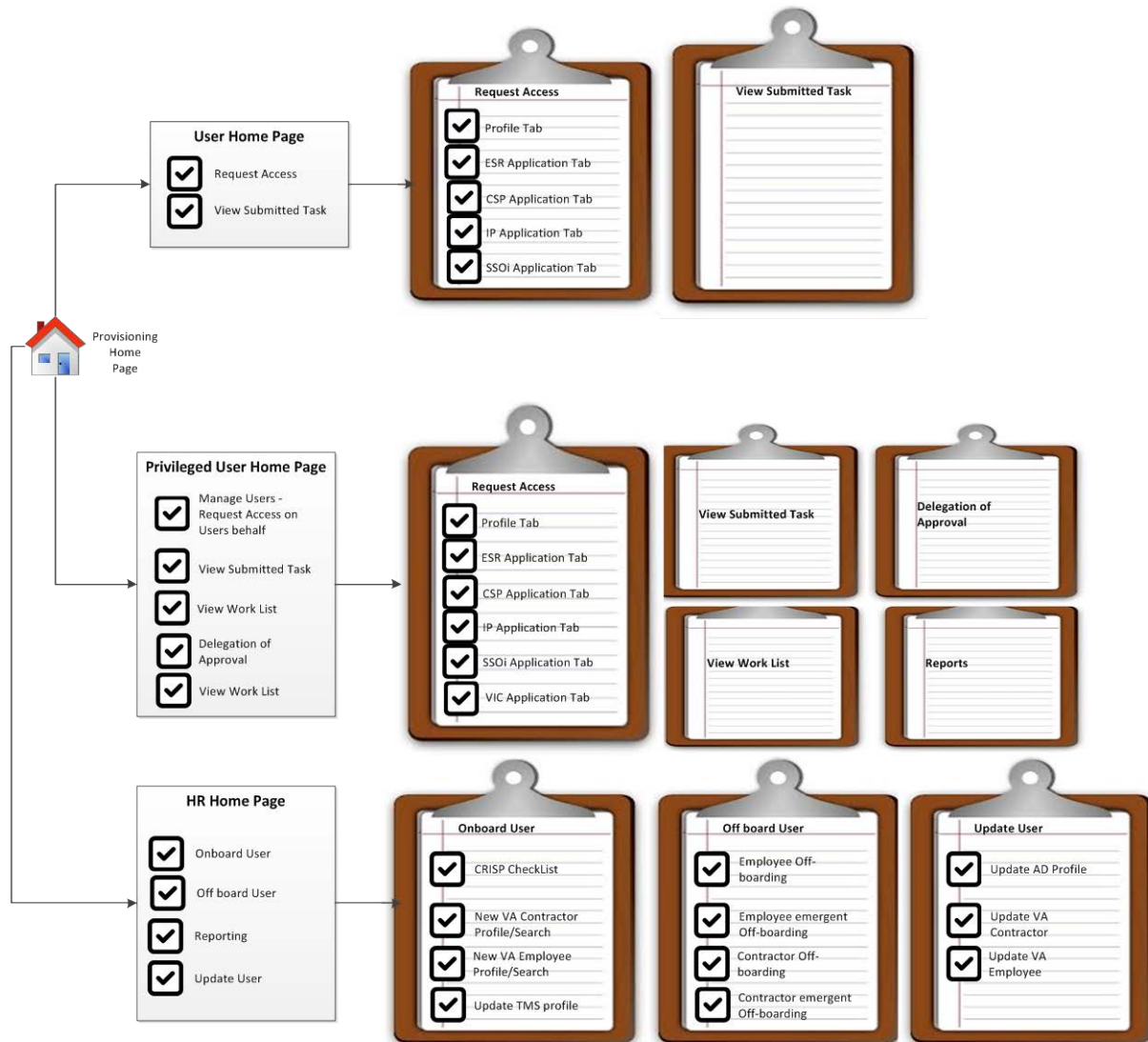


Figure 134: Provisioning Navigation Hierarchy

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 [REDACTED] 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 that meet FIPS requirement. CA IdentityMinder uses the Advanced Encryption Standard (AES) adapted by the US Government. CA IdentityMinder incorporates the RSA Crypto-J v3.5 and Crypt-C ME v2.0 cryptographic libraries, which have been validated as meeting the FIPS 140-2 Security Requirements for Cryptographic Modules. CA SiteMinder Policy Server uses certified FIPS140-2 (AES) compliant cryptographic libraries.

CA UARM uses its own trusted root certificate, which is incorporated across agent and component communications. For [REDACTED] 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 [REDACTED] environment, certificates issued by VA Internal CA will be used for securing communications between the [REDACTED] 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 [REDACTED] solution. The FIPS 140-2 encryption is applied on the identified PII and sensitive attributes stored in the [REDACTED] 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 and IP solutions do not allow duplicate identification values. Users are required to confirm their accounts by following instructions emailed to them. Therefore, the CSP and IP users have their e-mail addresses verified prior to getting a Level 1 or Level 2 credential. The CSP and IP components have appropriate roles established to address each facet of the associated business processes. These roles clearly provide separation of duties. Additionally, due to full auditing of transactions, any misuse of authority is discernible and traceable in the audit logs and reports.

9.2 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 hardware failover capability available within the CoSign product configuration. The DR environment hosts

a similarly configured setup as the primary Production site. For detailed site-to-site replication setup, refer to section 6.2.8 eSig Design.

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  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. It also provides 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  services.

10 Approval Signatures

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

Signed: _____



Integrated Project Team Chair and Business Sponsor

Date

Signed: _____



OIS Business Sponsor

Date

Signed: _____



IAM Program Manager

Date

Signed: _____



Program Manager

Date

Signed: _____



Chief Architect

Date

Signed: _____



Enterprise Architecture

Date

Signed: _____



SDE

Date

Appendix 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:



A.2. CRISP Onboarding/Offboarding Attributes

The following list provides the required/optional attributes for employees/contractors/Health Profession trainees/Volunteers:



A.3. RTM

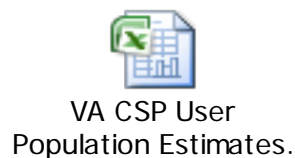
Refer to section 1.4 for a complete list of requirements documents that are applicable to the ■ solution.

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.



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.

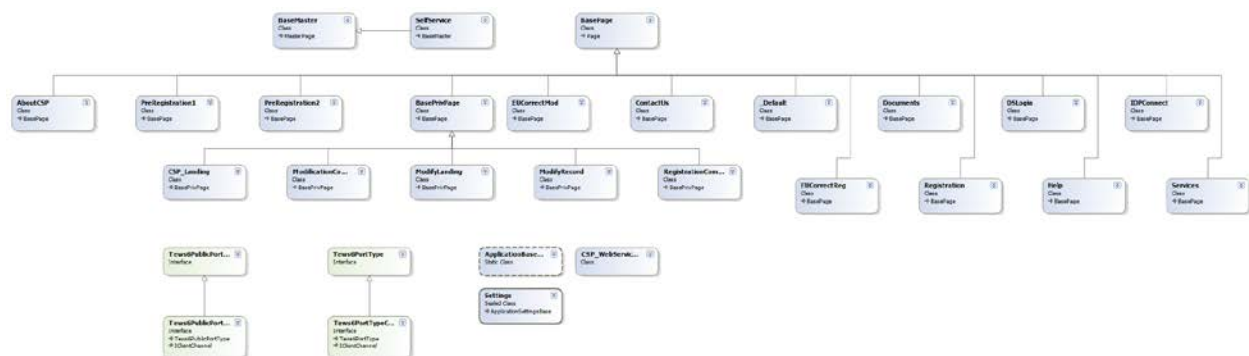


Figure 135: CSP Class Diagram

A.9. IP Class Diagram

The IP.NET wrapper class diagram is shown below.

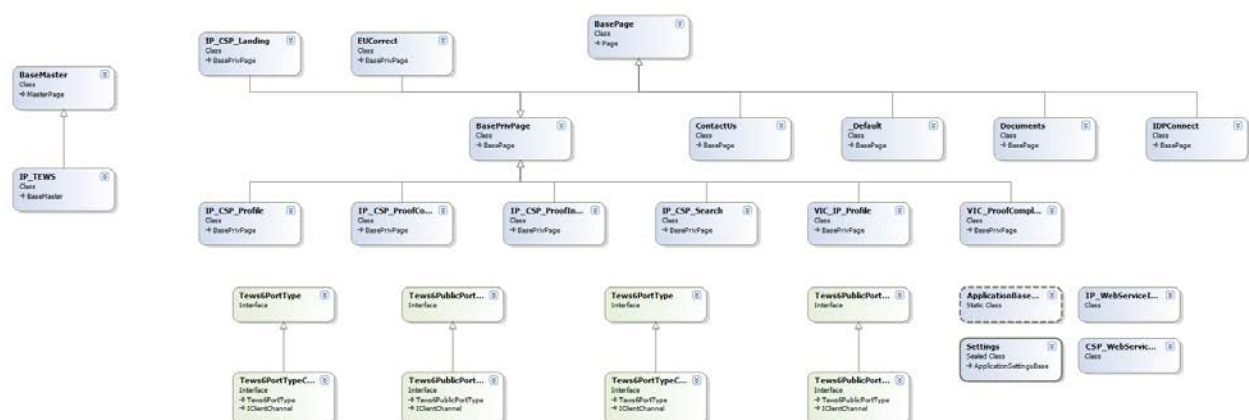


Figure 136: IP Class Diagram

A.10. Responses to Produce WS-Security Headers

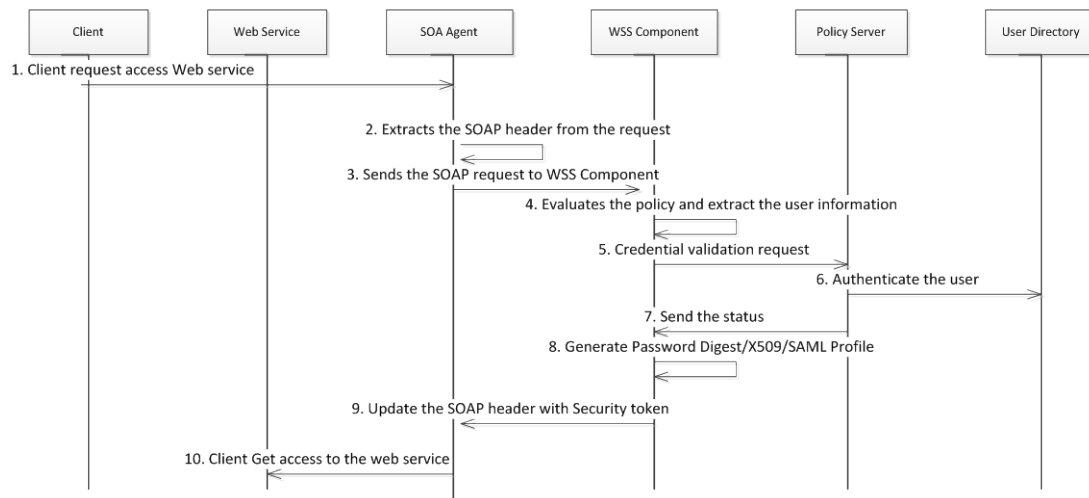


Figure 137: Responses to Produce WS Security Headers Sequence Diagram

Table 69: 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	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	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. Alternate Flow 1. Client sends WS SOAP request to web service end point

Field	Description
	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.
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

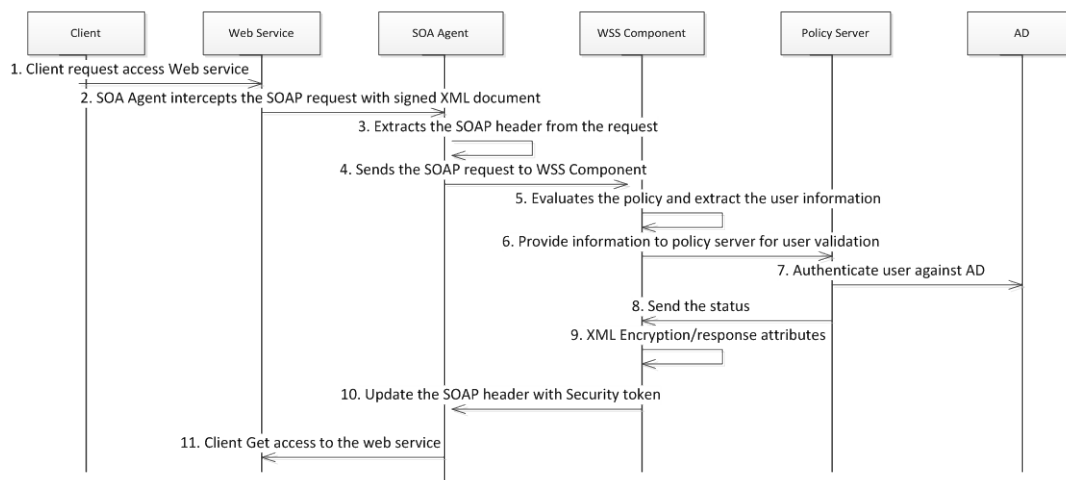


Figure 138: Responses to XML Encryptions, Decryptions and Digital Signature Sequence Diagram

Table 70: 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	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	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

Field	Description
	<ol style="list-style-type: none"> 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
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