

Department of Veterans Affairs

Identity and Access Management Access Services Solution Increment 2

System Design Document



December 2013

Version 2.1

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
1/31/2014	2.1	Re-formatted to coincide with the ProPath SDD template and made some text edits. Added email approval signatures to PDF version to post on the AcS TSPR.	NAME REDACTED
12/18/2013	2.1	Minor update to BRD reference after Formal Review	NAME REDACTED
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	NAME REDACTED
09/12/2013	1.9	Design elements to address RSD 2.0	NAME REDACTED
07/02/2013	1.8	Updates from peer review feedback.	NAME REDACTED
06/24/2013	1.7	Updates from peer review feedback.	NAME 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	NAME REDACTED
05/25/2013	1.5	Baselined for Increment 4	NAME REDACTED
02/11/2013	1.4	Updates to VIP and VM tables, additional diagram updates, and additional technical clarifications following formal review	NAME REDACTED
01/14/2012	1.3	Additional Updates from consolidated peer review feedback. Updated diagrams, tables and text to reflect REDACTED environments; added technical clarifications.	NAME REDACTED
12/12/2012	1.2	Updates from peer review feedback. Modification of location from AITC to REDACTED and Modification of patch levels.	NAME 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	NAME REDACTED
05/11/2012	1.0	Final- Addressed WP R comments.	NAME REDACTED
04/20/2012	0.1	Initial Draft	NAME 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	6
1.6. Constraining Policies, Directives and Procedures.....	6
1.7. Constraints	8
1.8. Design Trade-offs	10
1.9. User Characteristics.....	10
1.10. User Problem Statement.....	10
2. Background	10
2.1. Overview of the System	11
2.2. Overview of the Business Process	11
2.3. Assumptions.....	11
2.4. Legacy System Retirement.....	14
3. Conceptual Design.....	14
3.1. Conceptual Application Design.....	14
3.1.1. Application Context.....	14
3.1.2. High-Level Application Design	24
3.1.3. Application Locations	26
3.1.4. Application Users	28
3.2. Conceptual Data Design	29
3.2.1. Project Conceptual Data Model	29
3.2.2. Database Information	32
3.2.3. User Interface Data Mapping	33
3.3. Conceptual Infrastructure Design.....	56
3.3.1. System Criticality and High Availability.....	56
3.3.2. Special Technology	57
3.3.3. Technology Locations.....	57
3.3.4. Conceptual Infrastructure Diagram.....	57
4. System Architecture	60
4.1. Hardware Architecture	61
4.2. Software Architecture	69
4.3. Communications Architecture	83
4.4. Communication Channel Security	85

4.5.	AcS Inter-component Communications	85
4.5.1.	Production Server PKI Certificate List	95
5.	Data Design	102
5.1.	DBMS Files.....	102
5.2.	Non-DBMS Files.....	103
6.	Detailed Design	103
6.1.	Hardware Detailed Design	103
6.2.	Software Detailed Design	103
6.2.1.	Provisioning Conceptual Design.....	103
6.2.2.	SSOi Conceptual Design.....	113
6.2.3.	CSP Conceptual Design	140
6.2.4.	IP Conceptual Design	146
6.2.5.	SAC Conceptual Design.....	151
6.2.6.	eSig	157
6.2.7.	CAR	161
6.2.8.	Specific Requirements	166
6.3.	Communications Detailed Design.....	166
7.	External Interface Design	166
7.1.	Interface Architecture	166
7.1.1.	Federation with VAAFI.....	166
7.1.2.	Master Veteran Index.....	167

7.1.3. VA Active Directory	168
7.2. Interface Detailed Design.....	169
7.2.1. Federation with VAAFI.....	169
7.2.2. Master Veteran Index.....	169
8. Human-Machine Interface	169
8.1. Interface Design Rules.....	170
8.2. Inputs.....	170
8.3. Outputs.....	170
8.4. Navigation Hierarchy.....	170
8.4.1. CSP	170
8.4.2. IP	171
8.4.3. Provisioning	172
9. System Integrity Controls	173
9.1. CSP and IP	175
9.1.1. Confidentiality of Sensitive Information	175
9.1.2. Privacy of Personal Information	175
9.1.3. Process Integrity.....	176

9.2. eSig.....	176
9.2.1. Confidentiality of Sensitive Information	176
9.2.2. Privacy of Personal Information	176
9.2.3. Process Integrity.....	176
9.2.4. System Availability	176
9.3. SAC.....	176
9.3.1. Confidentiality of Sensitive Information	177
9.3.2. Privacy of Personal Information	177
9.3.3. Process Integrity.....	177
9.3.4. System Availability	177
9.4. Provisioning.....	177
9.4.1. Confidentiality of Sensitive Information	177
9.4.2. Privacy of Personal Information	177
9.4.3. Process Integrity.....	178
9.4.4. System Availability	178
9.5. SSOi.....	178
9.5.1. Confidentiality of Sensitive Information	178
9.5.2. Privacy of Personal Information	178
9.5.3. Process Integrity.....	178
9.5.4. System Availability	178
9.6. CAR.....	179
9.6.1. Confidentiality of Sensitive Information	179
9.6.2. Privacy of Personal Information	179
9.6.3. Process Integrity.....	179
9.6.4. System Availability	179
10. Approval Signatures	181
A. Additional Information.....	182
A.1. Data Dictionary	182
A.2. RTM.....	182
A.3. Packaging and Installation	182
A.4. Design Metrics	182
A.5. Acronym List and Glossary.....	182
A.6. Required Technical Documents	184
A.7. CSP Class Diagram	185
A.8. IP Class Diagram	185

List of Figures

Figure 1: AcS Solution Overview	15
---------------------------------------	----

Figure 2: CSP Context Diagram	16
Figure 3: IP Context Diagram	18
Figure 4: eSig Context Diagram	19
Figure 5: SAC Context Diagram	20
Figure 6: PROV Context Diagram	21
Figure 7: SSOi Context Diagram	22
Figure 8: CAR Context Diagram.....	24
Figure 9: AcS Solution Application Design	25
Figure 10: AcS Solution Conceptual Data Mode	30
Figure 11: New VA Employee/Contractor Profile Screen.....	34
Figure 12: New VA Employee/Contractor Profile Work Home Screen.....	35
Figure 13: New VA Employee/Contractor Profile Org Screen	36
Figure 14: New VA Employee/Contractor Screen Profile Misc. Screen.....	37
Figure 15: CRISP Checklist Screen	38
Figure 16: Modify Account: Step 1 User Profile	39
Figure 17: Modify Account: Step 2 Security Questions.....	40
Figure 18: Change Password	41
Figure 19: Upgrade to Level 2: Step 1 User Profile	42
Figure 20: Upgrade to Level 2: Step 2 Security Questions.....	43
Figure 21: Self-Registration: Step 1 User Profile	44
Figure 22: Self-Registration: Step 2 Security Questions	45
Figure 23: Identity Proof User: Step 1 User Profile	46
Figure 24: Identity Proof User: Step 2 Address Verification	47
Figure 25: Identity Proof User: Step 3 Primary Verification	47
Figure 26: Identity Proof User: Step 4 Secondary Identification.....	48
Figure 27: Update a User: Step 1 User Profile	49
Figure 28: Update a User: Step 2 Address Verification	50
Figure 29: Update a User: Step 3 Primary Identification.....	51
Figure 30: Update a User: Step 4 Secondary Identification.....	51
Figure 31: SSOi Centralized Login Page	52
Figure 32: SSOi PIV Only Login Page.....	53
Figure 33: Mobile Login Page	54
Figure 34: SAC PAP Landing Page.....	55
Figure 35: SAC PAP Landing Page.....	56
Figure 36: AcS Production Environments	58
Figure 37: Logical Network String Diagram.....	60
Figure 38: Network Communication Architecture	61

Figure 39: Software Architecture	70
Figure 40: AcS Network Security Topology	84
Figure 41: Provisioning Detail Design	104
Figure 42: SSOi Detailed Design	114
Figure 43: CSP Detailed Design	141
Figure 44: IP Conceptual Design	147
Figure 45: SAC Conceptual Design	151
Figure 46: eSig Conceptual Design	158
Figure 47: CAR Conceptual Design	162
Figure 48: CSP to VAAFI Interface Flow	167
Figure 49: MVI Interface Flow with Provisioning and IP	168
Figure 50: Provisioning – Active Directory Interface Architecture	169
Figure 51: CSP Navigation Hierarchy	171
Figure 52: IP Navigation Hierarchy	172
Figure 53: Provisioning Navigation Hierarchy	173
Figure 54: CSP Class Diagram	185
Figure 55: IP Class Diagram	185

List of Tables

Table 1: System Identification	2
Table 2: Scope Inclusions	3
Table 3: Scope Exclusion	4
Table 4: Project Documents	5
Table 5: Policies, Directives, and Procedures	6
Table 6: Assumptions and Constraints	11
Table 7: CSP Application Context Description	17
Table 8: IP Application Context Description	18
Table 9: eSig Application Context Description	19
Table 10: SAC Application Context Description	20
Table 11: PROV Application Context Description	21
Table 12: SSOi Application Context Description	23
Table 13: Activities in the High-Level Application Design	25
Table 14: AcS Solution Application Locations	26
Table 15: AcS Solution Users	28
Table 16: Database Inventory	30
Table 17: Database Inventory	32
Table 18: Special Technology Requirements	57
Table 19: Hardware Appliance	61

Table 20: Virtual Machines and Appliances.....	62
Table 21: AcS Products and Versions.....	71
Table 22: Software Components.....	72
Table 23: Programming Languages.....	82
Table 24: Operating Systems	83
Table 25: Port Communications and Protocols.....	85
Table 26: Pre-Production PKI Certificate List	90
Table 27: Production Cert List	95
Table 28: Database File System	102
Table 29: Potential Impact Categories for Authentication Errors	147
Table 30: AcS Solution Products	164
Table 31: Data Points and Security.....	174
Table 32: Data Type and Updates	175
Table 33: Glossary	182

1. Introduction

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

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

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

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

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

1.1. Purpose of this document

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

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

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

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

1.2. Identification

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

Table 1: System Identification

Name	Description	Abbreviation	Version	Release
VA AcS Solution	Core set of activities to definitively and consistently identify VA stakeholders and to establish supporting processes that provide the appropriate level of security required to protect and manage the identities, information, and interests of the VA stakeholders	AcS	V 3.0.0	Release 1 (Increment 2)

1.3. Scope

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

Table 2: Scope Inclusions

Includes
SSOi: <ul style="list-style-type: none">• Provides authentication and authorization support for VA internal facing applications• Accepts federated credentials 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 support for LOA 4 credentials• Provides global log off for integrated applications/services
CSP: <ul style="list-style-type: none">• Issues Level of Assurance (LOA) 1 and LOA 2 credentials to VA persons of interest• Federates the CSP/IP solution with VA Authentication Federation Infrastructure (VAAFI) using Security Assertion Markup Language (SAML) 2.0• Integrates with the Master Veteran Index (MVI)
eSig: <ul style="list-style-type: none">• Provides capability to electronically sign and verify documents using web service based task• Provides support for documents types –Word, Excel, PDF and web based email• Provides eSig enrollment services to allow the eligible external users for VA internal applications to sign the document. eSig is limited to external persons of interest, Veterans or non-Veterans that do not have credentials that carry signing certificates (hard token or soft token)• Provides functionality to delete user access
IP: <ul style="list-style-type: none">• Provides web service based tasks and GUIs for Identity Proofer to perform the IP process for a person of interest• Integrates with the Master Veteran Index (MVI)
PROV: <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

Includes
<p>and self-service based applications for both the internal and external user populations, such as AccessVA</p> <ul style="list-style-type: none"> • 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
SAC:
<ul style="list-style-type: none"> • Provides a Policy Decision Point (PDP) and Policy Administration Point (PAP) according to the OASIS eXtensible Access Control Markup Language (XACML) 3.0 standard • Provides available Software Development Kits (SDKs) for VA applications to perform Policy Enforcement Point (PEP) capabilities • Utilizes a virtual directory as the Policy Information Point (PIP)
CAR:
<ul style="list-style-type: none"> • Integrates with the AcS solution activities to provide the 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
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 party's 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

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
VA AcS FY14 Business Requirements Document: FY14 IAM Access Services BRD	Defines the “As Is” and “To Be” business area, operating environment, the system requirements and capabilities desired by stakeholders. Document provides performance and workload requirements along with availability requirements.
I2 Requirements Specification Document: VA AcS Solution RSD I2	Provides initial outline of the AcS solution requirements information for Increment 2.
I3 Requirements Specification Document: AcS Requirements Specification Document	Provides updated requirements information for AcS Solution Increment 3
I4 Requirements Specification Document: AcS Requirements Specification Document i4 V6	Provides updated requirements information for AcS Solution Increment 4
I3 Use Cases: VA AcS Solution Use Case Model i3_rev	Provides use cases for AcS solution
I4 Use Cases: VA AcS Solution UC Model i4 AC	Provides use cases for AcS solution
I3 Requirements Traceability Matrix: VA AcS Solution i3 RTM	Provides the requirements traceability matrix for the AcS solution
I4 Requirements Traceability Matrix: VA AcS Solution i4 RTM	Provides the requirements traceability matrix for the AcS solution
Identity Proofing Integration to the Master Veteran Index (MVI) Requirements Specification Document iRSD - Version 0.4 CSP IP MVI Integration RSD - 050513 Document Update.docx	IP integration to the MVI
Provisioning Security Identifier Integration to the Master Veteran Index (MVI) iRSD Version 0.16 MVI SEC ID RSD v0_16.docx	Provisioning SEC ID integration to MVI

1.5. Methodology, Tools, and Techniques

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

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

1.6. Constraining Policies, Directives and Procedures

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

Table 5: Policies, Directives, and Procedures

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA 6500 Handbook	<ul style="list-style-type: none">• Directive Information Security Program.• Defining overall Security Framework for VA.
2	VA	VA 6501 Directive	<ul style="list-style-type: none">• VA Identity Verification In Person Proofing (IPP) Process.• Defining overall Identity Proofing Methodology for VA IAM.
3	VA	VA 6300 Directive	<ul style="list-style-type: none">• Directive Records and Information Management.• Defines information management framework for VA Access Services.
4	NIST	SP 800-53-4	<ul style="list-style-type: none">• Special Publication - Recommended Security Controls for Federal Information Systems and Organizations.• Defines the required security controls for IT systems under the Federal Information Security Management Act (FISMA).
5	NIST	SP 800-63-2	<ul style="list-style-type: none">• Special Publication - Electronic Authentication Guideline.• Defines levels of assurance in user identities presented to IT systems over open networks.• Defines the data and procedural requirements for VA Access Services.
6	NIST	FIPS-201-2	<ul style="list-style-type: none">• Federal Information Processing Standards Publication - PIV of Federal Employees and Contractors.• Provides Identity Proofing, credentialing and chain of trust requirements and processes.• Defines the method for secure administrative interaction and control.
7	NIST	FIPS-140-2	<ul style="list-style-type: none">• Federal Information Processing Standards Publication (FIPS) - Security Requirements for Cryptographic Modules.• Defines the cryptographic standards and requirements.

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

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
18	VA	VA D 0735	<ul style="list-style-type: none"> Homeland Security Presidential Directive 12 (HSPD-12) Program Defines Department-wide policy, roles, and responsibilities for the creation and maintenance of systems and processes to implement VA's HSPD-12 Program necessary to implement Homeland Security Presidential Directive 12 (HSPD-12) program.
19	OMB	M-05-24	<ul style="list-style-type: none"> Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

1.7. Constraints

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

- **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 Licensing:** The deployment of Radiant Logic is limited to a specific number of processor cores specific to a given environment. The VA has purchased three (3) production licenses and two (2) development/test licenses. This allocation constrains the deployment to two (2) production, one (1) pre-production, one (1) SQA, One (1) development. There are no Disaster Recovery (DR) environment or tier licenses.
- **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).
- **CA Single Sign-On:** Must be configured to run in FIPS only mode. Product must be configured to run in FIPS only mode in order to satisfy FIPS140-2 requirements.
- **DataPower XML Security Gateway:** Appliance must be operated on FIPS 140-2 compliant hardware with embedded hardware security modules (HSM).
- **JRockit JRE:** Product may only be installed on machines running accepted WebLogic technologies. The use of different vendor JREs may create portability and configuration issues.
- **Oracle Database:** Known security vulnerabilities must be properly remediated prior to product deployment. Product must remain properly patched per Federal and Department standards in order to mitigate known and future security vulnerabilities. Per VA

Handbook 6500 (Appendix F) systems with a Moderate or High risk assessment are required to use a FIPS 140-2 compliant DBMS solution to protect information at rest or have mitigating controls documented in an approved System Security Plan (SSP) for the system. It is the responsibility of the system owner to determine that an appropriate DBMS technology is selected or that mitigating controls are in place and documented in the SSP. Additionally, if PII/PHI/VA sensitive information is involved, FIPS 140-2 certified encryption must be used to encrypt data in transit and the technology must be implemented within the VA production network (not in a DMZ) or additional mitigating controls must be documented in an accepted System Security Plan (SSP).

- **Oracle Database:** The 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.
- **Operating Systems:** AcS must use VA-approved operating systems.
- **ARX CoSign:** CoSign does not support access control lists. Access Control is required at the interface layer.
- **ARX CoSign:** CoSign does not support federation. All 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.
- **ARX CoSign:** CoSign does not support signing of Web Forms.
- **CA IdentityMinder:** CA IdentityMinder's connector Xpress cannot update certain attributes – record created by, record created date, record modified by, and record modified date in to membership mapping tables. This type of functionality would require a custom connector outside of the Connector Xpress and would therefore be proprietary.
- **Unique Identifiers:** The AcS solution has multiple types of identifiers, but has required the use of a Security Identifier that can uniquely identify a person with their many other credentials. The SECID will be used by AcS to build and link Identity records with system accounts and user information.
- **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 system.
- **CA SiteMinder:** 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).

1.8. Design Trade-offs

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

- The user and policy store will have read-intensive operations. Based on the projected usage demands, the policy store and user store should be created in their own CA Directory Servers instances. Alternatively, if the stores are consolidated to single servers that have a failover topology, the system could realize performance degradation between the read and write transactions. Additionally, if the read intensive operations are occurring in the same place where the data is being written then it is likely that data mismatch may occur at time of the reading transaction.
- Since CAR, SAC, eSig, and SSOi administrative UI does not support direct PIV authentication, as an alternative, the administration console links may be provided in the CA Single Sign-On system and rely on the Desktop PIV login. However, a username and password will still be required for the administration consoles.

1.9. User Characteristics

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

1.10. User Problem Statement

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

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

2. Background

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

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

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

2.1. Overview of the System

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

2.2. Overview of the Business Process

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

2.3. Assumptions

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

Table 6: Assumptions and Constraints

Assumptions and Constraints	
SSOi	<ul style="list-style-type: none"> The CA SSO client will be packaged and deployed on the end user workstation. The SSOi client must be deployed, tested and certified for use on desktop deployment images prior to operationalizing the solution. SSOi Activity OOTB standard reporting will be provided for applications integrated with CA SiteMinder and CA SSO toolset using CAR Activity. LOA 4 "Holder Of the Key" functionality is not supported with a Federated SAML profile. The Identity Provider (IdP), Service Provider (SP) and STS (Security Token Store) capabilities will be developed using AcS available product capabilities. The SSOi Activity will use VA Active Directory (AD) as primary authentication store and thereby provide desktop SSO capability only to users in VA AD. SSOi will also leverage the attribute service provided by the Radiant Logic virtual directory to retrieve attributes about an authenticated user. SSOi administrator interface, similar to SiteMinder Admin UI, does not support PIV

Assumptions and Constraints

	<p>authentication due to the COTS product limitation; therefore, PIV Authentication capability will not be enabled for the SiteMinder or CA SSO Administrator Interface.</p> <ul style="list-style-type: none"> • SiteMinder has limited capability on providing STS service (i.e. SiteMinder does not provide a web service interface for the token conversion). • 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 all 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 Appendix 10.3). • 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. • 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 CoSign. • 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

Assumptions and Constraints

	<p>authentication.</p> <ul style="list-style-type: none"> The eSig solution does not provide ability to sign the web forms due to product limitation. Horizontal scaling to increase capacity (number of users) is not a supported option for the eSig activity.
IP	<ul style="list-style-type: none"> VA will provide trained ID Proofer to perform the proofing process. They will follow approved VA policies and processes associated with the proofing process. Identity Proofing as a service will be used for choreographing IP functionality by providing the framework to establish an identity proofing task. The Identity Proofing activity supports LOA 2 Identity Proofing records. This capability is not a limitation in the activity, as the activity may support higher LOA proofing records. One or more Identity Proofing records may be associated with each VA enterprise identity record, allowing for versatile Identity information to be collected and used as part of user certification process.
PROV	<ul style="list-style-type: none"> Initial identity feed file provided by VA AD or other VA authoritative store will be structured in a previously and mutually agreed upon format for bulk loading (one time) the VA internal users into the Provisioning user store. The Provisioning Activity enforces separation of duties (SOD), based upon VA predefined parameters, through identity policy and execution of business rules, but does not provide 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 AcS will be through the use of the Identity Attribute SEC_ID.
SAC	<ul style="list-style-type: none"> The provisioning user store is currently the only 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.

Assumptions and Constraints

CAR	<ul style="list-style-type: none">• UARM does not store actual authoritative audit logs so it does not have the capability, nor is it intended, to protect the integrity of the authoritative audit data.• UARM does not support direct connections to a user store for collecting statical information.• UARM currently in its end of life. Any future enhancement will be limited with this product• UARM does not support PIV authentication. Since it is a flash based application it also cannot integrated with CA SSO
Infrastructure	<ul style="list-style-type: none">• This design assumes that Citrix Netscape Global Traffic Manager (GTM) module will be available at the time of production implementation.• Virtual machines used for the VA AcS infrastructure will be integrated in the appropriate VA Active Directory domain for each environment.• The AcS solution is designed to have 99.9% availability, and can be failed over to the Disaster Recovery site. However, this is contingent on the availability of other components outside of the AcS solution such as VAAFI and REDACTED 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 AcS infrastructure will be integrated in the appropriate VA Active Directory domain for each environment.

2.4. Legacy System Retirement

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

3. Conceptual Design

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

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

3.1. Conceptual Application Design

This section provides the conceptual design of the AcS solution.

3.1.1. Application Context

This section provides context for each of the activities developed for VA AcS solution. The aim of AcS solution is to deploy a cohesive and consistent foundational AcS architecture which is flexible, modular, extensible, and scalable in VA's infrastructure. VA AcS foundation

infrastructure enables internal users, external users and VA business partners to access various AcS activities such as:

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

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

Figure 1: AcS Solution Overview

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

3.1.1.1. Credential Service Provider

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

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

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

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

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

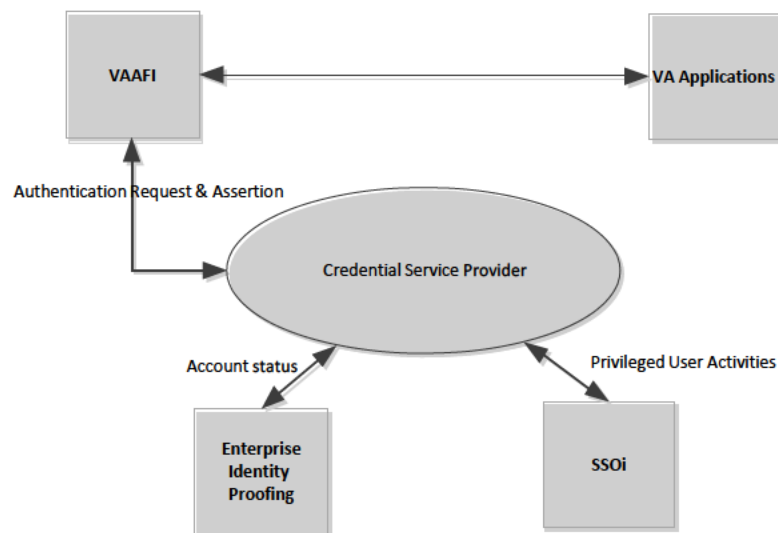


Figure 2: CSP Context Diagram

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

Table 7: CSP Application Context Description

ID	Interface Name	Input Messages	Output Messages	External Party
1	VAAFI	Authentication Request	Authentication Assertion, SAML 2.0	NA
2	Identity Proofing	HTTPS	HTTPS	VIC
3	Business Applications	SOAP over HTTP/HTTPS	SOAP over HTTP/HTTPS	Business Applications
4	Single Sign-On	Kerberos/SPNEGO	Kerberos/SPNEGO	SSOi

3.1.1.2. Identity Proofing

Identity Proofing (IP) is used to verify a user's identity in order to establish a level of assurance of the claim that the user is indeed who they represent themselves to be before the Identity Proofing official. The Identity Proofing processes are used for establishing the validity of a claim for authorization to VA applications, resources or benefits. The IP component capabilities allow for multitude of identity proofing processes to be defined as business needs dictate and be built to suit a specific purpose.

The IP process that is being implemented 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.

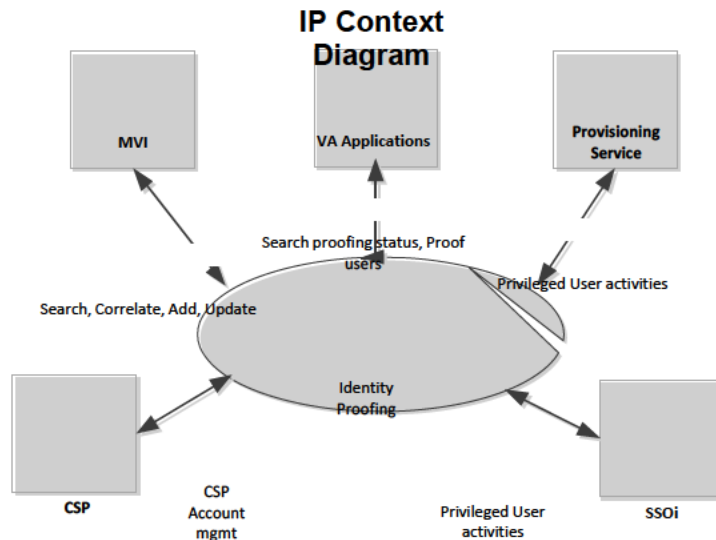


Figure 3: IP Context Diagram

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	SOAP over HTTPs	SOAP over HTTPs	Veteran
2	Business Applications	SOAP over HTTPs	SOAP over HTTPs	Business Applications
3	MVI record interface	SOAP over HTTP	SOAP over HTTP	MVI
4	SSOi	Kerberos/SPNEGO	Kerberos/SPNEGO	SSOi

3.1.1.3. Digital Signature

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

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

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

to perform the lifecycle management for the eSig identities

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

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

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

Figure 4: eSig Context Diagram

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

Table 9: eSig Application Context Description

ID	Interface Name	Input Messages	Output Messages	External Party
1	eSig Application	VA Integrated Applications	Document to be signed	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 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.

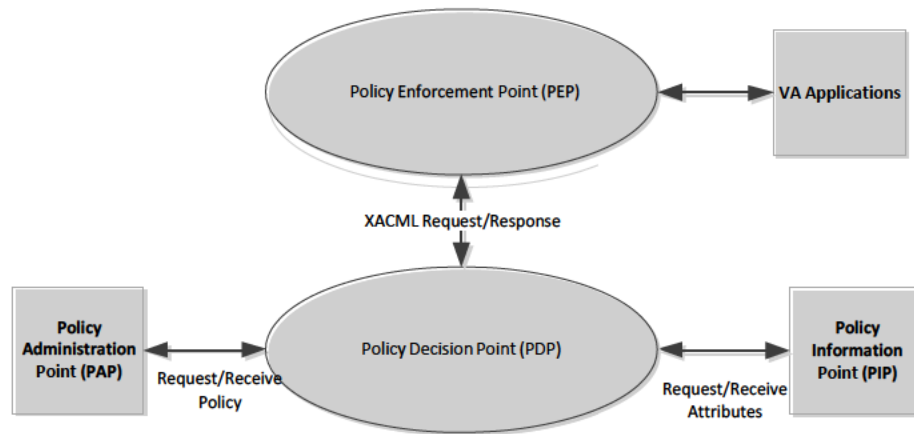


Figure 5: SAC Context Diagram

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	IAM PDP	XACML <Requess> sent via a SOAP envelop over HTTP(s)	Authorization Decision Response via a SOAP envelop over HTTP(s)
2	CRL	Certificate Authority (CA)	Certificate over HTTP(s)	Certificate status of 'good', 'revoked', or 'unknown'

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.

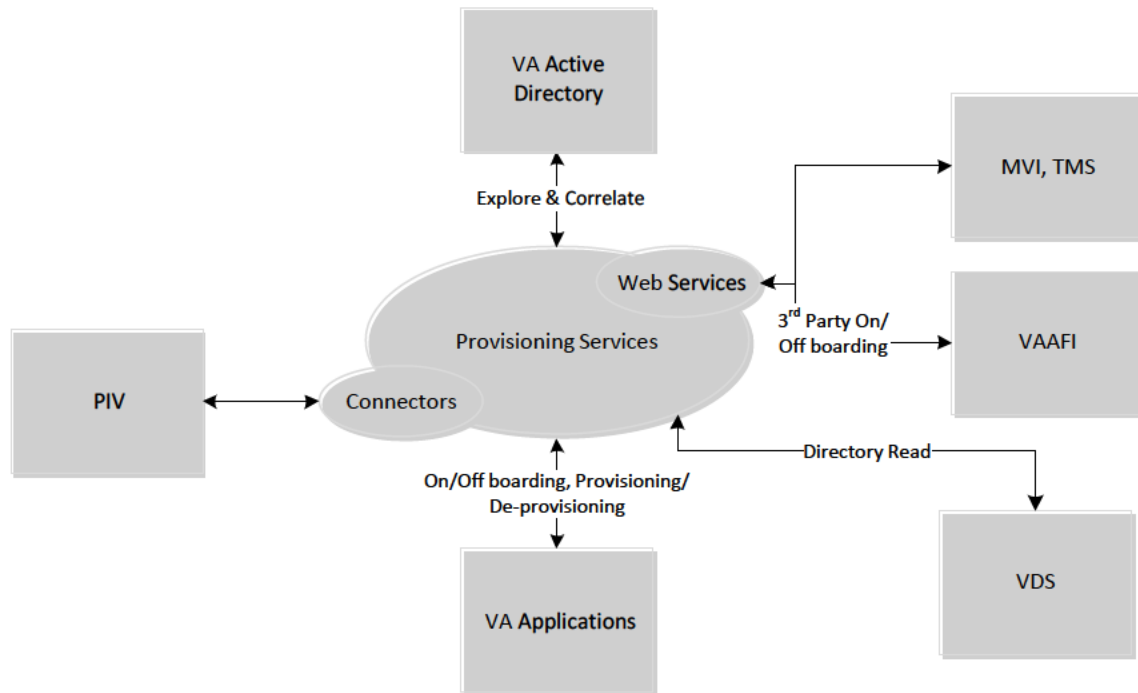


Figure 6: PROV Context Diagram

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)	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 and also as user profile data source.
2	VA Application (Web-based Front-End)	Provisioning Service	HTTP/HTTPS JDBC JNDI SOAP over HTTPS	HTTP/HTTPS JDBC JNDI SOAP over HTTPS	VA Applications consume the Provisioning Service using connectors (JNDI or JDBC calls) or through web services exposed as tasks for the Provisioning Service such Create User Task and Modify User Task.

3.1.1.6. 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 is both external and internal facing. VA users and applications. This service provides the capability to enhance the user experience by reducing time associated with multiple log-on/log-off activities, enriched password management, and reduction in help desk support. The SSOi service is client based service which allows internal VA users such as employees, contractors and partners within VA network to log on to integrated applications. The SSOi service connects to VA AD to validate user's credentials from desktop session or Kerberos token, uses Federation to support external cloud providers and accept users from SSOe while also utilizing HSPD-12 trust services to authenticate internal VA PIV users.

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

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

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

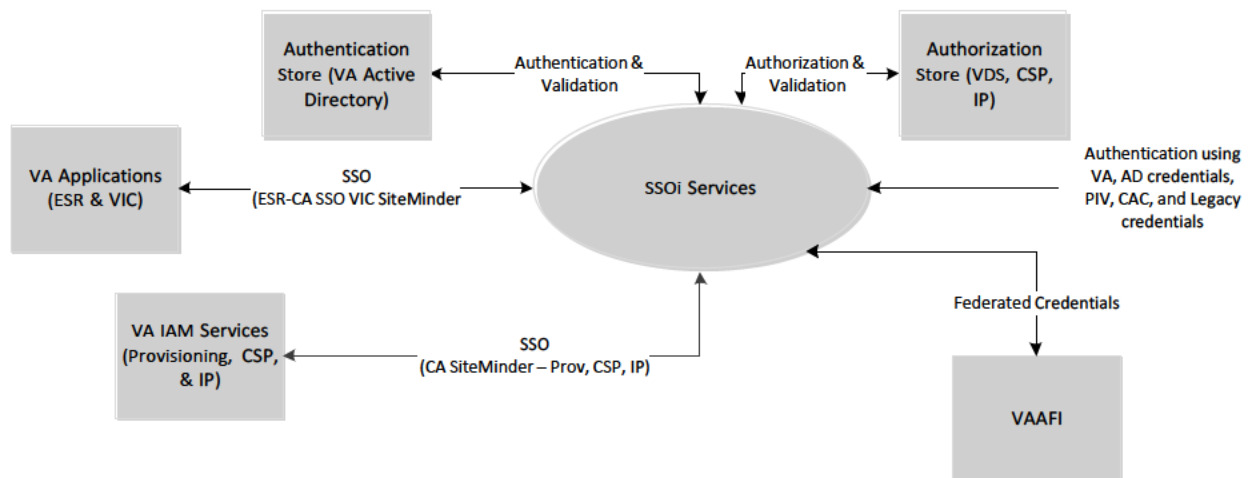


Figure 7: SSOi Context Diagram

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 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 Service	LDAP queries	LDAP response / search results	LDAP Interface. VA VDS is queried by SSOi Service to obtain VA internal/external user information and also provide attribute authorization. IAM (CA SiteMinder) uses the LDAP protocol to communicate with VDS. VDS is leveraged primarily to authorizing VA users.
3	CSP and IP Directory Service	SSOi 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.
3	SSOi Application	SSOi Service	HTTP/HTTPS	HTTP/HTTPS	All the SSOi hosted application like centralized logon pages are consumed by SSOi integrated applications
4	VA Applications	SSOi Service	HTTP/HTTPS	HTTP/HTTPS	VA application like ESR and VIC use the CA SSO desktop native connection methods to seamlessly log in users in to their web applications.

3.1.1.7. Compliance Audit and Reporting

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

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

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

Figure 8: CAR Context Diagram

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

3.1.2. High-Level Application Design

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

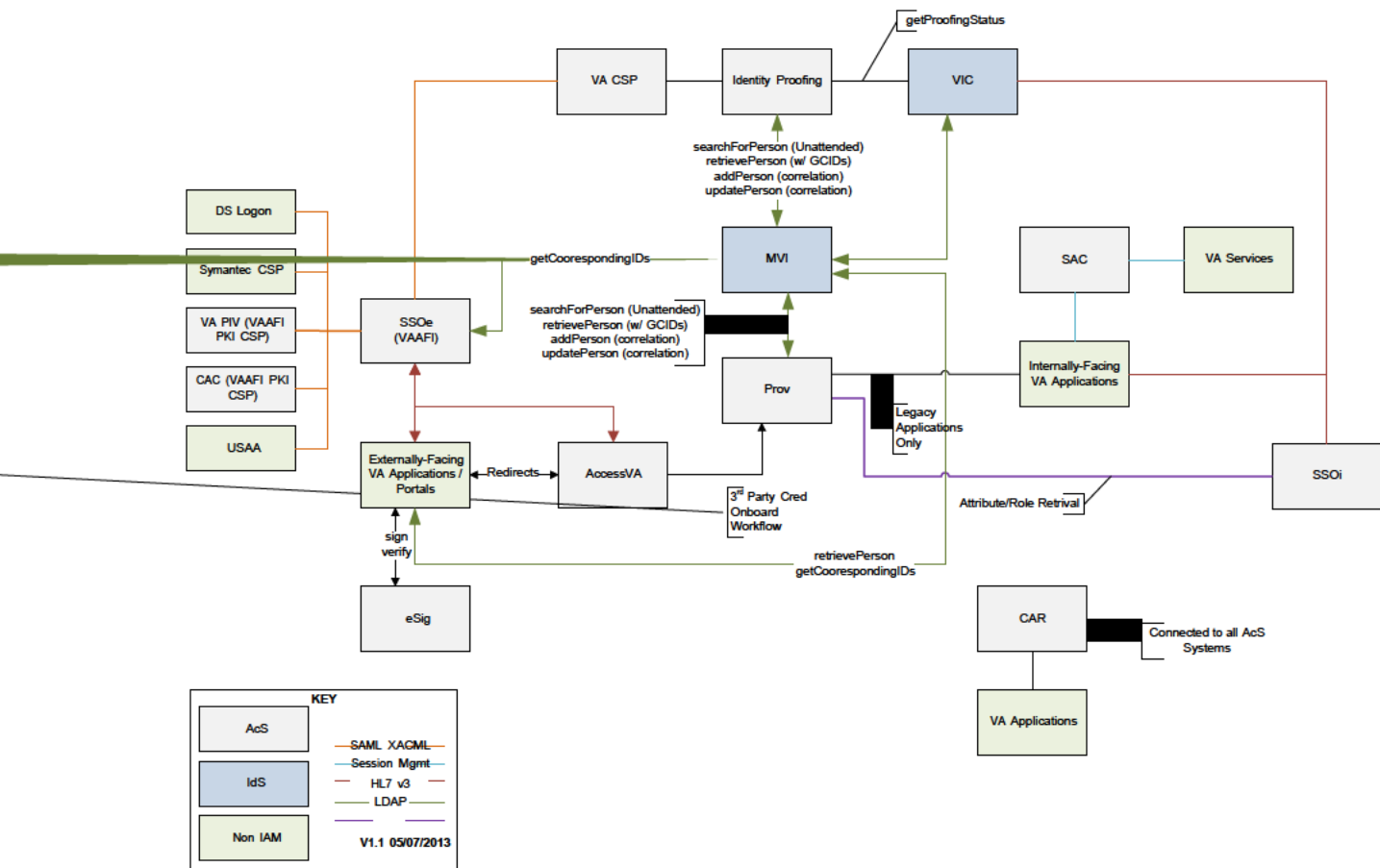


Figure 9: AcS Solution Application Design

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

Table 13: Activities in the High-Level Application Design

ID	Name	Description	Service or Legacy Code	External Interface Name	Internal Interface Name
1	CSP	CSP provides external user's credentials to VA applications that are not eligible for another VA approved credential.	Service	Self Service and Registration	VAAFI, IP, CAR
2	IP	IP facilitates evaluating and validating a user's identity to be true and unique to the degree (level) of confidence required by VA.	Service	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
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 parted 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 14: AcS Solution Application Locations

Application Component	Description	Location at Which Component is Run
IIS Web Server	Front end web server providing the administrative and self service interface to CA IdentityMinder	REDACTED
Servlet Exec	Application server for SiteMinder Federation option pack for CSP and SSOi partnerships with VAAFI.	REDACTED
Oracle Web Logic	Application server hosting CA IdentityMinder, Provisioning Server, SiteMinder and federation.	REDACTED

Application Component	Description	Location at Which Component is Run
Apache Tomcat	Application server hosting Axiomatics Services Manager, Policy Decision Point, and Policy Administration Point	REDACTED
CA IdentityMinder	COTS product for Provisioning and CSP.	REDACTED
CA SiteMinder	Is a set of features that provide Single Sign-On, session management, WS Security, Authentication and Authorization Policies, Policy Decision Point, and audit reporting for access controls.	REDACTED
CA Secure Proxy Server	Is a stand-alone server that provides a proxy-based solution for access control.	REDACTED
CA SSO Server	CA desktop single sign-on solution for legacy applications.	REDACTED
CA Directory	LDAP directory to support CA SiteMinder, CA SSO and CA IdentityMinder backend configuration and data store.	REDACTED
CA UARM	User Audit and Reporting Module.	REDACTED
Axiomatics ASM	COTS product for SAC	REDACTED
Axiomatics PAP	Policy Administration Point, an applications for managing policies used by the policy decision point (PDP).	REDACTED
Axiomatics PDP	Policy Decision point for fine-grained authorization decision requests.	REDACTED
Radiant Logic	COTS product for Data Virtualization. Can be used as a PIP and will be used to provide Attribute Services	REDACTED

Application Component	Description	Location at Which Component is Run
IBM DataPower	COTS XML Security Gateway	REDACTED
Oracle Database	Database to support CA IdentityMinder and audit logs from different components.	REDACTED
ARX CoSign Device	Stores the Key pair for the eSig Service.	REDACTED
Report Server	Report server for CA SiteMinder and CA IdentityMinder	REDACTED

3.1.4. Application Users

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

Table 15: AcS Solution Users

Application Component	Description	User
CSP	Performs administrative functions including controlling Identity Minder related configurations and tasks	CSP Administrator
	Responsible for managing the application and providing user lifecycle management functions including upgrading credentials, enabling/disabling accounts, and other administrative activities as needed	CSP Privileged User
	A user (Veteran, beneficiary, or other VA stakeholder) requesting or having a user credential of any level	End User
IP	Performs administrative functions including controlling Identity Minder related configurations and tasks and managing the proofing registration interfaces	IP Administrator
	Responsible for Identity Proofing users confirming identity of applicant to comply with SP 800-63 and VA 6501	Identity Proifiers
SAC	A user who attempts to access a protected VA application that subscribes to SAC activity for providing policy-based access control	End User
	Performs administrative functions including systems configuration, policy creation/updates, workflow management, etc.	SAC Administrator

Application Component	Description	User
eSig	Performs administrative functions including systems configuration, modifying user accounts, as well as performing and defining reporting and auditing functions	eSig Administrator
	A user who utilizes the eSig to electronically sign the approved document types; an eSig User is assumed to have an LOA of 2 or higher	End User
Provisioning	Performs administrative functions in Identity Minder including management of end users, workflows, connections to end points as well as configurations objects	Provisioning Administrator
	Responsible for registering, approving, and managing user provisioning and de-provisioning lifecycle	Provisioning Privileged User
	A user who uses provisioning to self-register, manage user profile, and check request status to gain access to integrated applications	End User
	A system that is authorized to use the provisioning web service functions for creating SECID and Add User.	Authorized Systems
SSOi	Performs administrative functions including management of SiteMinder, SSO and associated components	SSOi Administrator
	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
	Runs reports and tracks audit records to verify continual system conformance with security and policy	Auditor

3.2. Conceptual Data Design

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

3.2.1. Project Conceptual Data Model

This section describes the conceptual data model providing high-level representation of the data entities and relationships. The data objects within the AcS solution, how they are used, and how they relate to each other are provided in the figure below.

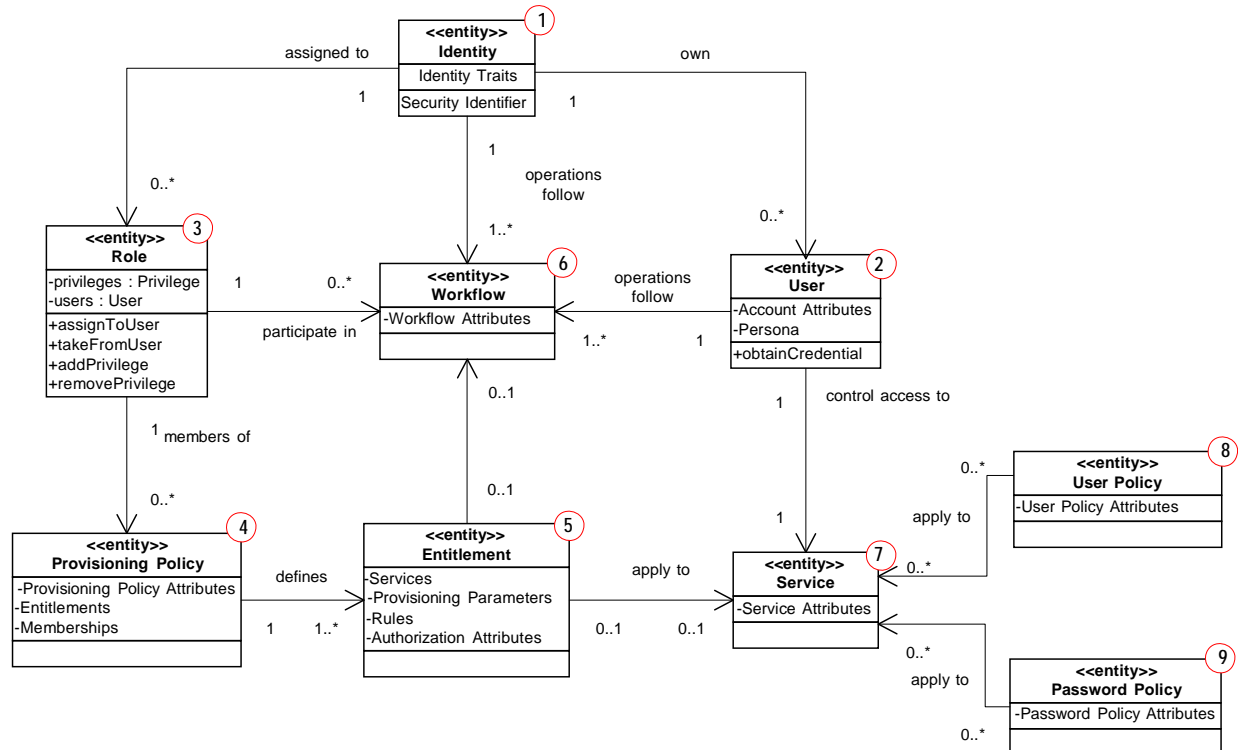


Figure 10: AcS Solution Conceptual Data Mode

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

Table 16: 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 coorelated and a secure identifier is assigned.	- 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) object is the set of parameters that define the login information associated with the	- One Account is owned by 0 or one Identity	<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

Ref	Object	Description	Input Relationship	Output Relationship
		access control for a managed resource		(add, modify, change password, suspend, restore, delete, etc.) follow one or more workflows
③	Role	The Role object is a container that is used to define a role and the associated privileges that can be assigned to a user.	<ul style="list-style-type: none"> - One Identity can be assigned 0 or more Roles 	<ul style="list-style-type: none"> - One Role can be members of 0 or more Provisioning Policies. - One Role can participate in 0 or more Entitlement Workflows.
④	Provisioning Policy	The Provisioning Policy object is a definition of the level of access that may be granted to a managed resource or service to particular membership(s) or Roles	<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 	

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

3.2.2. Database Information

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

Table 17: 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.	Create / Replace / Interface / Modify	VRM AcS Solution
CA IdentityMinder – Task Persistence Schema	Stores runtime tasks and in-process tasks (task sessions). Also includes Scheduler information. This store is for internal use only.	Create / Replace / Interface / Modify	VRM AcS 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.	Create / Replace / Interface / Modify	VRM AcS Solution
CA IdentityMinder – Reporting Schema	Stores snapshot data, which reflects the current state of objects in CA IdentityMinder at the time the snapshot is taken. Reports can be generated from this information to view the relationship between objects, such as users and roles.	Create / Replace / Interface / Modify	VRM AcS Solution
CA IdentityMinder – Task Persistence Archive Schema	Stores runtime task archives. This store is for internal use only.	Create / Replace / Interface / Modify	VRM AcS Solution
CA IdentityMinder – Audit Schema	Provides a historical record of operations that occur in an CA IdentityMinder.	Create / Replace / Interface / Modify	VRM AcS Solution
CA SiteMinder – Audit	Provides a historical record of operations that occur in Site Minder, and Reports are generated from of this data.	Create / Replace / Interface / Modify	VRM AcS Solution
eSig Audit	eSig Audit data collection store where auditable transaction logs are collected for reporting purposes.	Create / Replace / Interface / Modify	VRM AcS Solution

3.2.3. User Interface Data Mapping

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

3.2.3.1. Provisioning Screen Interface

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

3.2.3.1.1. New VA Employee/Contractor Profile Screen

Figure 11 represents the screen that is accessed to start the onboarding process.

Figure 11: New VA Employee/Contractor Profile 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.

3.2.3.1.2. New VA Employee/Contractor Profile Work Home Screen

Figure 12 below represents the screen to capture work location details.

Figure 12: New VA Employee/Contractor Profile Work Home 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.

3.2.3.1.3. New VA Employee/Contractor Profile Org Screen

Figure 13 below represents the screen that is used to capture organizational information.

VA Provisioning Service

New VA Employee: Profile Org

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

* Required

Organizational and Employment Information

Employment Status Choose One

Occupation Choose One

Department Choose One

Title

Manager Browse

Office Location Choose One

Cost Center Choose One

Special Security Access Required Choose One

Emergency Responder Choose One

Critical Employee Choose One

VA Provisioning Service

Contractor: Profile Org

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

Organizational and Employment Information

Advisor ID SEC ID Browse

IT PD Project

Project Manager Browse

Contract Number

Additional training Required Yes

Position Code Choose One

Employment Status Choose One

Department Choose One

Address Browse

Office Location Choose One

Center Choose One

Special Security Access Required Choose One

Emergency Responder Choose One

Critical Employee Choose One

Figure 13: New VA Employee/Contractor Profile Org 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.

3.2.3.1.4. New VA Employee/Contractor Profile Misc. Screen

Figure 14 below represents the screen that is used to capture the miscellaneous information.

Figure 14: New VA Employee/Contractor Screen Profile Misc. 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.

3.2.3.1.5. CRISP Checklist Screen

Figure 15 below represents the screen that is used to capture the data against the checklist.

Figure 15: CRISP Checklist Screen

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

3.2.3.2. CSP Screen Interface

This section provides the screens of the Graphical User Interface (GUI) that the AcS users will have access to in order to perform self-service registration, profile management and password management.

3.2.3.2.1. Modify Account: Step 1 User Profile

Figure 16 below represents the screen that captures the user information when modifying user information and security questions.

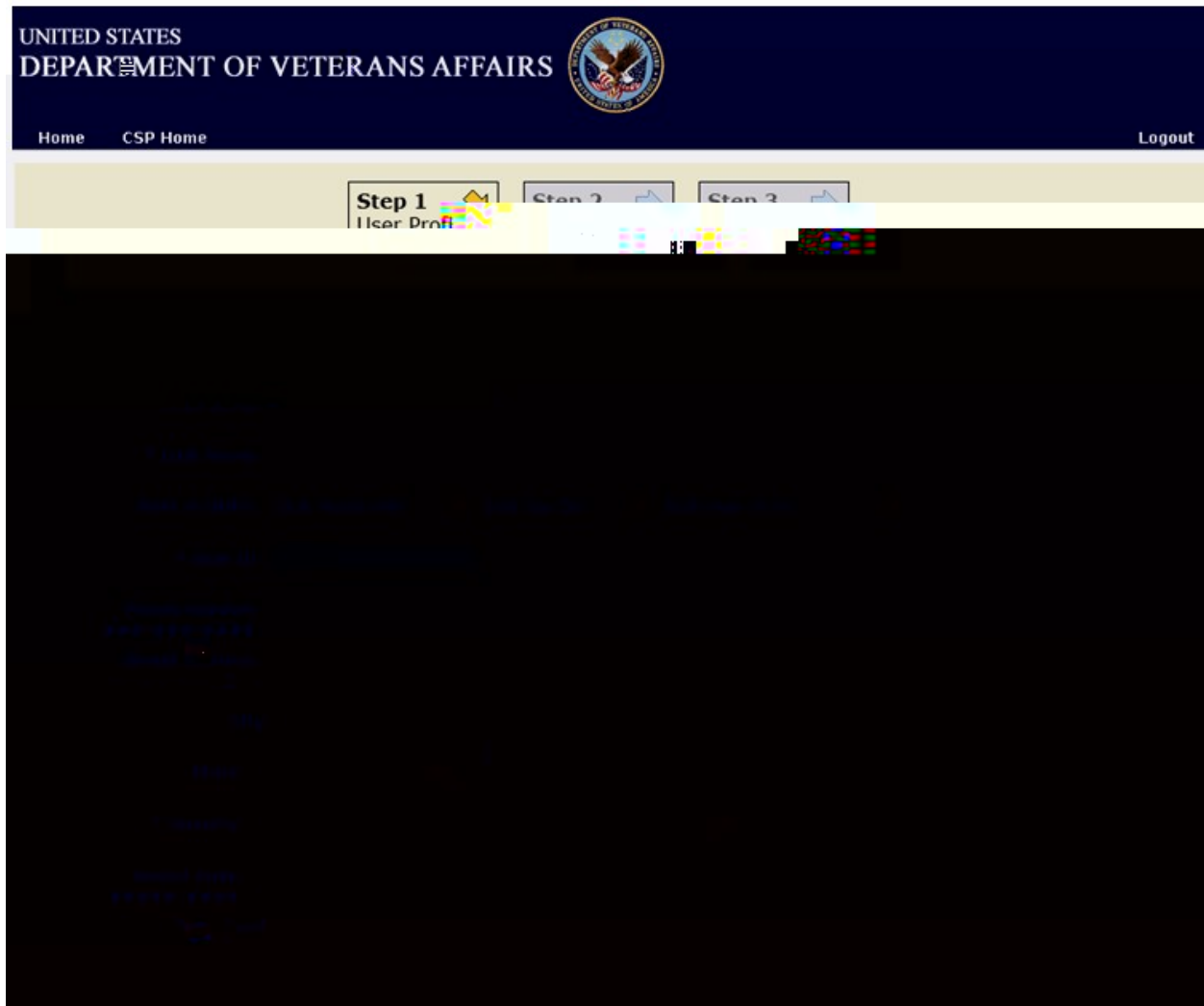


Figure 16: Modify Account: Step 1 User Profile

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

Figure 17 below represents the screen that captures the security questions and answers when modifying user information and security questions.

Figure 17: Modify Account: Step 2 Security Questions

Refer to [section A.1](#) below, whichs 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

Figure 18 below represents the screen that allows the user to change their password.

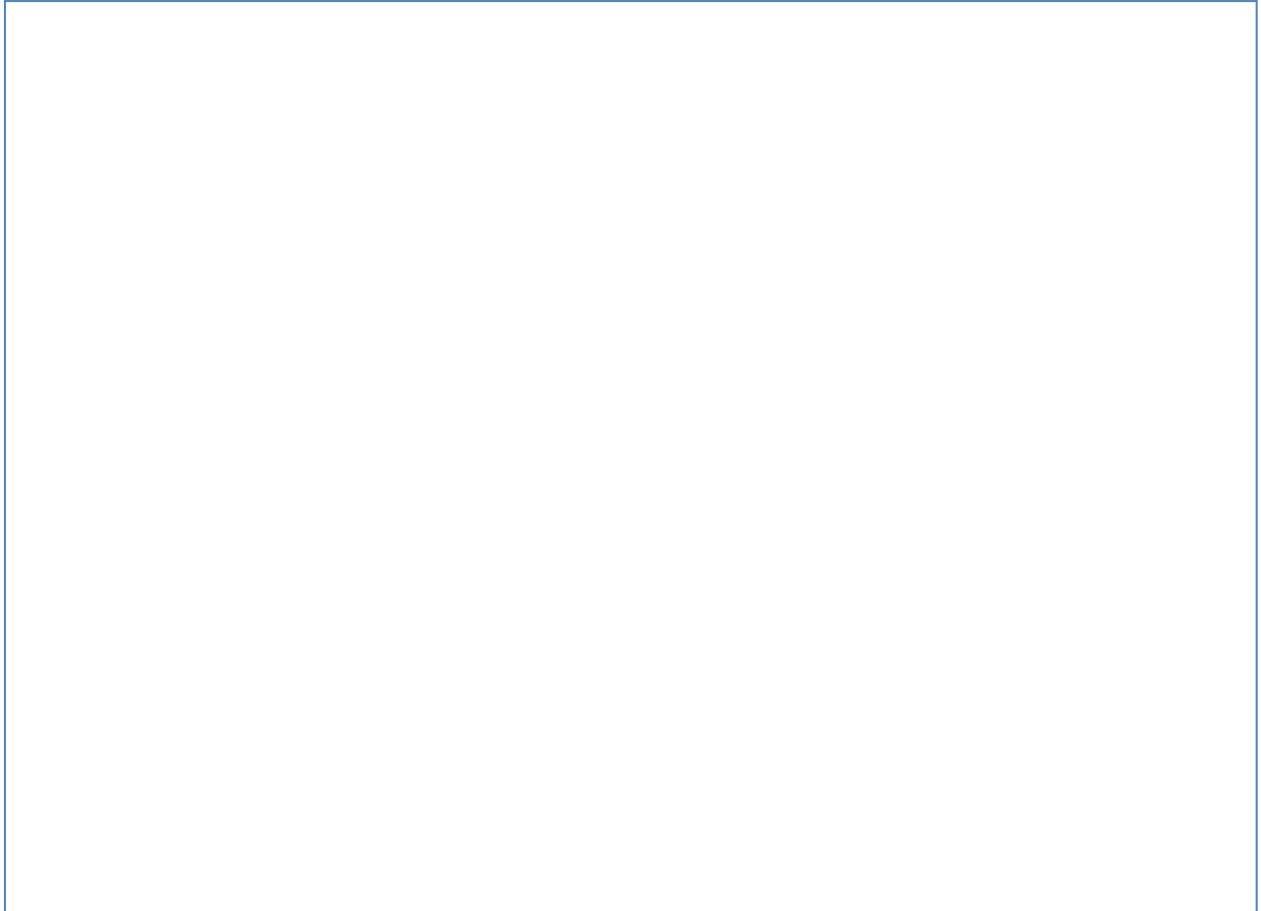


Figure 18: Change Password

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

Figure 19 below represents the screen that captures the user information when requesting to upgrade to level 2.

Figure 19: 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

Figure 20 below represents the screen that captures the security questions and answers when requesting to upgrade to a Level 2 credential.

Figure 20: 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

Figure 21 below represents the screen that captures the user information when self-registering.

Figure 21: 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

Figure 22 below represents the screen that captures the security questions when self-registering.

The screenshot shows the 'Step 2 Security Questions' screen of the VA Self-Registration process. At the top, the header includes the 'UNITED STATES DEPARTMENT OF VETERANS AFFAIRS' logo and navigation links for 'Home' and 'Help/Contact Us'. Below the header, there are three buttons: 'Go Back', 'Step 2 Security Questions' (which is highlighted with a red arrow), and 'Go Forward'. A 'Modify Account' link is also visible. The main content area contains eight pairs of input fields, each labeled 'Security Question #1' through 'Security Question #8' and 'Security Answer #1' through 'Security Answer #8'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

Figure 22: 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 provides the screens of the Graphical User Interface (GUI) that the AcS users will have access to in order to perform Identity Proofing.

3.2.3.3.1. Identity Proof User: Step 1 User Profile

Figure 23 below represents the screen that captures the user information when identity proofing a user.

Figure 23: 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.

3.2.3.3.2. Identity Proof User: Step 2 Address Verification

Figure 24 below represents the screen that captures the Address information of the candidate being identity proofed.

Figure 24: 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.

3.2.3.3.3. Identity Proof User: Step 3 Primary Identification

Figure 25 below represents the screen that captures the primary identification information of the candidate being identity proofed.

Figure 25: 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.

3.2.3.3.4. Identity Proof User: Step 4 Secondary Identification

Figure 26 below represents the screen that captures the secondary identification information of the candidate being identity proofed.

Figure 26: 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.

3.2.3.3.5. Update a User: Step 1 User Profile

Figure 27 below represents the screen that captures the user information when updating a user.

Figure 27: 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.

3.2.3.3.6. Update a User: Step 2 Address Verification

Figure 28 below represents the screen that captures the address information when updating a user.

Figure 28: 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.

3.2.3.3.7. Update a User: Step 3 Primary Identification

Figure 29 below represents the screen that captures the primary identification information of the candidate being updated.

Figure 29: 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.

3.2.3.3.8. Update a User: Step 4 Secondary Identification

Figure 30 below represents the screen that captures the secondary identification information of the candidate being updated.

Figure 30: 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 provides the screens of the GUI that the AcS users will have access to in order to authenticate to VA Applications through centralized login page.

3.2.3.4.1. Centralized Login Page

In order 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.

Figure 31 below represents the screen that is accessed by end users to authenticate to integrated VA applications with SSOi.

Figure 31: SSOi Centralized Login Page

3.2.3.4.2. Centralized PIV Only Login page

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

Figure 32 below represents the screen that is accessed by end users to authenticate to integrated VA applications with SSOi using only a PIV card.



Figure 32: SSOi PIV Only Login Page

3.2.3.4.3. Mobile Login Page

Figure 33 below represents the screen that is accessed by end users to authenticate to integrated VA applications with SSOi through a mobile device. In order 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.

Figure 33: Mobile Login Page

3.2.3.5. SAC Screen Interface

This section provides the screens of the GUI that the AcS users will have access to in order to administer the SAC service.

3.2.3.5.1. PAP Landing Page

Figure 34 below represents the screen that is provided to SAC privileged users once they initiate the Axiomatic thick client to create or open workspaces for policy authoring.

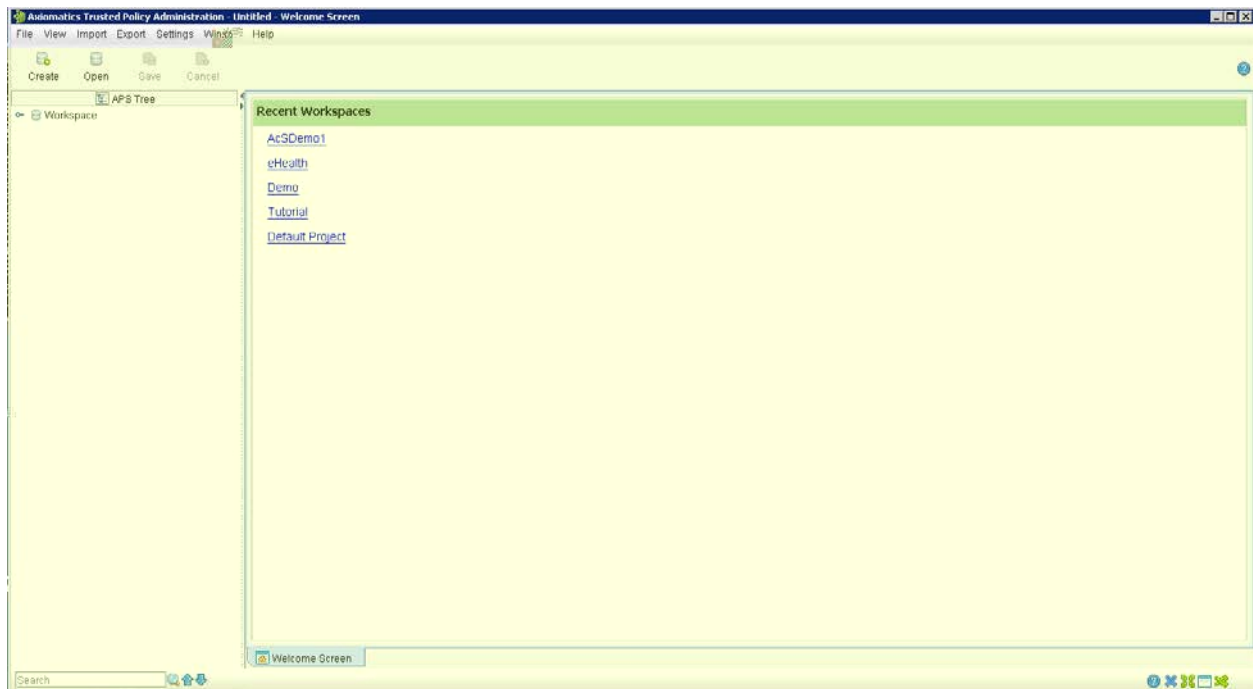


Figure 34: SAC PAP Landing Page

3.2.3.5.2. PAP Authoring Page

Once a workspace is opened or created by the privileged user, the screen in Figure 35 below displays. The screen shows the interface which the SAC privileged user creates/edits XACML 3.0 policies.

Figure 35: SAC PAP Landing Page

3.2.3.6. AcS Solution Report Interface

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

3.2.3.7. Unmapped Data Element

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

3.3. Conceptual Infrastructure Design

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

3.3.1. System Criticality and High Availability

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

The DR site is contingency site that will resume data center operations in the event of a site failure. Load balancing, fault tolerance, backups and archiving, is a function of the hosting facility, REDACTED 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 table below details all of the Special Technologies implemented as part of the AcS solution.

Table 18: Special Technology Requirements

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

3.3.3. Technology Locations

Refer to section 3.3.4.1 below for technology locations.

3.3.4. Conceptual Infrastructure Diagram

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

3.3.4.1. Location of Environments and External Interfaces

Figure 36 below shows the high-level conceptual infrastructure diagram for the VA AcS infrastructure. The diagram also depicts the communication between the REDACTED data centers in REDACTED REDACTED and REDACTED REDACTED. The VA AcS infrastructure environment is set up at the REDACTED data center in REDACTED REDACTED. The alternate site or disaster recovery site for VA AcS operations is the REDACTED data center in REDACTED REDACTED.

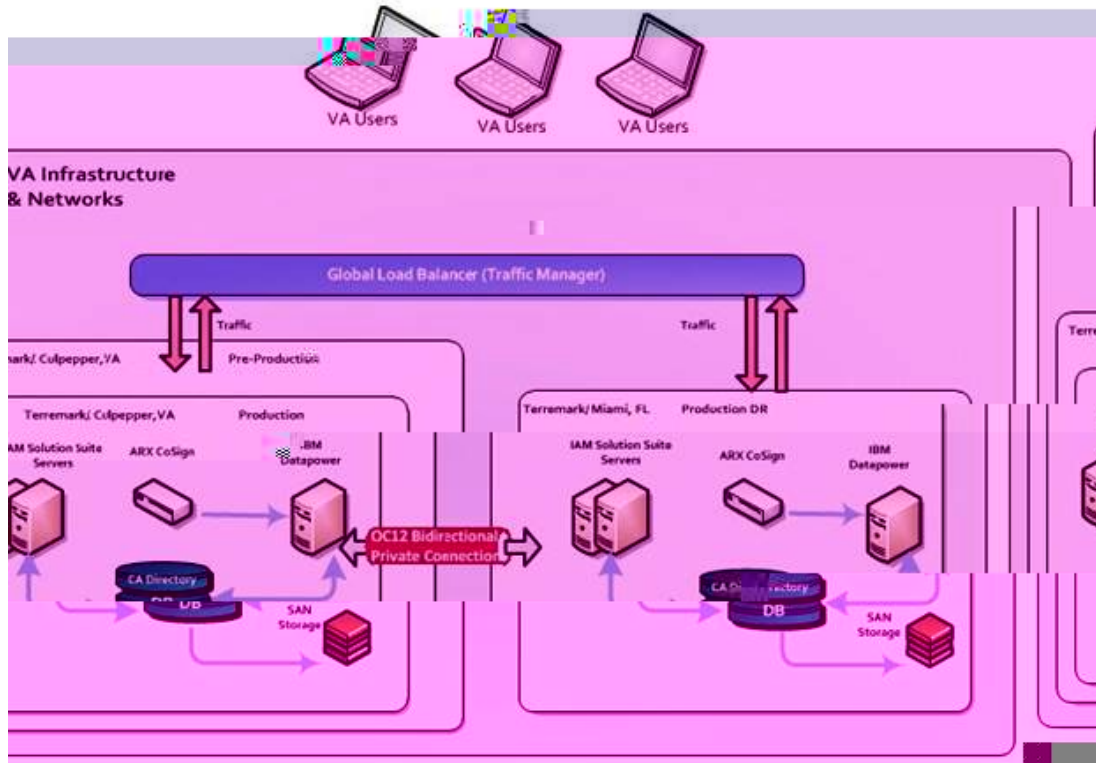


Figure 36: AcS Production Environments

Development Environment (DEV) AITC – Austin, TX

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

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

Production – [REDACTED] [REDACTED] VA

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

Production Disaster Recovery (DR) – [REDACTED] [REDACTED] [REDACTED]

- 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 [REDACTED] [REDACTED] [REDACTED] data centers. 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 [REDACTED] [REDACTED] VA and remotely at [REDACTED] [REDACTED] [REDACTED] 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 [REDACTED] [REDACTED] VA to the disaster recovery data center at [REDACTED] [REDACTED] [REDACTED] 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

Figure 37 below provides a logical view of the AcS solution components.

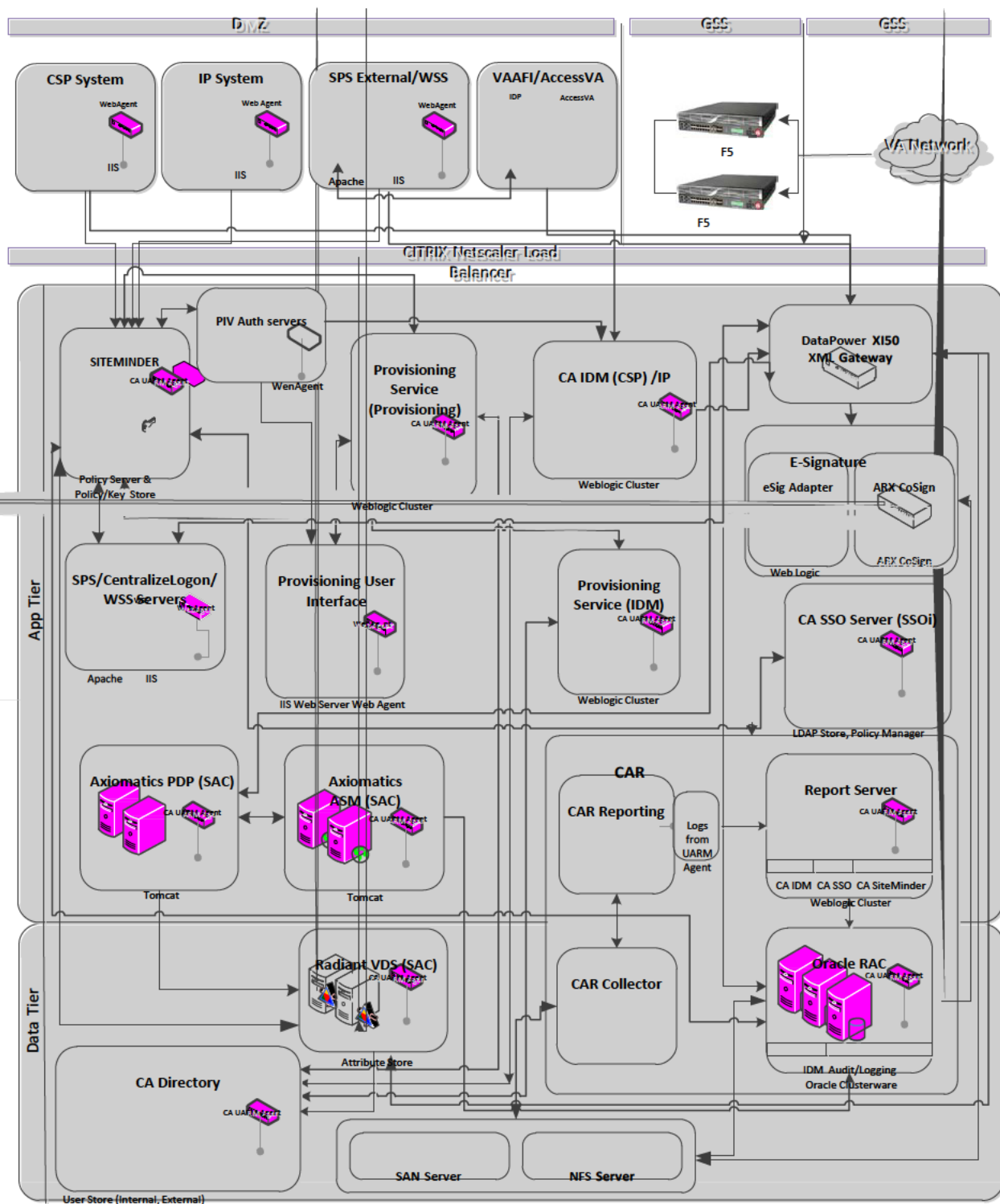


Figure 37: Logical Network String Diagram

4. System Architecture

The AcS solution system architecture includes the hardware, software, and communication architectures. The hardware architecture describes the physical components needed in the

system

and their relationship to one another. The software architecture describes the software products, components, and code needed to provide the AcS solution. The communication architecture describes the connection and security requirements needed between the hardware components.

4.1. Hardware Architecture

Figure 38 below displays the AcS solution hardware architecture and network topology.

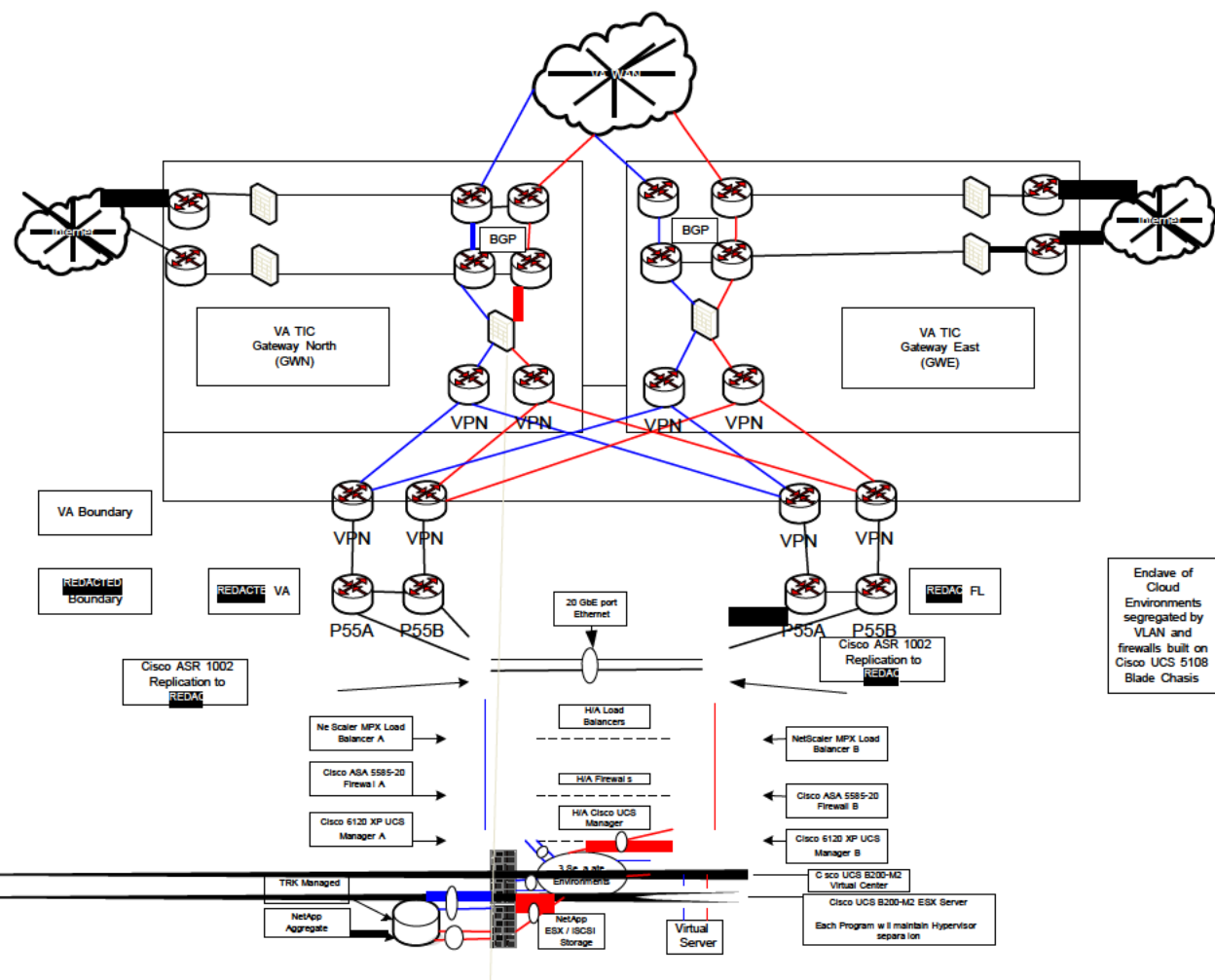


Figure 38: Network Communication Architecture

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

Table 19: Hardware Appliance

Hardware Appliance	Descriptions	High Availability (HA)
ARX Co-Sign (eSig)	CoSign is a PKI-based, off-the-shelf digital-signature solution enabling VA to embed digital	The ARX CoSign has a built in mechanism to provide HA capability. For high availability, several CoSign

Hardware Appliance	Descriptions	High Availability (HA)
	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.	appliances are installed where one of the CoSign appliances is defined as the primary while the others are designated as the alternate CoSign appliances. Information is replicated securely from the primary to the alternate appliances using the IPSEC protocol. In case of a failure, another attempt is made. The device will give up after a total of ten tries and an alert will be sent to the administrator. The eSig adapter talks to the primary device. The secondary device pulls the changes from primary and be completely synchronized with the primary device.

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

Table 20: Virtual Machines and Appliances

Application	Number of VMS	Number of Physical Servers	Hostname
SQA (REDACTED)			
CSP/IP/Federation Services WebUI/SPS/WSS (IIS, Tomcat)	5	N/A	HYPERLINK REDACTED
IdentityMinder supporting (Credential Service Provider and Identity Proofing) WebLogic	3	N/A	HYPERLINK REDACTED
Centralized Logon page, SPS, WSS (IIS)	2	N/A	HYPERLINK REDACTED
PIV Authentication Handler (IIS)	2	N/A	HYPERLINK REDACTED

Application	Number of VMS	Number of Physical Servers	Hostname
IdentityMinder support (Provisioning Service) (WebLogic)	2	N/A	HYPERLINK REDACTED
Provisioning WebUI (IIS)	2	N/A	HYPERLINK REDACTED
Provisioning Server	2	N/A	HYPERLINK REDACTED
CA Directory (CSP and IP)	3	N/A	HYPERLINK REDACTED
CA Directory (Provisioning)	2	N/A	HYPERLINK REDACTED
CA SSO Server	2	N/A	HYPERLINK REDACTED
CA UARM (Tomcat)	4	N/A	HYPERLINK REDACTED
CA Report Server (Weblogic)	2	N/A	HYPERLINK REDACTED
CA SiteMinder (Weblogic)	3	N/A	HYPERLINK REDACTED
Axiomatic PDP (Tomcat)	1	N/A	HYPERLINK REDACTED
Axiomatic ASM/PAP (Tomcat)	1	N/A	HYPERLINK REDACTED
Axiomatics Policy Auditor	1	N/A	HYPERLINK REDACTED
Radiant Logic VDS	Not Applicable	1	HYPERLINK REDACTED
Oracle RAC	Not Applicable	2	HYPERLINK REDACTED HYPERLINK REDACTED
DataPower XI50 (Appliance)	Not Applicable	N/A	Not Applicable

Application	Number of VMS	Number of Physical Servers	Hostname
ARX CoSign (Appliance)	Not Applicable	N/A	Not Applicable
eSig Weblogic Servers	2	N/A	HYPERLINK REDACTED
Pre-Production (REDACTED)			
CSP/IP/Federation Services WebUI/SPS/WSS (IIS, Tomcat)	4	N/A	HYPERLINK REDACTED
Centralized Logon page, SPS, WSS (IIS)	2	N/A	HYPERLINK REDACTED
PIV Authentication Handler (IIS)	2	N/A	HYPERLINK REDACTED
IdentityMinder supporting (Credential Service Provider and Identity Proofing) (Weblogic)	2	N/A	HYPERLINK REDACTED
IdentityMinder support (Provisioning Service) (Weblogic)	3	N/A	HYPERLINK REDACTED
Provisioning WebUI (IIS)	2	N/A	HYPERLINK REDACTED
Provisioning Server	2	N/A	HYPERLINK REDACTED

Application	Number of VMS	Number of Physical Servers	Hostname
CA Directory (CSP and IP)	2	N/A	HYPERLINK REDACTED
CA Directory (Provisioning)	2	N/A	HYPERLINK REDACTED
CA SSO Server	2	N/A	HYPERLINK REDACTED
CA UARM	3	N/A	HYPERLINK REDACTED
CA Report Server	1	N/A	HYPERLINK REDACTED
CA SiteMinder (Weblogic)	3	N/A	HYPERLINK REDACTED
Axiomatic PDP (Tomcat)	2	N/A	HYPERLINK REDACTED
Axiomatic ASM/PAP (Tomcat)	1	N/A	V HYPERLINK REDACTED
Radiant Logic VDS	N/A	2	HYPERLINK REDACTED

Application	Number of VMS	Number of Physical Servers	Hostname
Oracle Database	N/A	2	HYPERLINK REDACTED
DataPower XI50 (Appliance)	Not Applicable	N/A	Not Applicable NOTE: Placed inside the VAAFI Enclave
ARX CoSign (Appliance)	Not Applicable	N/A	Not Applicable
eSig Web logic Servers	2	N/A	HYPERLINK REDACTED
Production (REDACTED)			
CSP/IP/Federation Services WebUI/SPS/WSS (IIS)	4	N/A	HYPERLINK REDACTED
Centralized Logon page, SPS, WSS (IIS , Tomcat)	2	N/A	HYPERLINK REDACTED
PIV Authentication Handler (IIS)	2	N/A	HYPERLINK REDACTED
IdentityMinder (CSP and IP) (Weblogic)	2	N/A	HYPERLINK REDACTED
IdentityMinder (Provisioning) (Weblogic)	3	N/A	HYPERLINK REDACTED

Application	Number of VMS	Number of Physical Servers	Hostname
Provisioning WebUI (IIS)	2	N/A	HYPERLINK REDACTED
Provisioning Server	2	N/A	HYPERLINK REDACTED
CA Directory (CSP/IP)	2	N/A	HYPERLINK REDACTED
CA Directory (Provisioning)	2	N/A	HYPERLINK REDACTED
CA SSO Server	2	N/A	HYPERLINK REDACTED
CA UARM	3	N/A	HYPERLINK REDACTED
CA Report Server (Weblogic)	1	N/A	HYPERLINK REDACTED
CA SiteMinder (Weblogic)	3	N/A	HYPERLINK REDACTED
Axiomatic PDP (Tomcat)	2	N/A	HYPERLINK REDACTED

Application	Number of VMS	Number of Physical Servers	Hostname
Axiomatic ASM/PAP (Tomcat)	1	N/A	HYPERLINK REDACTED
Radiant Logic VDS	N/A	2	HYPERLINK REDACTED
Oracle Database	N/A	2	HYPERLINK REDACTED
DataPower XI52	Not Applicable	N/A	Not Applicable NOTE: Placed inside the HYPERLINK REDACTED
ARX CoSign	Not Applicable	N/A	Not Applicable
eSig Web logic Servers	2	N/A	HYPERLINK REDACTED
DR (REDACTED)			
CSP/IP/Federation Services WebUI (IIS)	4	N/A	HYPERLINK REDACTED
Centralized Logon page, SPS, WSS (IIS, Tomcat)	2	N/A	HYPERLINK REDACTED
PIV Authentication Handler (IIS)	2	N/A	HYPERLINK REDACTED
IdentityMinder (CSP) (Weblogic)	2	N/A	HYPERLINK REDACTED
IdentityMinder (Provisioning) (Weblogic)	3	N/A	HYPERLINK REDACTED
Provisioning WebUI (IIS)	2	N/A	HYPERLINK REDACTED

Application	Number of VMS	Number of Physical Servers	Hostname
Provisioning Server	2	N/A	HYPERLINK REDACTED
CA Directory (CSP and IP)	2	N/A	HYPERLINK REDACTED
CA Directory (Provisioning)	2	N/A	HYPERLINK REDACTED
CA SSO Server	2	N/A	HYPERLINK REDACTED
CA UARM	3	N/A	HYPERLINK REDACTED
CA Report Server (Weblogic)	1	N/A	HYPERLINK REDACTED
CA SiteMinder (Weblogic)	2	N/A	HYPERLINK REDACTED
Axiomatic PDP (Tomcat)	2	N/A	HYPERLINK REDACTED
Axiomatic ASM/PAP (Tomcat)	1	N/A	HYPERLINK REDACTED
Radiant Logic VDS	N/A	2	HYPERLINK REDACTED
Oracle Database	N/A	2	HYPERLINK REDACTED
DataPower XI52 (Appliance)	N/A	N/A	N/A
ARX CoSign (Appliance)	N/A	N/A	N/A
eSig Web logic Servers	2	N/A	HYPERLINK REDACTED

4.2. Software Architecture

The diagram in Figure 39 below depicts the complete software architecture of the VA AcS solution.

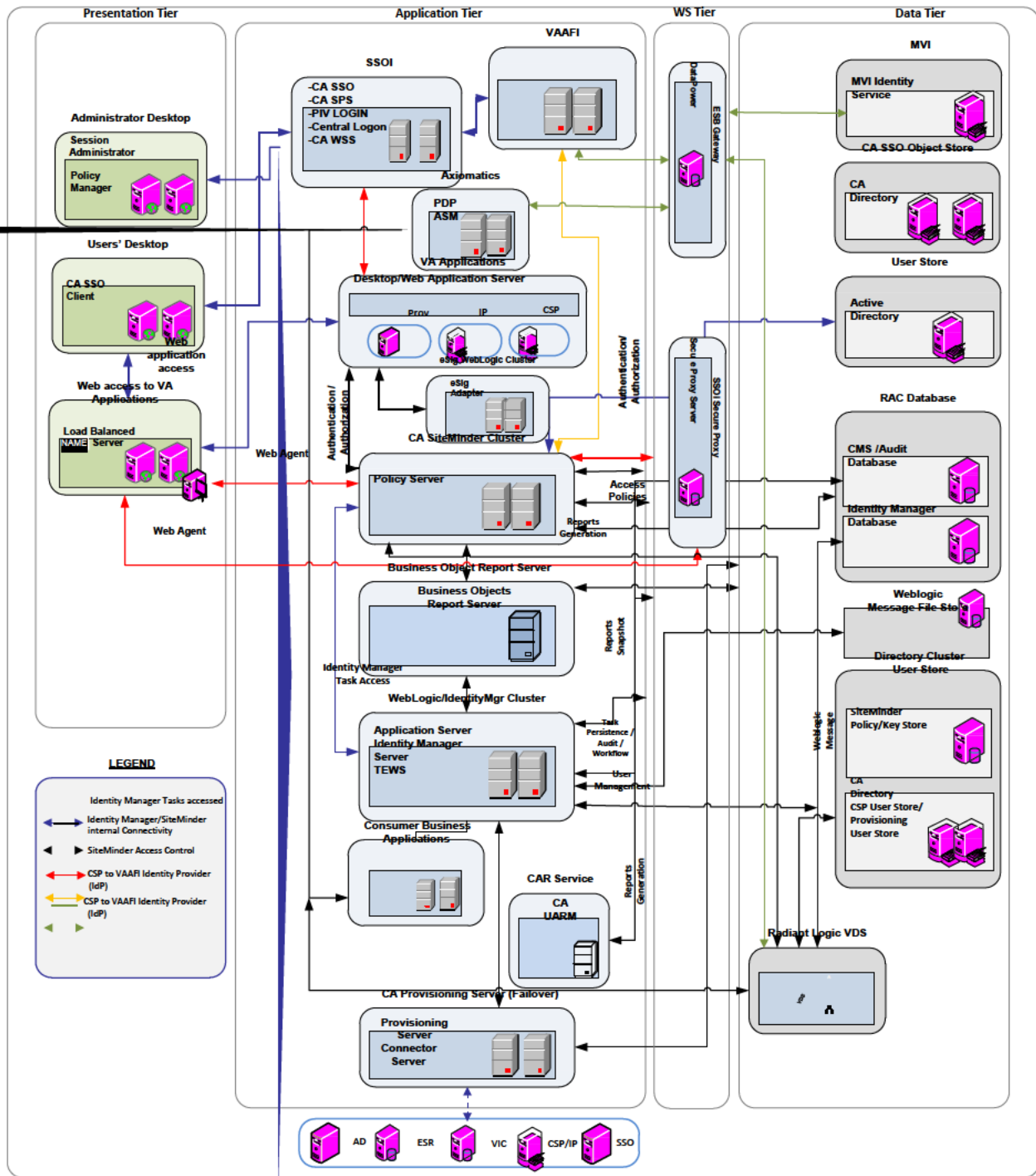


Figure 39: Software Architecture

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

Table 21: AcS Products and Versions

Access Services Service	Activity Name	Products	Abbreviation	Product Version/Release
Access Services	Credential Service Provider (CSP) and Identity Proofing (IP)	CA IdentityMinder	CA IdentityMinder	R12.6 SP1
		IIS Web Server	-	7.5
		CA Web Agent	-	SM r12.5 SP1
		CA Option Pack	-	SM r12.5 SP1
		Servlet Exec	-	6.0 Fixpack x
		WebLogic	-	10.3,6
		Oracle Database	-	11gR2
		CA Directory	LDAP directory	12.0 SP7
		CA SiteMinder	CA SM	SM r12.5 SP1
		CSP .NET Application	CSP App	ASP.NET 4
		IP .NET Application	IP App	ASP.NET 4
		MVI Web Service Client	MVI WS	Java 1.6
	Single Sign-On – Internal (SSOi)	CA Single Sign On	CA SSO	12.1 / R12.1
		Oracle Database	-	11gR2
		CA Directory	CA LDAP	12.0 SP7
		CA SiteMinder	CA SM	SM r12.51
		CA Option Pack for Federation	-	SM r12.51
		Login Page	LP	ASP.NET 4
	Provisioning (PROV)	CA IdentityMinder	CA IdentityMinder	R12.6 SP1
		IIS Web Sever	-	7.5
		CA Web Agent	-	SM r12.51/12.0SP3
		WebLogic	-	10.3,6
		Oracle Database	-	11gR2
		CA Directory	LDAP directory	12.0 SP7
		CA SiteMinder	CA SM and Proxy Server	SM r12.51
		CA WorkPoint	CA WP	R12.6 SP1

Access Services Service	Activity Name	Products	Abbreviation	Product Version/Release
		BLTH (Business Logic Task Handler)	BLTH	Java 1.6
		MVI Web Service Client	MVI WS	Java 1.6
		Radiant Logic VDS	Attribute Service & Policy Information Point	6.1.2
	Specialized Access Control (SAC)	Axiomatics PDP	Policy Decision Point	5.2.1
		Axiomatics ASM	Services Manager	5.2.1
		Axiomatics PAP	Policy Administration Point	5.2.1
		Apache Tomcat	Axiomatics Application Server	7.0.42
	Compliance Audit and Reporting (CAR)	CA User Activity Reporting Module	CA UARM	12.5 SP3 (12.5)
		CA User Activity Reporting Module Agent	CA UARM Agent	12.5 SP3 (12.5)
		SAC Connector	SAC Connector	UARM Regular Expressions
	e-Signature (eSig)	ARX Co-Sign	Digital Signature	v6.3

Table 22: Software Components

Software Component
Oracle Database 11gR2
The shared database environment will maintain the following table spaces required for the components of the AcS implementation. Database High Availability and Data Guard to synchronize and replicate a HOT Oracle database environment to REDACTED REDACTED REDACTED

Software Component	
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 AcS solution, database high availability is critical. A database outage can cause a multitude of errors to occur on the application side, thereby nullifying the high availability configurations on the application itself. It was planned for Raw Devices to be utilized by Oracle Automatic Storage Management (ASM) file system, working as the volume manager, overseeing the clusterware file systems. ASM, attached by each node, exposes the existing pool of storage and makes it available as an interface for the Oracle database files. The ASM is supported by Oracle Clusterware. If a single Oracle instance on a node fails, the ASM and database instances on the surviving nodes are designed to automatically failover. Due to the load dependency on the ASM file system storage, mirroring is needed to provide high availability.</p>
CA Directory	
<p>The CA Directory servers are a shared resource for the AcS solution. The CA Directory infrastructure will be configured in a multi-master replication configuration. The CA Directory comprises of various instances elaborated as follows.</p> <p>Note: CA Directory structure as applicable for each of the directory instance specific to a release and will be provided in each release. The holistic view of the CA Directory structure is provided in Software Detail Design Sections.</p>	
Directory Instances	<p>User store CA IdentityMinder for CSP solution and Provisioning services, Policy and Key store for CA SiteMinder for CSP service Object/policy store for CA SSO for SSOi services.</p>

Software Component	
High Availability	<p>There will be a master write server for each directory. The other supporting directories will be read directories.</p> <p>The CA Directory will provide intelligent and transparent chaining of queries to distributed servers. It performs transparent routing to re-route requests in the event of failure on a particular CA Directory server. The CA Directory router DSA distributes incoming requests evenly among DSAs in the same site. 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) are configured for multiwrite-DISP replication. This replication scheme combines the efficiency of multiwrite when DSAs are online (real-time updates), with the robustness of DISP to allow DSAs to recover after being offline (recovery).</p> <p>The DSA uses its routing capabilities to distribute requests evenly between systems while data replication keeps the data synchronized.</p>
Web Tier – IIS Web Server	
The Web Tier is comprised of the IIS web servers which provide reverse proxy and federation to the applications.	
IIS Web Server Instances	CA IdentityMinder Registration / user profile management/admin UI for CSP service

Software Component	
High Availability	<p>IIS Web Servers are used by the CSP, centralized logon, PIV Auth and Federation servers to support multiple services. They will be CSP Login / Registration, Provisioning, and protected by the SiteMinder Option Pack (Federation), PIV Authentication Servers, and Centralized Logon Server Page.</p> <p>The CSP Login / Registration will leverage five (5) IIS web servers, behind a Citrix NetScaler load balancer with a round robin algorithm which distributes equal load between the servers. The load balancers will be configured to maintain the session for the entirety of each user transaction. In the event that all of the IIS web servers fail on REDACTED REDACTED VA site, the Citrix NetScaler load balancer will be configured to route the traffic to REDACTED REDACTED REDACTED 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 REDACTED</p> <p>There are two IIS web servers required for PIV, Federation, and Centralized logon.</p>
Application Tier – WebLogic Application Server	
<p>The application tier for the Provisioning service is made up of a cluster of WebLogic application servers. The Application Tier is a shared environment for hosting application components. The AcS related applications hosted are listed below. The Report Server instance is a Business Objects environment that provides reporting services for Access Services. The CA Report server (SAP Business Objects XI R3.1 SP3) that constitutes the Reporting Infrastructure is hosted on a WebLogic cluster.</p>	
WebLogic Instances	<p>CA IdentityMinder for CSP and Provisioning solution</p> <p>CA SiteMinder Admin UI</p> <p>eSig Web Service</p>
High Availability	<p>The WebLogic servers will be configured for high availability. These WebLogic servers will be load balanced using the Round Robin algorithm provided by the Citrix NetScaler.</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. <p>The WebLogic cluster is designed as an active and passive failover. Therefore when the instances in a Clusternode fail, it will failover to the alternate cluster node.</p>
Application Tier –Tomcat Application Server	

Software Component	
The application tier for the SAC solution is comprised of Tomcat application servers. The Application Tier is a shared environment for hosting application components. The AcS related applications hosted are listed below. The Axiomatic PDP and ASM components are hosted on the Tomcat application servers.	
Tomcat Instances	Axiomatic ASM Axiomatic PDP
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 loadbalancing of the service requests via the 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.	
Axiomatic	
The Axiomatic components are integral to the specialized access control solution. It provides the necessary components for externalizing authorization. Axiomatic is comprised of the following components.	

Software Component	
Subcomponents	<p>Axiomatic 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 Axiomatic PAP Client. In addition, ASM may monitor the operational status of PDPs. Applicable data needed by ASM is stored in an external database.</p> <p>Policy Decision Point: Service that provides XACML-based authorization to Policy Enforcement Points (PEPs). The Axiomatic PDP provides externalized authorization and runs as a service on the network, exposing a web service interface that may be secured by SSL/TLS.</p> <p>Policy Administration Point: Development environment for XACML 3 policies that may be used in the Axiomatic authorization infrastructure. Provides graphical XACML policy editor, attribute dictionary, and simulating and tracing policies. Policies will be checked 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.	

Software Component	
Subcomponents	<p>IdentityMinder Server: Executes workflows within IdentityMinder. It includes the Management Console and the User Console deployed on a WebLogic cluster.</p> <p>Provisioning Server: Manages the lifecycle of user accounts on endpoint systems. This server is required as the CA IdentityMinder installation will support account provisioning.</p> <p>User store: The IdentityMinder user store is maintained by CA IdentityMinder. This is an existing store that contains the user identities that a company needs to manage. The user store for VA AcS solution is CA Directory as mentioned above.</p> <p>User store maintained by the Provisioning Server: The Provisioning Directory user store is maintained by the Provisioning Server. It is an instance of CA Directory and includes global users. It associates users in the Provisioning Directory with accounts on endpoints such as Microsoft Exchange, Active Directory, and SAP.</p>
High Availability	The CA IdentityMinder utilizes web logic clustering described above for high availability.
CA SiteMinder	
CA SiteMinder is an integral component of Access Services solution, providing CSP solution federation capabilities to integrate with VAAFI. CA SiteMinder is also utilized to protect the CA IdentityMinder application. CA SiteMinder is comprised of the following components.	

Software Component	
Subcomponents	<p>SiteMinder Policy Server: The Policy Server provides advanced authentication and password services to protected applications such 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 an 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 agents on IIS web servers will be configured to talk to primary policy server and will automatically connect to the secondary policy server when the primary policy server is unresponsive.</p>
CA SSO	
<p>The CA SSO server, Authentication services, and CA SSO desktop client enable the SSOi services for desktop single sign on usage. The authentication services communicate with the user store to provide credentials and authenticate the user to the SSOi solution. It also interacts with the CA Directory to maintain user logon information. The CA SSO is installed and configured in FIPS only mode as approved by TRM.</p>	

Software Component	
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>There are a number of components for CA SSO which will be configured for High Availability.</p> <p>CA SSO Server: A CA SSO server farm will be created. It is a system of two networked CA SSO Servers. The data on each server will be replicated to servers in the farm. The REDACTED REDACTED VA site and Terremark REDACTED REDACTED 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 REDACTED VA server farm and Terremark REDACTED REDACTED server farm is defined in the CA SSO client configuration for built-in failover.</p>
CA UARM	

Software Component	
<p>CA User Activity Reporting Module collects logs from a variety of applications and devices using agentless or agent-based methods. It then normalizes the log to CA Common Event Grammar (CEG) and reduces the volume of logs by filtering unwanted events based on pre-defined event filtering policies. Processed events are available for reporting, alerting, and multi-dimensional investigation. Based on log archival policy, CA UARM compresses logs and stores them on external storage systems for long term storage. The CA UARM component is installed and configured in FIPS only mode as per TRM.</p>	
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 Adapter	
<p>eSig Adapter is the engine that provides the basis for the eSig capability. eSig uses the CoSign appliance as a building block and provides the capability to digitally sign documents to various applications within VA. Moreover, the events are recorded and made available to the CAR service for reporting. The eSig system utilizes an inherent defense mechanism to reduce potential system security compromises.</p>	

Software Component	
Subcomponents	<p>DataPower devices: The DataPower devices are used to authenticate the machine to machine sessions.</p> <p>WebLogic Server: The WebLogic Server hosts the eSig adapter. The eSig adapter has the following components:</p> <p>eSig Servlet: The eSig Servlet receives the request and passes on to the eSig Façade. The Servlet currently receives only API calls but can be extended if required to include the web interface.</p> <p>eSig Façade: The eSig façade component carries out the following categories of operation:</p> <ul style="list-style-type: none"> ○ User Management: The user management function allows the service to add or remove a particular user. ○ Sign and Verify: This allows the applications to sign a given document. ○ Reporting Events: This category allows the eSig service to record events that will be reported via CAR service. <p>CoSign Device: The CoSign is a hardware appliance that stores the user certificates.</p>
High Availability	<p>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 that constitute a cluster can run on the same system, or be located on different systems. The eSig Servlet and eSig Façade run within the cluster domain and is highly available through multimode cluster and is load balanced by the F5.</p> <p>CoSign is highly available through internal functions that keep the appliances in sync with each other.</p>

The table below provides the programming languages used for development within the VA AcS solution.

Table 23: 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.

Programming Languages	Definition/Description
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.

The table below provides the operating systems used for the VA AcS solution.

Table 24: Operating Systems

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

4.3. Communications Architecture

The diagram in Figure 40 below depicts the communication channels between the different AcS components and protocols used.

REDACTED



Figure 40: AcS Network Security Topology

4.4. Communication Channel Security

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

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

4.5. AcS Inter-component Communications

The following table displays the necessary port communications and protocols used for each component-based server. The ports described must be open for both inbound and outbound communications.

Table 25: Port Communications and Protocols

Application	Network	Port(s)	Reason	Protocol(s)
Oracle Database	Internal	1521	Oracle SQL Net Listener	TCP
		1525	DataGuard	TCP
		1630	Connection Manager	TCP
		3938	Oracle Management Agent	TCP
		1158	Oracle Enterprise Database Console (HTTP Port)	HTTP
		5520	Oracle Enterprise Database Console (RMI Port)	TCP
		5540	Oracle Enterprise Database Console (JMS Port)	TCP

Application	Network	Port(s)	Reason	Protocol(s)
		6789	Agent command and control listening port	TCP
		17001	CA UARM collection server	TCP
CA Directory (CSP/IP, Provisioning)	Internal	20391	Provisioning router dsa	TCP
		20394	Provisioning main dsa	TCP
		20396	Provisioning common objects dsa	TCP
		20398	Provisioning inclusions dsa	TCP
		20404	Provisioning notify dsa	TCP
		8443	DXWebserver Listener (SSL)	HTTPS
		8005	DXWebserver Listener for shutdown command	TCP
		2123	Dxmanager-DXadmin communication	TCP
		636	CSP/PROV/SMPS Router DSA	LDAPS
		30636	CSP Data DSA	LDAPS
		40636	SMPS Data DSA	LDAPS
		50636	PROV Data DSA	LDAPS
		2125	DXadmin Secure LDAP	TCP
		6789	Agent command and control listening port	TCP
		17001	CA UARM Collection Server	TCP
Web Tier IIS Servers (CSP WebUI, IP WebUI, Provisioning WebUI)	DMZ	44441	Accounting port	TCP
		44442	Authentication port	TCP
		44443	Authorization port	TCP
		44444	Auditing Port	TCP
		443	SSL port for reverse proxy	HTTPS
		6789	Agent command and control listening port	TCP
		17001	CA UARM Collection Server	TCP
CA Report Server	Internal	7002	WebLogic Port for Report Server	HTTPS
		6400	Central Management Console Server Port	TCP
		6789	Agent command and control listening port	TCP
		17001	CA UARM Collection Server	TCP

Application	Network	Port(s)	Reason	Protocol(s)
Federation Option Pack	DMZ	8888	ServletExec port for listening incoming requests from IIS	TCP
		6789	Agent command and control listening port	TCP
		17001	CA UARM Collection Server	TCP
CA Identity Manager (CSP/IP, Provisioning)	Internal	8002	Administration Port	HTTPS
		8112	Manage Server Port	TCP
		5556	Node Manager	TCP
		6789	Agent command and control listening port	TCP
		17001	CA UARM Collection Server	TCP
Provisioning Server	Internal	20390	Provisioning Server	TCP
		6789	Agent command and control listening port	TCP
		17001	CA UARM Collection Server	TCP
CA SiteMinder	Internal	44441	Accounting port	TCP
		44442	Authentication port	TCP
		44443	Authorization port	TCP
		44444	Auditing Port	TCP
		443	SSL port for reverse proxy	HTTPS
		8002	WebLogic port for SiteMinder Admin UI	TCP
		6789	Agent command and control listening port	TCP
		17001	CA UARM Collection Server	TCP
CA Siteminder SPS	DMZ/Internal	80	Apache HTTP Port	HTTP
		443	Apache SSL port	HTTPS
		8080	Tomcat/ SPS HTTP Port	HTTP
		543	Tomcat/SPS SSL Port	HTTPS
CA UARM	Internal	5250	Administration Port for CA UARM	TCP
		443	SSL Port (reverse proxy to administration port 5250) for CA UARM	HTTPS
		514	Syslog port (UDP) for CA UARM server	TCP
		1468	Syslog TCP listening port for CA UARM	TCP

Application	Network	Port(s)	Reason	Protocol(s)
		6789	Agent command and control listening port	TCP
		17002	Communication port for ODBC /JDBC driver	TCP
		111	Audit client communication with port-mapper	TCP
		57000	Dispatcher SME listener	TCP
		2123	CA Directory LDAP DXadmin port (CA Directory bundled with CA UARM)	TCP
		57001	Dispatcher Service in SSL mode for events from Client Connector	TCP
CA SSO Server	Internal	445	Port for ticket granting agent (Windows Authentication Agent)	TCP
		8891	Access Control port bundled with CA SSO	TCP
		13389	LDAP communication port for CA Directory bundled with CA SSO for user directory	LDAPS
		13390	LDAP communication port for CA Directory bundled with CA SSO for token directory	LDAPS
		13981	TCP SSL port where the SSO Server will listen.	TCP
		6789	Agent command and control listening port	TCP
		17001	CA UARM Collection Server	TCP
DataPower XI50	Internal	443	SAC Service (PDP)	HTTPS
		9090	Administration port	TCP
ARX CoSign	Internal	8080	API Calls	HTTPS
eSig WebLogic	Internal	8002	Administration Port	HTTPS
		8112	Manage Server Port	TCP
		5556	Node Manager	TCP
Radiantlogic VDS	Internal	2636	LDAP SSL port	LDAPS
		4848	Application server Admin Port	HTTP
		9090	Application server HTTP Port	HTTP
		9191	Application server HTTPS port	HTTPS

Application	Network	Port(s)	Reason	Protocol(s)
		8686	Application server JMX port	TCP
		7070	Control Panel Web server port	HTTP
		7171	Control Panel Web server Port	HTTPS
		443	Web Services Port	HTTPS
Axiomatics	Internal	8080	HTTP Connector Port	HTTP
		8009	AJP Connector Port	TCP
		8005	Server Shutdown Port	TCP
		8443	HTTPS Connector Port	HTTPS

Table 26 and Table 27 below provide the AcS solution inter-component communications details.

Table 26: Pre-Production PKI Certificate List

Computer Name (Hostname)	Common Name (CN)	FQDN	Cert Type	Issuer	Cert Function	Description	Comments
REDACTED	REDACTED	REDACTED	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	
REDACTED	REDACTED	REDACTED					
			Internal	VA	Device	DataPower (SAC)	
			Internal	VA	Web URL	Data Power Mgmt. (SAC)	
			Internal	VA	Web URL	DataPower (SAC)	
			Internal	VA	Web URL	Data Power Mgmt. (SAC)	
			Internal	VA	Web URL	Siteminder SPS	
			External	VA	Web URL	Siteminder WSS	
			Internal	VA	Web URL	Siteminder WSS	
			Internal	VA	Web URL	PIV authentication	

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

Computer Name (Hostname)	Common Name (CN)	FQDN	Cert Type	Issuer	Cert Function	Description	Comments
<div>REDACTED</div>							
			Internal	VA	SSL	CA Directory	Management
			Internal	VA	Web Service	CA Directory	LDAPS
			Internal	VA	SSL	CA Directory	Management
			Internal	VA	Web Service	CA Directory	LDAPS
			Internal	VA	SSL	CA Directory	Management
			Internal	VA	Web Service	CA Directory	LDAPS
			Internal	VA	SSL	CA Directory	Management
			Internal	VA	Web Service	CA Directory	LDAPS
			Internal	VA	SSL	CA SSO	SSL listener
			Internal	VA	Web Service	CA SSO	SSL listener
			Internal	VA	Web Service	CA SSO	LDAPS with CA Directory
			Internal	VA	SSL	CA SSO	SSL listener
			Internal	VA	Web Service	CA SSO	SSL listener
			Internal	VA	Web Service	CA SSO	LDAPS with CA Directory

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

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

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

4.5.1. Production Server PKI Certificate List

Table 27: Production Cert List

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

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

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

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

Computer Name (Hostname)	Common Name (CN)	FQDN	Certificate Type	Issuer	Cert Function	Comments
<div>REDACTED</div>						
			Internal	VA	SSL	Management
			Internal	VA	Web Service	LDAPS
			Internal	VA	SSL	Management
			Internal	VA	Web Service	LDAPS
			Internal	VA	SSL	Management
			Internal	VA	Web Service	LDAPS
			Internal	VA	SSL	
			Internal	VA	Web Service	SSL listener
			Internal	VA	Web Service	LDAPS with CA Directory
			Internal	VA	SSL	
			Internal	VA	Web Service	SSL listener
			Internal	VA	Web Service	LDAPS with CA Directory
			Internal	VA	URL	
			Internal	VA	Server	

Computer Name (Hostname)	Common Name (CN)	FQDN	Certificate Type	Issuer	Cert Function	Comments
REDACTED			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	
			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

Computer Name	Common Name (CN)	FQDN	Certificate Type	Issuer	Cert Function	Comments
<div>REDACTED</div>			Internal	VA	SSL	Management
			Internal	VA	Server	Also serve as auditing cert
			Internal	VA	SSL	Management
			Internal	VA	Server	Also serve as auditing cert
			Internal	VA	SSL	Management
			Internal	VA	Server	Also serve as auditing cert
			Internal	VA	SSL	Management
			Internal	VA	SSL	WebLogic port
			Internal	VA	SSL	WebLogic port
			Internal	VA	SSL	WebLogic port
			Internal	VA	SSL	WebLogic port
			Internal	VA	Device	
			Internal	VA	Device	

5. Data Design

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

5.1. DBMS Files

The AcS solution uses Oracle 11gR2 Database and CA Directory for persistent data storage. The Oracle database “ACSDb” will be 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

Table 28: 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

5.2. Non-DBMS Files

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

- **CSP, IP, and Provisioning:** User store schema within CA Directory is customized to store registered user record information (refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions).
- **CAR:** Stores data in UARM logs and leverages information present in AcS activities and integrated applications for reporting (refer to [section A.1](#) below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions).


6. Detailed Design

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

6.1. Hardware Detailed Design

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

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

20131108  AcS
IAM TerreMark
PreProd a

6.2. Software Detailed Design

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

6.2.1. Provisioning Conceptual Design

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

The Provisioning activity provides centralized management of user account creation, termination, and modification for VA applications. It provides VA users a means to initiate

self-

service requests for account creation and modification for integrated applications, then automatically route the provisioning request to the designated Approver. Once approved, accounts will be provisioned automatically.

Figure 41 below provides a conceptual 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.

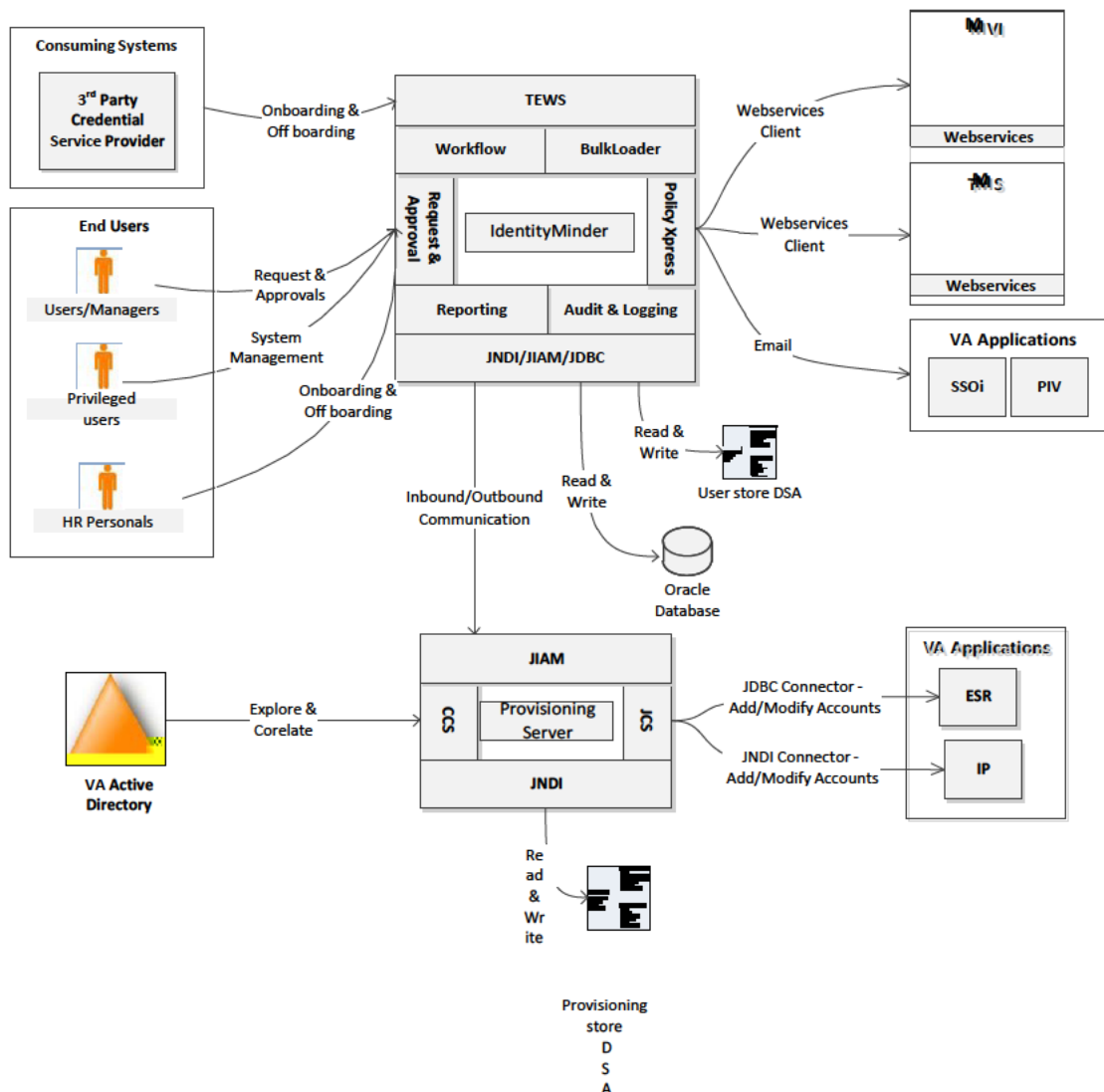


Figure 41: Provisioning Detail Design

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 if a user already exists in the system by searching for a user before user is added and a unique identifier SEC ID is issued

- **Active Directory:** The user accounts will be correlated to the IdentityMinder global user based on SAM Account name and an 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 Web logic application server cluster, which implements the provisioning activity. It is integrated with SiteMinder providing SSO capability and supporting access control to VA users for accessing the registration features. The major modules of CA IdentityMinder implemented for VA include the following:

- **Workflow:** A feature that helps control the flow of provisioning and de-provisioning across the VA enterprise. For the AcS solution, it is mostly used for approvals and delegations.
- **Policy Express:** Policy Express helps to create complex business logic (policies) without the need to develop custom code
- **Task Execution Web Services (TEWS):** A web service interface that allows third-party applications to submit remote tasks to CA IdentityMinder for execution.
- **Provisioning server:** Provisioning engine of the architecture, which acts as a broker between IdentityMinder and Connector server
- **Connector Server:** Endpoint server which connects with various endpoints for provisioning and de-provisioning

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

6.2.1.1. Provisioning: User Onboarding

Field	Description
Use Case Name	User CRISP Onboarding
Description	This use case describes the process by which a new VA Employee/Contractor is on boarded.
Actors	1. Provisioning Service 2. HR/Sponsor/COR 3. VA Manager 4. TMS 5. MVI 6. Account Administrators
Pre-Conditions	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

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

Field	Description
Sequence Diagram	
Main Success Scenarios	<ol style="list-style-type: none"> 1. Successful generation of Sec ID for VA employee/contractor 2. Creation of VA employee/contractor in provisioning system with Sec ID as unique identifier
Main Failure Scenarios	<ol style="list-style-type: none"> 1. Sec ID creation process error out 2. Failure in creation of user in provisioning system

6.2.1.2. Provisioning: Third-Party / CAC 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 3 rd party or CAC user
Actors	<ol style="list-style-type: none"> 1. Provisioning Service 2. VA / External System 3. CA IdentityMinder 4. MVI
Pre-Conditions	<ol style="list-style-type: none"> 1. The VA system have appropriate access privileges to access provisioning service to onboard user
Trigger	<ol style="list-style-type: none"> 1. The VA / External System calls Provisioning service for on boarding
Actions	<ol style="list-style-type: none"> 1. The VA / External System calls Provisioning web service function VATHirdPartyOnboardUserProfile to initiate onboarding of end user (3rd party or CAC) 2. The VA / External System passes the primary user traits to CA IdentityMinder system for user creation 3. CA IdentityMinder makes a call to MVI, to check the existence of the record 4. If the user record exists with corresponding Sec ID, then the CA

Field	Description
	<p>IdentityMinder creates a new identity record with the SEC ID returned from MVI and correlates it to the MVI record</p> <ol style="list-style-type: none"> 5. If the user record exists without an associated SEC ID, then the CA IdentityMinder generates the SEC ID and initiates an “Add Person” and correlates it to the MVI record 6. If the user does not exists in MVI, then the CA IdentityMinder generates the SEC ID and call the “Add Person-implicit” MVI service to create an identity record within the MVI System and correlates the SEC ID to that record 7. The user will be created in the user store of provisioning system 8. Provisioning system sends a response to the VA system on the status of the operation
Sequence Diagram	
Main Success Scenarios	<ol style="list-style-type: none"> 3. Successful generation of Sec ID for third party user 4. Creation of third party user in provisioning system with Sec ID as unique identifier
Main Failure Scenarios	<ol style="list-style-type: none"> 3. Sec ID creation process error out 4. Failure in creation of user in provisioning system

6.2.1.3. Provisioning: User Offboarding

Field	Description
Use Case Name	User Offboarding
Description	This use case describes the process by which an existing VA Employee/Contractor is off boarded.
Actors	<ol style="list-style-type: none"> 1. Provisioning Service 2. HR/Sponsor/COR 3. VA Manager 4. TMS 5. Account Administrators
Pre-Conditions	<ol style="list-style-type: none"> 1. All the human actors have appropriate access privileges in provisioning service to perform the actions
Trigger	<ol style="list-style-type: none"> 1. VA Employee/Contractor provides notice for separating from employment to VA Manager. 2. VA Manager/Sponsor is notified of breach of rules by VA Employee

Field	Description
Actions	<ol style="list-style-type: none"> 1. Requester with proper privileges login to CA IdentityMinder to initiate user off boarding process 2. Requestor access the appropriate form to submit a request for off boarding a user 3. Workflow associated with the task gets triggered and appends a work item to the HR/Sponsor/COR queue. 4. Workflow sends an email to the HR/Sponsor/COR to Approve/Reject the off boarding of user to the provisioning system 5. 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 6. 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 7. Provisioning system will de provision accounts for managed endpoints via connector server 8. User is deactivated in the user store and roles / group membership are updated accordingly
Sequence Diagram	
Main Success Scenarios	VA employee/contractor is deactivated in the provisioning system Associated accounts of VA employee/contractor are removed from the VA applications
Main Failure Scenarios	Error during deactivation of VA employee/contractor in the provisioning system

6.2.1.4. 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.

Field	Description
Actors	<ol style="list-style-type: none"> 1. Provisioning Service 2. Employee/Contractor 3. VA Manager 4. Account Administrators
Pre-Conditions	<ol style="list-style-type: none"> 2. 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 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
Sequence Diagram	
Main	VA employee/contractor is provisioned to the requested VA application

Field	Description
Success Scenarios	
Main Failure Scenarios	VA employee/contractor is not provisioned to the requested VA application

6.2.1.5. 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 2. Employee/Contractor 3. VA Manager 4. Account Administrators
Pre-Conditions	<ol style="list-style-type: none"> 1. All the human actors have appropriate access privileges in provisioning service to perform the actions
Trigger	<ol style="list-style-type: none"> 2. VA Employee/Contractor transfers from one organization unit to another 3. VA Employee/Contractor job function is changed
Actions	<ol style="list-style-type: none"> 1. Requester with proper privileges login to CA IdentityMinder to request de-provisioning of a to a managed endpoint 2. Requestor accesses the access request form and submits a request for de-provisioning an access 3. Workflow associated with the task gets triggered and appends a work item to the appropriate approver's queue 4. Workflow sends an email to the approver to Approve/Reject the provisioning request 5. Approver logs into CA IdentityMinder and selects the work item specific to the access request and validates the user data and approves the request to revoke access from the endpoint 6. If the endpoint is not managed through CA IdentityMinder, a policy express script associated with the task gets triggered and corresponding emails will be sent to account administrators of the endpoint to de-provisioning the access 7. If the endpoint is managed through CA IdentityMinder, then CA IdentityMinder evaluates the requested role and calls the Provisioning Server to de-provision the access. 8. Provisioning Server connects with the appropriate connector server and connects to the endpoint and de-provision the request privileges

Field	Description
Sequence Diagram	
Main Success Scenarios	VA employee/contractor is de-provisioned from the requested VA application
Main Failure Scenarios	VA employee/contractor is not de-provisioned from the requested VA application

6.2.1.6. Explore and Correlate from Endpoints

Field	Description
Use Case Name	Explore and Correlate from Endpoints
Description	This workflow describes the technical activities and associated data exchanges through which user identity record is explored and correlated with integrated endpoints.
Actors	<ol style="list-style-type: none"> 1. Provisioning Service 2. Employee/Contractor 3. VA Manager 4. Account Administrators
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 all 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

Field	Description
	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
Sequence Diagram	
Main Success Scenarios	The identities from the VA application are explored and correlated successfully
Main Failure Scenarios	Failure to run the explore and correlate job

6.2.2. SSOi Conceptual 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.

Figure 42 below provides a conceptual view of the SSOi activity.

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.

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.

6.2.2.1. SSOi Support for LOA 2/3/4

Field	Description
Use Case Name	Authentication support for Level of Assurance (LOA 2/3/4)
Description	This use case describes the process through which a user authenticates to the SSOi service using approved LOA 2/3/4.
Actors	1. Internal Users 2. SSOi 3. Centralized Logon Page 4. SSOi Integrated Application(s)
Pre-Conditions	User has valid credential for each type of authentication method and tries to access the protected application.

Field	Description
Trigger	The internal user tries to access the application protected by SSOi.
Actions	<p>Centralized Log On page with Windows Authentication</p> <ol style="list-style-type: none"> 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. Collects the NTLM V2/Kerberos credentials 5. 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 8. SSOi creates SiteMinder Token and then Notifies Windows Authentication Logon Server 9. The Logon server redirects the user to application <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. Authenticate and authorize user against Active Directory 8. Create SiteMinder Token 9. User is authenticated and authorized to access the resource 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.

Field	Description
	<p>9. CA SiteMinder verifies that the certificate credentials and the basic credentials represent the same user.</p> <p>10. If the user is authorized to access the resource, the PIV Logon server redirects the user to application</p> <p>Centralize Page With PIV Only authentication (LOA4)</p> <ol style="list-style-type: none"> 1. SSOi Web Agent Intercepts the user request to access integrated application 2. The Web Agent verifies it with Policy Server if the application is protected by higher level 10 authentication. 3. If the resource is protected Web Agent redirects to centralized PIV log on page where a user can hit login button to login using PIV card. 4. Central login server sends the requests to PIV logon server. 5. PIV Logon prompts to select Client certificate 6. The user selects the client certificate and enters the PIN 7. The SSL server maps the user's certificate to the server 8. PIV certificate authentication happens at the TLS layer, higher authentication level (10) configured on policy server 9. CA SiteMinder verifies the user exists. 10. CA SiteMinder verifies the user's basic credentials. 11. CA SiteMinder verifies that the certificate credentials and the basic credentials represent the same user. 12. if the user is authorized to access the resource, the PIV Logon server redirects the user to application
Sequence Diagram	

Field	Description

Field	Description
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 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/Passwd uthentication 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.

6.2.2.2. CAC SSOi Integration with VAAFI

Field	Description
Use Case Name	CAC-SSOi Integration Flow
Description	This use case describes the process by which an SSOi User performs SSO to

Field	Description
	one or more integrated application.
Actors	<ol style="list-style-type: none"> 1. CAC User 2. VAAFI 3. SSOi Integrated Application(s)
Pre-Conditions	<ol style="list-style-type: none"> 1. The SECID which will be received from VAAFI and will be available as correlated attribute in Provisioning store 2. A valid CAC card user access the SSOi protected application through Access VA
Trigger	External CAC User initiates the application session by clicking on the target application from Access VA
Actions	<ol style="list-style-type: none"> 1. An external CAC user accesses an SSOi service provider via public URL. 2. The user will be redirected to IdP 3. The IdP will authenticate the external user and generate the SAML assertion with user attributes (SECID, Firstname, Lastname, EDIPI, email, target). 4. VAAFI SAML service posts the generate SAML Assertion to the SSOI SAML Assertion Consumer URL. 5. SSOI SAML Consumer server makes a call to the SiteMinder Policy server to validate SAML assertion. 6. SM Policy server validates SAML assertion by verifying the digital signature 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, Lastname, EDIPI, and email address. 9. If the user is valid, Policy server creates the SM token and redirect to the target application with all required header variables.
Sequence Diagram	

Field	Description
Main Success Scenarios	User is authenticated and Application is presented to the user.
Main Failure Scenarios	In the event of an exception or error during attribute consumption default SAML assertion error will be generated and returned it to VAAFI All the failure scenarios like Session timeout, authentication and authorization failures will covered on the external integrations with VAAFI as this would specific for the application integration

6.2.2.3. SSOi Mobility Support

Field	Description
Use Case Name	SSOi Mobility Support
Description	This use case describes the process by which SSOi user performs authentication through mobile devices. Mini and SM Session cookies are supported.
Actors	1. Mobile User 2. SSOi Integrated Application(s)
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. A User accesses the application URL through a mobile device 2. CA Secure proxy server intercepts the requests and check for the mini cookie availability 3. If http Session cookie is valid then it 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

Field	Description
	<ol style="list-style-type: none"> 5. Policy server validates the credentials by verifying it against user directory 6. After user validation completed 7. Redirect to Mobile application 8. Present 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 authentication method configured for that specific application 3. User enters credentials 4. Policy server validates the credentials 5. Verify the credentials against user directory 6. Receive valid user response 7. After user validation completed 8. Redirect to the application 9. SPS creates and sets the http Session 10. Pass the control to the application. 11. 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. 2. Authentication Web service validates the credentials 3. Validate against policy server/user store. 4. Receive validated user notification 5. If successful then mini session cookie is returned as part of response code 6. Application call Authorization service to get permit /deny response from Authorization web service else fail result code is returned as response
Sequence Diagram	

Field	Description
Main Success Scenarios	User is authenticated successfully and application is presented to the user
Main Failure	<ul style="list-style-type: none"> Default failed UserId/Passwd uthentication will redirect the user to the

Field	Description
Scenarios	<p>centralized log Username/Password page but can be customized to redirect to any application page based on the policies.</p> <ul style="list-style-type: none"> • Default failed UserID/Password authorization will redirect the user to centralized login page but can be customized to redirect to any application page based on the policies. • For Native Since it utilizing the SSOI web service the error codes are mentioned in the table 6.2.2.11

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

Field	Description
Use Case Name	Federation Identity Provider (IdP) and Service Provider (SP) Services
Description	This use case describes the process by which a federated user is authenticated to the SSOi activity.
Actors	<ol style="list-style-type: none"> 1. Internal Users 2. SSOi 3. SSOi Integrated Applications
Pre-Conditions	A valid integration/trust between Identity Provider (IdP) and Service Provider (SP)
Trigger	User Access application protected with SAML federation authentication mechanism
Actions	<p>Identity Provider (IdP) – Without a Valid Session Cookie</p> <ol style="list-style-type: none"> 1. An internal user accesses an application (IdP-protected URL) which is at service provider without a SiteMinder session cookie. 2. User redirected to centralized log on page and prompted for authentication credential 3. User enters the credentials 4. Validated against SiteMinder Policy server/User store. 5. Authentication and Authorize the user 6. Communicate validated user to SiteMinder Policy Server 7. Redirect to SAML URL 8. SiteMinder Policy server generates the SAML Assertion by: 9. Adding all the required attributes such as user Principal Name (UPN), email , firstname and lastname 10. IdP posts the SAML assertion to the Service Provider SAML Assertion Consumer service: 11. Generate HTML Form Post with SAML assertion 12. Redirect with HTML form post response 13. Post to SAML assertion to Service Provider 14. Service provide Consumes the SAML assertion generated by SSOi and grants

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

Field	Description
Sequence Diagram	

Field	Description
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. <p>VA as SP:</p> <ul style="list-style-type: none"> • All the failure scenarios like Session timeout, authentication and authorization failures are covered on the external integrations.

6.2.2.5. WS Federation for Internal Users

Field	Description
Use Case Name	WS Federation for Internal Users
Description	This use case describes the process by which a user gets seamless access to the Relying partner application using WS trust.
Actors	<ol style="list-style-type: none"> 1. Internal Users 2. SSOi 3. SSOi Integrated Application(s)
Pre-Conditions	A valid WS integration/ trust between Identity 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. Redirect 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 with attributes such as user Principal Name (UPN), email , firstname, lastname 12. Notify Web Agent 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. Validate WD-FED 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 9. Validate WD-FED

Field	Description
	10. Redirect to Target Application
Sequence Diagram	
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-Fed assertions.

6.2.2.6. SSOi Support for Attribute Service

Field	Description
Use Case Name	SSOi Support for Attribute Service
Description	This use case describes the process by which SiteMinder calls the attribute service from VDS during authorize policy evaluation.
Actors	<ol style="list-style-type: none"> 1. Users 2. SSOi 3. SSOi Integrated Application(s)

Field	Description
Pre-Conditions	A valid WS integration/ trust between Identity and Relying partner
Constraints	SSOi will be depend the capability of VDS attribute service capability to get appropriate attributes
Trigger	User authenticated with SSOi and needs specific attributes from VDS
Actions	<ol style="list-style-type: none"> 1. User authenticates in to SSOi 2. Redirect to Logon Server 3. Prompt for Credentials 4. User enters credentials 5. Authentication and authorize user against user store 6. SiteMinder session token is generated 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.
Sequence Diagram	
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.

6.2.2.7. SSOi Proxy Authentication Request

Field	Description
Use Case Name	SSOi Proxy Authentication Request
Description	This use case describes the process by exchanges which SiteMinder offers proxy capability for the authentication request. The centralized login page will be integrated with SPS for implementing SSOI using multiple authentication methods

Field	Description
	(LOA2, LOA3, LOA4).
Actors	<ol style="list-style-type: none"> 1. Users 2. SSOi 3. SSOi Integrated Application(s)
Pre-Conditions	All application access requests go through SPS
Trigger	User accesses application protected and proxy through SPS
Actions	<ol style="list-style-type: none"> 1. The user access to the application which proxy through Secure proxy server 2. The Secure proxy Server verifies the policy server to check the resource is protected 3. If the resource is protected SPS prompts the user for credentials 4. User submits credentials 5. Secure proxy server validates the credentials with policy server 6. Authenticate and authorize user against User Store 7. Policy server sets the cookie and passes control back to SPS 8. Secure Proxy Server invokes proxy engine and passes control to the application
Sequence Diagram	
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.

6.2.2.8. Responses to Produce WS-Security Headers

Field	Description
Use Case	Responses to Produce WS-Security Headers

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

Field	Description
Main Failure Scenarios	SOAP fault with authentication failure message returned to client in case of validation of user credential fail

6.2.2.9. Responses to XML Encryptions, Decryptions, and Digital Signature

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

Field	Description
Sequence Diagram	
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

6.2.2.10. Session Management

Field	Description
Use Case Name	Session Management
Description	This use case describes the process by which SiteMinder manages session tokens.
Actors	<ol style="list-style-type: none"> 1. Users 2. Client 3. Web Service
Trigger	<ol style="list-style-type: none"> 1. User stays idle (more than 60 minutes) after getting access to the application. 2. User clicks log out button available in the application
Pre-Conditions	A user has a valid single sign-on token
Actions	<p>SSOi Session idle time out</p> <ol style="list-style-type: none"> 1. A user logs in to the SiteMinder protected application 2. Validate the SiteMinder Cookie 3. Send session specs to Policy Server 4. Policy Server evaluates the session time set for each authorization 5. If the user idles greater than the time out set on SSOi policy it will log out the user 6. Redirect to the Logon page for re-authentication <p>Limit refresh session token</p>

Field	Description
	<ol style="list-style-type: none"> 1. A user logs in to the SiteMinder protected application 2. Validate the SiteMinder Cookie 3. Send session specs to Policy Server 4. SiteMinder evaluates the max session time set for each authorization request 5. If the user session is greater than the max time out set on policy, it will log out the user 6. Prompt for the authentication again <p>SSOi Session Logout</p> <ol style="list-style-type: none"> 1. A user clicks log out on SiteMinder protected application 2. Validate the session cookie 3. Web agent calls logout method call to policy server 4. Policy Server clears all the session cookie 5. Web agent redirected it to log on page
Sequence Diagram	
Main Success Scenarios	Session management policy is enforced
Main Failure Scenarios	N/A

6.2.2.11. STS Support

Field	Description
Use Case	STS Support

Field	Description
Name	
Description	This use case describes the process through which SiteMinder translates various session tokens and service interfaces for the end user.
Actors	<ol style="list-style-type: none"> 1. Users 2. Client 3. Web Service
Pre-Conditions	A user has a valid single sign-on token
Trigger	Client accesses a web service endpoint protected by SOA agent
Actions	<p>Session translation</p> <ol style="list-style-type: none"> 1. A user logs in to the application using PIV card and PIN 2. User moves to application accepting different Token –e.g. SAML token - PIV protected applications requests access to U/P protected application 3. Send the SiteMinder token for validation 4. SiteMinder generates a SSO token to provide access to the application 5. Policy server translates SSO token in to the SAML assertions ** 6. Evaluate the policy and session specs 7. Authorize the user 8. Translate SiteMinder session specs with application session policy 9. Provide the access to user seamlessly 10. Return the updated session spec 11. Update the session cookie 12. Grant the user access to the application 13. **Token supported by SSOi for the above translation are – SAML, WS FED, NTLMV2,Kerberos, SAML,U/P, PIV <p>SSOi Web service</p> <p>Authentication Web service</p> <ol style="list-style-type: none"> 1. Client formulate a REST/SOAP base request to SiteMinder Authentication web service with ApplID, resource string , action, user credential as inputs 2. SiteMinder detects the request and passes it to the endpoint. 3. SiteMinder web service validates the user credentials based on the policy configuration 4. Evaluate the login 5. Pass the credentials to the user store 6. Validate the credentials 7. Return the session specs 8. Return response code as SSOi session token as back to the client. 9. Send the SOAP authenticated response 10. Receive updated SOAP response with user session <p>Authorization Web service</p> <ol style="list-style-type: none"> 1. Client formulate a REST/SOAP base request to SSOi Authorization web

Field	Description
	<p>service with AppID, resource string , action, Session token as inputs</p> <ol style="list-style-type: none"> 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. Authorize 5. Get session attribute from SOAP request 6. Authorize user against user store 7. Return updated session specs if valid 8. Return the result code and updated SSOi session token as response code back to the client. 9. Send the SOAP authentication response with the status message 10. Receive updated SOAP response with user session
Sequence Diagram	

Field	Description
Main Success Scenarios	<ol style="list-style-type: none"> 1. User is authenticated 2. Application is presented to the user
Main Failure Scenarios	<ol style="list-style-type: none"> 3. The Authentication web service will return Authentication failure in case of wrong user ID and Password. 4. The Authorization web service will return Access denied error message when Authorization failure occurs. 5. Any communication error at service end point will result in SOAP /REST fault codes as response <p>Web service methods throws below error message upon failure authentication –</p> <p>Sample message for login()</p> <pre><message>Authentication Failed</message> <resultCode>LOGIN_FAILED</resultCode></pre> <p>Sample message for Authorize()</p> <pre><message>Authorization Failed</message> <resultCode>NOTAUTHORIZED</resultCode>.</pre>

6.2.2.12. Centralized Login Page

In order 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.

The central 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 user is provided 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 is displayed.
7. If user submits user ID and password, the request is sent 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 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 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 to access the resource then a token is generated
12. SSOi creates SiteMinder Token and redirects the user to application

6.2.3. CSP Conceptual 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

Figure 43 below provides a conceptual view of the complete CSP system at VA and its interaction with VAAFI and other actors.

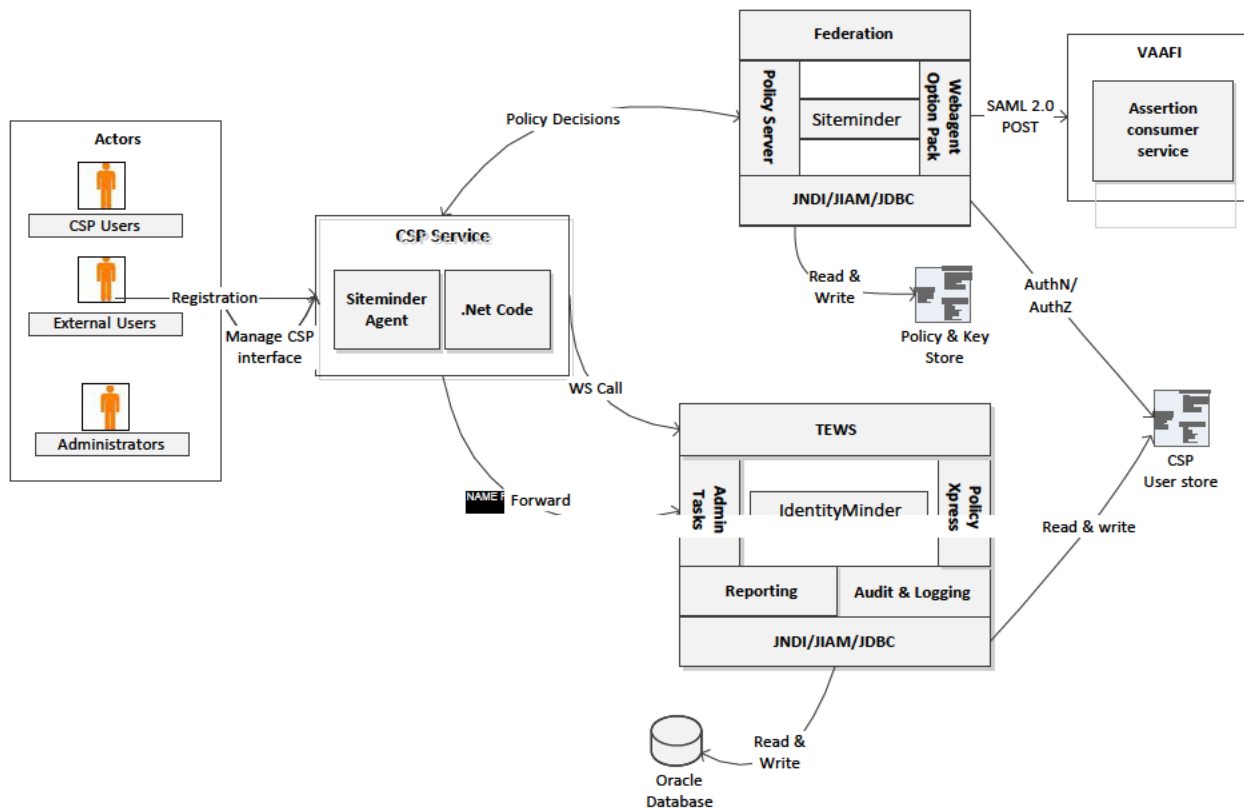


Figure 43: CSP Detailed Design

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

6.2.3.1. Credential Issuance

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

Field	Description
Sequence Diagram	
Actions	<ol style="list-style-type: none"> 1. External user access the CSP service landing page 2. Navigate to the registration page and initiate the self-registration process for requesting a LOA 1 or LOA 2 3. Provide all 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

6.2.3.2. Revoke/Reissue Credential

Field	Description
Use Case Name	Credential Issuance
Description	This workflow describes the technical activities and associated data exchanges through which CSP user credential is revoked or reissued.
Actors	1. CSP Service 2. CSP Service administrator
Pre-Conditions	CSP Service administrator have the required access to perform the credential revoke/reissue function
Trigger	Credential revocation/ reissue request received from a trusted partner system
Sequence Diagram	Third-Party 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

6.2.3.3. Federation with VAAFI

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
Sequence Diagram	
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 store is 6. The user is successfully authenticated and authorized. 7. SiteMinder federation option pack generated a SAML 2.0 token with assurance level of the user as an attribute 8. The option pack redirects the user with a SAML POST to VAAFI 9. VAAFI consumes the SAML token and based on the assurance level (LOA 1 or LOA2) it displays the list of application the user can access

Field	Description
Main Success Scenarios	Successfully single sign on to VAAFI application
Main Failure Scenarios	Failure to Single Sign on to VAAFI application

6.2.4. IP Conceptual Design

The IP processes used by Government and commercial entities to establish the required level of assurance vary widely based on the target subject population, the purpose of the resulting identity proofed record, etc. A common goal for each of these identity proofing processes is to allow the enterprise to comply with legal, regulatory and due diligence requirements based on one or more of the following references FIPS 201¹, HSPD-12², OMB A-130, Appendix I³, VA Information Security Policies and Directives (e.g. VA Handbook 6500, Appendix F), NIST SP800-63⁴, and others, before the enterprise can interact with the subject, do business transactions or issue credential(s) and/or account(s) to said subject.

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

Table 29 below, as defined in OMB M04-04⁶, is referenced to the NIST SP 800-63 Identity proofing processes and drives their scope and extensiveness.

¹ **HYPERLINK REDACTED**

■ **REDACTED**

■ **REDACTED**

■ **REDACTED**

■ **REDACTED**

■ **REDACTED**

■ **REDACTED**

Table 29: Potential Impact Categories for Authentication Errors

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

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

Figure 44 below provides the conceptual view of complete IP system at VA and its interaction with various systems and actors.

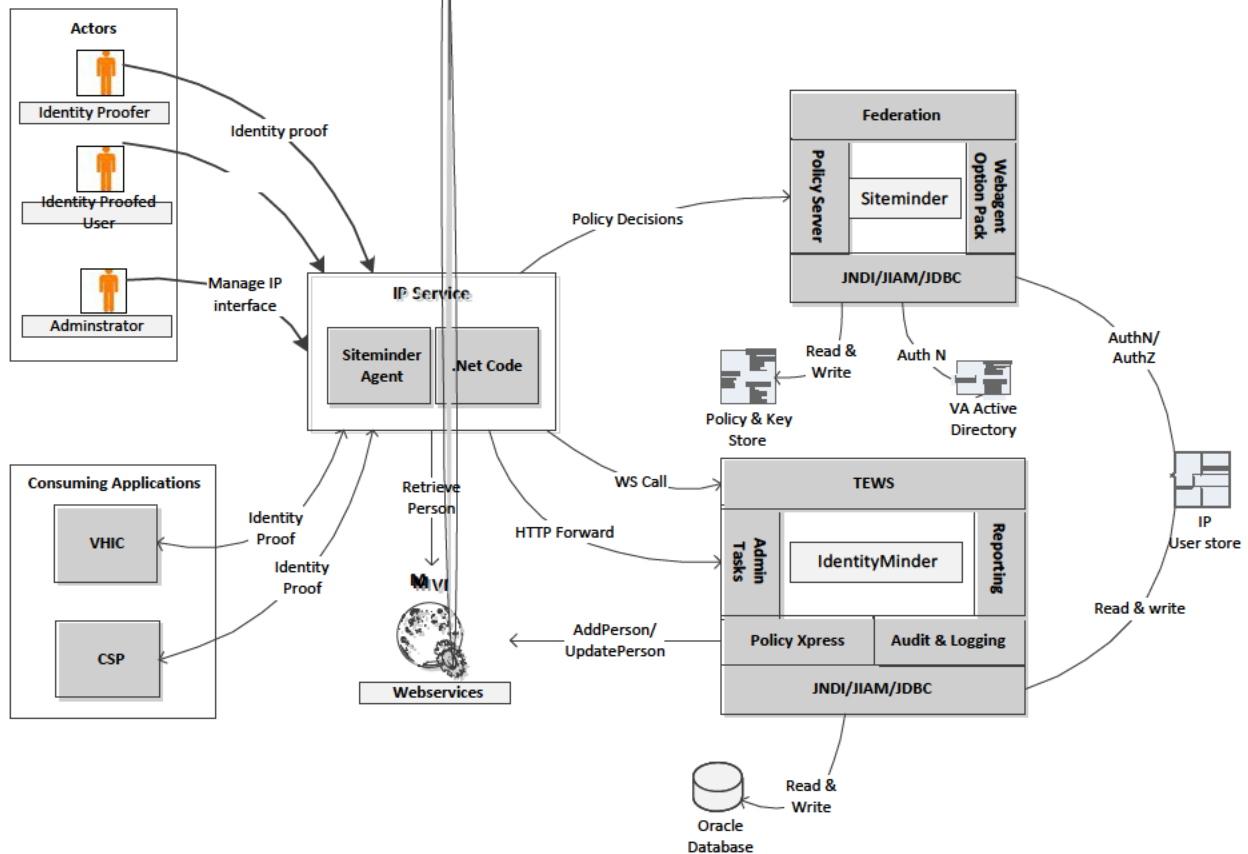


Figure 44: IP Conceptual Design

CA IdentityMinder:

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

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

IP Service:

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

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

6.2.4.1. Identity Proof a User

Field	Description
Use Case Name	Identity Proof a User
Description	This use case describes the process by which a person or a system with the role of Identity Proofer or higher can perform an in-person identity proofing.
Actors	1. IP Service 2. Identity Proofer/System 3. CSP TEWS Web services 4. CA Identity Minder
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	1. Identity Proofer logs into IP service 2. Identity proofer initiate an identity proof task on the IP service 3. IP service presents the user with a search screen 4. Identity Proofer enters the user information based on the primary and secondary identification document provided by the CSP user 5. IP service calls the CSP TEWS Web services 6. Searches for the user from CSP store 7. Displays search results in the IP service 8. Identity Proofer enters needed details about the CSP user, as part of proofing and submits the record

Field	Description
	9. IP service calls the CSP TEWS Web services to update the user's assurance level 10. CSP service updates the user credential level at the CSP user store 11. IP services creates the user profile in the IP user store
Sequence Diagram	
Main Success Scenarios	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

6.2.4.2. Create Proofing Record

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

Field	Description
	<ol style="list-style-type: none"> 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
Sequence Diagram	
Main Success Scenarios	Created of LOA 2 user in Identity Proofing system
Main Failure Scenarios	Error during create proofing record

6.2.5. SAC Conceptual 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.

Figure 45 below provides a conceptual view of the complete SAC system at VA and its interaction with various systems and actors.

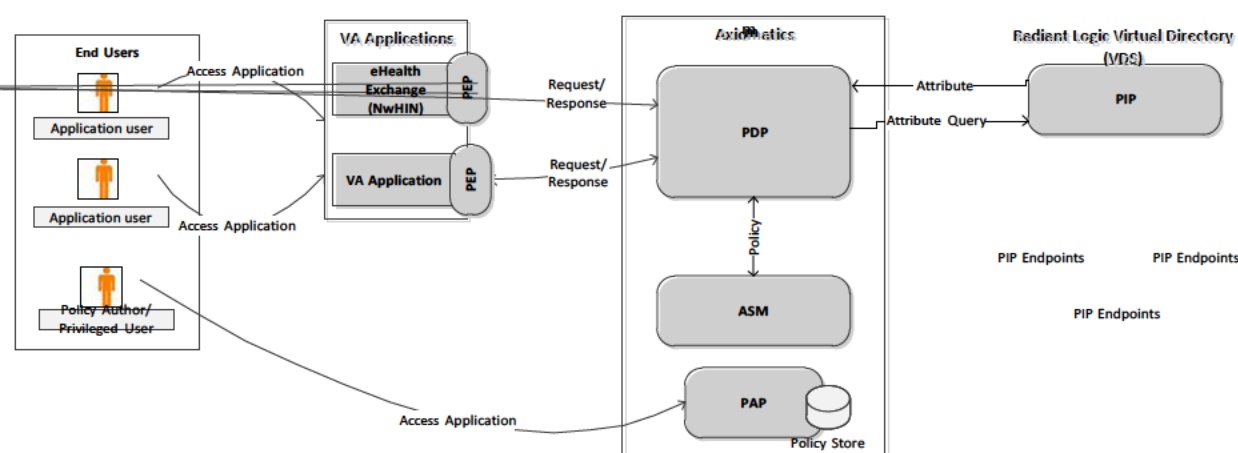


Figure 45: SAC Conceptual Design

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). The DataPower is used as a security measure to protect the web service communication between the PEP and PDP.

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

render a decision. The PDP receives authorization requests from PEP and evaluates these requests against authorization policies authored from the PAP. The XACML 3.0 security policies are cached at the PDP. It has two web service interfaces used for communication with the ASM and PEPs. The ASM communicates with the PDP through the management interface web service on the PDP. PEPs communicate with the PDP through the PDP endpoint address web service. The PEP sends XACML 3.0 requests to the PDP for access control decisions. The PDP then determines the correct security policy to use then determines which attributes are needed for a decision. The PDP queries the attribute service to retrieve any attribute not in the PEP's request. After the PDP uses attributes from within the XACML request and from the attribute service along with the corresponding XACML 3.0 policy it will generate an access control decision, which is sent back to the PEP that made the request.

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

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.

6.2.5.1. Enforce Access Control Decision

Field	Description
Use Case Name	Enforce Access Control Decision
Description	This use case describes the process by which a Policy Enforcement Point (PEP) interacts with a consuming application and the SAC service to facilitate an authorization request and enforce an access control decision.
Actors	<ol style="list-style-type: none">1. Application2. PEP3. DataPower4. PDP
Pre-Conditions	<ol style="list-style-type: none">1. Enter User has authenticated session with Application2. TLS session is established between the Application and PEP
Trigger	The PEP receive a request for an authorization from an application
Actions	<ol style="list-style-type: none">1. End-User attempts to access protected application.2. PEP intercepts access request3. The PEP can reside between the end user and the application4. The PEP can reside within the application itself5. PEP verifies request is valid and contains authentication attributes that can be used to uniquely identify the user6. PEP translates access request to XACML 3.07. Includes authentication attributes (SECID, ICN, unique identifier)8. May include client preferences, data restrictions, user security, contextual constraints9. Forwards XACML 3.0 request to DataPower10. DataPower performs XML threat reduction and forwards request to PDP11. PDP evaluates appropriate policy (ies) and attributes (within XACML request and from PIPs) and generates an access control decision.12. The PDP response is sent to the DataPower13. DataPower sends PDP response to the PEP. PEP receives XACML 3.0 access control decision response from the PDP.14. PEP enforces access control that it received from PDP.

Field	Description
Sequence Diagram	
Main Success Scenarios	<ol style="list-style-type: none"> 1. If Decision is Permit, access is granted to the user to access the protected resource. 2. If Decision is Deny, access is denied. The user is not allowed to access the protected resource. 3. The processing of Indeterminate or Not Applicable is determined by the application requirements.
Main Failure Scenarios	<ol style="list-style-type: none"> 1. Message format/contents are not valid 2. PDP is non-responsive and decision is not provided to application

6.2.5.2. Security Policy Authoring

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

Field	Description
	<ol style="list-style-type: none"> 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
Sequence Diagram	
Main Success Scenarios	Policy is created successfully.
Main Failure Scenarios	Policy creation fails and user has to start over.

6.2.5.3. Manage Access Control Policies

Field	Description
Use Case Name	Manage Access Control Policies
Description	This use case describes the process through which a SAC Privileged User manages access control policies across PDPs.
Actors	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 1. Privileged User determines proper PDP group to deploy policy package 2. Upload validated policy package

Field	Description
	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
Sequence Diagram	
Main Success Scenarios	Policy is pushed to PDP successfully
Main Failure Scenarios	Policy upload fails and user has to start over.

6.2.5.4. Make Access Control Decisions

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

Field	Description
Actions	<ol style="list-style-type: none"> 1. PEP request is received and PDP examines the request attributes to determine the correct policy to apply 2. Once the correct policies have been determined the PDP queries the PIP for attributes required by policy (ies) 3. The PDP uses the attributes found in the XACML 3.0 request, the attributes retrieved from the PIP, and the XACML 3.0 security policies to generate an access control decision 4. The XACML 3.0 response/access control decision is sent to the DataPower 5. DataPower sends the XACML 3.0 response/access control decision to the requested PEP 6. PDP logs the access request and response
Sequence Diagram	
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

6.2.6. eSig

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.

Figure 46 below provides a conceptual view of the complete eSig system at VA and its interaction with various systems and actors.

Figure 46: eSig Conceptual Design

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

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

Visible Signature:

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

Example:

6.2.6.1. User Management – Sign Document

Field	Description
Use Case Name	User Management – Sign Document
Description	This Use Case describes the process through which a User signs a document electronically.
Actors	<ol style="list-style-type: none">1. Signing user2. DataPower3. eSig Adapter4. ARX CoSign5. Oracle RAC
Pre-Conditions	The document allows electronic signature to be captured.
Trigger	The user authenticates to the VA application and clicks to signs a document electronically. The VA application sends the request to eSig for signing.
Actions	<ol style="list-style-type: none">1. DataPower intercepts the signature request from the user and sends it to the eSig Adapter.2. Upon receipt, the ARX CoSign checks to see if the user exists.3. If the user exists:4. ARC CoSign returns the user information5. The eSig Adapter compares the CN6. The eSig Adapter updates the user information in the ARX CoSign7. The eSig Adapter logs the sign event with the Oracle RAC8. If the user does not exist, eSig Adapter generates and stores the encrypted password and user data.9. The eSig Adapter signs the document and sends the success response to ARX CoSign.10. The eSig Adapter logs the sign event and returns results to the DataPower.

Field	Description
Sequence Diagram	
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.

6.2.6.2. User Management – Verify Document

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

Field	Description
Trigger	An already signed document is presented for verification.
Actions	<ol style="list-style-type: none"> 1. DataPower intercepts a request to validate a signature and sends it to the eSig Adapter. 2. Upon receipt, the ARX CoSign is checked to if 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 the DataPower.
Sequence Diagram	
Main Success Scenarios	The electronic signature is verified and response is sent to requestor.
Main Failure Scenarios	The electronic signature is not valid.

6.2.7. CAR

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)

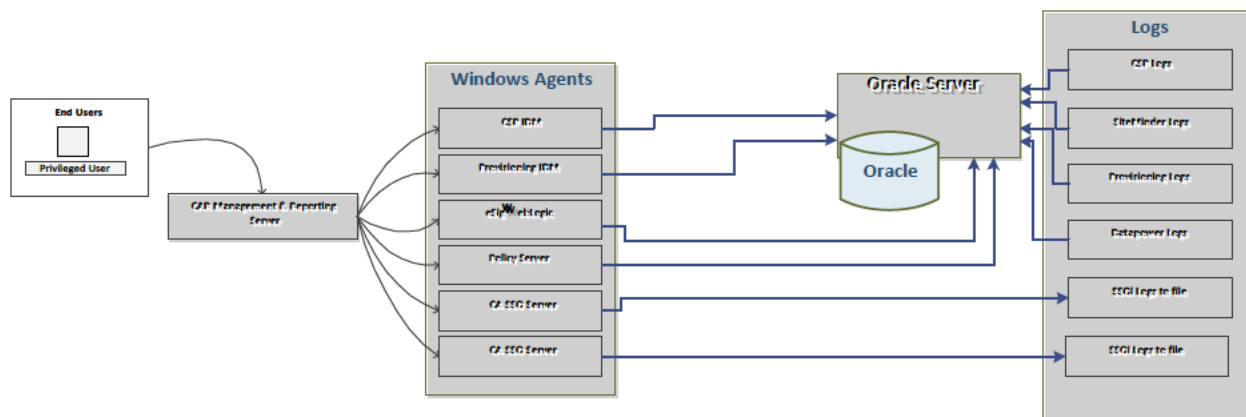


Figure 47: CAR Conceptual Design

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.

6.2.7.1. Process Activity Logs to generate reports

Field	Description
Use Case Name	Process Activity Logs
Description	This Use Case describes the process through which CAR will consume and process the data from the audit logs to generate reports.
Actors	<ol style="list-style-type: none"> 1. Agent 2. Connector 3. UARM Connector 4. Oracle RAC/File Log
Pre-Conditions	The ACS activities has captured the audit logs and CAR is setup to connect with audit log store
Trigger	The audit logs connector is invoked by the ACS activity agent.

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.
Sequence Diagram	
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.

6.2.7.2. Product Perspective

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

6.2.7.2.1. User Interfaces

Refer to section 3.2.3 for information on user interfaces.

6.2.7.2.2. Hardware Interfaces

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

6.2.7.2.3. Software Interfaces

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

6.2.7.2.4. Communications Interfaces

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

6.2.7.2.5. Memory Constraints

This section is not applicable to the AcS solution.

6.2.7.2.6. Special Operations

This section is not applicable to the AcS solution.

6.2.7.3. Product Features

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

Table 30: AcS Solution Products

#	Software	Description
1	CA IdentityMinder	A scalable, configurable identity management solution that automates on-boarding, modification and off-boarding of users, enables self-service requests and automates proactive identity compliance processes.
2	CA SiteMinder Web Access Manager	SiteMinder Web Access Manager is a web access management system that enables user authentication and secure Internet SSO (single sign-on), policy-driven authorization, federation of identities, and auditing of access to the web applications it protects.
3	CA Directory	<p>CA Directory provides directory services and security for online applications for organizations. For example, it enables customers to access their electronic accounts; employees can access critical business data.</p> <p>This product is generally considered a highly scalable and distributable implementation of directory services, including security services (e.g., authentication).</p> <p>CA Directory is supported on a variety of Windows and UNIX platforms, as well as 64-bit operating systems such as Linux 64, Solaris 10/Intel 64, UltraSparc 64, IBM Power5 64 and HP-UX Itanium 64.</p> <p>CA Directory supports open standards including: LDAP (and related RFCs), X.500 (DAP, DSP, DISP), Security (SSL, TLS, password hashes), Management (SNMP and related RFCs), Network (IPv6, RFC1006), and US Federal Government standards (FIPS 140-2, Common Criteria EAL3, and Section 508).</p>

#	Software	Description
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 HealthVet (MHV) and the Clinical Information Support System (CISS) are deployed with WebLogic Portal.</p>
5	Oracle Database	The Oracle relational database management system. There are several Oracle editions (Express, Personal, Standard, Enterprise, and Real Application Cluster). This assessment is concerned with the Standard and Enterprise editions of Oracle.
6	CA Single Sign-On	CA Single Sign-On improves security and simplifies user access by automating login to applications through a single authentication. This enables implementation of stronger security practices without burdening users with remembering multiple username and password combinations.
7	CA User Activity Reporting Module (UARM)	CA User Activity Reporting Module is a high-performance log management solution.
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. All 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.

6.2.7.4. User Characteristics

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

6.2.7.5. Dependencies and Constraints

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

6.2.8. Specific Requirements

This SDD provides the foundational detailed design for AcS activities under VA Development Support program. VA AcS components leverage the installation and configuration of COTS products to meet the technical requirements that sufficiently meet the detailed functional requirements. The design applies specific configurations and customizations made to the base infrastructure to create the technical solution necessary to meet the business requirements provided in requirements documents listed in section 1.4 in Table 4 above.

6.3. Communications Detailed Design

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

7. External Interface Design

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

7.1. Interface Architecture

7.1.1. Federation with VAAFI

The CSP activity interfaces with VAAFI where CSP asserts identity credentials 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.

In Figure 48 below, VAAFI is the Service Provider; CSP is the Identity Provider; the User Agent is the web browser of the user accessing the VAAFI protected applications.

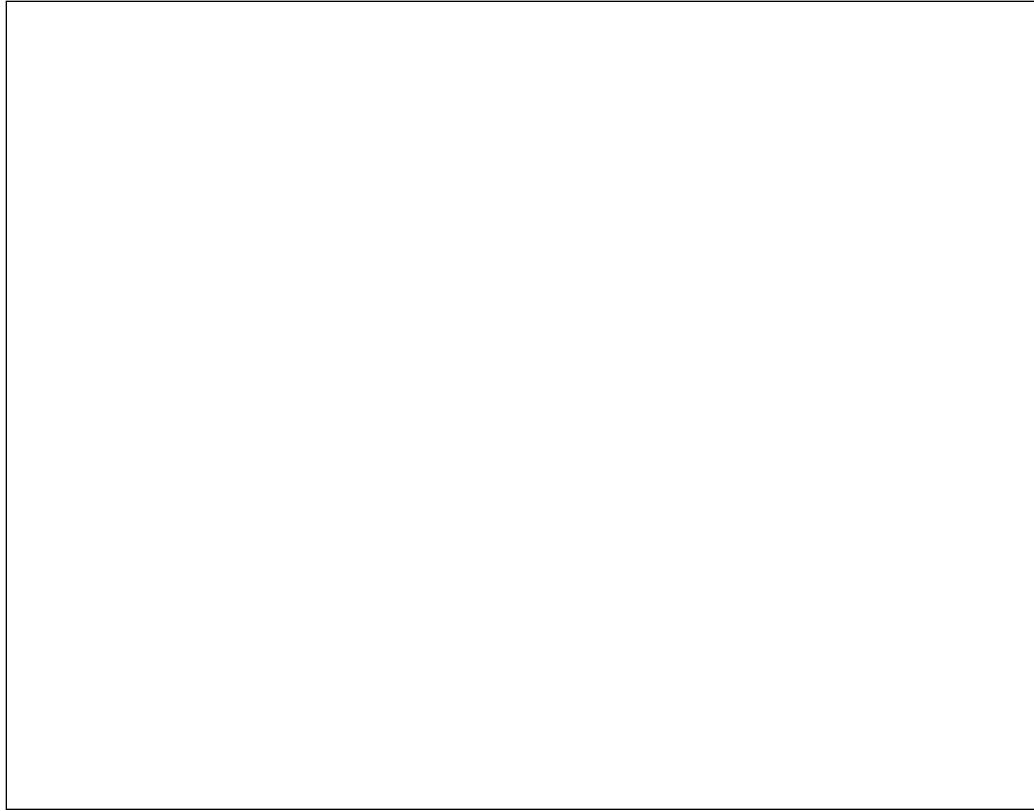


Figure 48: CSP to VAAFI Interface Flow

7.1.2. Master Veteran Index

The AcS activities will integrate with the Master Veteran Index (MVI) by making calls to the MVI web service as defined in the MVI Service Design document. Web service calls consist of SOAP messages submitted over HTTPS. Communication between MVI and CSP 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 and IP activity integrates with MVI for the following functions:

- Add Person
- Add Correlation
- Update Person
- Search Person by Traits
- Retrieve Person by Source ID
- Get Corresponding IDs by ICN
- Get Corresponding IDs by Source ID

The diagram in Figure 49 depicts the high-level integration of MVI with AcS activities.

Figure 49: MVI Interface Flow with Provisioning and IP

7.1.3. VA Active Directory

The integration between the Provisioning activity and VA Active Directory (AD) is mandated by several contract documents, including the AcS Increment 2 and Increment 3 RSDs, Provisioning Integration to Active Directory (AD) and Personal Identity Verification (PIV) System iRSD, version 1.2 from May 2013, and 2013 IAM VRM Business Requirements Document (BRD). The integration structure follows the process models (specific to AD) identified in the CRISP ProPath Onboarding and Offboarding sequences. The diagram in Figure 50 below describes the high-level interface structure.

Figure 50: Provisioning – Active Directory Interface Architecture

7.2. Interface Detailed Design

7.2.1. 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 all 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 all the assertion and provide the seamless access to the user. The details of the flow are described in section 6.2.2.2.

7.2.2. Master Veteran Index

Section 6.2.1 and section 6.2.4 describe the communication flow with the Master Veteran Index (MVI) for the Provisioning and IP activities.

8. Human-Machine Interface

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

- **HYPERLINK REDACTED**
HYPERLINK REDACTED
HYPERLINK REDACTED

- Radiant Logic site: [REDACTED]radiantlogic.com
- Axiomatics site: [REDACTED]axiomatics.com

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

8.1. Interface Design Rules

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

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

8.2. Inputs

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

Refer to section 8.4 for each of the web interface screen information regarding inputs to the system.

8.3. Outputs

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

- PDF
- Comma Separated File (CSF)
- Excel

8.4. Navigation Hierarchy

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

8.4.1. CSP

CSP supports three primary user functions: credential management, self-service, and administrator functions. Figure 51 below depicts the flow for CSP.

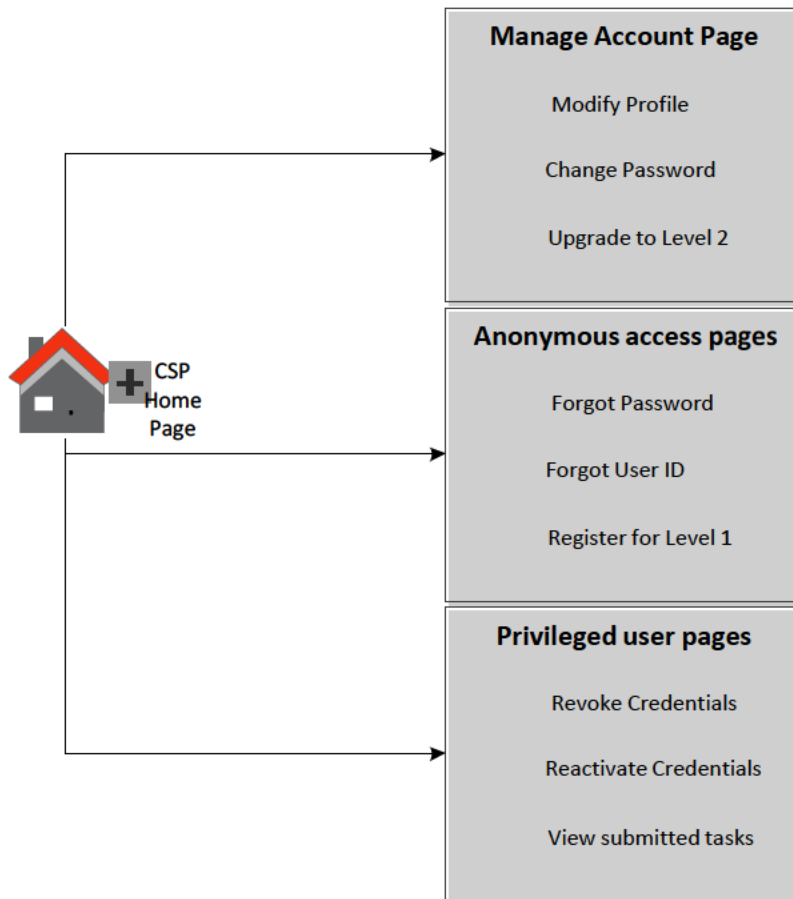


Figure 51: CSP Navigation Hierarchy

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 two primary user functions: IP and administrator functions. Figure 52 below depicts the flow for IP.

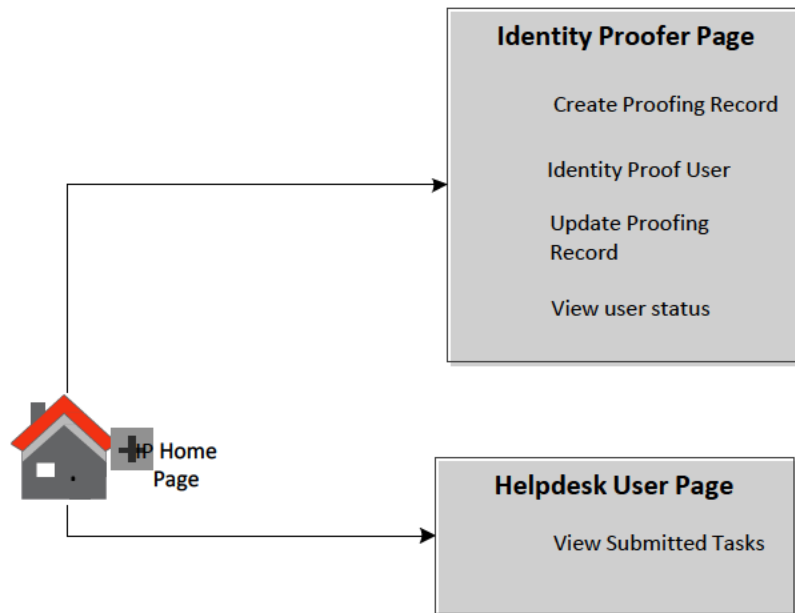


Figure 52: IP Navigation Hierarchy

8.4.3. Provisioning

The navigation hierarchy for Provisioning is depicted in Figure 53 below. Pages require authentication and authorization to access them. Provisioning offers users the ability to perform self-service for application account access, as well as provide administration functions.

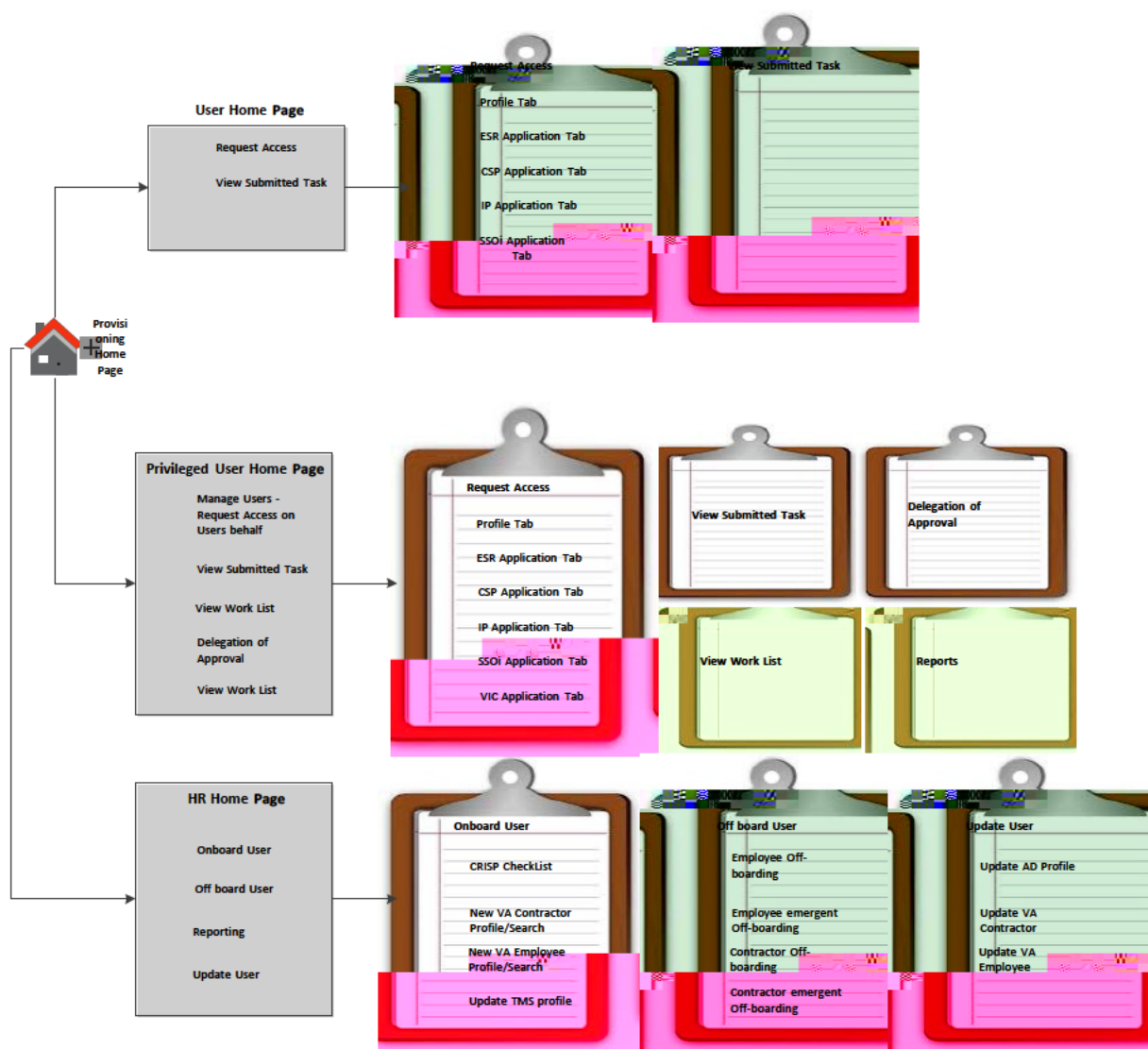


Figure 53: Provisioning Navigation Hierarchy

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 all user information and ensure that data in motion as well as rest is secured properly. For the AcS solution, the following security measures and integrity controls are in place.

Data in Motion:

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

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

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

Data at Rest:

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

Table 31: 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.

The security controls for the data at rest are managed through the encryption of sensitive attributes at the directory level for the AcS solution. The FIPS 140-2 encryption is applied on all

the identified PII and sensitive attributes stored in the AcS solution directory attributes. The following table provides the data types (refer to [section A.1](#) below for data type groupings) and who can make updates accordingly.

Table 32: 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 following integrity controls to enable acceptable security standards are met.

9.1.1. Confidentiality of Sensitive Information

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

9.1.2. Privacy of Personal Information

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

9.1.3. Process Integrity

The CSP and IP solution is designed to provide validation for input forms before storing the information in the user record. Each attribute that is entered in the user screens has regular expression filtering built-in to confirm the validity prior to storage. Additionally, for data elements such as states, countries and dates, the input uses enumeration types via dropdowns to limit the data to acceptable values. The CSP/IP solution does not allow duplicate identification values. Users are required to confirm their accounts by following instructions emailed to them. Therefore, a CSP/IP user has their e-mail address verified prior to getting a Level 1 or Level 2 credential. CSP/IP has definitive roles established to fulfill each business process. These roles clearly provide separation of duties. Additionally, due to full auditing of transactions, any misuse of authority is discernible and traceable in the audit logs and reports.

9.2. eSig

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

9.2.1. Confidentiality of Sensitive Information

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

9.2.2. Privacy of Personal Information

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

9.2.3. Process Integrity

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

9.2.4. System Availability

The eSig solution implementation is highly available and provides controls to minimize system failures, and access control to minimize man-made failures. The eSig service has software failover capability available within the CoSign product configuration, and shall also be supported by the DR environment.

9.3. SAC

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

9.3.1. Confidentiality of Sensitive Information

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

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

9.3.2. Privacy of Personal Information

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

9.3.3. Process Integrity

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

9.3.4. System Availability

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

9.4. Provisioning

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

9.4.1. Confidentiality of Sensitive Information

The Provisioning service stores user profile and authentication information required for authentication and authorization. Additionally provisioning stores personally identifiable information (PII) such as social security number, date of birth, and other personal identifiers. This information is stored encrypted. Provisioning stores the user password in an encrypted /hashed format in CA Directory. The transmission of information occurs over an SSL channel.

9.4.2. Privacy of Personal Information

The AcS Provisioning service collects and stores a wide range of identity data within its identity store(s) and manages several user account endpoints (e.g., ESR, CSP, TMS). PII is collected by Provisioning during a person's participation in the CRISP onboarding processes. The PII is then stored within the Provisioning user stores and the applicable endpoints. Provisioning provides

security controls, such as data at rest (database and directory store encryption services), communication confidentiality and integrity controls (data in motion) when exchanging data as part of its operations as well as authorization/access control to specific data components, to enforce only authorized individuals with a need to know and proper access are granted rights to view/modify users' identity record (including PII).

9.4.3. Process Integrity

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

9.4.4. System Availability

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

9.5. SSOi

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

9.5.1. Confidentiality of Sensitive Information

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

9.5.2. Privacy of Personal Information

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

9.5.3. Process Integrity

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

9.5.4. System Availability

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

9.6. CAR

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

9.6.1. Confidentiality of Sensitive Information

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

9.6.2. Privacy of Personal Information

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

9.6.3. Process Integrity

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

9.6.4. System Availability

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

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

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

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

10. Approval Signatures

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



Signed: _____ 1/29/2014

NAME REDACTED, Integrated Project Team Chair and Business Sponsor

Date



Signed: _____ 1/30/2014

NAME REDACTED, OIS Business Sponsor

Date



Signed: _____ 1/09/2014

NAME REDACTED, IAM Program Manager

Date



Signed: _____ 1/09/2014

NAME REDACTED, AcS Program Manager

Date



Signed: _____ 1/09/2014

NAME REDACTED, Enterprise Architecture

Date

A. Additional Information

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

A.1. Data Dictionary

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



A.2. RTM

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

A.3. 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.4. 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.5. Acronym List and Glossary

The acronyms and terms used this document are defined in the table below.

Table 33: Glossary

Term	Meaning
Active/Passive	A failover or disaster recovery method where one environment is a replica of the other environment. These servers run as the primary and a secondary standby environment waits ready to be manually enabled in the event of a primary failure.

Term	Meaning
Algorithm	A computational procedure used for performing a set of tasks such as an encryption process, a digital signature process, or cardholder verification.
Assertion	See SAML Assertion.
Attributes	Specific pieces of data stored about each instance of a given entity.
Authentication (AuthN)	The process of validating a presented identity. An identity can be presented by several types of objects including an end user, a specific device, or a specific computer process. The methodology utilized for authentication the identity of these different types of objects can be very different.
Authorization (AuthR)	The mechanism by which a system determines the level of access a particular authenticated user should have to secure resources controlled by the system policies. Although the Federation Credential Service Providers authenticate users, VA Agency Applications will continue to perform authorization.
Credential	An electronic representation of an individual's identity, such as PINS, usernames, passwords, and smartcards.
CSP	Credential Service Provider
Demilitarized Zone (DMZ)	A computer network that is accessible from two other computer networks that have no direct contact with each other. Often, one of these networks is the Internet and the other is a local, internal network.
End User Identification (Uid)	The Uid is a user specific number from the CSP that is combined with the CSPid then hashed for use in headers to help identify an end user to an application.
Entity	A class of persons, places, objects, events, or concepts about which data needs to be captured and stored.
Citrix Netscaler Device	Acts as a load balancer among available servers and system resources.
Federated Identity Management (FIM)	A system that allows individuals to use the same user name, password, or other personal identifier to sign on to the networks of more than one system or enterprise in order to conduct transactions.
Federation	Members of a federation system depend on each other to authenticate their respective users and vouch for their access to services offered by other members of the federation.
Firewall	A set of related programs, located at a network gateway server, which protects the resources of a private network from users from other networks.
Tivoli Identity and Access Manager (TIAM)	Provides authentication and authorization services and allows end users to use a single identity to log in once to the enterprise portal to gain access to resources according to authorization rules.

Term	Meaning
IBM WebSphere DataPower XS40 Security Gateway Appliance	Is a specialized network device that insures complete security for XML web services.
Identity Provider	Entity responsible for issuing a credential and validating it at run time.
Level of Assurance (LOA)	Per OMB-04-04 and NIST 800-63, level assurance refers to the required strength of identity proofing and credentials to gain access to federal systems. LOA is determined by doing a risk assessment of the impact of unauthorized access to the system. Level 1 is the weakest (no proofing, anonymous/weak credentials, while Level 4 is the strongest (Federal HSPD-12 PIV Card).
Lightweight Directory Access Protocol (LDAP)	A protocol for accessing on-line directory services.
Load Balancing	A technique (usually performed by load balancers) to spread work between many computers, processes, disks or other resources in order to get optimal resource utilization and decrease computing time.
Relationship	An association that exists between one or more database elements
SAML Assertion	SAML assertions are transferred between partners and components of VAAFI. Assertions contain statements that service providers use to make access control decisions. Three types of statements are provided by SAML: 1) Authentication statements, 2) Attribute statements and 3) Authorization decision statements.
Service Provider	Entity that accepts an assertion from an Identity Provider it trusts in order to allow authentication to their services.
Stateless	The stateless protocol is a communications protocol that treats each request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses. A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests.
Virtual Server	A server that runs on emulated hardware rather than actual hardware.
VA Authentication Federation Infrastructure (VAAFI)	The infrastructure implemented by VA Authentication Federation Infrastructure Project to provide Federated Identity Management within the Department of Veterans Affairs.
WebSphere	A family of IBM software products that provide a development and deployment environment for basic web publishing and for transaction-intensive, enterprise-scale e-business applications.

A.6. Required Technical Documents

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

A.7. CSP Class Diagram

The CSP .NET wrapper class diagram is shown in Figure 54 below.

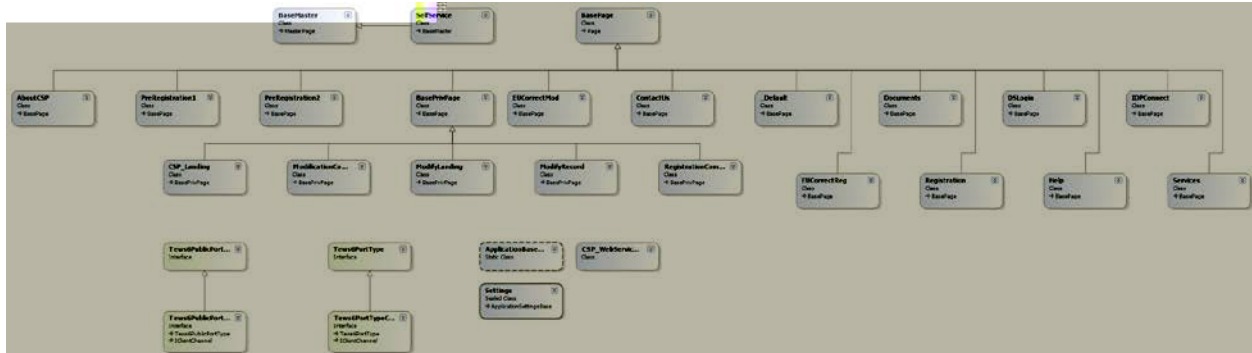


Figure 54: CSP Class Diagram

A.8. IP Class Diagram

The IP.NET wrapper class diagram is shown in Figure 55 below.

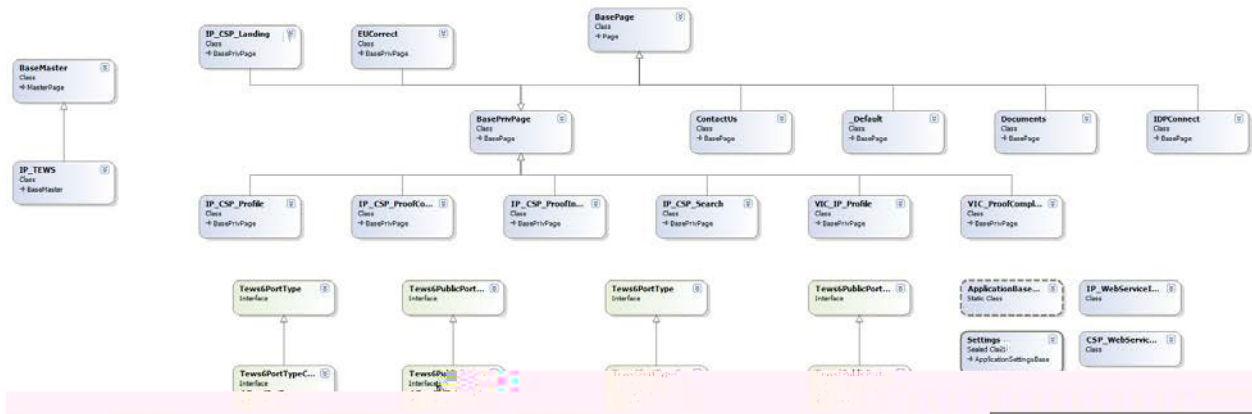


Figure 55: IP Class Diagram