

**Identity and Access Management
Access Services 2.0 Increment 5
CSP System Design Document**



Department of Veterans Affairs

March 2015

Version 1.1

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
04/24/2015	1.1	Updated per anomalies	Insignia
3/17/2015	1.0	Reformatting to comply with new template and add i5 information	

Artifact Rationale

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

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

Table of Contents

1. Introduction.....	8
1.1. Purpose of the SDD	8
1.2. Identification.....	9
1.3. Scope	9
1.3.1. Increment 5 CSP Scope.....	10
1.4. Constraining Policies, Directives and Procedures	10
1.5. User Characteristics	12
1.6. Relationship to Other Documents and Plans	12
1.7. Definitions, Acronyms, and Abbreviations.....	12
1.8. References	12
2. Background.....	13
2.1. Overview of the System	13
2.2. Overview of the Business Process	14
2.3. Business Benefits.....	25
2.4. Assumptions and Constraints.....	25
2.4.1. Design Assumptions	25
2.4.2. Design Constraints.....	26
2.4.3. Design Trade-offs	27
2.5. Overview of the Significant Requirements	27
2.5.1. Overview of Significant Functional Requirements	27
2.5.2. Overview of Functional Workload / Performance Requirements	44
2.5.3. Overview of Operational Requirements.....	45
2.5.4. Overview of the Technical Requirements.....	45
2.5.5. Overview of the Security or Privacy Requirements.....	46
2.5.6. Overview of System Criticality and High Availability Requirements.....	46
2.5.7. Single Sign-on Requirement.....	47
2.5.8. Requirement for Use of Enterprise Portals	47
2.5.9. Special Device Requirements.....	47
2.6. Legacy System Retirement	47
3. Conceptual Design	48
3.1. Conceptual Application Design.....	48
3.1.1. Application Context.....	49
3.1.2. High-Level Application Design	50
3.1.3. Application Locations	53
3.2. Conceptual Data Design.....	54
3.2.1. Project Conceptual Data Model	55
3.2.2. Database Information	59

3.2.3. User Interface Data Mapping	63
3.2.3.1. Application Screen Interface.....	63
3.2.3.1.1. Modify Account: Step 1 User Profile	63
3.2.3.1.2. Modify Account: Step 2 Security Questions.....	65
3.2.3.1.3. Change Password.....	65
3.2.3.1.4. Upgrade to Level 2: Step 1 User Profile	67
3.2.3.1.5. Upgrade to Level 2: Step 2 Security Questions	68
3.2.3.1.6. Self-Registration: Step 1 User Profile.....	69
3.2.3.1.7. Self-Registration: Step 2 Security Questions.....	70
3.2.3.2. Application Report Interface	71
3.2.3.3. Unmapped Data Element	71
3.3. Conceptual Infrastructure Design	71
3.3.1. System Criticality and High Availability.....	72
3.3.2. Special Technology	73
3.3.3. Technology Locations.....	73
3.3.4. Conceptual Infrastructure Diagram.....	75
3.3.4.1. Location of Environments and External Interfaces.....	76
3.3.4.2. Conceptual Production String Diagram.....	76
3.3.5. CA Identity Manager	78
3.3.6. CA SiteMinder Policy Server/Federation Security Services (FSS)	78
3.3.7. CA Directory	78
3.3.8. Identity Manager Workflow DB, Oracle Database Server	78
3.3.9. CA Report Server	79
3.3.10. Microsoft IIS HTTP/HTTPS Server & SiteMinder Web Agent.....	79
4. System Architecture	80
4.1. Hardware Architecture	80
4.2. Software Architecture.....	86
4.2.1. Presentation Tier.....	87
4.2.2. Application Tier.....	87
4.2.3. Data Tier	87
4.3. Network Architecture.....	95
4.4. Service Oriented Architecture / ESS	95
4.5. Enterprise Architecture	96
5. Data Design	97
5.1. DBMS Files	97
5.2. Non-DBMS Files	97
5.3. Data View.....	98
6. Detailed Design.....	102
6.1. Hardware Detailed Design.....	102
6.2. Software Detailed Design.....	102
6.2.1. Conceptual Design	102
6.2.1.1. Product Perspective	104

6.2.1.1.1.	User Interfaces	104
6.2.1.1.2.	Hardware Interfaces	104
6.2.1.1.3.	Software Interfaces	104
6.2.1.1.4.	Communications Interfaces	104
6.2.1.1.5.	Memory Constraints	104
6.2.1.1.6.	Special Operations	104
6.2.1.2.	Product Features	104
6.2.1.3.	User Characteristics	105
6.2.1.4.	Dependencies and Constraints	106
6.2.1.5.	Credential Issuance	106
6.2.1.6.	Revoke/Reissue Credential	108
6.2.1.7.	Federation with VAAFI	109
6.2.2.	Specific Requirements	110
6.2.2.1.	Database Repository	110
6.2.2.2.	System Features	110
6.2.2.3.	Design Element Tables	110
6.2.2.3.1.	Routines (Entry Points)	110
6.2.2.3.2.	Templates	110
6.2.2.3.3.	Bulletins	110
6.2.2.3.4.	Data Entries Affected by the Design	111
6.2.2.3.5.	Unique Record(s)	111
6.2.2.3.6.	File or Global Size Changes	111
6.2.2.3.7.	Mail Groups	111
6.2.2.3.8.	Security Keys	111
6.2.2.3.9.	Options	111
6.2.2.3.10.	Protocols	111
6.2.2.3.11.	Remote Procedure Call (RPC)	111
6.2.2.3.12.	Constants Defined in Interface	111
6.2.2.3.13.	Variables Defined in Interface	111
6.2.2.3.14.	Types Defined in Interface	111
6.2.2.3.15.	GUI	111
6.2.2.3.16.	GUI Classes	111
6.2.2.3.17.	Current Form	112
6.2.2.3.18.	Modified Form	112
6.2.2.3.19.	Components on Form	112
6.2.2.3.20.	Events	112
6.2.2.3.21.	Methods	112
6.2.2.3.22.	Special References	112
6.2.2.3.23.	Class Events	112
6.2.2.3.24.	Class Methods	112
6.2.2.3.25.	Class Properties	112
6.2.2.3.26.	Uses Clause	112
6.2.2.3.27.	Forms	112
6.2.2.3.28.	Functions	112
6.2.2.3.29.	Dialog	112
6.2.2.3.30.	Help Frame	112
6.2.2.3.31.	HL7 Application Parameter	112
6.2.2.3.32.	HL7 Logical Link	112
6.2.2.3.33.	COTS Interface	113
6.3.	Network Detailed Design	113
6.4.	Service Oriented Architecture / ESS Detailed Design	113

6.4.1. Service Description for CSP	115
6.4.2. Service Design for CSP	115
6.4.2.1. Introduction	115
6.4.2.1.1. Purpose and Scope of Service.....	115
6.4.2.1.2. Links to Other Documents	116
6.4.2.2. Service Details	116
6.4.2.2.1. Service Identification.....	116
6.4.2.2.2. Service Versions	116
6.4.2.2.3. Summary of Design and Platform Details	116
6.4.2.2.3.1. SOA Pattern(s) Implemented.....	116
6.4.2.2.3.2. COTS Platform vendor names and versions for hosting platform.....	116
6.4.2.3. Dependencies	116
6.4.2.4. Service Design Details	116
6.4.2.4.1. Interface Technical Specs	116
6.4.2.4.1.1. Service Invocation Type	116
6.4.2.4.1.2. Service Interface Type	116
6.4.2.4.1.3. Service Name	116
6.4.2.4.1.4. Interface	116
6.4.2.4.1.5. End Points	116
6.4.2.4.1.6. Operations or Methods.....	117
6.4.2.4.1.7. Message Schemas	117
6.4.2.4.2. Information Model.....	117
6.4.2.4.2.1. Class Diagram and Description of Entities Involved.....	117
6.4.2.4.2.2. Mappings from ELDM to Standards Based Schemas.....	117
6.4.2.4.3. Behavior Model (AKA Use Case Realization).....	117
6.4.2.4.3.1. Use Cases (Use Case Model).....	117
6.4.2.4.3.2. Interaction Diagrams.....	117
6.4.2.5. Gap Analysis	117
6.4.2.5.1. Variances from Enterprise Target Architecture	117
6.4.2.5.2. Variances from SLDs.....	117
6.4.2.5.3. Variances from Standards and Policies.....	117
6.4.2.5.4. Justification for Exceptions and Mitigation.....	117
7. External System Interface Design	118
7.1. Interface Architecture.....	118
7.1.1. VA CSP Federation with VAAFI	118
7.2. Interface Detailed Design	119
7.2.1. VA CSP Federation with VAAFI	119
7.2.2. Provisioning - CSP Connector.....	120
7.2.2.1. Processing	122
7.2.2.2. Local data structures	123
8. Human-Machine Interface	124
8.1. Interface Design Rules	124
8.2. Inputs	124
8.3. Outputs	125
8.4. Navigation Hierarchy	125
8.4.1. CSP	125
9. Security and Privacy.....	126

9.1. Security.....	127
9.1.1. Confidentiality of Sensitive Information	127
9.1.2. Privacy of Personal Information	127
9.1.3. Process Integrity.....	128
9.1.4. eSig Controls	128
9.2. Privacy	128
Attachment A – Approval Signatures.....	129
A. Additional Information.....	130
A.1. RTM.....	130
A.2. Packaging and Installation.....	130
A.3. Design Metrics	130
A.4. Acronym List and Glossary	130
A.5. Required Technical Documents	130
A.6. Attach Documents	130
A.7. CSP Class Documents	131
A.8. Data Dictionary.....	132

1. Introduction

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

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

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

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

The VRM IAM Program has deployed and maintains a VA CSP. The CSP is used to issue and administer NIST 800-63 compliant credentials to VA persons of interest. Currently VA accepts federated Level 1 and Level 2 DoD Self-service Logon (DS Logon) credentials, Level 4 VA PIV cards, Level 4 DoD CACs, and a commercial Level 1 through 4 federated credentials from approved credential service providers. The CSP has self-service registration, self-service profile management, and self-service password management capabilities and also includes delegated administration functionality for monitoring and report viewing. The CSP provides enterprise Level of Access 1 and 2 credentials to be consumed by external facing VA applications

1.1. Purpose of the SDD

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

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

- VA, Department of Defense (DoD), business partners, and other federal agencies

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

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

1.2. Identification

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

Table 1: System Identification

Name	Description	Abbreviation	Version	Release
VA AcS 2.0	Core set of activities to definitively and consistently identify VA stakeholders and to establish supporting processes that provide the appropriate level of security required to protect and manage the identities, information, and interests of the VA stakeholders	AcS	V 2.0.0	Release 5 (Increment 5)
Credential Service Provider	Provides trusted credentials to SSO. Credential is issued to users of interest to VA.	CSP	v2.4.1 Build 001	N/A

1.3. Scope

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

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

Table 2: Scope Inclusions

Includes
Issues Level of Assurance (LOA) 1 and LOA 2 credentials to VA persons of interest

Includes
Federates the CSP solution with VAAFI using Security Assertion Markup Language (SAML) 2.0

Table 3: Scope Exclusions

Excludes
Issuance of Level 3 or 4 credentials are deferred
Relying Party Initiated SAML SSO with any other relying parties other than VAAFI

1.3.1. Increment 5 CSP Scope

There are no Enterprise requirements for CSP in this increment.

1.4. Constraining Policies, Directives and Procedures

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

Table 4: Policies, Directives, and Procedures

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
1	VA	VA 6500 Handbook	<ul style="list-style-type: none"> • Directive Information Security Program. • Defining overall Security Framework for VA.
2	VA	VA 6501 Directive	<ul style="list-style-type: none"> • VA Identity Verification In-Person Proofing (IPP) Process. • Defining overall Identity Proofing Methodology for VA IAM.
3	VA	VA 6300 Directive	<ul style="list-style-type: none"> • Directive Records and Information Management. • Defines information management framework for VA Access Services.
4	NIST	SP 800-53-4	<ul style="list-style-type: none"> • Special Publication – Recommended Security Controls for Federal Information Systems and Organizations. • Defines the required security controls for IT systems under the Federal Information Security Management Act (FISMA).
5	NIST	SP 800-63-2	<ul style="list-style-type: none"> • Special Publication – Electronic Authentication Guideline. • Defines levels of assurance in user identities presented to IT systems over open networks. • Defines the data and procedural requirements for VA Access Services.

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

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
15	US Congress	E-Government Act of 2002	<ul style="list-style-type: none"> Federal Management and Promotion of Electronic Government Services. Defines the requirements for electronic services.
16	US Congress	The Privacy Act of 1974	<ul style="list-style-type: none"> § 552a. Records maintained on individuals. Defines VA Access Services Privacy assessment and control requirements.
17	National Archives and Records Administration (NARA)	Federal Records Act	<ul style="list-style-type: none"> Establishes the framework for records management programs in Federal Agencies.
18	VA	VA D 0735	<ul style="list-style-type: none"> Homeland Security Presidential Directive 12 (HSPD-12) Program Defines Department-wide policy, roles, and responsibilities for the creation and maintenance of systems and processes to implement VA's HSPD-12 Program necessary to implement Homeland Security Presidential Directive 12 (HSPD-12) program.
19	OMB	M-05-24	<ul style="list-style-type: none"> Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

1.5. User Characteristics

The user community of the CSP consists of internal users including VA employees, contractors and affiliates requiring logical access to VA business applications.

1.6. Relationship to Other Documents and Plans

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

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

1.7. Definitions, Acronyms, and Abbreviations

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

1.8. References

The document references are listed in above.

2. Background

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

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

2.1. Overview of the System

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

The VRM IAM Program has deployed and maintains a VA CSP. The CSP is used to issue and administer NIST 800-63 compliant credentials to VA persons of interest. Currently VA accepts federated Level 1 and Level 2 DoD Self-service Logon (DS Logon) credentials, Level 4 VA PIV cards, Level 4 DoD CACs, and a commercial Level 1 through 4 federated credentials from approved credential service providers. The CSP has self-service registration, self-service profile management, self-service password management capabilities and also includes delegated administration functionality for monitoring and report viewing. The CSP provides enterprise Level of Access 1 and 2 credentials to be consumed by external facing VA applications.

Credential Service Provider (CSP) is an element of an authentication service, most typically identified as a separate entity in a Federated Authentication System. In any authentication system, some entity is required to authenticate the user on behalf of the target application or service. The purpose of CSP is to permit a user to access multiple applications while providing his or her credentials (such as user identifier (ID) and password) only once. It also allows web applications to authenticate users without gaining access to a user's security credentials, such as a password.

2.2. Overview of the Business Process

Refer to the [Use Case Model](#) for CSP for applicable diagrams to support this section and the following Use Cases:

Table 5: Use Cases

Business Process ID	Business Process Name	Type	Owner	Description
1	VA IAM CSP Use Case Model	CSP Use Cases and Use Case Model	PD OIT	Use Cases to support CSP System
1	VA 2.0 Increment 2 Use Case Model Document	Use Cases	PD OIT	Use Case Model Document
2	VA i4 Use Case Model	Use Cases	PD OIT	i4 Use cases
3	CAR Use Case Model	Use Cases	PD OIT	i4 CAR Use cases

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

The CSP system supports the business process for an external user to register for and receive an E-Authentication Level 1 credential. This capability is completely self-service and offered over the internet. The CSP solutions allow the user to assert an identity and manage an account. Additionally, the user can register for and request to receive an E-Authentication Level 2 credential. This registration can either be an upgrade from a Level 1 or just requesting a Level 2. The CSP also provides administrative support for the CSP system. The CSP provides the ability to Revoke, Suspend and Reactivate a credential based on some external business processes. Additionally, the CSP provides standardized reports for managing the system. Finally, the CSP provides an ability to assign and manage roles and privileges.

Table 6: Business Processes

Business Process ID	Business Process Name	Owner	Description
1	New User Registration for Level 1 Credential	VA IAM	Provides the ability for new user to register for a VA e-auth Level 1 credential
2	New User Registration for Level 2 Credential	VA IAM	Provides the ability for new user to register for a VA e-auth Level 2 credential
3	Upgrade User Credential from Level 1 to Level 2	VA IAM	Provides the ability for new user to update VA e-auth Level 1 credential to a Level 2
6	User Authentication - Local	VA IAM	Provides the ability for a User to log into the CSP to modify their record or other maintenance activities. The CSP service (s) is designed to comply with applicable VA Security processes for management of security questions.

Business Process ID	Business Process Name	Owner	Description
7	User Authentication - Federated	VA IAM	Provides a means to support the use of the credential for federated access to VA business application integrated with VAAFI.
8	User Self-Service Inside Account	VA IAM	Provides a means to update user record information after User Authentication The CSP service (s) is designed to comply with applicable VA Security processes for management of security questions. The CSP service (s) is designed to comply with applicable VA Security processes for management of passwords. Security officers can configure CSP to force password change at designated intervals, prohibit password reuse, and enforce password quality requirements on cryptographic keys. Because the credentials are used for single-sign-on, these security policy settings are then enforced for connected applications.
9	Self-Serve Ext	VA IAM	Provides a means to update user record information after External User Authentication The CSP service (s) is designed to comply with applicable VA Security processes for management of security questions. The CSP service (s) is designed to comply with applicable VA Security processes for management of passwords. Security officers can configure CSP to force password change at designated intervals, prohibit password reuse, and enforce password quality requirements on cryptographic keys. Since the credentials are used for single-sign-on, these security policy settings are then enforced for connected applications.
10	Administration – Assign Roles	VA IAM	Provides a means to establish, assign and manage Roles. The CSP service (s) is designed provide the ability to manage Roles/Privileges for both privileged users.
11	Administration – Manage Accounts	VA IAM	Provides a means to manage accounts The CSP service (s) is designed to provide the ability to revoke a credential upon the subscriber status and activity change. This is currently designated as “disable”. The CSP service (s) is designed to provide the ability to restore a revoked credential upon a request from the Provisioning Service. This is currently designated as “enable”.
12	Administration – Provide Basic Reports	VA IAM	Provides standard reports to VA administrators The CSP service (s) is designed to provide the ability to generate reports on permissions, roles, and subscriber status and activity.

The following activity diagrams detail how the CSP solution has been designed to meet the 10 business functions detailed in the table above. The use case activity flows represent the actors involved, the systems involved, and the

steps of the process from start to finish. Following each activity flow diagram, a further description of the steps within the flow diagrams is provided.

The diagrams can be categorized into three main areas:

- Credential Registration and Issuance
- Credential Usage
- Credential Management

The Credential Registration & Issuance flows include:

- New User Registration for Level 1 Credential
- New User Registration for Level 2 Credential
- Upgrade from a Level 1 to Level 2 Credential

Figure 1: New User Registration for Level 1 Credential

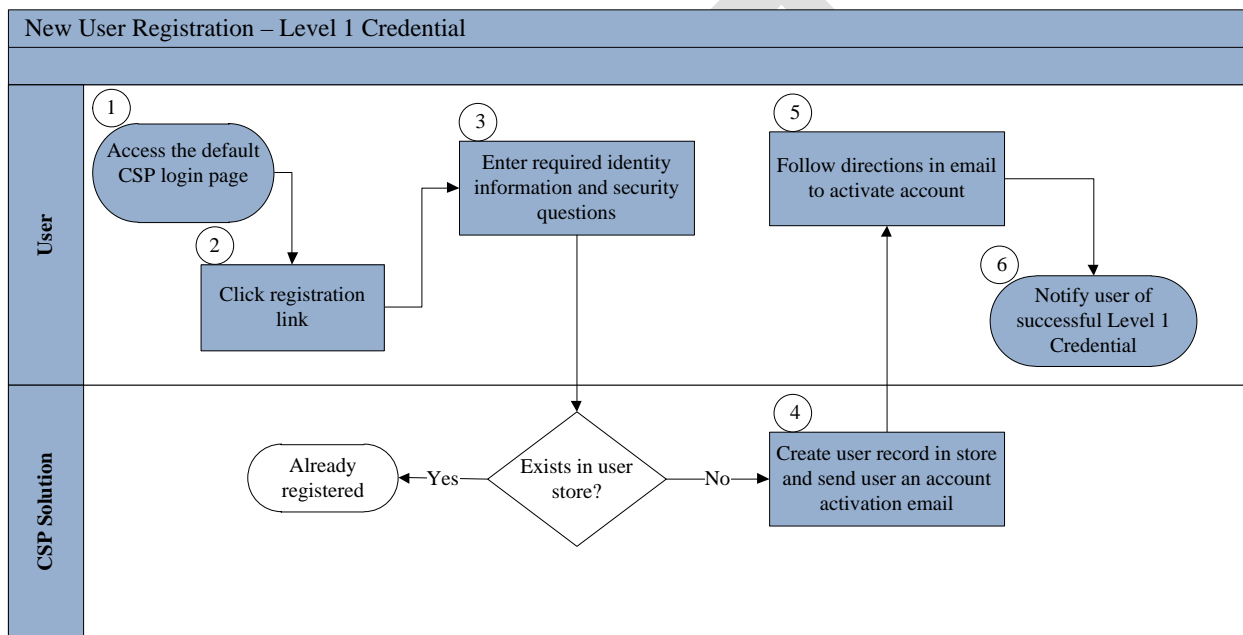


Table 7: New User Registration for Level 1 Credential Description of Actions

Step	Description of Actions
1	Access the CSP Login page. The CSP does not control the entry point for a user to get to this page.
2	The user has ability to choose options based on their privileges. On this page, the user is advised that if they have a DS Login, they should go through the DS Login process. If it is a new user who hasn't gone through the process, the new user can choose to start the process to get a credential.
3	At this step, the user fills in the data necessary for a Level 1 credential including the automated security questions. The data model is minimized to require the least amount of data to support a Level 1 credential.
4	The system creates an entry for the user and sends the user an e-mail to verify the user's e-mail address. If the SMTP server is down, the system queue's the message and sends later.
5	The user follows the instructions from the e-mail. This causes the user to log back in and set a new password.
6	The system notifies the user that they have successfully established a Level 1 user account.

Figure 2: New User Registration – Level 2 Credential

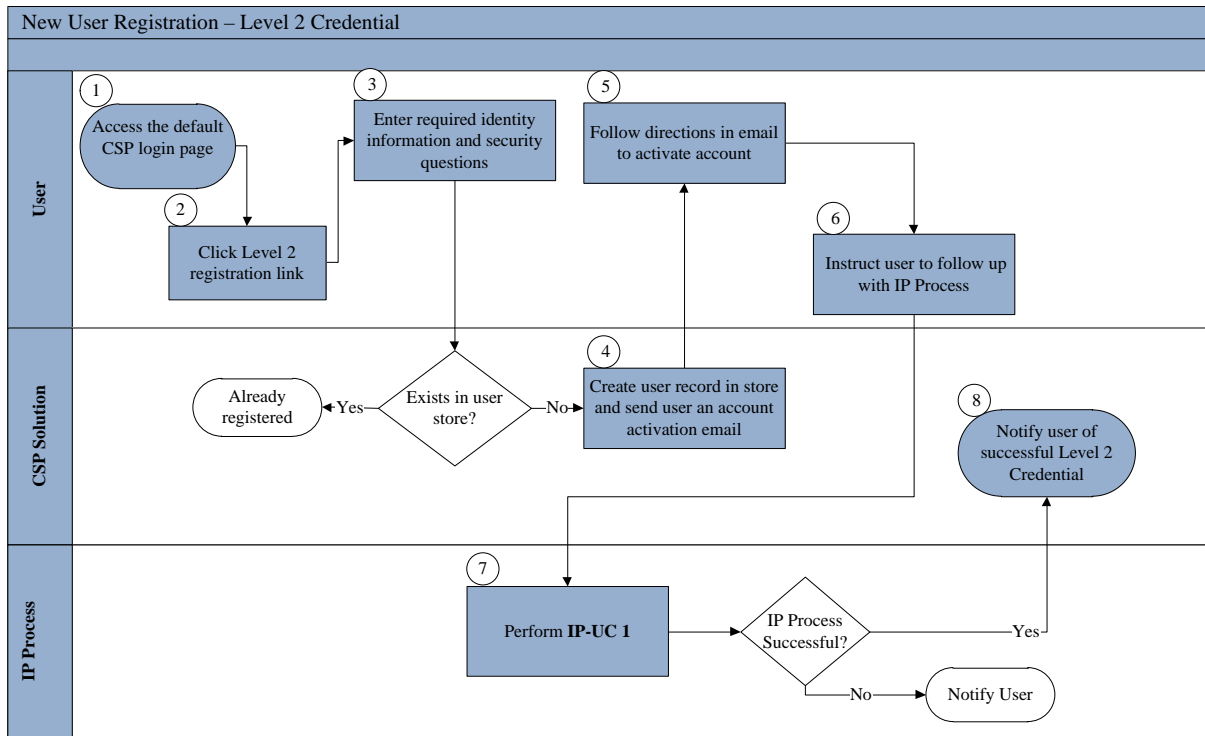


Table 8: New User L2 Business Process Flow

Step	Description of Actions
1	Access the CSP Login page. The CSP does not control the entry point for a user to get to this page.
2	The user has ability to choose options based on their privileges. On this page, the user is advised that if they have a DS Login, they should go through the DS Login process. If it is a new user who hasn't gone through the process, the new user can choose to start the process to get a credential.
3	At this step, the user fills in the data necessary for a Level 2 credential including the automated security questions. The data model is minimized to require the least amount of data to support a Level 2 credential.
4	The system creates an entry for the user and sends the user an e-mail to verify the user's e-mail address. If the SMTP server is down, the system queue's the message and sends later.
5	The user follows the instructions from the e-mail. This causes the user to log back in and set a new password

Figure 3: Upgrade User Credential from Level 1 to Level 2

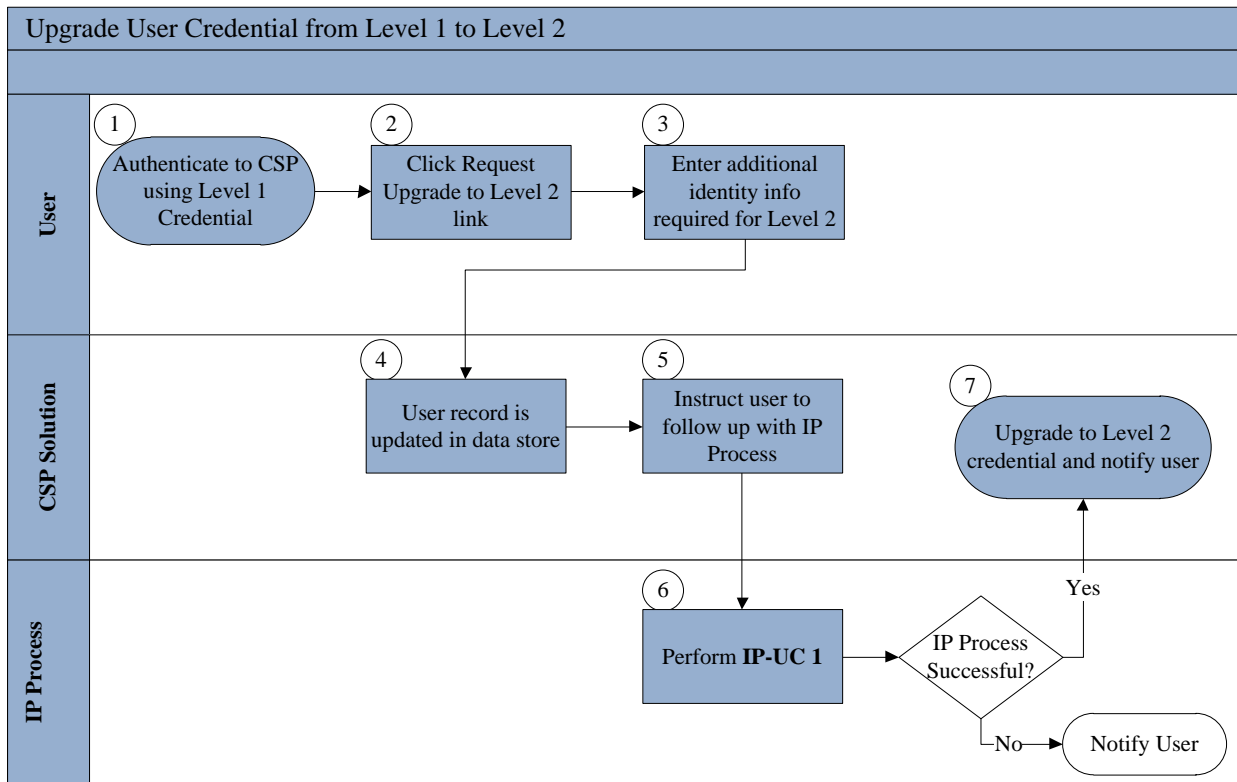


Table 9: L1 to L2 User Credential Business Process Flow

Step	Description of Actions
1	Access the CSP Login page. The user uses their Level 1 credential to access the CSP.
2	The user has ability to choose options based on their privileges. On this page, the user uses the link to upgrade their Level 1 to a Level 2. The user requests to upgrade.
3	At this step, the user fills in the data necessary for upgrading a Level 1 to a Level 2 credential. The data model is minimized to require the least amount of data to support a Level 2 credential.
4	The system updates the entry for the user.
5	The system instructs the user to go get Identity Proofed
6	The User goes to an identity proofing location with support documents and is identity proofed.
7	The system notifies the user that they have successfully established a Level 2 user account.

Figure 4: Level 2 User Identity Proofing

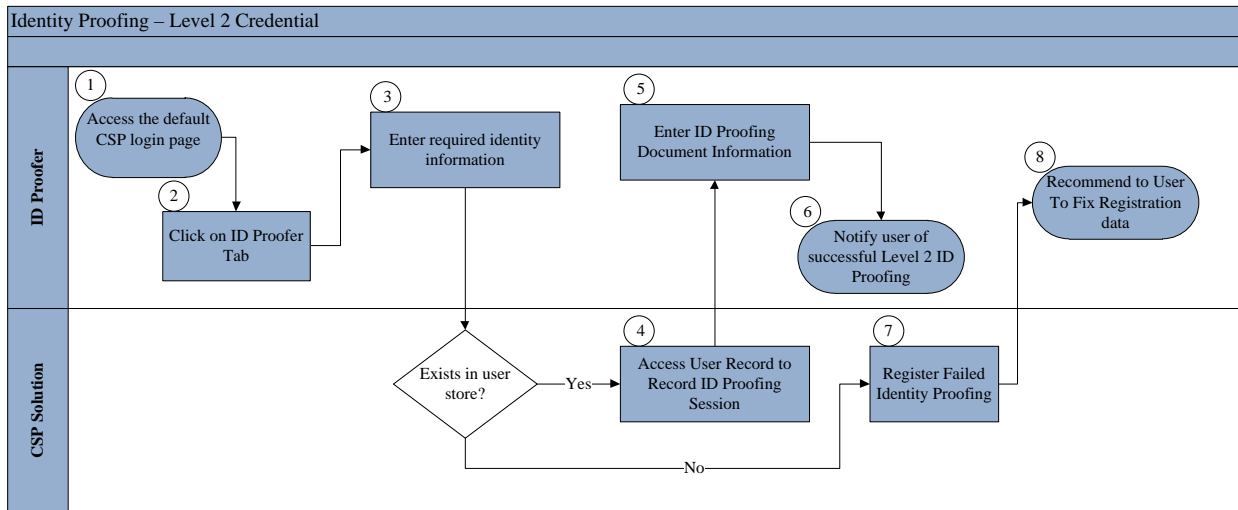


Table 10: L2 Identity Proofing Business Process Flow

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

Figure 5: User Authentication - Local

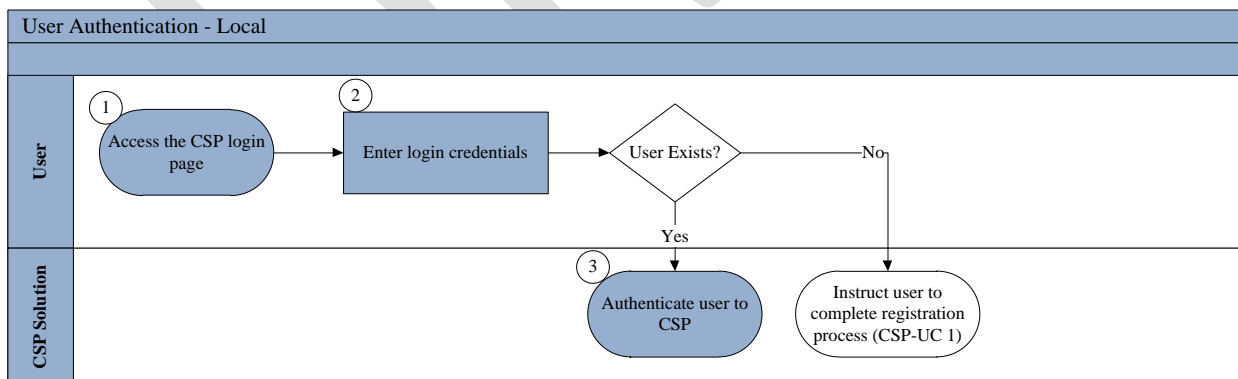


Table 11: Local User Authentication Business Process Flow

Step	Description
1	Access the CSP Login page.
2	The User uses their credential to access the CSP.
3	At this step, the system validates the user credential and allows the user to perform maintenance

Step	Description
	or review CSP data.

Figure 8: User Authentication - Federated

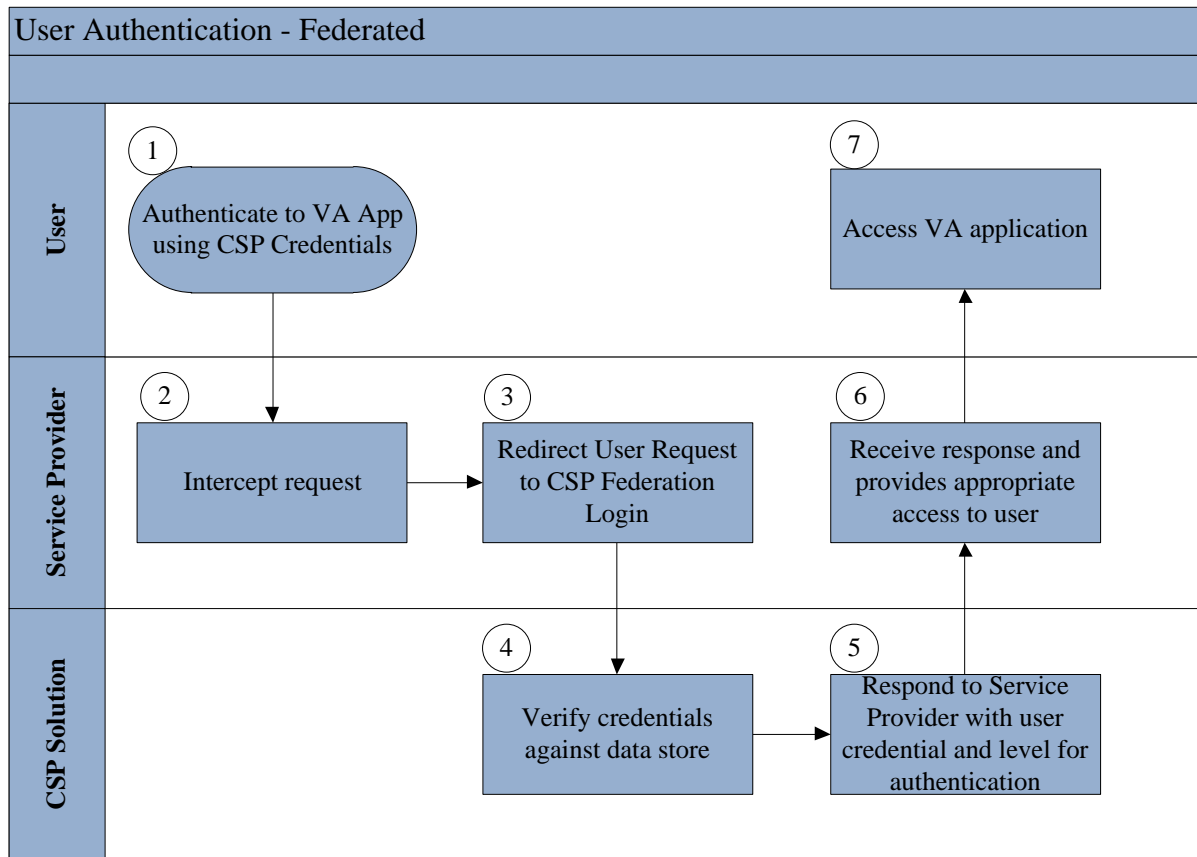
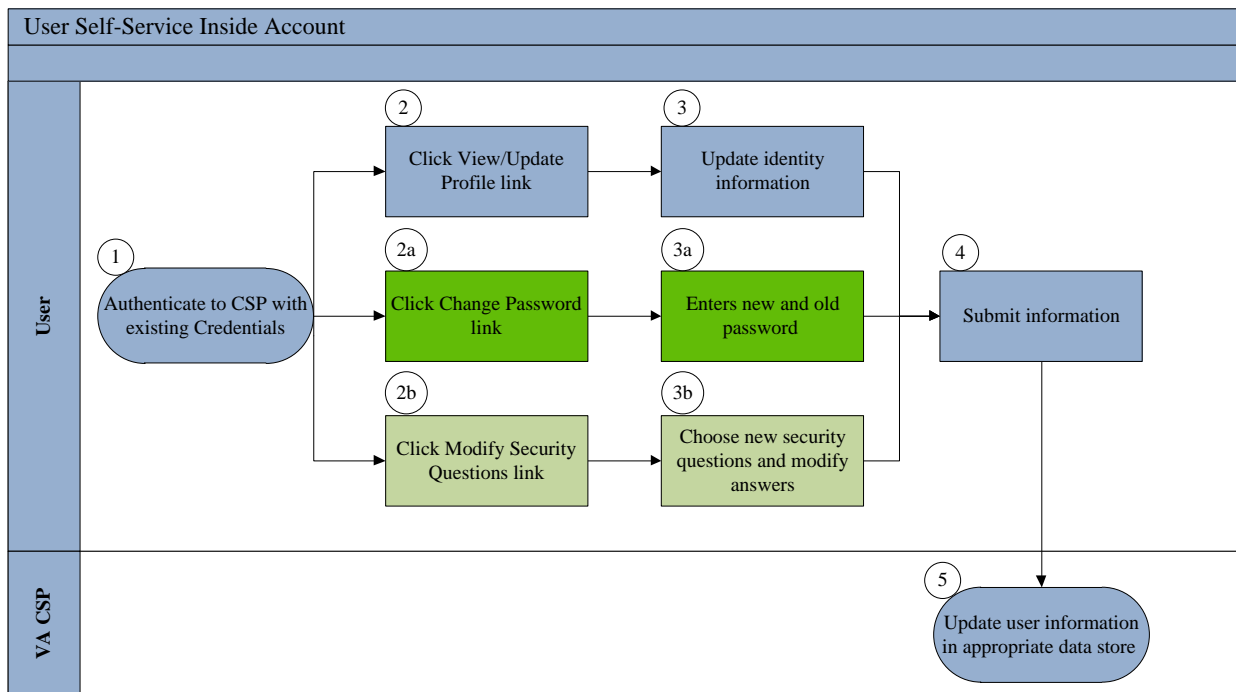


Table 12 - Federated Authentication Business Process Flow

Step	Description
1	The User accesses an application or resource protected by VAAFI using their CSP credential.
2	The VAAFI service recognizes that it is a CSP credential.
3	The VAAFI service sends an authentication request to the CSP.
4	The CSP verifies the credential.
5	The CSP responds to VAAFI with a SAML 2.0 assertion.
6	VAAFI receives the SAML assertion and provides feedback to the User that they are either allowed to access the resource or denied, based on the credential.
7	If successful, the User is allowed to access the resource.

Figure 9: User Self-Service Inside Account

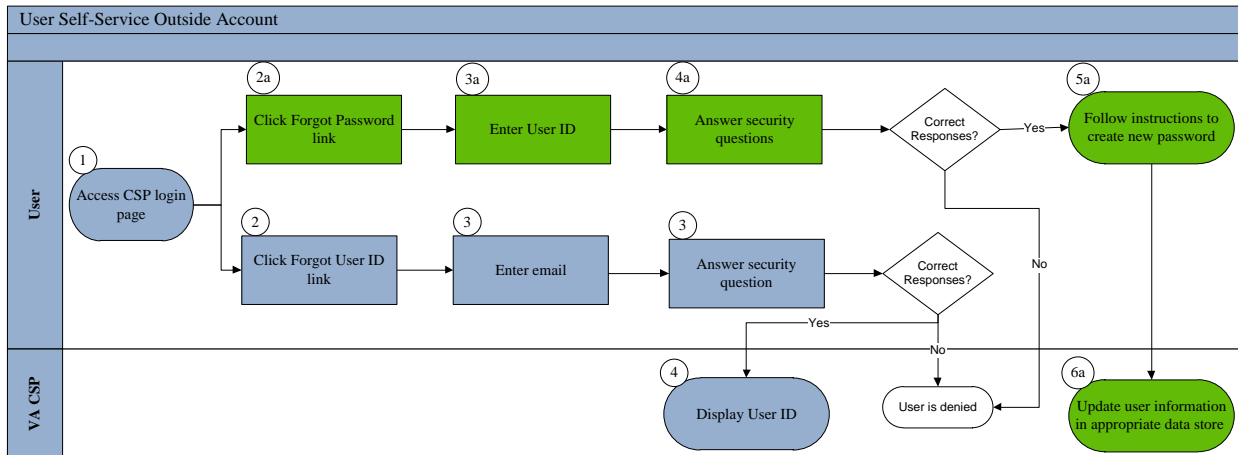


NOTE: The colors provide indication of separate flows. Additionally, the numbering mechanism is setup with an (a) or (b) suffix for the same purpose.

Table 12: User Self Service Inside Account Business Process Flow

Step	Description
1	The User authenticates to CSP using their CSP credential.
2	The User selects the tab either: View/Update Record, Change Password, Perform maintenance on security questions
3	If the user chooses to update their record, they update the information. NOTE: the user must get Identity Proofed again if they have a Level 2 credential & update specified information
4	If the User needs to adjust their password, they provide their old and new password in a self-service mode.
5	If the user needs to modify their security questions, they can choose new questions & answers
6	The User submits the change.
7	The CSP stores the updated information.

Figure 10: User Self-Service Outside Account



NOTE: The colors provide indication of separate flows. Additionally, the numbering mechanism is setup with an (a) or (b) suffix for the same purpose.

Table 13: User Self Service Outside Account Business Process Flow

Step	Description
1	The User has forgotten their Userid or Password. They go to the CSP Login page.
2	The User selects the link for either: Forgot Userid or Forgot Password.
3	If the user has forgotten their Userid, the User enters their e-mail address
3a	If the User has forgotten their password, they provide their Userid.
4	The user needs to answer their security questions.
4a	If the security questions are answered correctly, the system displays the user's Userid.
5	If the security questions are answered correctly, the user is instructed to set a new password
5a	The system captures the new password.
6	If the security questions are answered incorrectly, the user's request is denied.

Figure 11: Administration – Assign Roles

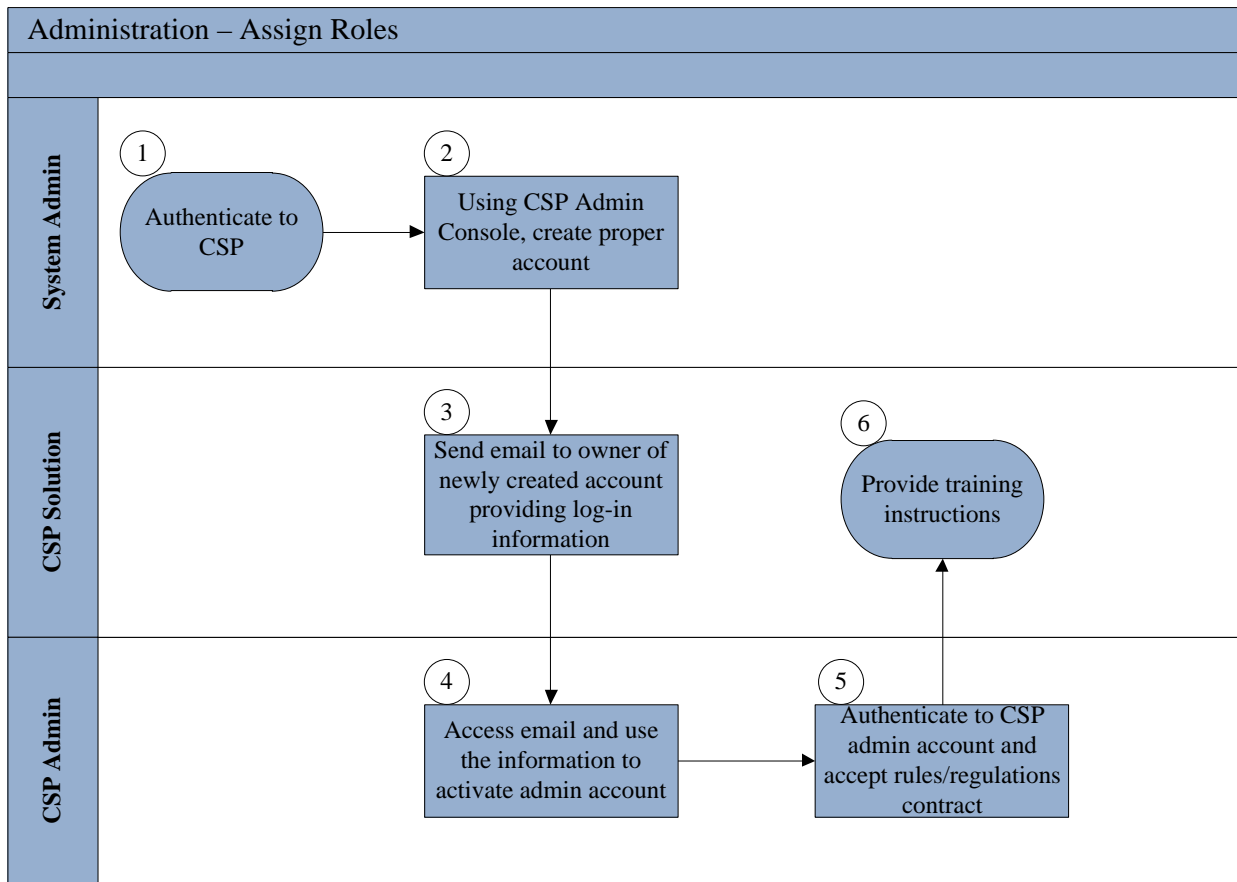
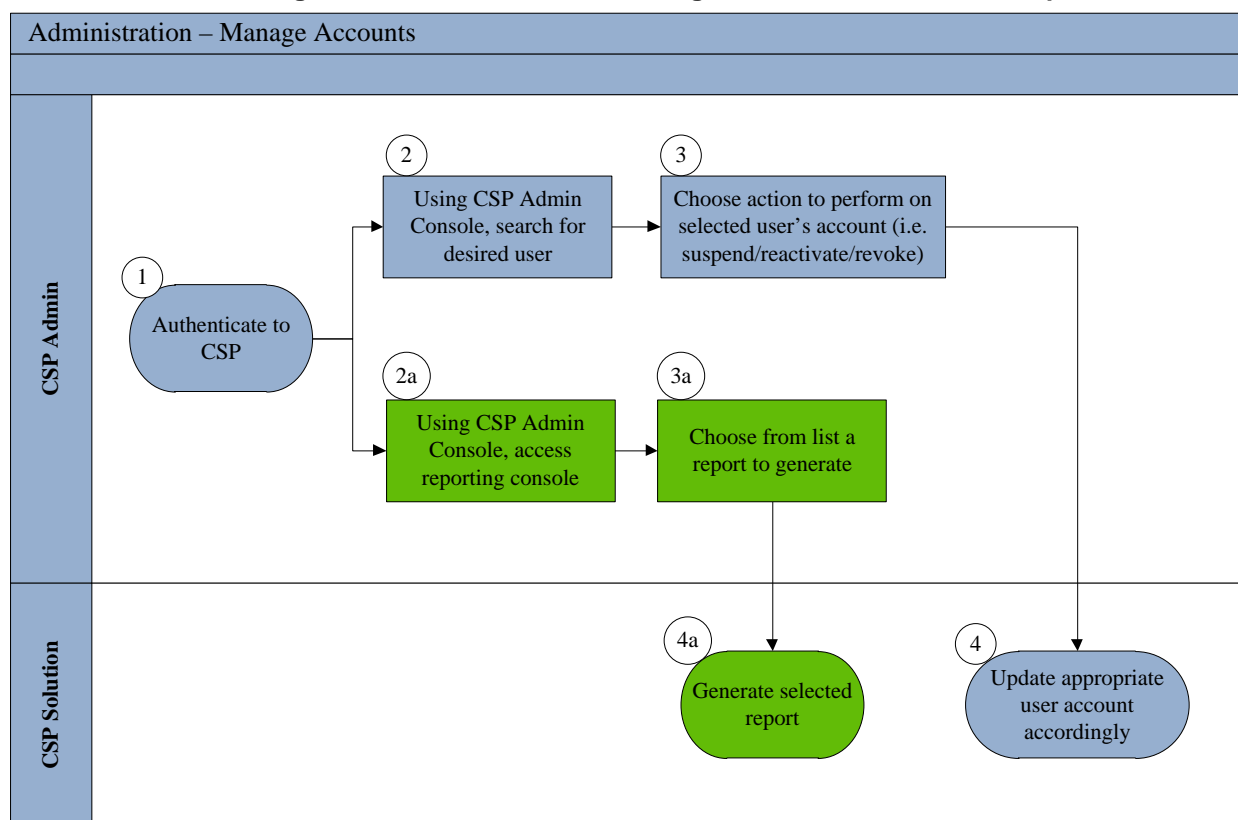


Table 14: Administration – Assign Roles Business Process Flow

Step	Description
1	The System Administrator logs into the CSP using their System Administration account.
2	The System Administrator selects the Administrative Console & creates an account
3	The CSP sends a notification e-mail to the account owner.
4	The User follows the instructions from the e-mail to activate their account
5	The User authenticates to the CSP and accepts the usage rules.
6	The CSP provides online training to step the User through their new role.

Figure 12: Administration – Manage Accounts and Access Reports



NOTE: The colors provide indication of separate flows. Additionally, the numbering mechanism is setup with an (a) or (b) suffix for the same purpose.

Table 15: Administration –Manage Accounts and Access Reports Business Process Flow

Step	Description
1	The System Administrator logs into the CSP using their System Administration account.
2	If the System Administrator needs to perform an action on an individual account, the System Administrator selects the Administrative Console & searches for an individual user.
2a	If the System Administrator needs to run reports, the System Administrator selects the Reporting Console.
3	The System Administrator selects the appropriate action – Revoke, Suspend or Reactivate
3a	The System Administrator selects the report from a list of canned reports.
4	The CSP solution updates the User record.
4a	The CSP causes the report to be run.

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

2.3. Business Benefits

CSP provides the VA with a system that is capable of issuing credentials to VA persons of interest (POI) that wish to access online services. It provides user choice of the credential type they wish to use as they interact online with the VA. The primary business benefit to this system is that VA does not need to rely on or send Veterans to external organizations to get credentials for use with VA systems.

In addition, a centralized enterprise CSP solution provides the means for users to have a single credential to use for access to business applications integrated with the SSOe. These benefits are realized by both the end users as well as the business applications consuming the credentials.

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

2.4. Assumptions and Constraints

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

2.4.1. Design Assumptions

Table 16: Assumptions

Component	Assumption
CSP	<ul style="list-style-type: none">• The CSP design will not deny a potential user a credential, if requested, even if the user already has a DS Logon. However, design considerations have been made to direct those users with DS Logon or the ability to obtain a DS Logon to the appropriate place.• CSP information provided by the VA will be utilized for sizing estimates (refer to section A.4).• CSP identity records (account data) and access controls will be separated logically from the Identity Proofing process and associated interfaces and security controls.• CSP will be a client of Identity Proofing as a separate service and provide the identity data input for completing the identity proofing process and creation of the identity proofing record.• CSP utilizes in-person Identity Proofing process for vetting each LOA 2 identity record and associated account credential.• 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.
Infrastructure	<ul style="list-style-type: none">• The AcS 2.0 is designed to have 99.9% availability, and can be failed over to the Disaster Recovery site. However, this is contingent on the availability of other components outside of the AcS 2.0 such as VAAFI and Terremark, which only support 99.6% and 99.9% availability, respectively. Therefore, if the solution components support 99.9% availability, this may not be achieved due to external dependencies which may be limited to the VAAFI 99.6% figure.

2.4.2. Design Constraints

This section describes the design constraints that may affect the requirements and architecture stated in this document. The design constraints are as follows:

DRAFT

Table 17: Design Constraints

Design Constraints
CSP credentials are limited to Level 1 and Level 2 as defined in SP 800-63, VA 6500 and 6501
CSP credential integration is with VAAFI only. VAAFI enablement, performed under a separate activity, perform credential integration with VA applications.

2.4.3. Design Trade-offs

This section describes the design tradeoffs/characteristics relevant to CSP, as defined by VA requirements. The below table lists the design tradeoffs in addition to the infrastructure components involved with development of the solution design for CSP:

Table 18: Design Trade-Offs

Design Trade –Offs
The design will not deny a user a CSP credential if they have a DSLogon. Currently there is no requirement to do anything relative to a user's capability to get a CSP credential if they are eligible for DSLogon; however the expectation is that this issue may be addressed in a future phase.
The data from Level 1 and pre-ID Proofed Level 2 are not sufficient to initiate an entry in MVI
SiteMinder will be used to control external access for CSP
SAML 1 has been noted for deprecation, CSP will support SAML 2.0
The CSP solution is designed to reduce the collection, storage, or transmission of the SSN in any fashion. 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.
The CSP solution is currently designed to use the Identity Manager user interface. This interface provides easy configuration and little development, but does not allow for a high level of customization of the interface.

2.5. Overview of the Significant Requirements

This section provides an overview of the requirements that are within the scope for CSP.

2.5.1. Overview of Significant Functional Requirements

The table below provides an overview of the Functional requirements that are within the scope for CSP.

Table 19: CSP Functional Requirements

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
8.01	The Credential Service shall receive an online Credential request from a service/application.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.02	The Credential Service shall receive Credential request from the IDP service.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
8.03	The Credential Service shall receive a request to generate a Level 1 Credential.	SP 800-63, Section 5	High		FY13 4/25/2013
8.04	The Credential Service shall receive a request to generate a Level 1 Credential.	SP 800-63, Section 5	High		FY13 4/25/2013
8.05	The Credential Service shall receive a request to generate a Level 1 Credential.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.06	The Credential Service shall receive a request to generate a Level 2 Credential.	SP 800-63, Section 5	High		FY13 4/25/2013
8.07	The Credential Service shall receive Credential request from the Provisioning Service.	FICAM v2, Section 12.1	High		FY13 4/25/2013
8.08	The Credential Service shall receive a request to generate a Level 1 Credential.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.09	The Credential Service shall support a Level 1 Credential.	FICAM v2, Section 12.2.1	High		FY13 4/25/2013
8.10	The Credential Service shall receive a request to generate a Level 2 Credential.	SP 800-63, Section 5	High		FY13 4/25/2013
8.11	The Credential Service shall validate proofing with the IDP service.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.12	The Credential Servicer shall verify DS Logon does not exist.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
8.13	The Credential Service shall receive a response from the IDP service of the individual's ID Proofing Status.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.14	The Credential Servicer shall verify DS Logon does not exist.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.15	The Credential Service shall redirect if a DS Logon does exist.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.16	The Credential Service shall proceed if a DS Logon does not exist	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.17	The Credential Service shall store the response from the IDP service.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.18	The Credential Service shall generate a Credential.	SP 800-63, Section 5	High		FY13 4/25/2013
8.19	The Credential Service shall generate a Credential after receiving a positive response from the IDP service.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.20	The Credential Service shall return a rejection of Credential after receiving a negative response from the IDP service.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.24	The Credential Service shall send the VA application that requested the Credential a notification.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
8.25	The Credential Service shall receive a request to upgrade Credential Level.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.26	The Credential Service shall receive a Credential upgrade request from the IDP service.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.28	The Credential Service shall receive a request to upgrade to a Level 2 Credential from the IDP service.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.29	The Credential Service shall receive Credential request from the Provisioning Service.	FICAM v2, Section 12.1	High		FY13 4/25/2013
8.31	The Credential Service shall receive a request to upgrade to a Level 2 Credential from the Provisioning Service.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.32	The Credential Service shall upgrade Credential level.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.33	The Credential Service shall upgrade a Level 1 Credential to a Level 2 Credential.	IPT Approved (2012) CSP Business Packets	High		FY13 4/25/2013
8.34	The Credential Service shall store new Credential.	SP 800-63, Section 5	High		FY13 4/25/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
Credentialing Lifecycle Management – Provide a digital process of maintaining a credential and associated support over the full credential life cycle.			High	* Credentials at Assurance Levels 2+ * Support Multiple Credential types (DSLogon, NSTIC, USAA) * Support Proxy Request to DS Logon and verification	FY14 8/15/2013
9.01	The system shall support multiple credentials for a given identity.	SP800-63, Section 5.1	High		FY14 8/15/2013
9.02	The system shall support credentials at every level of assurance for a given identity.	SP800-63, Section 5 and 8.2	High		FY14 8/15/2013
9.03	The system shall have the ability to limit the numbers of active credentials allowed for a given level of assurance for an identity through administrative controls.	SP800-63, Section 7 and 7.2.2	High		FY14 8/15/2013
9.04	The system shall support creation of pseudonym identities and tokens.	SP800-63, Section 5	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.05	The system shall restrict the ability to create pseudonym identities and tokens as a controlled administrative over-ride function.	SP800-63, Section 5	High		FY14 8/15/2013
9.06	The system shall allow the use of higher assurance credentials for access to lower assurance resources.	SP800-63, Section 6	High		FY14 8/15/2013
9.07	The system shall have the capability to consume credentials at Assurance Levels 4, 3, and 2 that are created and issued external to VA.	SP800-63, Section 7.3	High		FY14 8/15/2013
9.08	The system shall have the capability to consume identity data from credentials at Assurance Levels 4, 3, and 2 that have been created and issued external to VA.	SP800-63, Section 7.3	High		FY14 8/15/2013
9.09	The Credential Service shall receive a message to revoke credential from Provisioning Service.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.10	The Credential Service shall receive Automated Message for deactivation from Provisioning Service.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.11	The Credential Service shall receive Automated Message for deactivation from Provisioning Service for Termination.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.12	The Credential Service shall receive Automated Message for inactivation from Provisioning Service for Temporary Suspension.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.13	The Credential Service shall identify Credential to be revoked.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.14	The Credential Service shall accept multiple User listing of Credentials to be revoked.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.15	The Credential Service shall accept single User of Credentials to be revoked.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.16	The Credential Service shall revoke the Credential.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.17	The Credential Service shall revoke the Credential immediately.	FICAM v2,	High		FY14 8/15/2013
9.18	The Credential Service shall maintain a date and time stamp of being revoked.	Section 5.3 and SP 800-63, Section 8.2	High		FY14 8/15/2013
9.19	The Credential Service shall suspend the Credential immediately.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.20	The Credential Service shall maintain a date and time stamp of suspension.	FICAM v2, Section 8.2.2 and VA Handbook 6500, Section 18	High		FY14 8/15/2013
9.21	The Credential Service shall hold a revoked credential per VA Policy.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.22	The Credential Service shall send confirmation of revoked credential to the Provisioning Service.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.23	The Credential Service shall send confirmation of revoked credential to the Provisioning Service immediately.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.24	The Credential Service shall maintain an audit log for all revoked credentials.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.25	The Credential Service shall maintain a Security Audit log for all revoked credentials.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.26	The Credential Service shall maintain a System Audit log for all revoked credentials.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.27	The Credential Service shall receive a restore request from the Provisioning Service.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.28	The Credential Service shall send a notification to the Provisioning Service that request was received.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.29	The Credential Service shall send a notification to the Provisioning Service to verify this action was requested.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.30	The Credential Service shall identify the Credential to be restored.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.31	The Credential Service shall verify credential in revoked status matches Credential identified to be restored.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.32	The Credential Service shall restore the Credential.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.33	The Credential Service shall set status of Credential to active.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.34	The Credential Service shall record the restoration of Credential.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.35	The Credential Service shall send confirmation of restoration to the Provisioning Service.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.36	The Credential Service shall provide a user interface to receive request for Ad-Hoc report.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.37	The Credential Service shall provide the ability to identify data elements on which to report.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.38	The Credential Service shall provide a notification that request was received.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.39	The Credential Service shall provide the ability to schedule the required report.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.40	The Credential Service shall provide the ability to customize report parameters.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.41	The Credential Service shall provide the ability to store customize report parameters specific to a user.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.42	The Credential Service shall process requested Ad-Hoc report.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.43	The Credential Service shall compile requested data elements.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.44	The Credential Service shall produce report within scheduled parameters.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.45	The Credential Service shall save the report in a VA Approved exportable file format.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.46	The Credential Service shall offer the report in a PDF file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.47	The Credential Service shall offer the report in a CSV file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.48	The Credential Service shall offer the report in a text file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.49	The Credential Service shall forward request Ad-Hoc report to Requestor.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.50	The Credential Service shall deliver a report on identified data elements to Requestor.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.51	The Credential Service shall deliver report within scheduled parameters.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.52	The Credential Service shall deliver report in a VA approved file format.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.53	The Credential Service shall deliver a report in a PDF file format	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.54	The Credential Service shall deliver a report in a CSV file format	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.55	The Credential Service shall deliver a report in a text file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.56	The Credential Service shall receive request for Standard report from the request log.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.57	The Credential Service shall provide the ability to identify data elements on which to report.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.58	The Credential Service shall provide a notification that request was received.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.59	The Credential Service shall provide the properly authorized user the ability to schedule the required report.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.60	The Credential Service shall provide the ability to customize report parameters.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.61	The Credential Service shall provide the ability to store customize report parameters.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.62	The Credential Service shall process requested Standard report.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.63	The Credential Service shall compile requested data elements.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.64	The Credential Service shall produce report within scheduled parameters.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.65	The Credential Service shall provide the ability to automatically generate scheduled standard reports.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.66	The Credential Service shall save the report in a VA Approved exportable file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.67	The Credential Service shall save the report in a PDF file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.68	The Credential Service shall save the report in a CSV file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.69	The Credential Service shall save the report in a text file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.70	The Credential Service shall display request Standard report to Requestor.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.71	The Credential Service shall display a report on identified data elements to Requestor.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.72	The Credential Service shall display report in a PDF file format	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.73	The Credential Service shall display a report in a CSV file format	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.74	The Credential Service shall display a report in a text file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.75	The Credential Service shall deliver a report within scheduled parameters.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.76	The Credential Service shall deliver a report within identified date range.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.77	The Credential Service shall deliver a report based on action taken.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.78	The Credential Service shall deliver a report based on volume of activity.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.79	The Credential Service shall deliver a report based on source of request.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.80	The Credential Service shall deliver a report based on rejected request.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.81	The Credential Service shall deliver a report in any VA approved specified file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.82	The Credential Service shall deliver a report in a PDF file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.83	The Credential Service shall deliver a report in a CSV file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.84	The Credential Service shall deliver a report in a text file format.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.85	The Credential Service shall receive request for password change from online service.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.86	The Credential Service shall process password change request.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.87	The Credential Service shall validate permission for request.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.88	The Credential Service shall validate with challenge questions.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.89	The Credential Service shall validate with current password.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.90	The Credential Service shall store successful password change.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.91	The Credential Service shall retain password change for audit service.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.92	The Credential Service shall deliver the password through a VA approved delivery mechanism.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.93	The Credential Service shall meet security requirements for audit data.	VA Handbook 6500, Section 16	High		FY14 8/15/2013
9.94	The Credential Service shall return a notice for unsuccessful password change.	VA Handbook 6500, Section 10	High		FY14 8/15/2013
9.95	The Credential Service shall retain unsuccessful password change for audit service.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.96	The Credential Service shall meet security requirements as identified in the current VA Handbook for audit data.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.97	The Credential Service shall receive request from online service to change Security Question.	VA Handbook 6500, Section 10	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
9.98	The Credential Service shall receive request when time has expired.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.99	The Credential Service shall receive request when user requests a change.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.100	The Credential Service shall process Security Question change.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.101	The Credential Service shall maintain a set list of questions to select from a predetermined list.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.102	The Credential Service shall require each question to be unique.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.103	The Credential Service shall retain user supplied answer.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.104	The Credential Service shall store successful security question change.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013
9.105	The Credential Service shall log the successful security question change.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.106	The Credential Service shall notify the user of the successful security question change.	FICAM v2, Section 9.4	High		FY14 8/15/2013
9.107	The Credential Service shall display error message to user when security question changes are unsuccessful.	IPT Approved (2012) CSP Business Packets	High		FY14 8/15/2013

OWNR #	Owner Requirement (OWNR)	Source	Priority	Comments	Release Date
Authentication					
Credential Validation – Provide a capability that establishes the validity of the identity credential presented as part of the authentication transaction.			Medium	* Credentials at Assurance Levels 2+ * Verify DSLogon account	FY14 8/15/2013
10.01	Provide the capability to validate multiple credentials for a given identity.	FICAM v2, Section 12.3.3	Medium		FY14 8/15/2013
10.02	Provide the capability to support credentials at every level of assurance (1-4) for a given identity.	FICAM v2, Section 12.3.3	Medium		FY14 8/15/2013
10.03	Provide the capability to limit the numbers of active credentials allowed for a given level of assurance for an identity through administrative controls.	FICAM v2, Section 12.3.3	Medium		FY14 8/15/2013
10.04	Provide the capability to allow the use of higher assurance credentials (level 2-4) for access to lower assurance resources.	FICAM v2, Section 3.2.5	Medium		FY14 8/15/2013
10.05	Provide the capability to consume credentials at Assurance Levels 4, 3, and 2 that are created and issued external to VA.	FICAM v2, Section 4.5.2, and 5.2.1.2	Medium		FY14 8/15/2013

User Profile: VA Employee or Contractor on the VA Network accessing the CSP service to update, upgrade, suspend, or revoke a credential to be used to access a VA application

2.5.2. Overview of Functional Workload / Performance Requirements

The CSP service shall support the following:

Operation	
Name	CSP (Credential Registration)
Usage Profile (Registration Events)	
Mean Daily volume	0
Projected Growth	1000/year
Peak Daily volume	0
Projected Growth	1000/year
Peak Hourly volume	0
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	8am-10p.m.Eastern
Maximum Response Time	10 seconds

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

Table 20: Performance Specifications

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

The performance specifications include the following:

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

The metric data indicating the performance characteristics of the system to support application monitoring is provided.

2.5.3. Overview of Operational Requirements

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

Table 21: Service Availability Level 4

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

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

2.5.4. Overview of the Technical Requirements

The CSP system design relies heavily on the basic installation and configuration of COTS products to meet the technical requirements that sufficiently meet the detailed functional requirements. The CSP solution design leverages primarily the Identity Manager and SiteMinder CA components of the IAM infrastructure and applies specific configurations and customizations to the base infrastructure to create the technical solutions necessary to meet the business requirements outlined in previous section. Where necessary, web pages have been designed and developed to provide richer content and a higher level of customizations not available with the basic product installation and configurations.

Please refer to the Master RTM below for Technical Requirements.

2.5.5. Overview of the Security or Privacy Requirements

Per Section 2.13 of the AcS 2.0 RSD, the security specifications include the following:

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

2.5.6. Overview of System Criticality and High Availability Requirements

Per Section 2.11 of the AcS 2.0 RSD, the VA AcS infrastructure supports critical business systems. The current availability requirement for mission critical systems is 99.9%. The current data centers support 99.6% availability. The Production, Preproduction, and Disaster Recovery (DR) Data Center is hosted by Terremark in Culpeper, Virginia and Miami, Florida. Terremark does not currently support an active/active geographic failover and load balancing thus failover to the DR site could take between one (1) and eight (8) hours. To mitigate the risk of not having a complete site failover, the AcS production infrastructure is intended to be scalable with limited single points of failure. The primary production platform is virtualized with a physical servers dedicated to Oracle RAC and VDS.

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

- Full backups are taken of virtual machines on a weekly basis
- Backups of virtual machines must be transported off-site at least monthly

- Backups of specific databases will be taken daily between the hours of 2 a.m. and 5 a.m. Locations of the databases will be provided in the POM.

2.5.7. Single Sign-on Requirement

VA CSP is a credential provider that is integrated with SSOe to allow single sign-on. CSP leverages SSOi use for admin access. Therefore this section is N/A.

2.5.8. Requirement for Use of Enterprise Portals

N/A

2.5.9. Special Device Requirements

N/A

2.6. Legacy System Retirement

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

Figure 13 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.

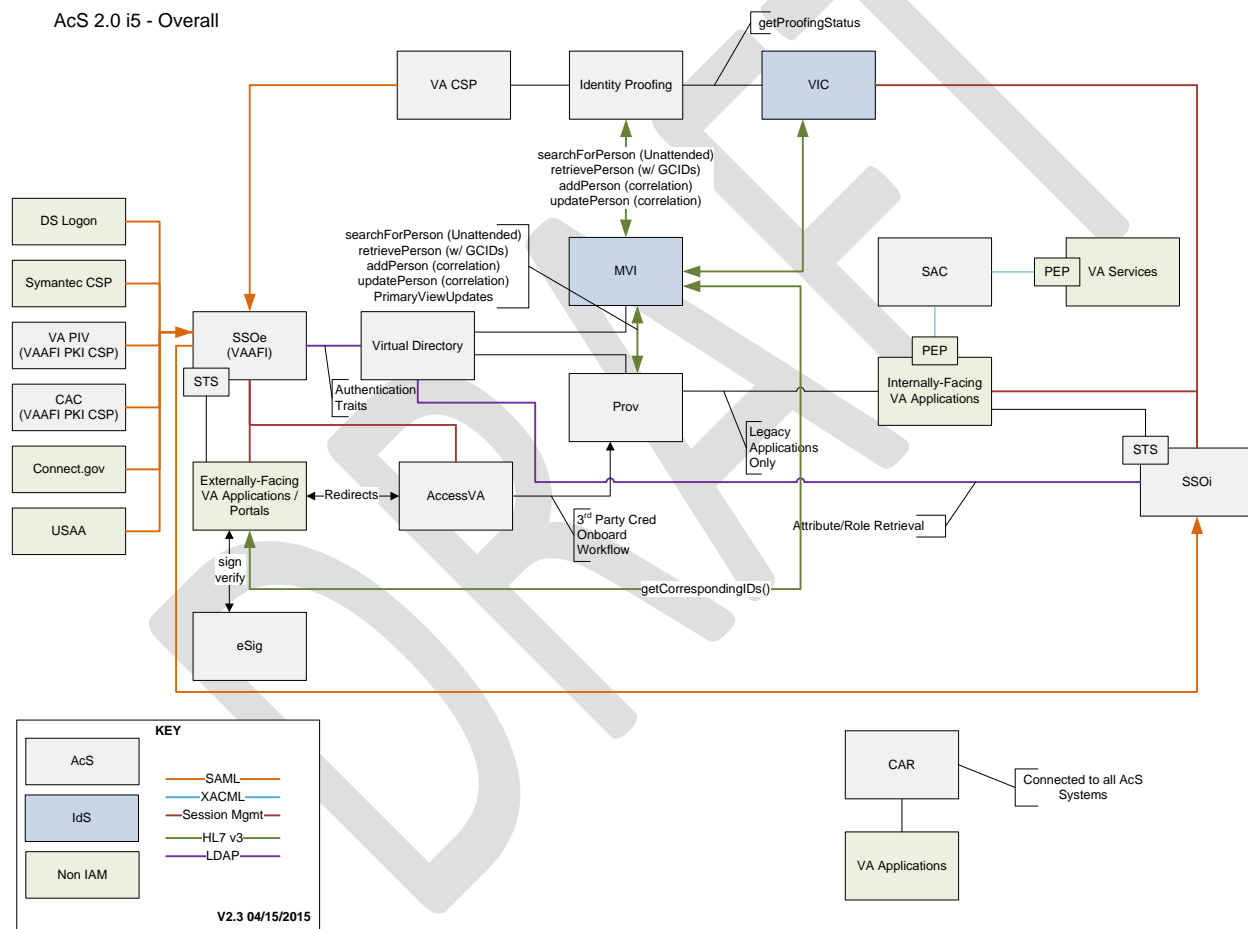


Figure 13: AcS 2.0 Overview

The CSP solution activities is described in greater detail below.

3.1.1. Application Context

Credential Service Provider (CSP) is an integral component of the VA 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 14 below is an expansion of CSP process from Figure 13 above.

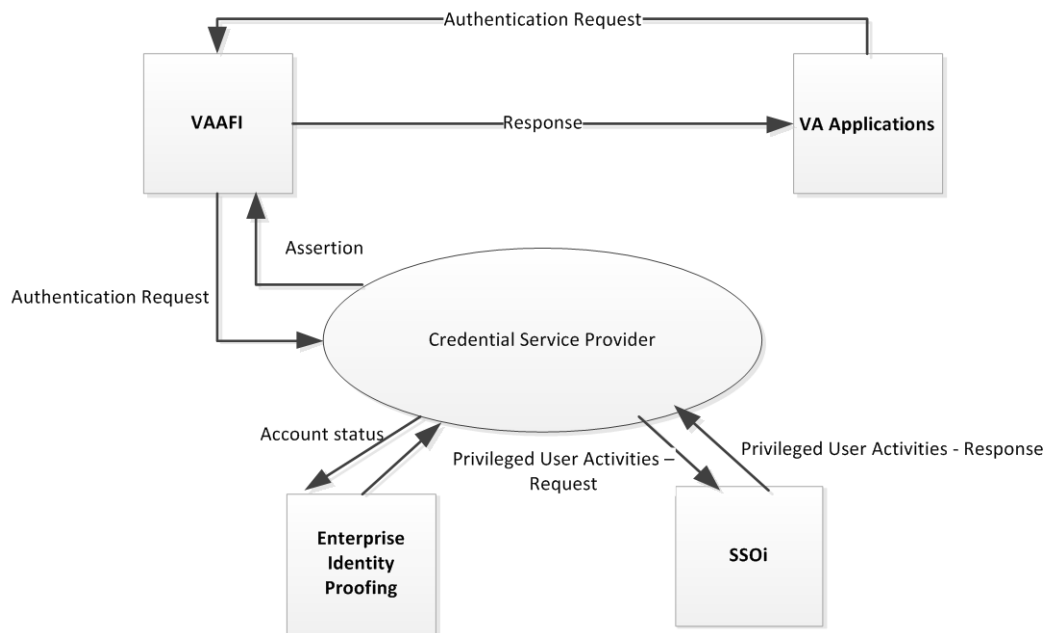


Figure 14: CSP Context Diagram

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

Table 22: CSP Application Context Description

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

3.1.2. High-Level Application Design

Figure 15 below provides a high-level application design for the CSP and identifies the major activities and/or relationships with VA applications.

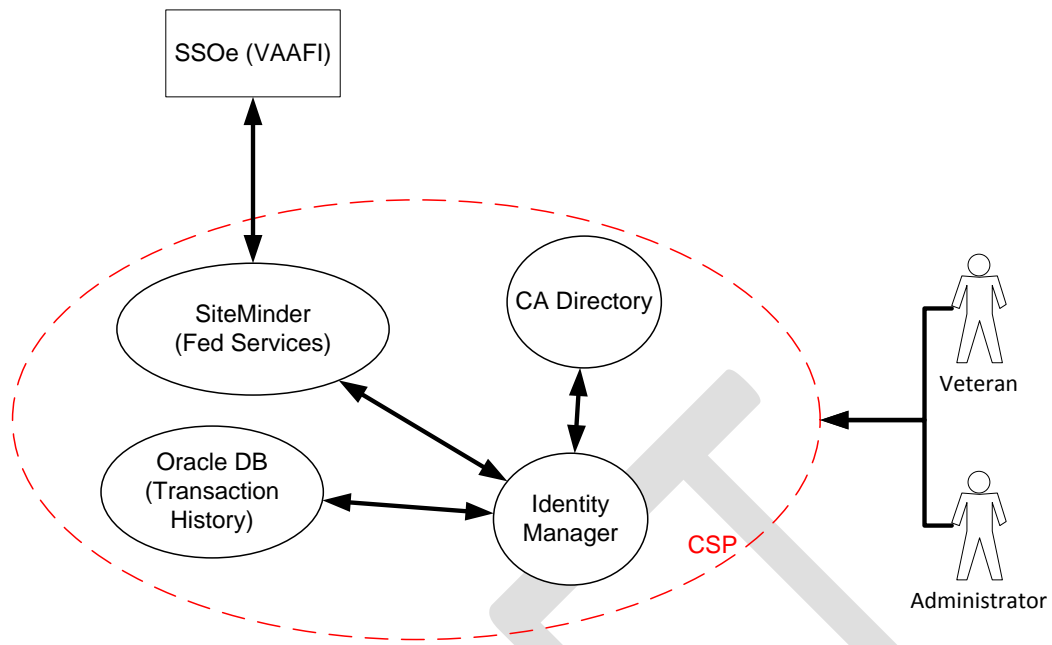


Figure 15: CSP Application Design

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

As depicted in the high level diagram, the CSP system components are highly integrated and together provide the end-to-end solution. Table below shows how the design utilizes the software components and the related infrastructure component CSP. The external interfaces are interfaces for systems outside of VA and internal interfaces are interfaces for systems within VA.

Table 23: Activities in the High-Level Application Design

Objects								
Name	ID	Description	Service or Legacy Code	External Interface Name	External Interface ID	Internal Interface Name	Internal Interface ID	SDP Sections 1&2
Identity Manager	1	Front end for managing users profiles and credentials both via self-service and administratively	Service	SSOe VAAFI	1	CA Directory Provisioning Workflow SiteMinder	4 2 3	n/a
SiteMinder (Federation Services)	3	Frontend service for authenticating CSP users and providing SSOe (VAAFI) with authentication assertions	Service	None	n/a	Identity Manager	1	n/a
Internal Data Stores								
Name	ID	Data Stored		Steward		Access		
CA Directory	4	Identity data - Backend storage for Identity Manager		CSP – Identity Manager		Create, Read, Update, Delete		
Oracle Database		Transaction Audit Data & System Log Data		CSP – Identity Manager				

3.1.3. Application Locations

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

Table 24: CSP Solution Application Locations

Application Component	AcS Service	Description	Location of Component
IIS Web Server	SSOi, Provisioning, CSP, IP	Front end web server providing the administrative and self-service interface to CA IdentityMinder	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
Oracle WebLogic	Provisioning, CSP, IP	Application server hosting CA IdentityMinder, Provisioning Server, SiteMinder and federation.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
CA IdentityMinder	Provisioning, CSP, IP	CA IdentityMinder delivers a unified solution for user provisioning that manages users' identities throughout their entire lifecycle, providing them with timely, appropriate access to applications and data.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
CA Directory	SSOi, Provisioning, CSP, IP	LDAP directory to support CA SiteMinder, CA SSO and CA IdentityMinder backend configuration and data store.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
Oracle Database	SSOi, Provisioning, CSP, IP	Database to support CA IdentityMinder and audit logs from different components.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)
Report Server	SSOi, Provisioning, CSP, IP	Report server for CA SiteMinder and CA IdentityMinder	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)

3.1.4. Application Users

The CSP application is designed to provide access to external users and internal administrators. The two user types can be further defined by system level roles. Table below provides the application users and user functions that have been designed for the solution.

Table 25: CSP Application Users

Application Component	Role	Description	Source	Location
CA Identity Manager	Top Administrator	Highest-level administrator of CSP, controls SiteMinder	All	Terremark

Application Component	Role	Description	Source	Location
		Policies		
CA Identity Manager	Role Administrator	Responsible for assignment of Roles & Privileges	Identity Manager via CSP GUI	Terremark
CA Identity Manager	Auditor	Responsible for running reports and tracking individual audit records and verifying continual system conformance with security and policy	Identity Manager via CSP GUI	Terremark
CA Identity Manager	Helpdesk	Responsible for specific user support	Identity Manager via CSP GUI	Terremark
CA Identity Manager	ID Proofer	Responsible for Identity Proofing users to comply with SP 800-63 and VA 6501	Identity Manager via CSP GUI	Terremark
CA Identity Manager	Level 1 User	General user of the system	Identity Manager via CSP GUI	Terremark
CA Identity Manager	Level 2 User	Identity proofed user	Identity Manager via CSP GUI	Terremark
CA Identity Manager	ID Proofer Manager	Manager for ID proofer	Identity Manager via CSP GUI	Terremark
CA SiteMinder	SiteMinder Admin	Administrator to manage CSP related domain objects	Siteminder UI	Terremark
CA Directory	Directory Admin	Administrator to manage the CSP directory module	CA directory	Terremark
Oracle Database	Oracle Admin	Oracle role which provides access to IM related tables	Oracle Database	Terremark

3.2. Conceptual Data Design

The CSP data model is designed to provide a schema that covers the data attributes necessary to meet the functional requirements, as well as provisions for the security of sensitive data types. The CSP data model design leverages the default schema of the CA Directory, and provides specific extension to the default scheme to meet the specific requirements of credentialing and ID proofing. The following sections provide the conceptual data design for the CSP 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 conceptual data model for the CSP contains known entities required to persist user and administrator information to fulfill CSP Level 1 and Level 2 credentialing requirements. The following diagram represents the conceptual data design separated by the major data categories that make up the total data schema:

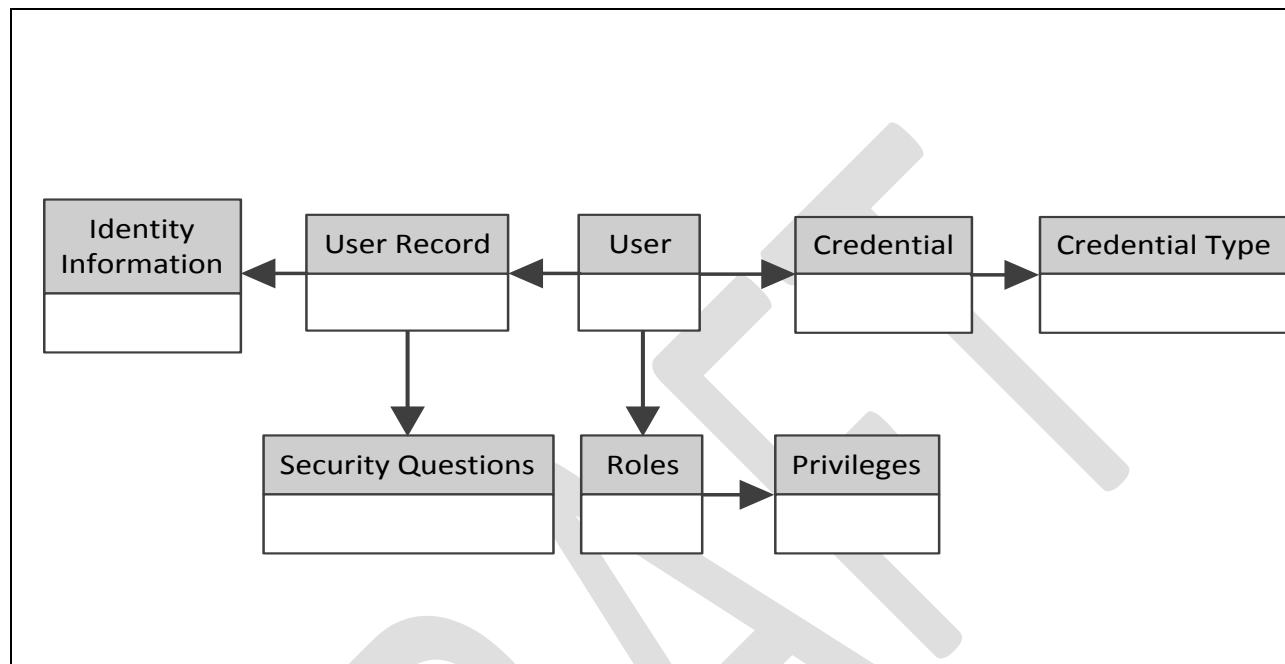


Figure 16: CSP Conceptual Data Model

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

Table 26: Conceptual Data Model Description

Index	Identifier	Description
1	User	Entity that represents a user that has completed registration or has been manually added by an administrator. Please note, CSP stakeholders that wish to use credentials to access VA services will NOT be manually created. Manual creation is available for administrators to create additional administrator accounts
2	Credential	The user ID and password of a registered user
3	Credential Type	Denotes the rules specific to credential, (e.g. E-Authentication), and level of assurance (e.g. Level 1, Level 2), the credential represents
4	User Record	Management information stored about the user
5	Identity Information	Demographic and identity-specific information stored about the user
6	Security	User defined questions utilized when a user forget their credential

Index	Identifier	Description
	Questions	
7	Roles	Assignment of a Role provides a set of Privileges for specific user
8	Privileges	Fine grained entitlements that grant access to specific objects with the CSP

DRAFT

Table 27: Database Inventory

Ref	Object	Description	Input Relationship	Output Relationship
①	Identity (Person)	The Identity object is a set of attributes that define an identity in the VA. Identity traits are correlated and a secure identifier is assigned.	<ul style="list-style-type: none"> - One Identity 	<ul style="list-style-type: none"> - One Identity can be assigned to 0 or more Roles. - One Identity can own 0 or more Accounts. - One Identity has only one security identifier for the lifetime of the identity.
②	User (Account)	The User (Account) attributes define the login information associated with the access control for a managed resource as well as information deemed necessary to perform the business processes or data synchronization requirements.	<ul style="list-style-type: none"> - One Account is owned by 0 (means orphan account) or one Identity (the base identity to which other accounts are linked). 	<ul style="list-style-type: none"> - A user account is represented by a credential which is used for authorization and access to Services. - Account operations (add, modify, change password, suspend, restore, delete, etc.) follow one or more workflows.
③	Role	The Role attributes defines the role and the associated privileges that can be assigned to a user.	<ul style="list-style-type: none"> - One Identity can be assigned 0 or more Roles. 	<ul style="list-style-type: none"> - One Role can be members of 0 or more Provisioning Policies. - One Role can participate in 0 or more Entitlement Workflows.
④	Provisioning Policy	The Provisioning Policy object is a definition of the level of access that may be granted to a managed resource or service to particular membership(s) or Roles. The provisioning policy defines identity reconciliation and identity feed.	<ul style="list-style-type: none"> - One Role can be assigned to 0 or more Provisioning Policies. - Each Provisioning Policy may have 0 or more Roles. 	<ul style="list-style-type: none"> - One Provisioning Policy may define 1 or more Entitlements.

Ref	Object	Description	Input Relationship	Output Relationship
⑤	Entitlement	The Entitlement object is a part of the Provisioning Policy that contains the service targets and associated provisioning parameters.	<ul style="list-style-type: none"> - One Provisioning Policy may have 1 or more Entitlements. 	<ul style="list-style-type: none"> - One Entitlement can apply to 0 or more Services. It may also apply to a type of service or all services. - One Entitlement can start 0 or 1 Workflows to govern the creation or modification of accounts on an associated service.
⑥	Workflow	The Workflow object represents a business process that is associated with an action or a policy. A workflow implements the steps that are required to approve or reject a request, such as a request to provision a person with a new account.	<ul style="list-style-type: none"> - 0 or 1 Workflow can be started by 0 or more Entitlements. - 0 or more Roles can participate in workflows. - 1 or more Workflows can be started by Identity operations. - 1 or more Workflows can be started by Account operations. 	N/A
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. 	N/A
⑧	User Policy	The User Policy contains the rules by which a user's account is created on a managed resource.	N/A	<ul style="list-style-type: none"> - One user policy can be applied to 0 or more Services.
⑨	Password Policy	The Password Policy object sets rules that passwords must meet.	N/A	<ul style="list-style-type: none"> - One password policy can be applied to 0 or more Services.

3.2.2. Database Information

CSP's primary data repository is in the form of directory, based on Lightweight Directory Access Protocol (LDAP) v3. Based on the CA tool suite selected for use, the LDAP service persists data within a Relational Database Management System (RDBMS). Direct access to the RDBMS will not be allowed. All data queries will be executed against the directory with valid LDAP syntax. The following table identifies the Oracle Database instances that will be created or interfaced with by the different activities.

Table 28: Database Information

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

The CSP application stores data in several locations. The CA Directory server is used by SiteMinder and Identity Manager for storing user and configuration information. SiteMinder will use a CA Directory server that is installed locally for Policy and Configuration information. Identity Manager will use a CA Directory server that is running on its own VMs where it will store credentials and identity attributes in a User Container or (User Store). The CSPP application makes use of Oracle database for storage of workflow information as well as auditing, reporting, and logging information.

The table below defines the LDAP schema designed to meet the needs of the CSP system and associated functional and technical requirements. The schema makes use of both existing and extended CS Directory attributes. The Shareable Column indicates only that the data is available for sharing if required, but does

not mean they are shared at this time. In addition, the only systems accessing this user store will be the Identity Manager and it will not be available for direct access by any users other than system admins.

DRAFT

Table 29: LDAP Attributes

Index	Attribute	Attribute Description	Data Format	Why	Shareable	Indexed
1	Userid	Login Username	Clear Txt - Any alphanumeric character, plus space and dash	Ops	y	y
2	VAIAM CSP ID	Internal identifier	Clear Txt - "VACSP" Prefix w/(8) Alpha	Ops	y	n
3	First Name	First Name	Clear Txt - Letters, plus apostrophe and dash	SP 800-63	y	y
4	Last Name	Last Name	Clear Txt - Letters, plus apostrophe and dash	SP 800-63	y	y
5	Middle Initial	Middle Initial	Clear Txt - Letter or Blank	Support	y	n
6	e-mail addr	Validated e-mail address	Clear Txt - Any alphanumeric, dot or dash before the @, then allows alphanumeric and dash, then requires a dot and then a string of 2-4 alphanumeric	Ops	y	n
7	VA Affiliation	VA Affiliation of User	Clear Txt - Enumeration/Pull-down List	Support	y	n
8	Passwd	Password set by User	Hashed - VA Password Complexity Rules	Ops	n	n
9	Security Question & Answer #1-5	Identifier of which question + txt answer	Encrypted - Any text	Ops	n	n
10	Assurance Level	Level of assurance tied to user	Clear Txt - Enumeration	SP 800-63	y	y
11	Status of User	Active/Disabled	Clear Txt - Enumeration	Ops	n	n
12	DOB	Date of Birth	Encrypted - Date	SP 800-63	n	n
13	User Phone Number	Phone number following US Standard (E.164 future)	Encrypted - 10 digit	Ops	y	n
14	Address	Number, Street, Unit	Encrypted - Any alphanumeric character, plus dot, dash	SP 800-63	y	y
15	City	City	Clear Txt - Any alphanumeric character, plus dot, dash	SP 800-63	y	n
16	State	State	Clear Txt - Enumeration	SP 800-63	y	n

Ind ex	Attribute	Attribute Description	Data Format	Why	Sharea ble	Index ed
17	Postal Code	Postal Code	Encrypted - Numbers	SP 800- 63	y	n
18	Country	Country (Default to US)	Clear Txt - Enumeration	SP 800- 63	y	n
19	Proofed Address	Number, Street, Unit	Encrypted - Any alphanumeric character, plus dot, dash	SP 800- 63	n	y
20	Proofed City	City	Clear Txt - Any alphanumeric character, plus dot, dash	SP 800- 63	n	n
21	Proofed State	State	Clear Txt - Enumeration	SP 800- 63	n	n
22	Proofed Postal Code	Postal Code	Encrypted - Numbers	SP 800- 63	n	n
23	Proofed Country	Country (Default to US)	Clear Txt - Enumeration	SP 800- 63	n	n
24	Address Validation Method	Verified by Utility Bill, Letter from VA, Personnel Letter	Clear Txt - Enumeration	SP 800- 63	n	n
25	Postmark Date	Postmark Date of mail used for Address Validation	Clear Txt - Date	800- 64	n	n
26	Primary Gov Photo ID Type	Driver's Lic, Passport, National ID	Encrypted - Enumeration	SP 800- 63	n	y
27	Primary Gov Photo ID Country	Country of Issuance	Encrypted - Enumeration	SP 800- 63	n	n
28	Primary Gov Photo ID State/Pro vince	State/Province of Issuance	Encrypted - Enumeration	SP 800- 63	n	n
29	Primary Gov Photo ID Number	Identifying number	Encrypted - Any text	SP 800- 63	n	y
30	Primary Gov Photo ID Exp Date	Expiration Date	Encrypted - Date	SP 800- 63	n	y

Ind ex	Attribute	Attribute Description	Data Format	Why	Shareable	Indexed
31	Secondary GOV ID Type	Driver's Lic, Passport, National ID	Encrypted - Enumeration	VA 6501	n	y
32	Secondary GOV ID Country	Country of Issuance	Encrypted - Enumeration	VA 6501	n	n
33	Secondary GOV ID State	State/Province of Issuance	Encrypted - Enumeration	VA 6501	n	n
34	Secondary GOV ID Number	Identifying number	Encrypted - Any text	VA 6501	n	n
35	Secondary GOV ID Exp Date	Expiration Date	Encrypted - Date	VA 6501	n	n
37	ID Proofer	VAIAM CSP ID Internal Identifier of ID Proofer	Clear Txt - "VACSP" Prefix w/(8) Alpha	SP 800-63	n	y
38	ID Proofing Location	Location of identity proofer	Clear Txt - Enumeration	Ops	n	y
39	ID Proofing Status Comments	Comments for failed identity proof status; failed other	Clear Txt - Enumeration	Ops	n	y
40	Role	Store the admin role of the users	Clear Txt - Enumeration	Ops	y	y
41	Policy	Store the policy express rules executed for the user	Clear Txt - Enumeration	Ops	n	y

3.2.3. User Interface Data Mapping

This section describes and defines the data that will be available for users of the CSP 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. Application Screen Interface

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

3.2.3.1.1. Modify Account: Step 1 User Profile

The following screen, Figure 17, is used to capture the user information when modifying user information and security questions.

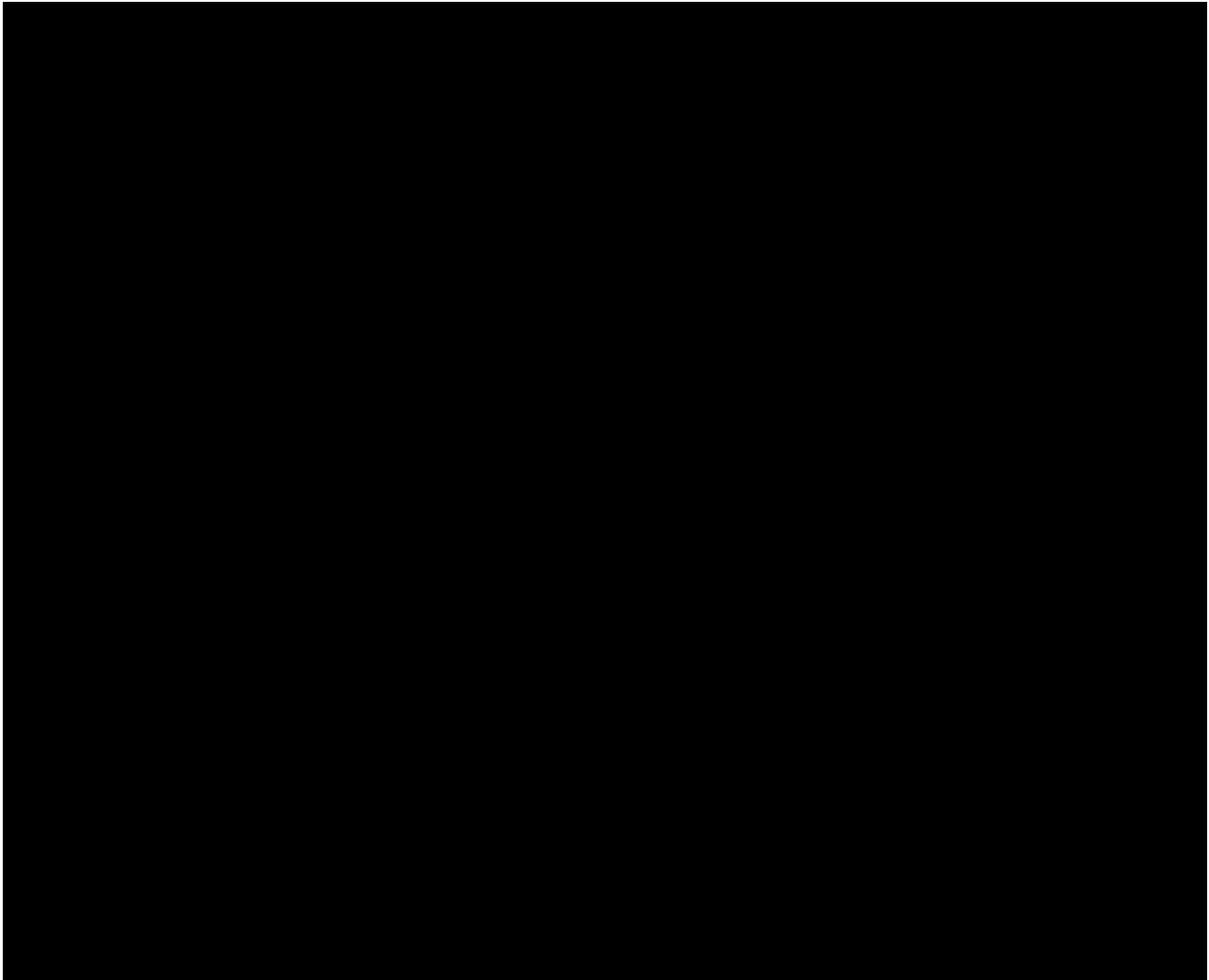


Figure 17: Modify Account: Step 1 User Profile Screen

Refer to section A.8 below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

Table 30: Modify Account: Step 1 User Profile Screen Description

Graphical User Interface (GUI) Field	Table (Database Table that field connects to)	Field (Field in Table that the GUI field connects to)	Comments
First Name	given name	First Name	Non-multivalued String. Maximum length of 100.
Last Name	sn	Last Name	Non-multivalued String. Maximum length of 100
User ID	uid	User Id	Non-multivalued String. Maximum length of 100
Street Address	postalAddress	Address	Encrypted Non-multivalued String. Maximum length of 100

Graphical User Interface (GUI) Field	Table (Database Table that field connects to)	Field (Field in Table that the GUI field connects to)	Comments
City	city	City	Non-multivalued String. Maximum length of 100
State	st	State	Non-multivalued String. Maximum length of 100
Country	c	Country	Non-multivalued String. Maximum length of 100
Postal Code	postalCode	Postal code	Non-multivalued String. Maximum length of 100

3.2.3.1.2. Modify Account: Step 2 Security Questions

The following screen, Figure 18, is used to capture the security questions and answers when modifying user information and security questions.

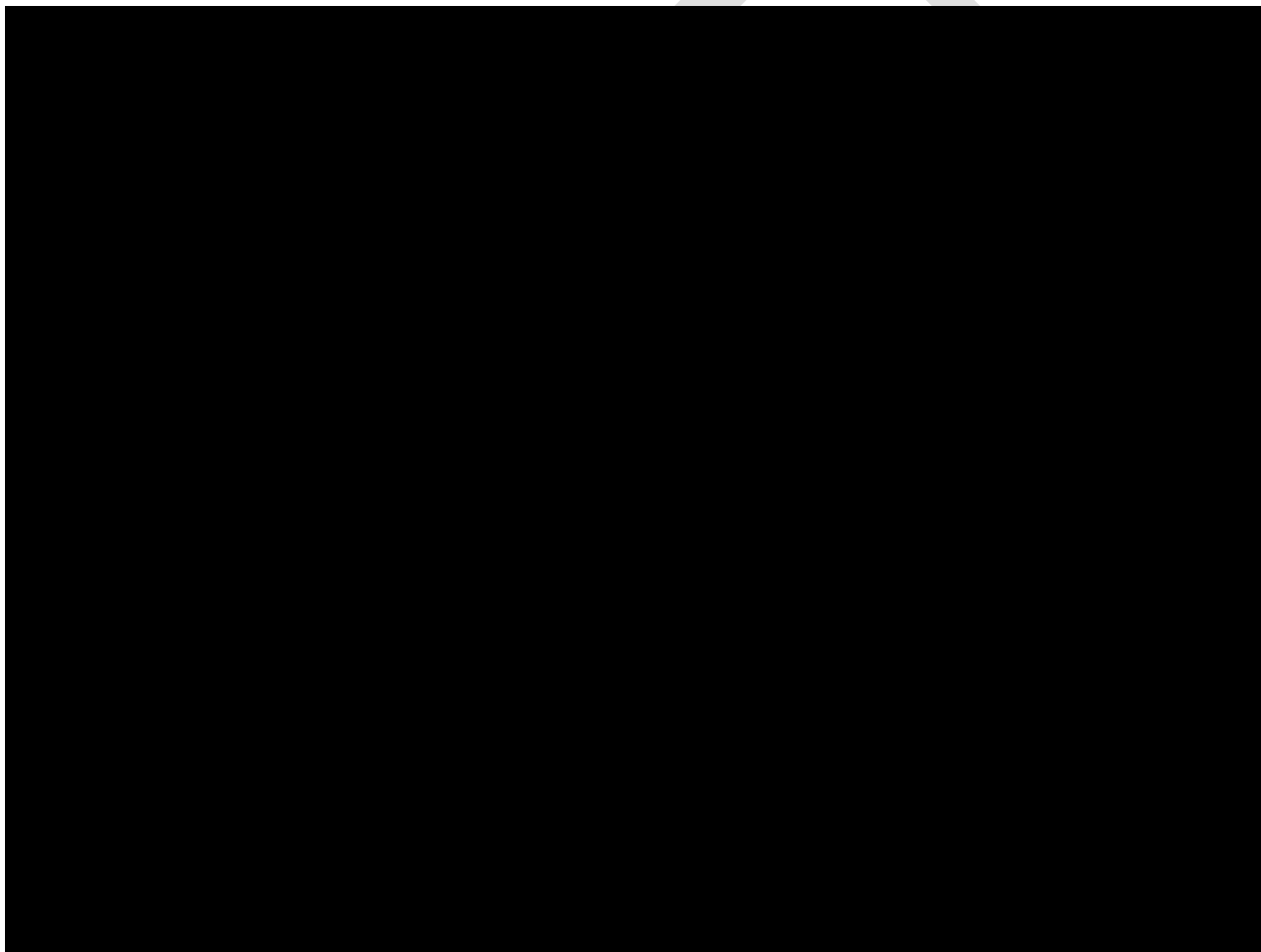


Figure 18: Modify Account: Step 2 Security Questions Screen

3.2.3.1.3. Change Password

The following screen, Figure 19, allows the user to change their password.

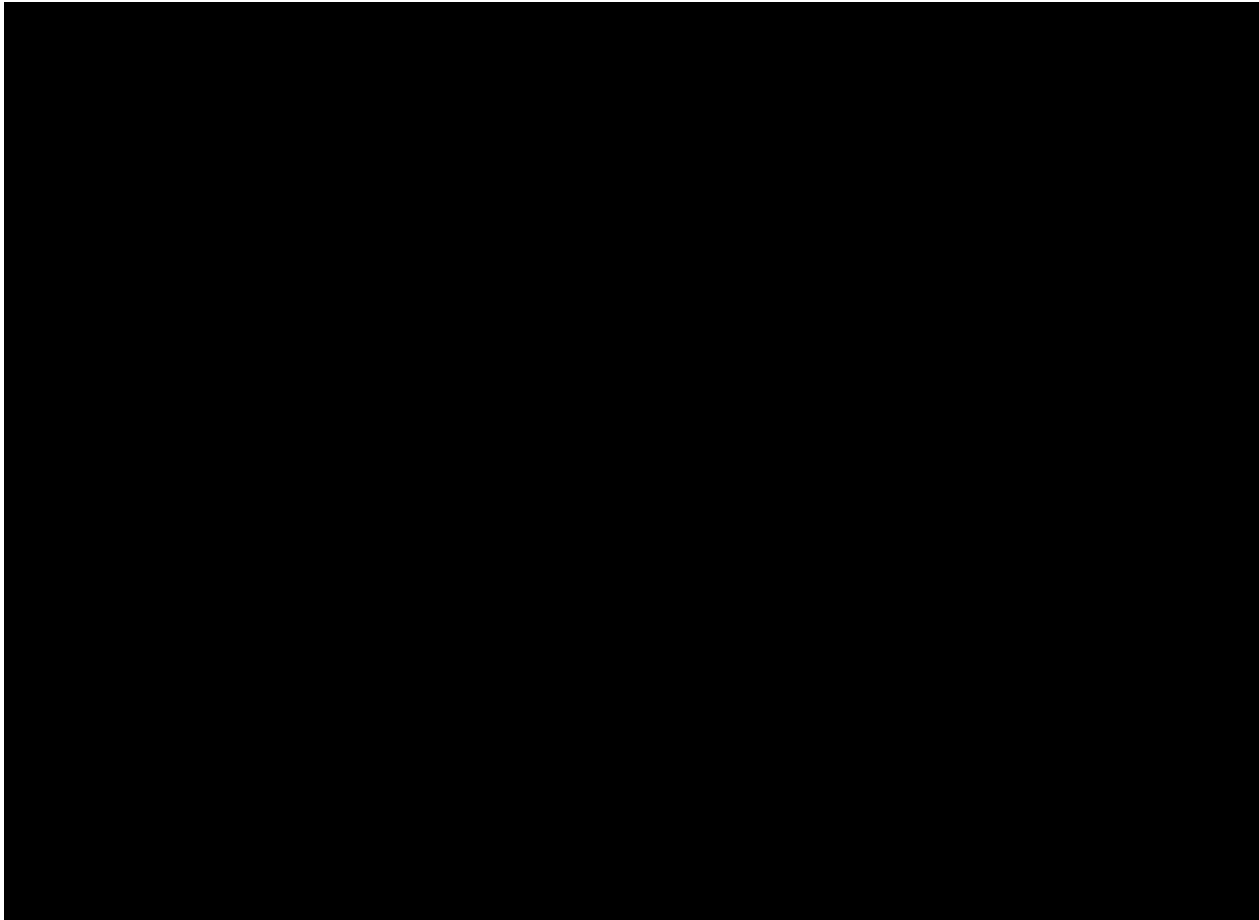


Figure 19: Change Password Screen

Refer to section A.8 below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

Table 31: Change Password Screen Description

Graphical User Interface (GUI) Field	Table (Database Table that field connects to)	Field (Field in Table that the GUI field connects to)	Comments
First Name	given name	First Name	Non-multivalued String. Maximum length of 100.
Last Name	sn	Last Name	Non-multivalued String. Maximum length of 100
User ID	uid	User Id	Non-multivalued String. Maximum length of 100
Password	userPassword	password	Hashed Non-multivalued String. Maximum length of 100

3.2.3.1.4. Upgrade to Level 2: Step 1 User Profile

The following screen, Figure 920: Upgrade to Level 2: Step 1 User Profile Screen, captures the user information when requesting to upgrade to level 2.



Figure 20: Upgrade to Level 2: Step 1 User Profile Screen

Refer to section A.8 below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

Table 32: Upgrade to Level 2: Step 1 User Profile Screen Description

Graphical User Interface (GUI) Field	Table (Database Table that field connects to)	Field (Field in Table that the GUI field connects to)	Comments
First Name	given name	First Name	Non-multivalued String. Maximum length of 100.
Last Name	sn	Last Name	Non-multivalued String. Maximum length of 100
User ID	uid	User Id	Non-multivalued String. Maximum length of 100
Street Address	postalAddress	Address	Encrypted Non-multivalued String. Maximum length of 100
City	city	City	Non-multivalued String. Maximum length of 100
State	st	State	Non-multivalued String. Maximum length of 100

Graphical User Interface (GUI) Field	Table (Database Table that field connects to)	Field (Field in Table that the GUI field connects to)	Comments
Country	c	Country	Non-multivalued String. Maximum length of 100
Postal Code	postalCode	Postal code	Non-multivalued String. Maximum length of 100

3.2.3.1.5. Upgrade to Level 2: Step 2 Security Questions

The following screen, Figure 21, captures the security questions and answers when requesting to upgrade to a Level 2 credential.

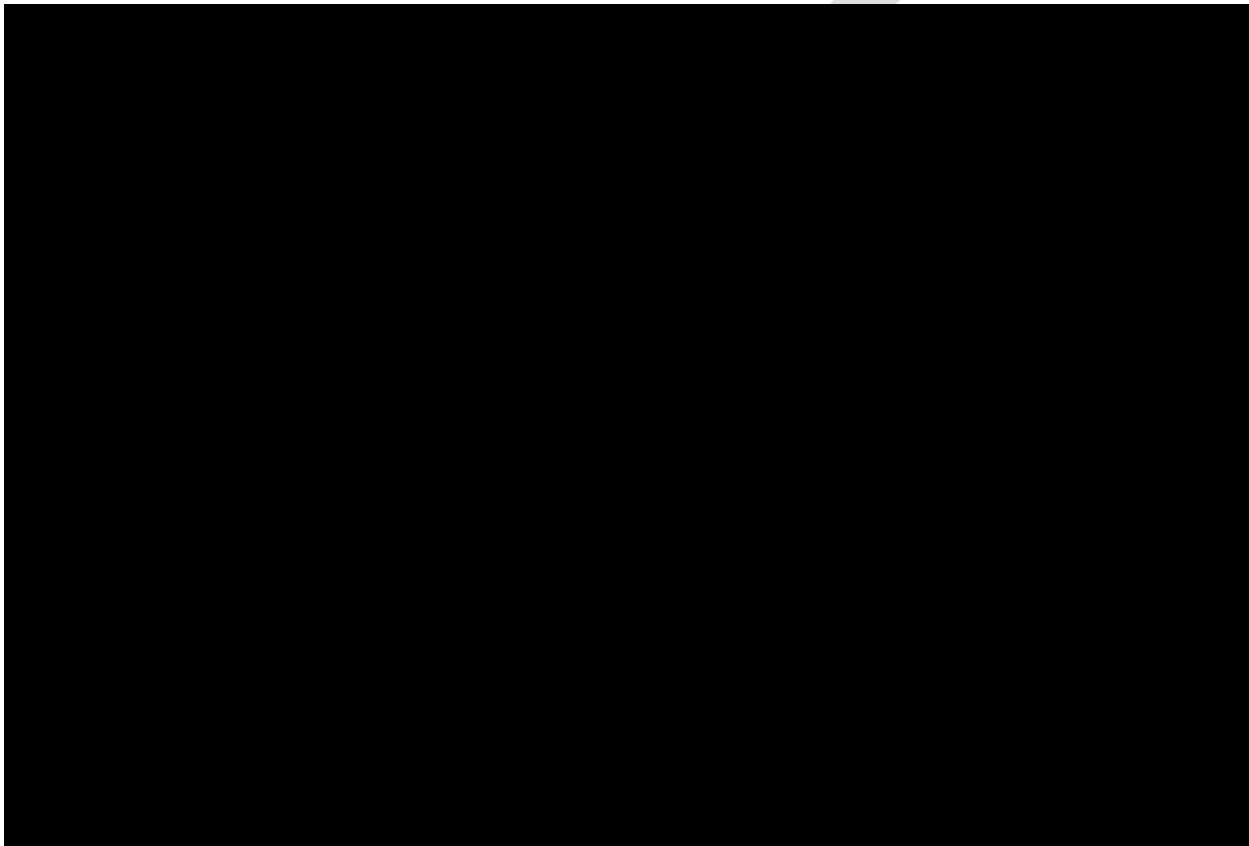


Figure 21: Upgrade to Level 2: Step 2 Security Questions Screen

3.2.3.1.6. Self-Registration: Step 1 User Profile

The following screen, Figure 22, captures the user information when self-registering.

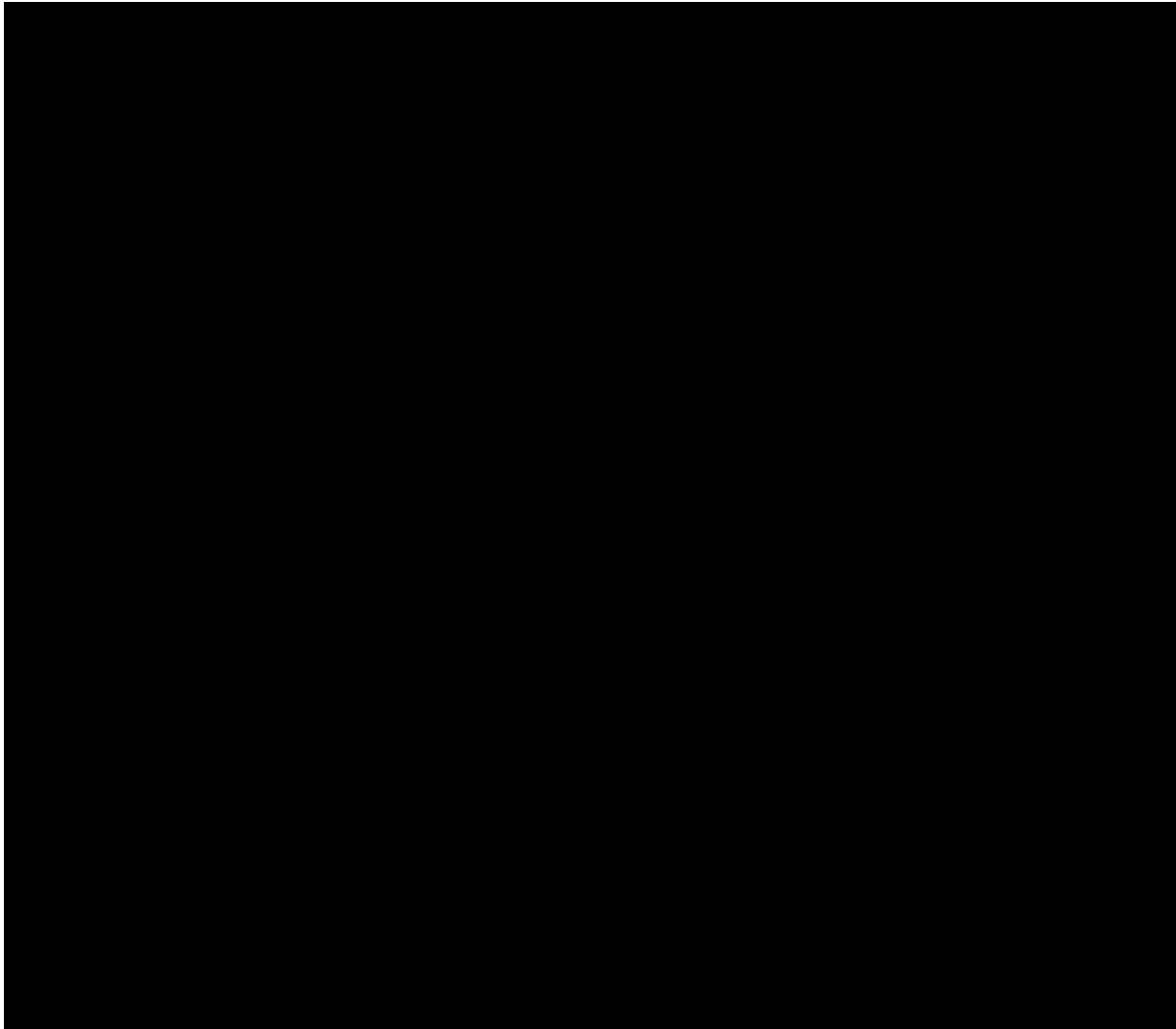


Figure 22 Self-Registration: Step 1 User Profile Screen

Refer to section A.8 below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions under the CSP tab.

Table 33: Self-Registration: Step 1 User Profile Screen Description

Graphical User Interface (GUI) Field	Table (Database Table that field connects to)	Field (Field in Table that the GUI field connects to)	Comments
First Name	given name	First Name	Non-multivalued String. Maximum length of 100.
Last Name	sn	Last Name	Non-multivalued String. Maximum length of 100
User ID	uid	User Id	Non-multivalued String. Maximum length of 100

Graphical User Interface (GUI) Field	Table (Database Table that field connects to)	Field (Field in Table that the GUI field connects to)	Comments
Street Address	postalAddress	Address	Encrypted Non-multivalued String. Maximum length of 100
City	city	City	Non-multivalued String. Maximum length of 100
State	st	State	Non-multivalued String. Maximum length of 100
Country	c	Country	Non-multivalued String. Maximum length of 100
Postal Code	postalCode	Postal code	Non-multivalued String. Maximum length of 100

3.2.3.1.7. Self-Registration: Step 2 Security Questions

The following screen, Figure 23: Self-Registration: Step 2 Security Questions Screen, captures the security questions when self-registering

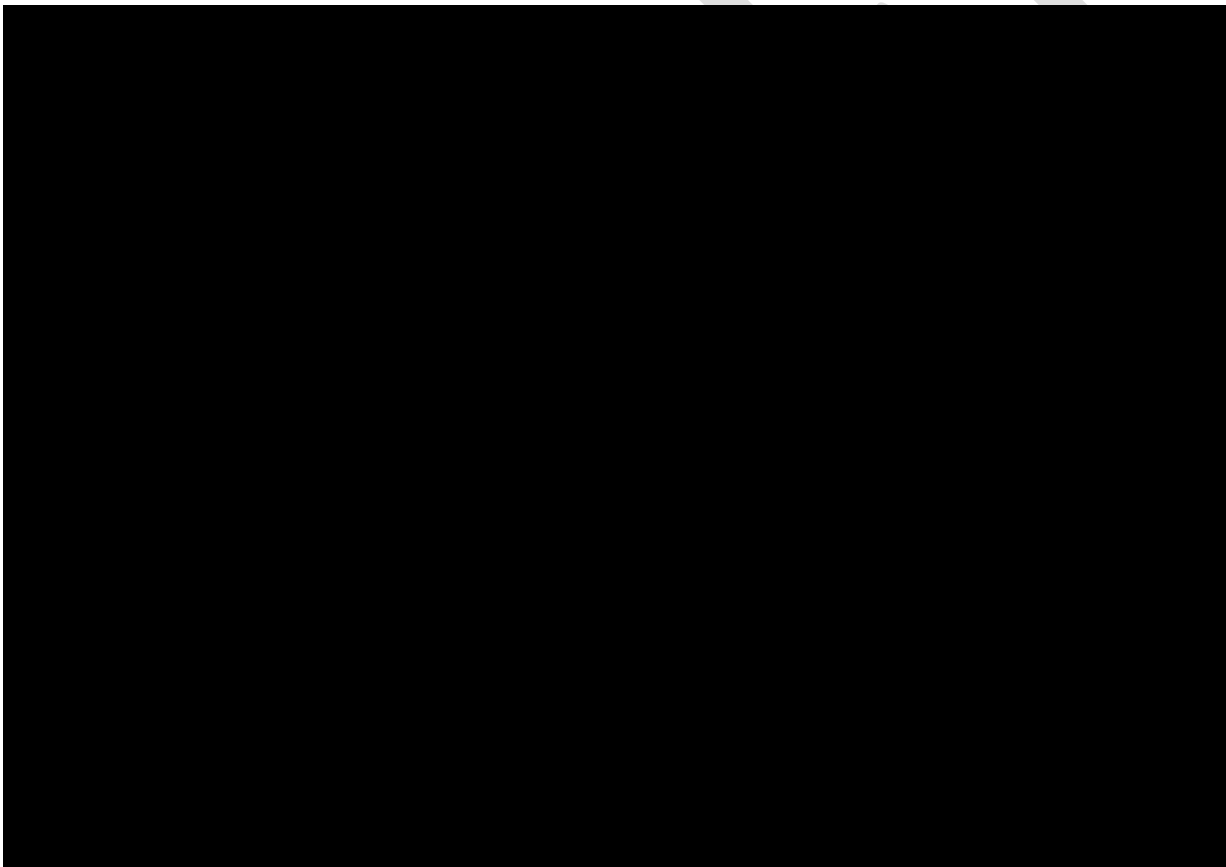


Figure 23: Self-Registration: Step 2 Security Questions Screen

3.2.3.2. Application Report Interface

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

3.2.3.3. Unmapped Data Element

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

Type	Attribute Name	Description	Object Class	Screen Name	Value type	multivalued	Maximum length	Encryption	Permission
Identity Information	cn	FullName	inetOrg	Full Name	String	no	100	None	READWRITE
	givenName	First Name	inetOrg	Last Name	String	no	100	None	READWRITE
	initials	initials	inetOrg	initials	String	no	100	None	READWRITE
	sn	Last Name	inetOrg	Last Name	String	no	100	None	READWRITE
	uid	User ID	inetOrg	User ID	String	no	100	None	WRITEONCE
	userPassword	Password	inetOrg	Password	String	no	100	Hashed	READWRITE
User Information	c	Country	country	Country	String	no	100	None	READWRITE
	city	City	inetOrg	City	String	no	100	None	READWRITE
	l	Location	inetOrg	Location	String	no	100	None	READWRITE
	mail	mail	inetOrg	mail	String	no	100	None	READWRITE
	postalAddress	Address	inetOrg	Address	String	no	100	Encrypted	READWRITE
	postalCode	Postal code	inetOrg	Postal code	String	no	100	None	READWRITE
	st	State	inetOrg	State	String	no	100	None	READWRITE
Access Control Attributes	telephoneNumber	Business Phone	inetOrg	Business Phone	String	no	100	None	READWRITE
	VACCESSROLES	Admin Roles Admin (IdM)	VAPerson	Admin Roles Admin (IdM)	String	yes	100	None	READWRITE
	VACCESSROLESADMIN	Access Roles Admin (IdM)	VAPerson	Access Roles Admin (IdM)	String	yes	100	None	READWRITE
	VADMINROLES	Used as a constraint for IM admin roles	VAPerson	Admin roles	String	yes	100	None	READWRITE
CSP Information	VADMINROLESADMIN	Admin Roles Admin (IdM)	VAPerson	Admin Roles Admin (IdM)	String	yes	100	None	READWRITE
	VACCOUNTSTATUS	Status of User	VAPerson	VACCOUNTSTATUS	String	no	100	None	READWRITE
	VAAFFILIATION	VA Affiliation of User	VAPerson	VAAFFILIATION	String	no	100	None	READWRITE
	VAASSURANCELEVEL	Assurance Level	VAPerson	VAASSURANCELEVEL	String	no	100	None	READWRITE
	VACREXPDATE	Credential Expiration Date	VAPerson	VACREXPDATE	String	no	100	None	READWRITE
	VACREDSTAT	Credential Status	VAPerson	VACREDSTAT	String	no	100	None	READWRITE
	VADOB	Date of birth	VAPerson	VADOB	String	no	100	Encrypted	READWRITE
	VAFORGOTTENQUESTIONS	Password Hint	VAPerson	VAFORGOTTENQUESTIONS	String	no	100	Encrypted	READWRITE
	VAIDPROOFSTATUS	VA ID Proofer Status	VAPerson	VAIDPROOFSTATUS	String	no	100	None	READWRITE
	VAPASSWORDDATA	Used by password policies	VAPerson	VAPASSWORDDATA	String	no	100	None	READWRITE
	VAREGDATE	Credential Registration Date	VAPerson	VAREGDATE	String	no	100	None	READWRITE

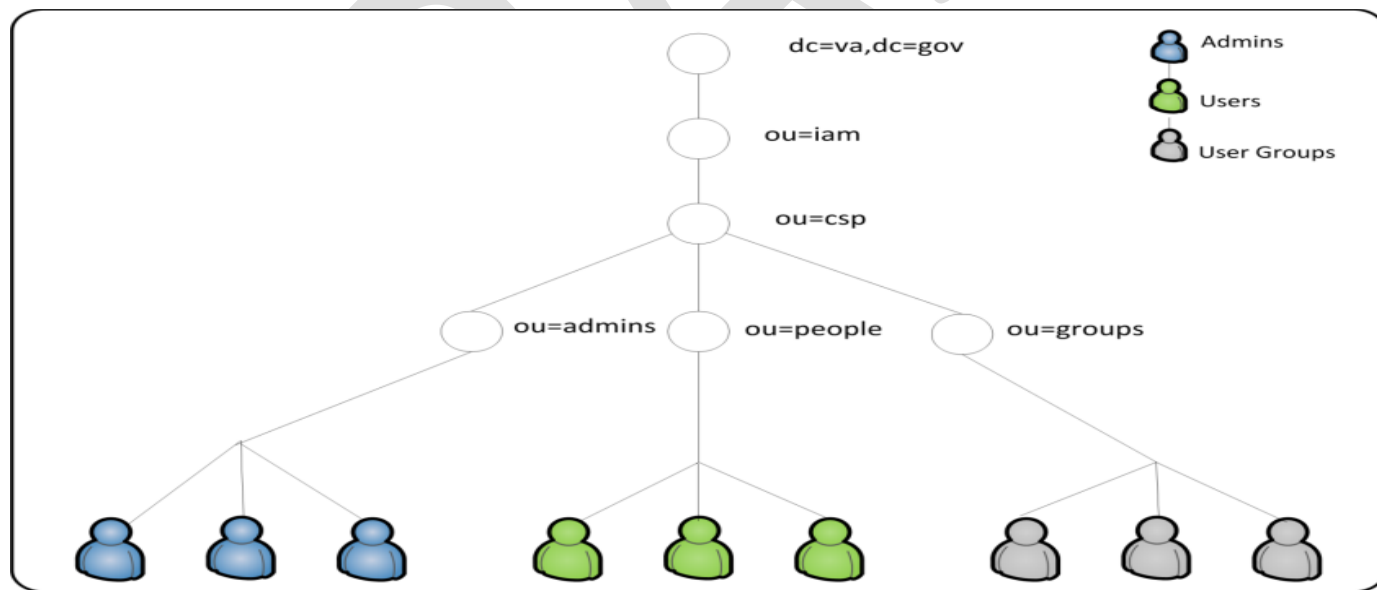


Figure 22: CSP Data Elements

3.3. Conceptual Infrastructure Design

The CSP system is the aggregate of a number of components that interact to form the basic structure of the CSP application. By coordinating the components, CSP provides a secure interface for users to self-register, perform ID proofing activities, authenticate and provide SAML assertions to VAAFI for federated access to VA systems, and

for administrators to monitor and manage the CSP application and users. The following set of products forms the basis for the system architecture.

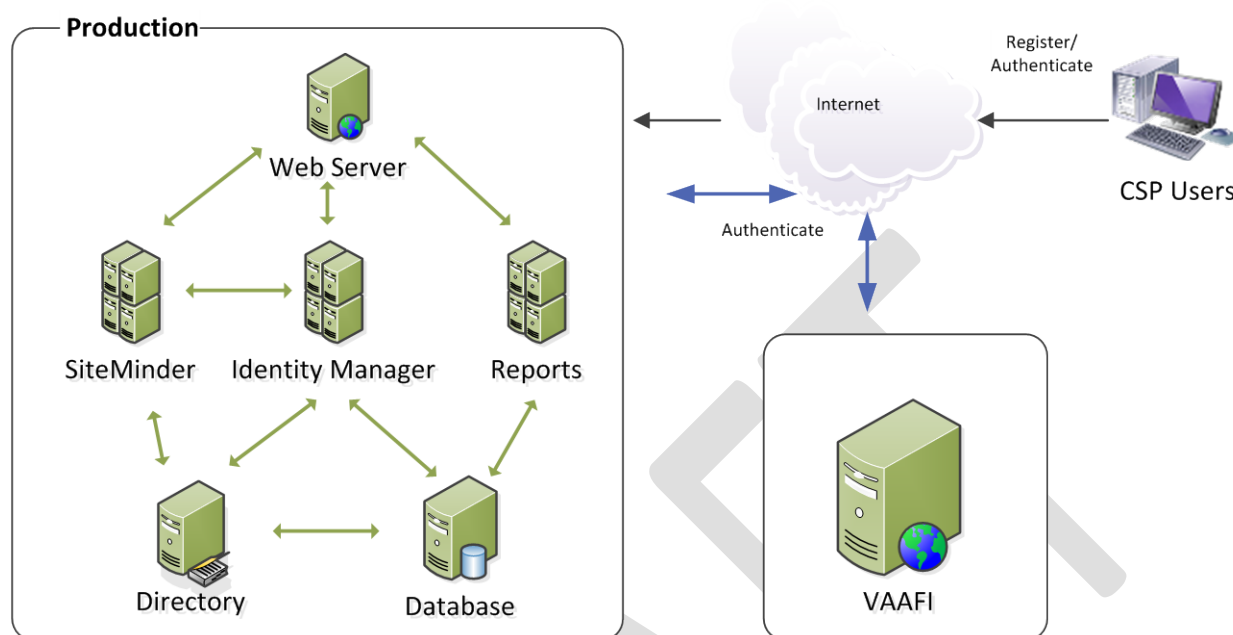


Figure 23: CSP Conceptual Infrastructure Diagram

3.3.1. System Criticality and High Availability

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

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

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

3.3.2. Special Technology

N/A

3.3.3. Technology Locations

The high-level conceptual infrastructure diagram for the VA AcS infrastructure is shown in Figure 13 below. The diagram also depicts the communication between the Terremark data centers in Culpeper, Virginia and Miami, Florida. The VA AcS infrastructure environment is set up at the Terremark data center in Culpeper, Virginia. The alternate site or disaster recovery site for VA AcS operations is the Terremark data center in Miami, Florida.

Being Developed

Figure 24: CSP Production Environments

Development Environment (DEV) AITC – Austin, TX

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

Software Quality Assurance (SQA) AITC – Austin, TX

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

Pre-Production – Terremark Culpeper, VA

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

Production – Terremark Culpeper, VA

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

Production Disaster Recovery (DR) – Terremark Miami, FL

- This site provides hot failover capability so that services and data are maintained in the event of a failure in Production.
- This environment is identical to the Production environment.
- Once the change to Production is verified, the change is implemented in the DR environment.
- The DR environment is in the Terremark Miami, FL data center. The environment is configured with an Active-Passive topology.

- The identity services components like CA IdentityMinder, CA SiteMinder, Provisioning Manager, CA report server, CA UARM would be configured to be on software load balanced on their local site.
- There will be a directory and database synchronized across a private OC-12 connection between both sites. Multiple instances of CA Directory are deployed locally at Terremark Culpeper, VA and remotely at Terremark Miami, FL data centers in a multi-write replication mode. Multi-write replication is a mechanism for replicating updates to a number of instances to maintain that the user stores are synchronized for internal and external users.
- Oracle Data Guard is utilized for database replication from the Production data center at Terremark Culpeper, VA to the disaster recovery data center at Terremark Miami, FL sending the archive logs at an incremental time span asynchronously down to as low as 1 second.

3.3.4. Conceptual Infrastructure Diagram

This section depicts the CSP 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.

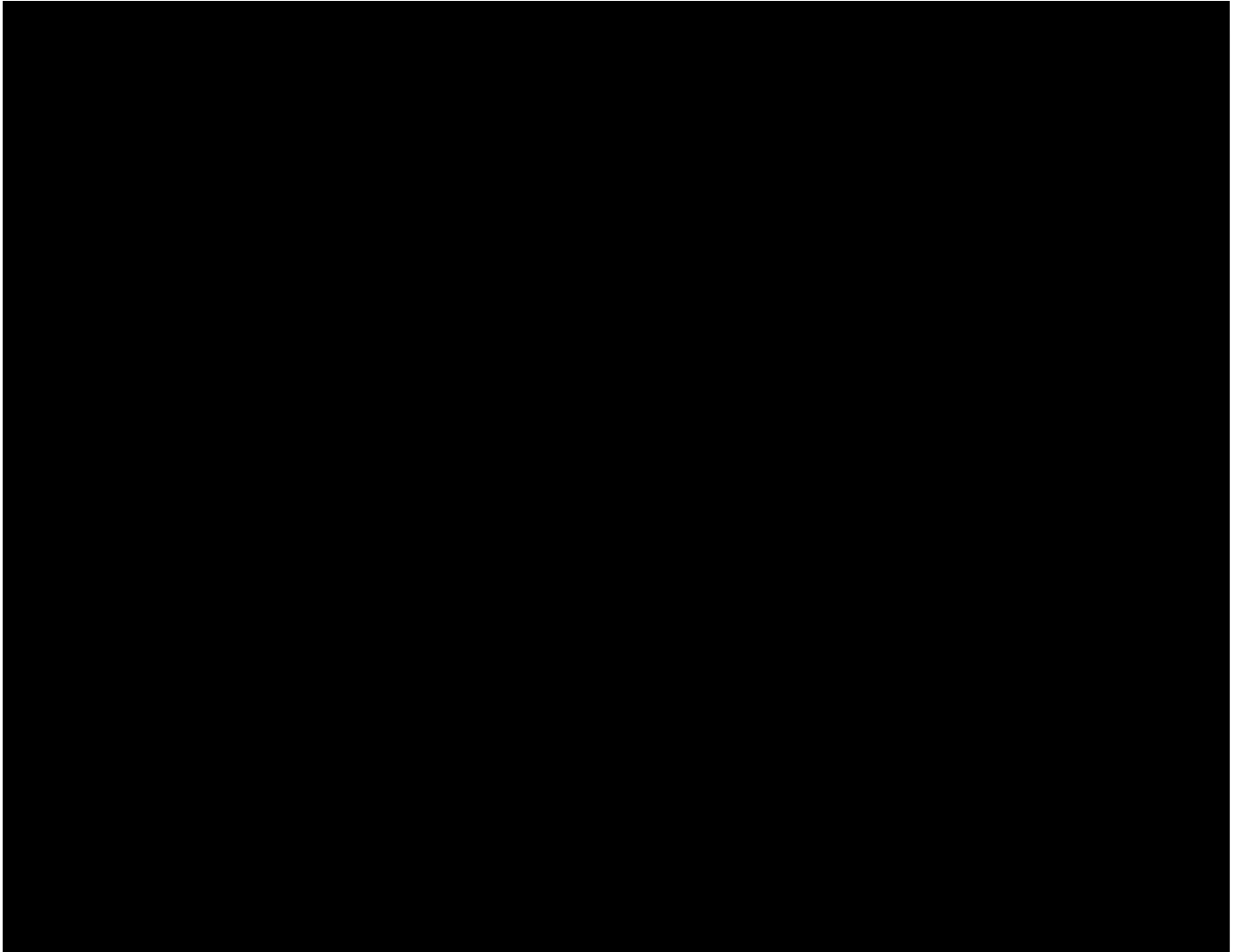


Figure 25: Sample Conceptual Networks and Environments

3.3.4.2. Conceptual Production String Diagram

The following diagram, Figure 26, provides a logical view of the CSP components.

CSP Logical/Network Architecture



Figure 26: Logical Network String Diagram

3.3.5. CA Identity Manager

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

- Creation of ID Management tasks that map to specific functional requirements.
- User provisioning, self-service requests, identity governance, and other key processes.
- The automation of on-boarding, off-boarding, and other parts of the identity life cycle.
- Support of password management, delegated administration, and role and policy management and analysis.
- Workflow capabilities and a host of connectors to provision and de-provision users to backend repositories such as Microsoft Active Directory.
- Access to scripts for designing the workflow processes.

A typical Identity Manager environment is shown in the figure to the right.

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

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

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

The CA SiteMinder and FSS services provide:

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

3.3.7. CA Directory

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

3.3.8. Identity Manager Workflow DB, Oracle Database Server

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

3.3.9. CA Report Server

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

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

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

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

The CSP application is also designed to be an identity provider to the VAAFI SSOe system. This is accomplished through the use of the SiteMinder Federation services. Once a user has a credential with the CSP, that person can use that credential to login to applications that are integrated with VAAFI through the federation of SAML 2.0 assertions. The CSP is designed to receive authentication requests from VAAFI when a user attempts to access a protected business application. The user is redirected to the CSP federation login to authenticate. Once authenticated the SAML assertion is created and the user is redirected back to VAAFI and ultimately to the business application. This process is designed to be seamless to the user. Additionally, once the user is authenticated in this manner, they will have single-sign-on to other business applications under the same security domain.

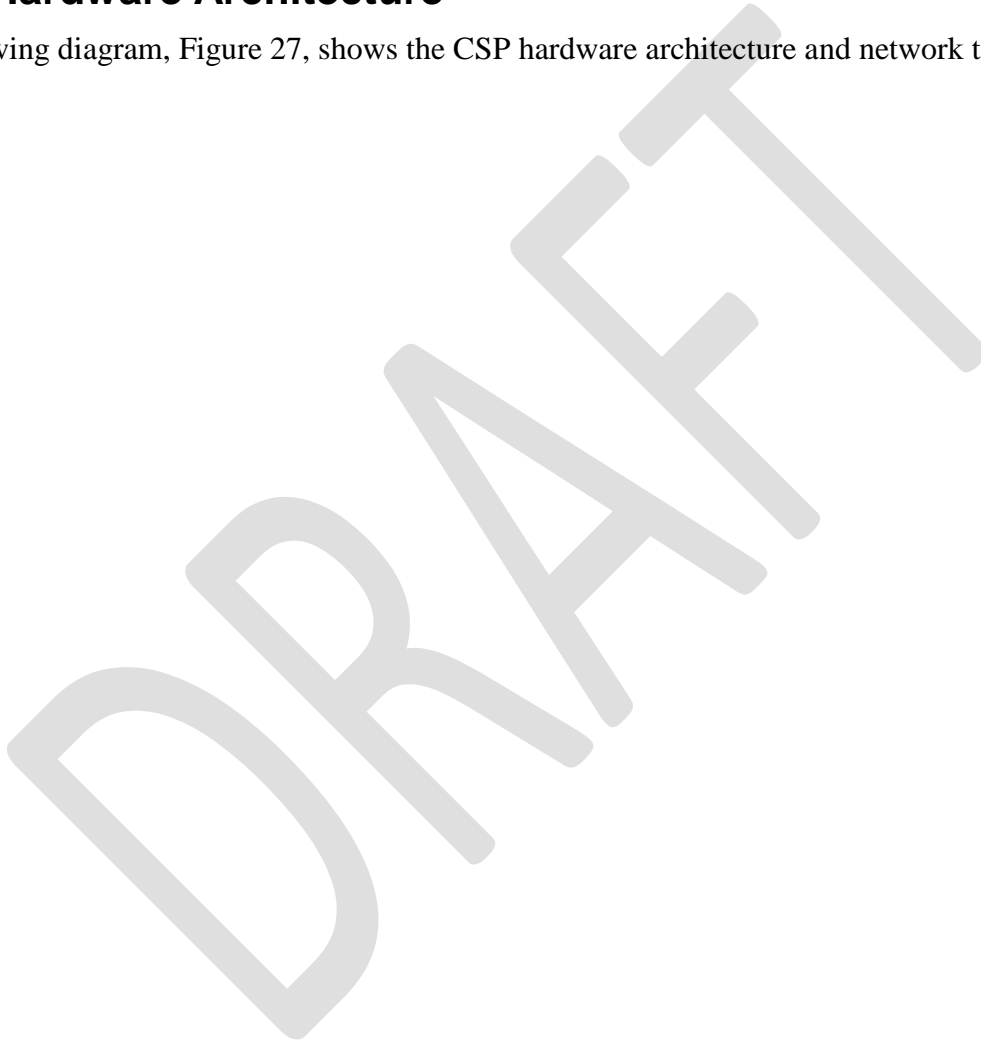
The CSP application is designed to produce highly detailed logging and auditing information. The CA IDM and SM products are configured to process logging with each transaction. The logging can be pushed to log files and then stored in the log database where the report server can generate valuable audit and management reports. For example, each time a user authenticates to the CSP application, an event is logged. That data is stored and can be pulled up in a report to determine the number of authentications that have occurred in the last day, week, month, etc.

4. System Architecture

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

4.1. Hardware Architecture

The following diagram, Figure 27, shows the CSP hardware architecture and network topology.



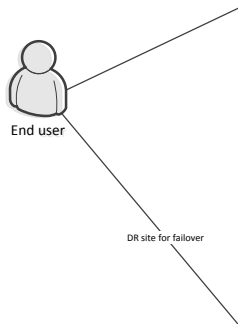


Figure 5: CSP Hardware Architecture

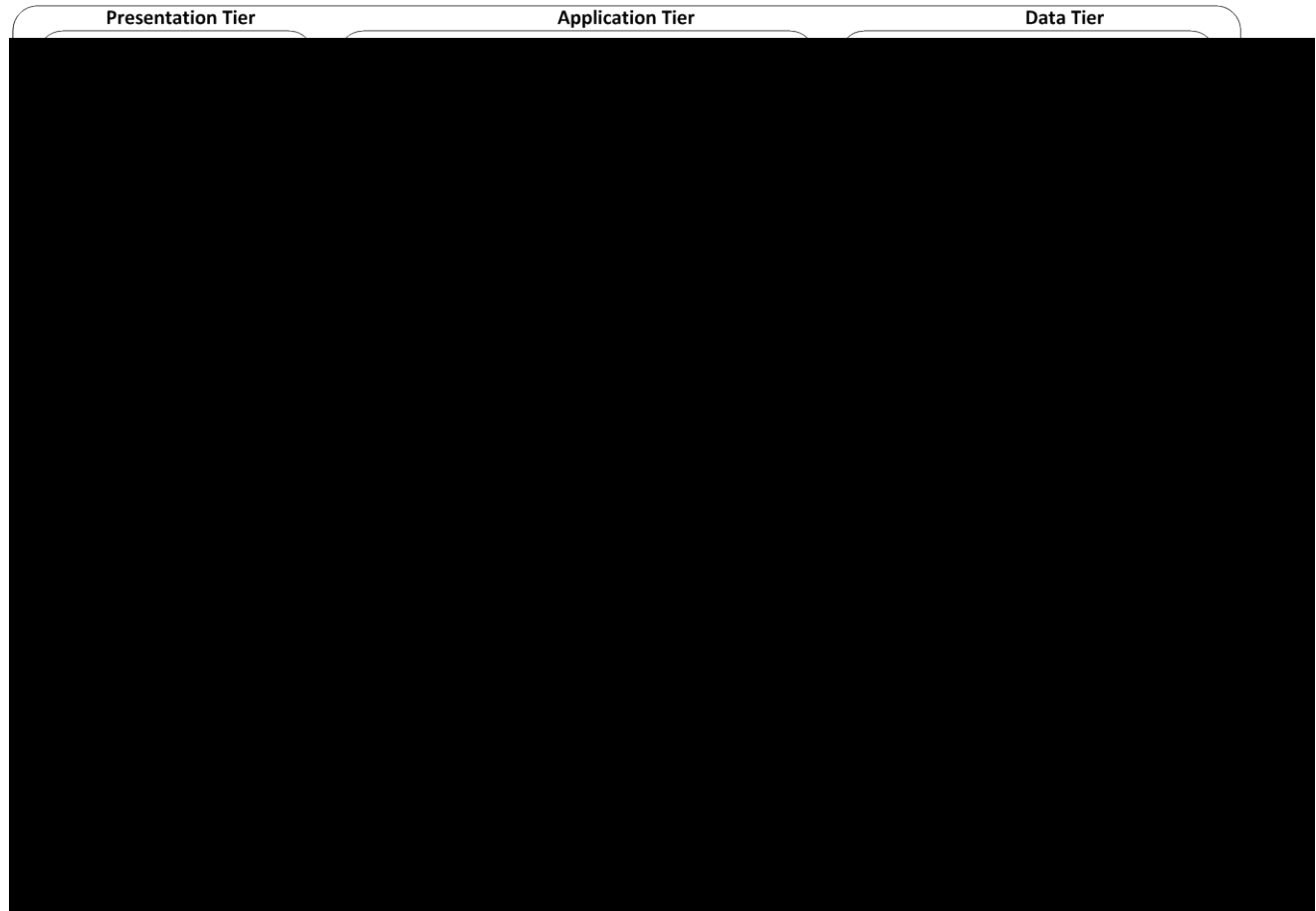


Figure 27: Network Communication Architecture

CSP solution architecture is composed of following components:

- **CA Identity Manager:** An integrated identity administration solution that serves as the foundation for CSP.
- **CA SiteMinder Policy Server – CA SiteMinder Federation Services:** The CSP federation engine component.
- **CA Directory:** Stores user information in the LDAP repository.
- **Identity Manager Workflow/Oracle Database Server:** Stores CA Identity Manager data.
- **Report Server:** Contains information from the Identity Manager object store and the Identity Manager user store.
- **Apache HTTP Server/ SiteMinder Web Agent:** The server that enables Federation Manager SSL federation traffic and secures the back channel for HTTP-Artifact single sign-on. The embedded Tomcat web server allows secured access to the UI.

The uniform resource locators (URLs) for CSP for production, pre-production and SQA are provided in the table below. The AcS components residing in the DMZ are the external facing web servers that contain the CSP pages and federation components. These components will be load balanced by the Citrix Netscalers located in the Terremark GSS. The remaining AcS application components will reside in the

GSS. The following table provides details on the AcS 2.0 machines such as ports, URLs, protocols hostnames for each application in every environment.

Table 34: Virtual Machines and Appliances

Application	Number of VMs	Number of Physical Servers	Hostname
CSP, IP, Federation Services WebUI, SPS, WSS (IIS- Single instance on each, Tomcat)	5	N/A	[REDACTED]
IdentityMinder supporting (Credential Service Provider and Identity Proofing) WebLogic cluster Admin service on primary node	3	N/A	[REDACTED]
CA Directory (CSP and IP)	3	N/A	[REDACTED]
CA Report Server (WebLogic)	2	N/A	[REDACTED]
CA SiteMinder (WebLogic) includes CA Directory instance for SiteMinder Admin service on primary node Admin UI on primary node	3	N/A	[REDACTED]

Pre-Production (Terremark Culpeper, VA)

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

Application	Number of VMs	Number of Physical Servers	Hostname
IdentityMinder supporting (Credential Service Provider and Identity Proofing) (WebLogic) Admin service on primary node	2	N/A	[REDACTED]
CA Directory (CSP and IP)	2	N/A	[REDACTED]
CA SiteMinder (WebLogic) includes CA Directory instance for SiteMinder Admin service on primary node Admin UI on primary node	3	N/A	[REDACTED]

Production (Terremark Culpeper, VA)

Application	Number of VMs	Number of Physical Servers	Hostname
CSP, IP, Federation Services WebUI, SPS, WSS (IIS) Single IIS instance on each	4	N/A	[REDACTED]
IdentityMinder (CSP and IP) (WebLogic) Admin service on primary node	2	N/A	[REDACTED]
CA Directory (CSP,IP)	2	N/A	[REDACTED]

Application	Number of VMs	Number of Physical Servers	Hostname
CA SiteMinder (WebLogic) includes CA Directory instance for SiteMinder Admin service on primary node Admin UI on primary node	3	N/A	[REDACTED]

DR (Terremark Miami, FL)

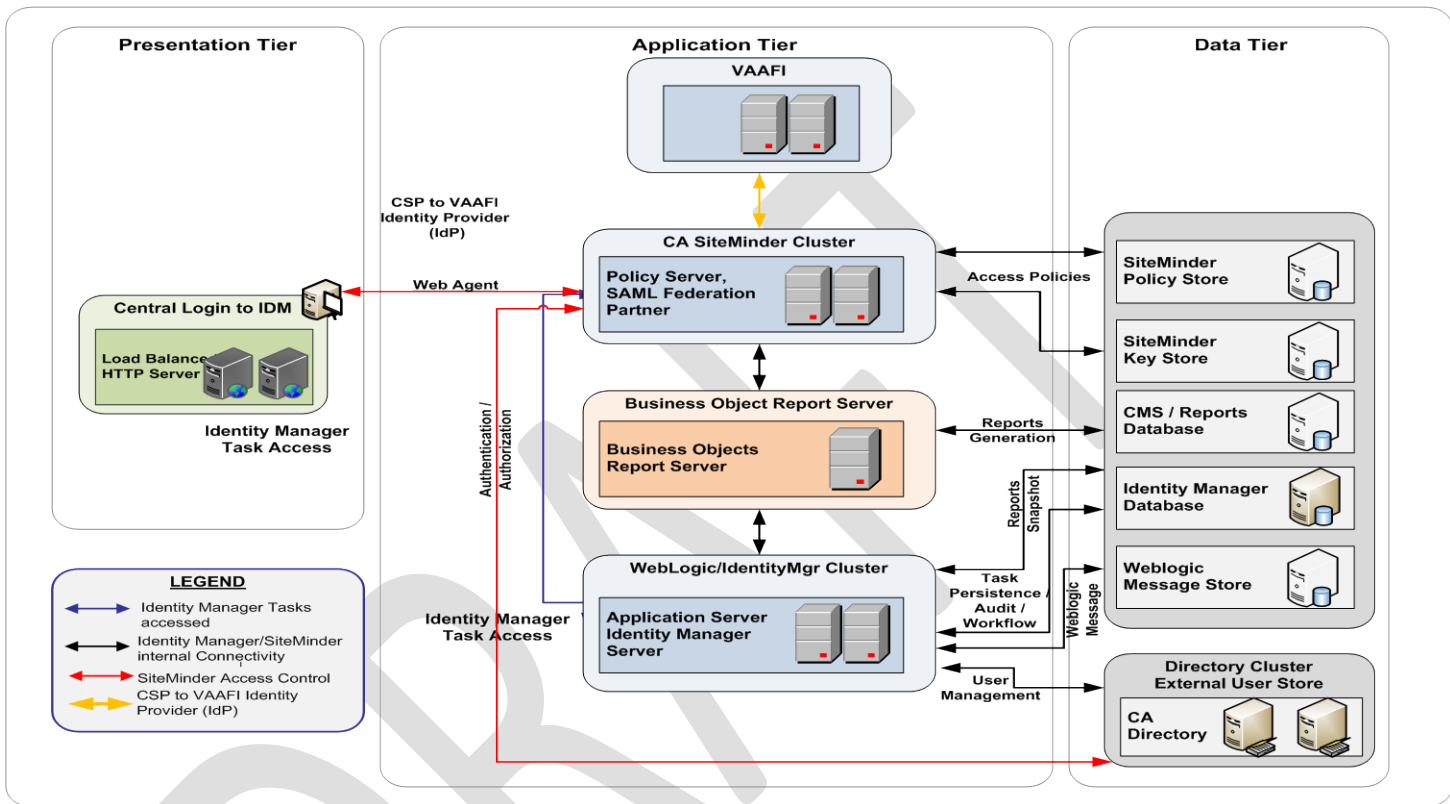
Application	Number of VMs	Number of Physical Servers	Hostname
CSP, IP, Federation Services WebUI (IIS)	4	N/A	[REDACTED]
IdentityMinder (CSP) (WebLogic)	2	N/A	[REDACTED]
CA Directory (CSP and IP)	2	N/A	[REDACTED]
CA SiteMinder (WebLogic) includes CA Directory instance for SiteMinder	2	N/A	[REDACTED]

4.2. Software Architecture

The following diagram shows the complete software architecture of CSP.

This section describes the overall software architecture for the CSP solution in the VA’s production environment. The below diagram provides the core components and interactions between components.

Figure 28: CSP Software Architecture



4.2.1. Presentation Tier

The presentation tier consists of the servers required to enable web-based access to the CSP solution. The CSP solution is based on the Microsoft Internet Information Services (IIS). The IIS server is also configured with the .NET framework in order to serve the custom web pages developed to supplement the IDM and SM pages. In addition, the SiteMinder web server is installed and configured on the IIS web server and connected to the SiteMinder policy server in the application tier. The web agent acts as the policy enforcement point for SiteMinder site protection services. In addition to the CSP application interface, a second IIS interface provides the federation capability to the CSP application. This IIS serves the sole purpose of providing the federated authentication mechanism. This technology is a web agent, configured with the specific agent required for federation. This agent is connected with the Policy Server to perform policy enforcement for the Federation component.

4.2.2. Application Tier

The application tier consists of the various application components of the CSP solution. These include the application servers hosting CA IDM, the Business Objects reporting server and SiteMinder Policy Server. Application servers for IDM are loaded with WebLogic to provide the application run time environment.

4.2.3. Data Tier

The data tier consists of the different data stores in the CSP solution, specifically the CA directory user store, SiteMinder policy store, reporting & logging database, CA IDM workflow database and the message stores.

Table 35 below describes each component of the CSP Software Architecture.

Table 35: CSP Software Components

Component	Description	Type
IIS Web Server	Front end web server providing GUI for CSP users and administrator activity for CA IDM, CA SiteMinder and CA UARM.	Presentation Tier
WebLogic Server	Application server hosting application CA IDM for CSP and Provisioning and SiteMinder Federation option pack for CSP.	Application Tier
CA IDM	COTS product for Provisioning and CSP	Application Tier
CA SiteMinder	COTS product for CSP	Application Tier
CA SSO Server	COTS product for SSOi	Application Tier
CA Directory	LDAP directory to support CA SiteMinder, CA SSO and CA IDM for data store	Data Tier
CA UARM	COTS product for CAR which will be the major report service for CSP	Application Tier
IBM Datapower	COTS product for communication to VAAFI	Application Tier

Component	Description	Type
Oracle RAC	Database to support CA IDM and audit logs from different components	Data Tier

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

Table 36: AcS Products and Versions
Credential Service Provider (CSP)

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

The following table provides information about the software components.

Table 37: Software Components
Oracle Database 11gR2

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

Characteristic	Description
Database Table spaces	Data Table spaces: CSPIPIDM_DATA, Index Table spaces: CSPIPIDM_INDX, Users Temp Rollback Undo

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

CA Directory

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

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

Characteristic	Description
Directory Instances	User store CA IdentityMinder for CSP solution and Provisioning services, Policy and Key store for CA SiteMinder for CSP service Object/policy store for CA SSO for SSOi services.

Characteristic	Description
High Availability	<p>There will be a master write server for each directory. The other supporting directories will be read directories.</p> <p>The CA Directory will provide intelligent and transparent chaining of queries to distributed servers. It performs transparent routing to re-route requests in the event of failure on a particular CA Directory server. The CA Directory router DSA distributes incoming requests evenly among DSAs in the same site. The clients accessing router dsa are configured to maintain the list of AcS CA Directory router DSA's and the failover occurs from the client's end. This improves performance, allowing CA Directory's replication mirroring to provide synchronized in real-time and consistent servers.</p> <p>CA IdentityMinder, CA SSO, and CA SiteMinder will leverage the directories through a round robin load balancing configuration. Multiwrite-DISP replication is a replication scheme that uses Multiwrite replication for real-time updates and DISP for recovery. By default, the Directory System Agent (DSA) is configured for Multiwrite-DISP replication. This replication scheme combines the efficiency of Multiwrite when DSAs are online (real-time updates), with the robustness of DISP to allow DSAs to recover after being offline (recovery).</p> <p>The DSA uses its routing capabilities to distribute requests evenly between systems while data replication keeps the data synchronized.</p>

Web Tier – IIS Web Server

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

Characteristic	Description
IIS Web Server Instances	CA IdentityMinder Registration / user profile management/admin UI for CSP service

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

Application Tier – WebLogic Application Server

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

Characteristic	Description
WebLogic Instances	<p>CA IdentityMinder for CSP and Provisioning solution</p> <p>CA SiteMinder Admin UI</p>

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

CA IdentityMinder

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

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

CA SiteMinder

CA SiteMinder is an integral component of Access Services solution, providing CSP solution federation capabilities to integrate with VAAFI. CA SiteMinder is also utilized to protect the CA IdentityMinder application. CA SiteMinder is comprised of the following components.

Characteristic	Description
Subcomponents	<p>SiteMinder Policy Server: The Policy Server provides advanced authentication and password services to protected applications such as CA IdentityMinder. The policy server communicates with the CA Directory, which stores the required policy objects, key objects and user data to provide federation services as well.</p> <p>Secure Proxy Server: The Secure Proxy Server provides agentless web based integration as well as provides secure web services calls supported by centralized policies defined in SiteMinder.</p> <p>Policy/Key Store: The policy store / key store is CA Directory instance which stores configured policies, objects and keys required by CA SiteMinder.</p> <p>Web Agents: The agents to be installed on the web server protect the resources.</p> <p>Admin User Interfaces: The Admin UI hosted in admin VLAN to manage CA SiteMinder and policies.</p> <p>FSS Administrative UI: The Federation Admin UI is hosted on same VM as CA SiteMinder to manage CA SiteMinder for federation configuration. It requires a web server as provided in the web tier above.</p> <p>Audit: The SiteMinder Audit sub-system stores audit events for SiteMinder authentication and authorization transactions. The data is stored in the oracle database and is secured from modifications.</p>
High Availability	<p>CA SiteMinder will be installed on three (3) servers. These servers will be load balanced using the native CA SiteMinder software configuration.</p> <p>The CA SiteMinder web agent HA is depending on Application Web server HA. If there are multiple IIS instance for the protected application, webagent is also on HA as it is installed on individual Web server. Webagent configured to talk to all the SiteMinder Policy Server available and internally it load balance the request in a round robin mode.</p>

The following tables shows the programming languages used for system CSP solution:

Table 38: Programming Languages

Programming Languages	Definition/Description
Java	Java language was used to develop custom class/jar file for Identity Manager BLTH.
C#/.net	C-Sharp/.net for development of custom applications
HTML / DHTML	Provides basic web page language
XML	Common configurations are stored as XML files.
ASP	Active Server Pages for development of web-pages. The SiteMinder login.fcc page was customized using this language.
XACML	XML-based language for development of privileges/role management

The following table lists the operating systems used for the VA AcS 2.0.

Table 39: Operating Systems

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

4.3. Network Architecture

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

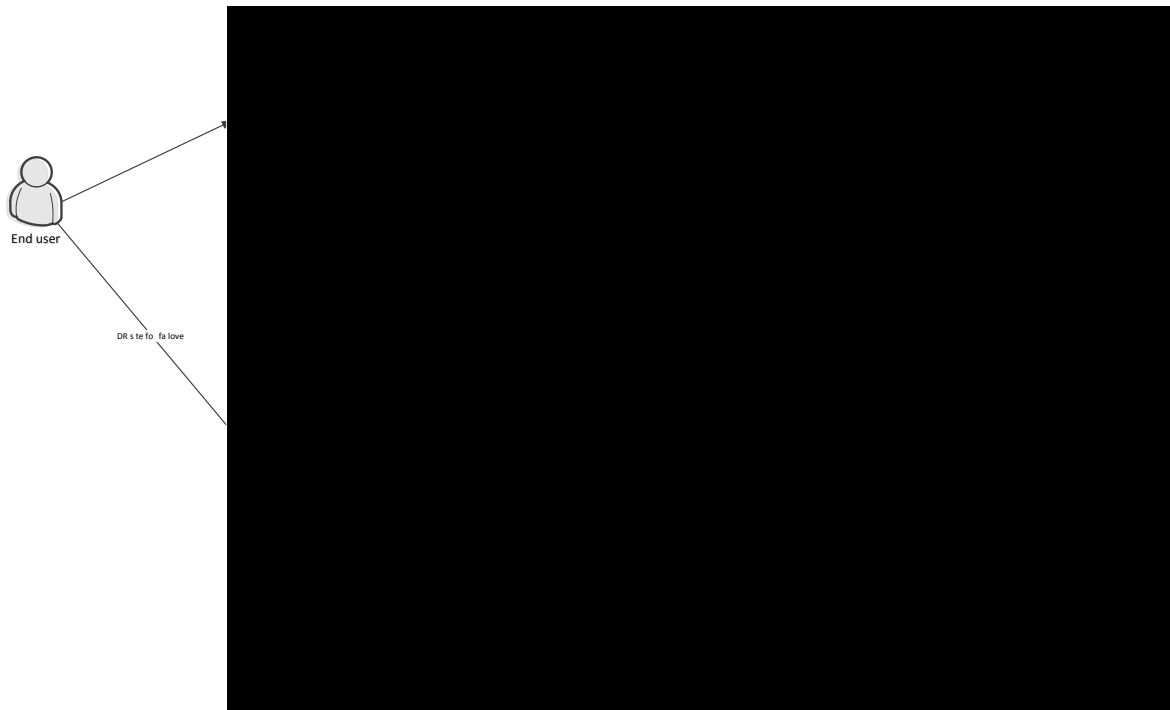


Figure 29: CSP Network Security Topology

The CSP system is designed with external communication in mind. The CSP application is designed to provide web-based access the CSP web pages over standard HTTP/HTTPS. In addition, the CSP is design to perform Federated Identity Management (Federation) Single Sign-On (SSO) and Security Assertions Markup Language (SAML) exchange to interact with VAAFI using Level 1 and Level 2 credentials. This interaction enables secure communication between trusted parties. In particular, SAML enables recognition and access for a user or machine so that SAML documents can be passed between Web servers of federated organizations that share live services. In addition, SAML can be wrapped in a Simple Object Access Protocol (SOAP) message for the computer-to-computer communications needed for Web services. Communication between CSP components is handled through proprietary HTTPS and HTTPS protocols.

4.4. Service Oriented Architecture / ESS

The CSP Service provides a self-service interface which provides the ability to request / issue self-asserted Level 1 credentials and Level 2 credentials once the applicant has been identity proofed in-person at an approved proofing location. When Credential Applicants / CSP Users first register for a CSP credential, the credential is assigned a Level 1 by default and is secured through the use of user IDs, passwords, and a set of challenge questions. The CSP solution will also provide the user with

instructions for the in-person proofing process required to obtain a Level 2 credential. The CSP Service will further provide CSP Privileged Users the means to generate reports based on predefined parameters, metrics, and auditable events via integration with the CAR Service.

CSP provides the following web services:

- Generate L1 Credential
- Generate L2 Credential
- Upgrade from L1 to L2 Credential
- Perform Self Service
- Authenticate Credential

4.5. Enterprise Architecture

CSP is implemented as a standards based .NET application using VA approved technologies in conformance with the TRM. Refer to Table 19 for the specific technologies upon which CSP is based. Please see the COTS Product Roadmap located on the [AcS TSPR](#) site for more information.

5. Data Design

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

5.1. DBMS Files

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

- CA IDM schema is built during the installation via COTs pre-bundled scripts
- CA SiteMinder audit schema is built during the installation via COTs pre-bundled scripts to store audit information
- CA IDM audit schema is built during the installation via COTs pre-bundled scripts to store audit information
- Similarly, CA Directory will be used for the following purposes:
 - CSP User Store is built to store user attributes for external VA users

Table 40: Database File System

Table Spaces	Data Files
SYSTEM	+ORADATA/acsdb/datafile/system
SYSAUX	+ORADATA/acsdb/datafile/sysaux
USERS	+ORADATA/acsdb/datafile/users
UN DO1	+ORADATA/acsdb/datafile/und01
UNDO2	+ORADATA/acsdb/datafile/und02
CSPIDM_DATA	+ORADATA/acsdb/datafile/cspidm_data
CPIPIDM_INDX	+ORADATA/acsdb/datafile/cspidm_indx
SYSTEM	+ACSDb_DATA/sailpt/datafile/system.280.828271109
SYSAUX	+ACSDb_DATA/sailpt/datafile/sysaux.284.828271115
UNDOTBS1	+ACSDb_DATA/sailpt/datafile/undotbs1.290.828271119
UNDOTBS2	+ACSDb_DATA/sailpt/datafile/undotbs2.285.828271135
USERS	+ACSDb_DATA/sailpt/datafile/users.287.828271139
IDENTITYIQ_TS	+ACSDb_DATA/sailpt/datafile/identityiq_ts.286.828271127

5.2. Non-DBMS Files

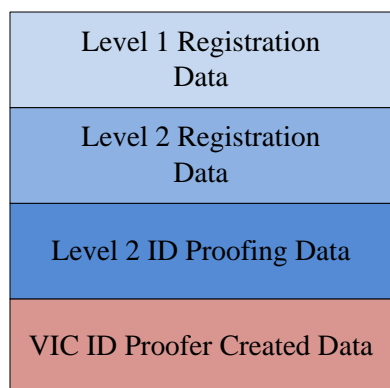
For the CSP solution, non-DBMS files are used for the following activities:

- User store schema within CA Directory is customized to store registered user record information (refer to section A.8 below, which shows the data element description, object class, screen name, value type, multivalued, length, encryption, and permissions). The data dictionary for account and feed object attributes are covered as part of the **VAProvPerson** object class attributes (refer to Provisioning in section A.1).

5.3. Data View

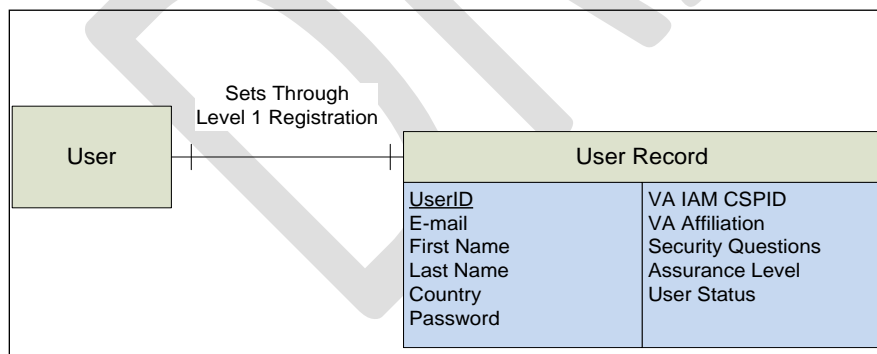
The diagrams below show the Entity Relationships of the CSP at the discrete states of credentialing, identity proofing, authentication, and identity management. In the diagrams that follow, the User Record data elements that are stored contain Identity Information (5), Security Questions (6), Roles (7), and Privileges (8). In the CSP, the User Records are based on the CA Directory which uses the LDAP format. The User Records contain information from various CA classes; inetorgperson, person and a class established for CSP VAPerson. This diagram is color-coded as shown in Figure 30. There is a one-to-one relationship between a User and a User Record. Since these are LDAP records and not database records, some of the database constructs such as a Foreign or Secondary Key are not shown. User Records use the VA IAM CSPID as the Surrogate Key for resolving records. The User ID is considered the Primary key during the stages of the process.

Figure 30: Color-coded Model based on steps in the process



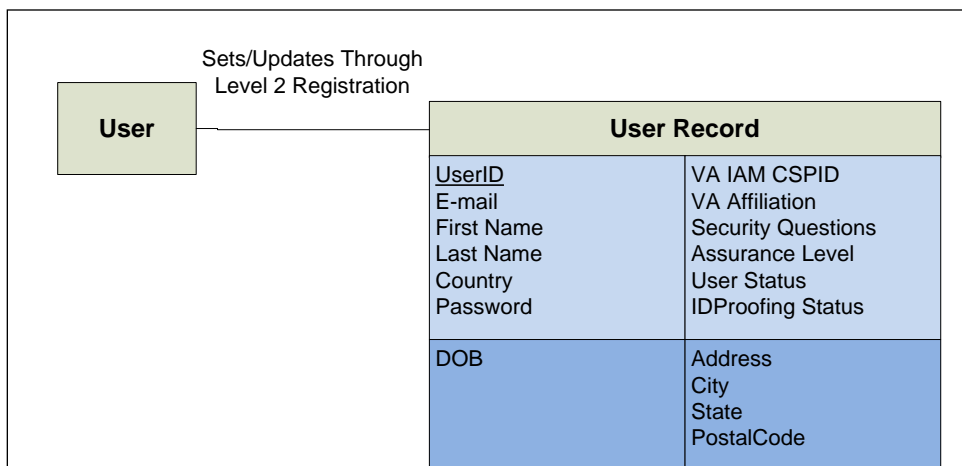
The Level 1 User Registration step is where a new user creates an identity in the CSP. Figure 31 shows the Entity Relation Diagram for required data. Note that there is a one-to-one relationship between Users and User Records in the CSP.

Figure 31: Level 1 User Registration



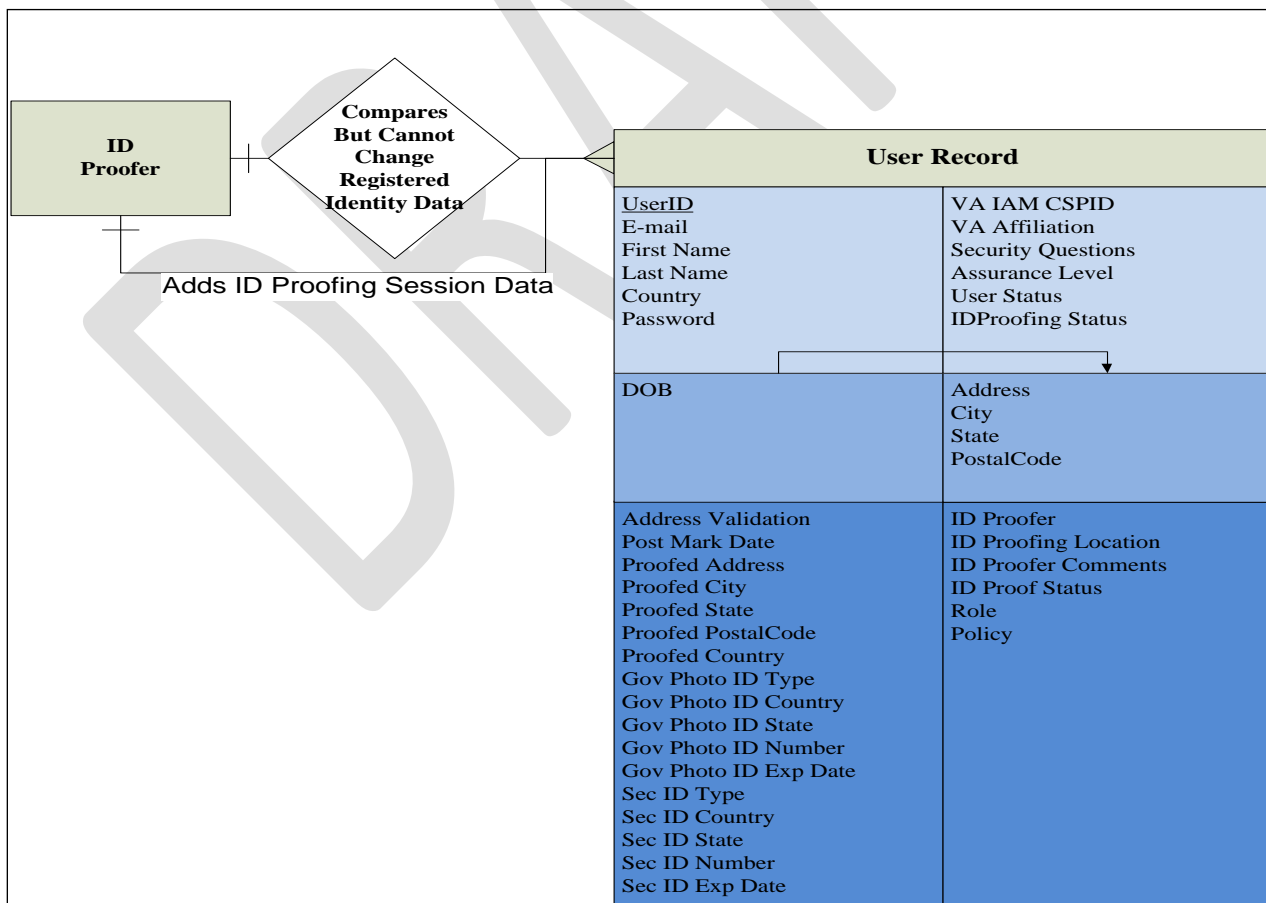
The Level 2 User Registration step is where a new user creates or updates an identity in the CSP. The Figure 32 shows the Entity Relation Diagram for required data. Note that there is a one-to-one relationship between Users and User Records in the CSP.

Figure 32 – L2 User Registration



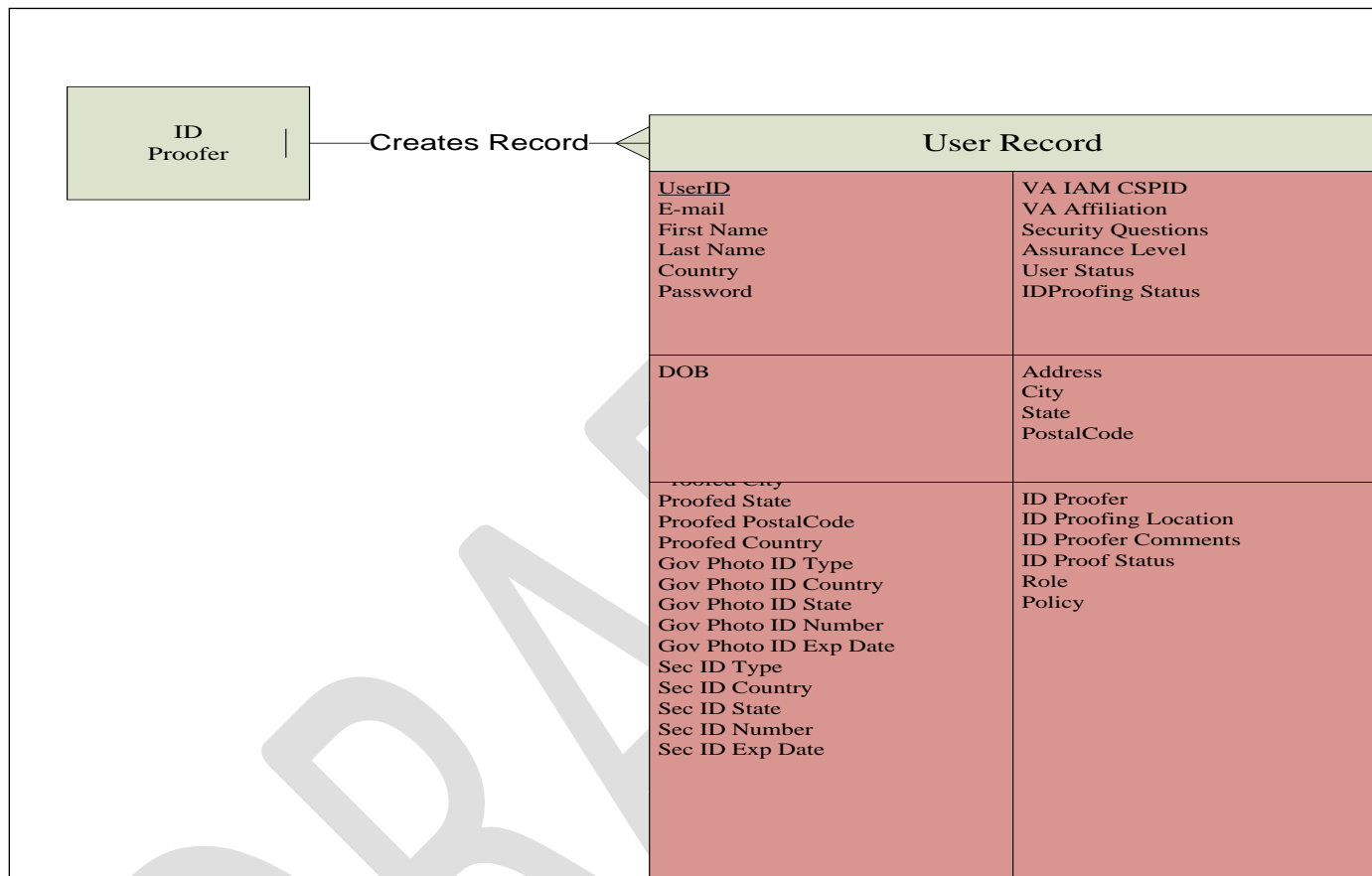
The Level 2 ID Proofing step is where a trained and certified ID Proofer validates an identity in the CSP. The Figure 33 shows the Entity Relation Diagram for required data. Note that there is a many-to-one relationship between Users and User Records in the CSP.

Figure 33: L2 User Registration



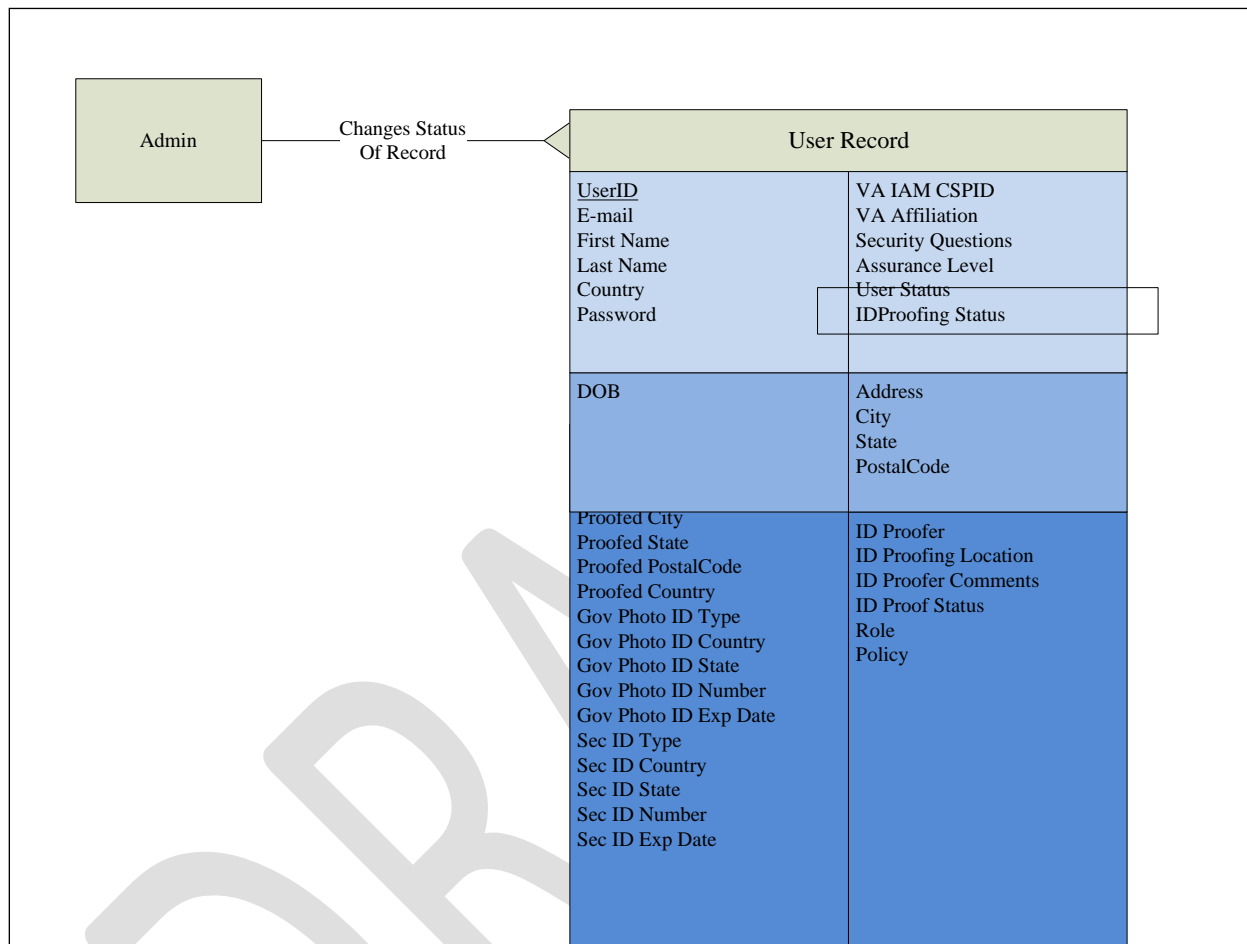
The Figure 34 shows the Entity Relation Diagram for required data. Note that there is a many-to-one relationship between Users and User Records in the CSP.

Figure 34: Proofing Record Creation and Identity Proofing



The Figure 35 shows the Entity Relation Diagram for required data. Note that there is a many-to-one relationship between Admins and User Records in the CSP.

Figure 35: Admin Based Revocation, Suspension or Reactivation



6. Detailed Design

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

6.1. Hardware Detailed Design

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

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



20131108 - AcS IAM
TerreMark PreProd ar

6.2. Software Detailed Design

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

6.2.1. 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

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

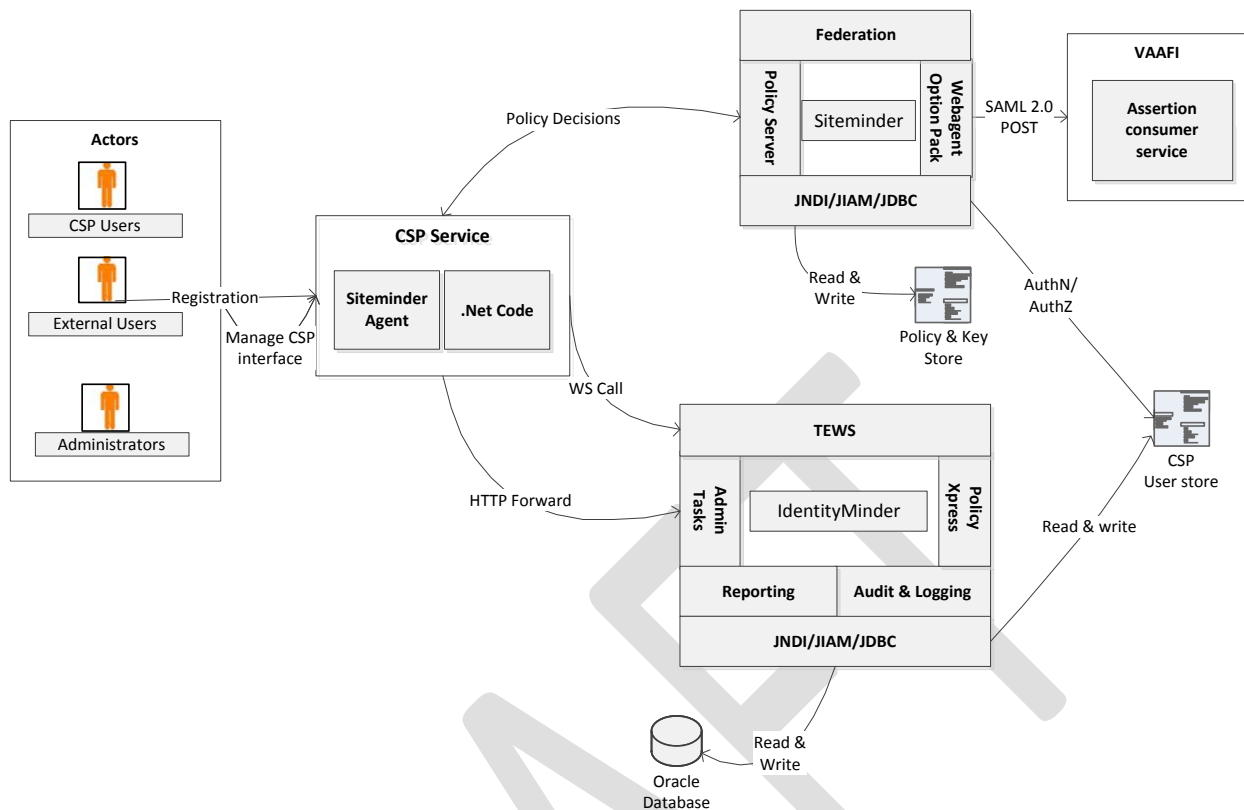


Figure 36: CSP Detailed Design

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

6.2.1.1. Product Perspective

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

6.2.1.1.1. User Interfaces

Refer to section 3.2.3 for information on user interfaces.

6.2.1.1.2. Hardware Interfaces

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

6.2.1.1.3. Software Interfaces

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

6.2.1.1.4. Communications Interfaces

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

6.2.1.1.5. Memory Constraints

This section is not applicable to the AcS 2.0.

6.2.1.1.6. Special Operations

This section is not applicable to the AcS 2.0.

6.2.1.2. Product Features

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

Table 41: AcS 2.0 Products

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

#	Software	Description
2	CA SiteMinder Web Access Manager	SiteMinder Web Access Manager is a web access management system that enables user authentication and secure Internet SSO (single sign-on), policy-driven authorization, federation of identities, and auditing of access to the web applications it protects.
3	CA Directory	<p>CA Directory provides directory services and security for online applications for organizations. For example, it enables customers to access their electronic accounts; employees can access critical business data.</p> <p>This product is generally considered a highly scalable and distributable implementation of directory services, including security services (e.g., authentication).</p> <p>CA Directory is supported on a variety of Windows and UNIX platforms, as well as 64-bit operating systems such as Linux 64, Solaris 10/Intel 64, UltraSparc 64, IBM Power5 64 and HPUX Itanium 64.</p> <p>CA Directory supports open standards including: LDAP (and related RFCs), X.500 (DAP, DSP, DISP), Security (SSL, TLS, password hashes), Management (SNMP and related RFCs), Network (IPv6, RFC1006), and US Federal Government standards (FIPS 140-2, Common Criteria EAL3, and Section 508).</p>
4	WebLogic	<p>BEA WebLogic Portal is now known as WebLogic Portal. WebLogic Portal is a well-known, widely used, Java-based portal product and a portal framework. The WebLogic Portal product is out-of-the-box software that aggregates information, content, applications, business processes and knowledge assets into a personalized display. The WebLogic Portal framework is the portal product in kit form, providing a set of tools to extensively build and customize a portal with specialized functionality. The WebLogic Portal framework comes packaged with an Eclipse-based integrated development environment (IDE) to assemble and extend the capabilities of the portal using the provided API and tools. The paired IDE is known as Oracle Workshop for WebLogic (formerly Workspace Studio).</p> <p>WebLogic Portal offers support for industry standards, enterprise-class portal federation, publication, and syndication capabilities including bidirectional integration with other portals and Web applications. My Health^eVet (MHV) and the Clinical Information Support System (CISS) are deployed with WebLogic Portal.</p>
5	Oracle Database	The Oracle relational database management system. There are several Oracle editions (Express, Personal, Standard, Enterprise, and Real Application Cluster). This assessment is concerned with the Standard and Enterprise editions of Oracle.

6.2.1.3. User Characteristics

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

Table 42: AcS 2.0 Users

Application Component	Description	User
CSP	Performs administrative functions including controlling Identity Minder related configurations and tasks	CSP Administrator
CSP	Responsible for managing the application and providing user lifecycle management functions including upgrading credentials, enabling/disabling accounts, and other administrative activities as needed	CSP Privileged User
CSP	A user (Veteran, beneficiary, or other VA stakeholder) requesting or having a user credential of any level	End User

Also refer to section 1.8.

6.2.1.4. Dependencies and Constraints

Refer to section 2.4.1 for AcS 2.0 constraints and dependencies.

6.2.1.5. Credential Issuance

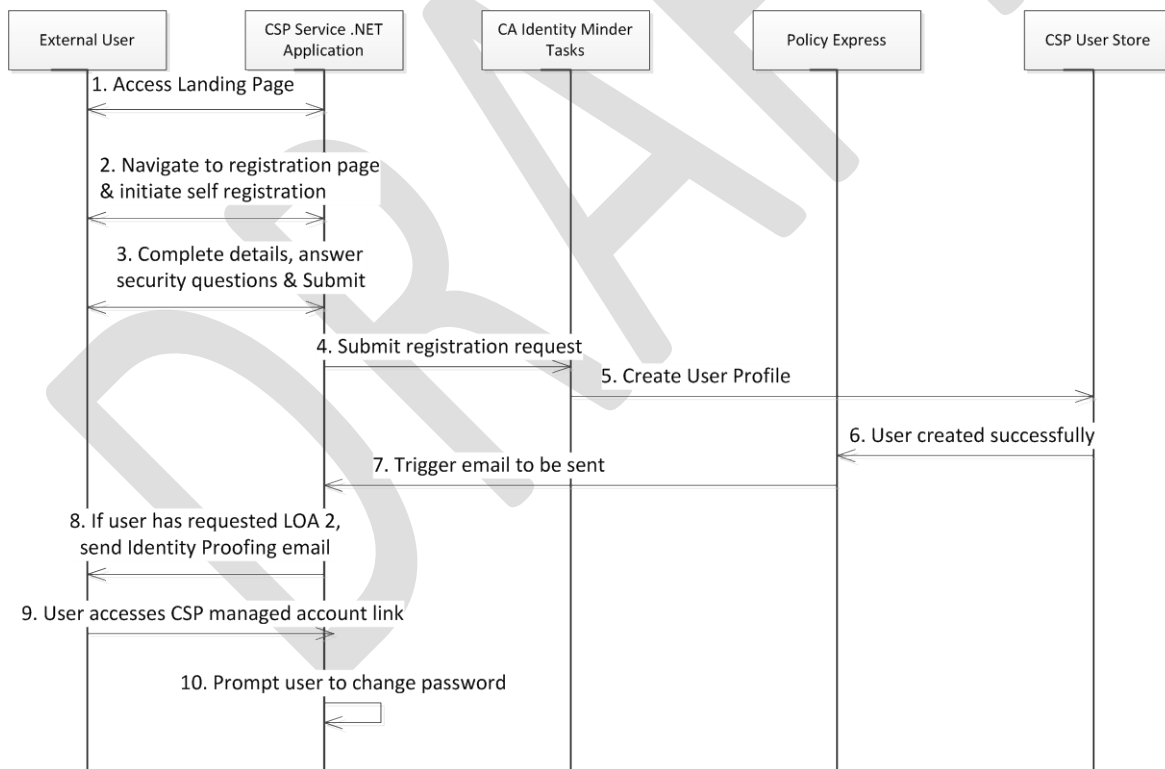


Figure 37: Credential Issuance Sequence Diagram

Table 43: 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	<ol style="list-style-type: none">1. CSP Service2. External User3. CA Identity Minder Tasks
Pre-Conditions	External user have a valid email address
Trigger	An external user requires LOA1 or 2 credential
Actions	<ol style="list-style-type: none">1. External user access the CSP service landing page2. Navigate to the registration page and initiate the self-registration process for requesting a LOA 1 or LOA 23. Provide the user related details, and register answers for security questions and submit the request4. The CSP Service ASP.NET code make a web service call to CA IdentityMinder TEWS interface and submits the registration request5. CA IdentityMinder task creates the user profile in CSP user store6. Notify policy express the user was successfully created7. The policy express rule gets triggered to send the user with user ID and temporary password in two separate emails8. If the user has requested for LOA 2, then an separate email to the user to appear in-person for identity proofing will be sent9. User follows the instructions provide in the email sent from CSP service and access the CSP manage account link10. 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

6.2.1.6. Revoke/Reissue Credential

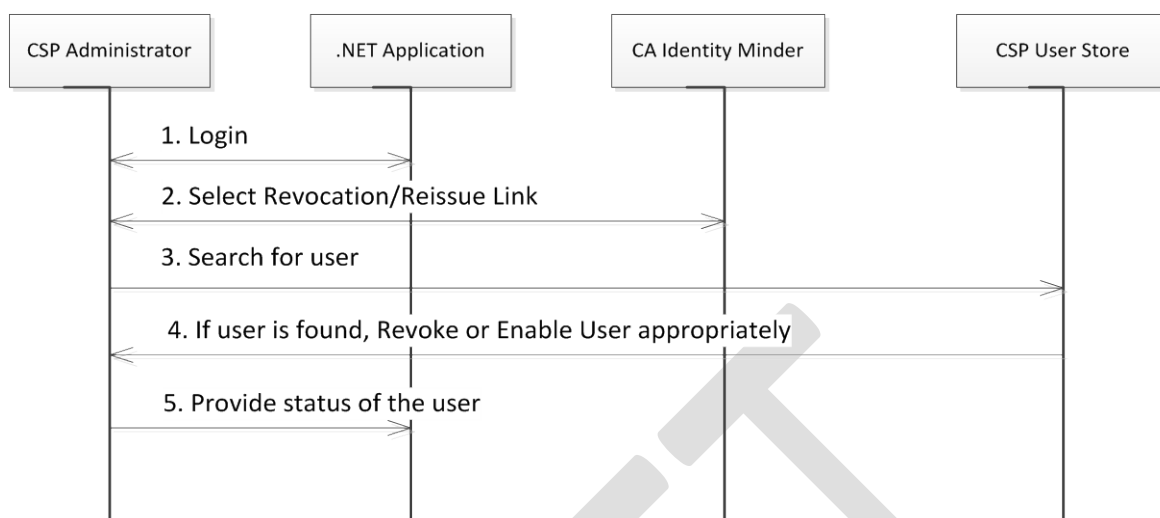


Figure 38: Revoke/Reissue Credential Sequence Diagram

Table 44: Revoke/Reissue Credential

Field	Description
Use Case Name	Credential Issuance
Description	This workflow describes the technical activities and associated data exchanges through which CSP user credential is revoked or reissued.
Actors	1. CSP Service 2. CSP Service administrator
Pre-Conditions	CSP Service administrator have the required access to perform the credential revoke/reissue function
Trigger	Credential revocation/ reissue request received from a trusted partner system
Actions	1. CSP administrator log into CSP service .NET application as an administrator 2. Administrator click on the revocation/reissue of credential link, which gets forwarded to the specific CA Identity Minder task 3. Administrator search for the specific user and if the user is found, based on the type of request the user will be revoked or enabled in CSP user store 4. CSP administrator respond to the trusted partner system on the status of the task
Main Success Scenarios	User is successful revoke or reissued a credential
Main Failure Scenarios	Failure during revoke or reissue of credential

6.2.1.7. Federation with VAAFI

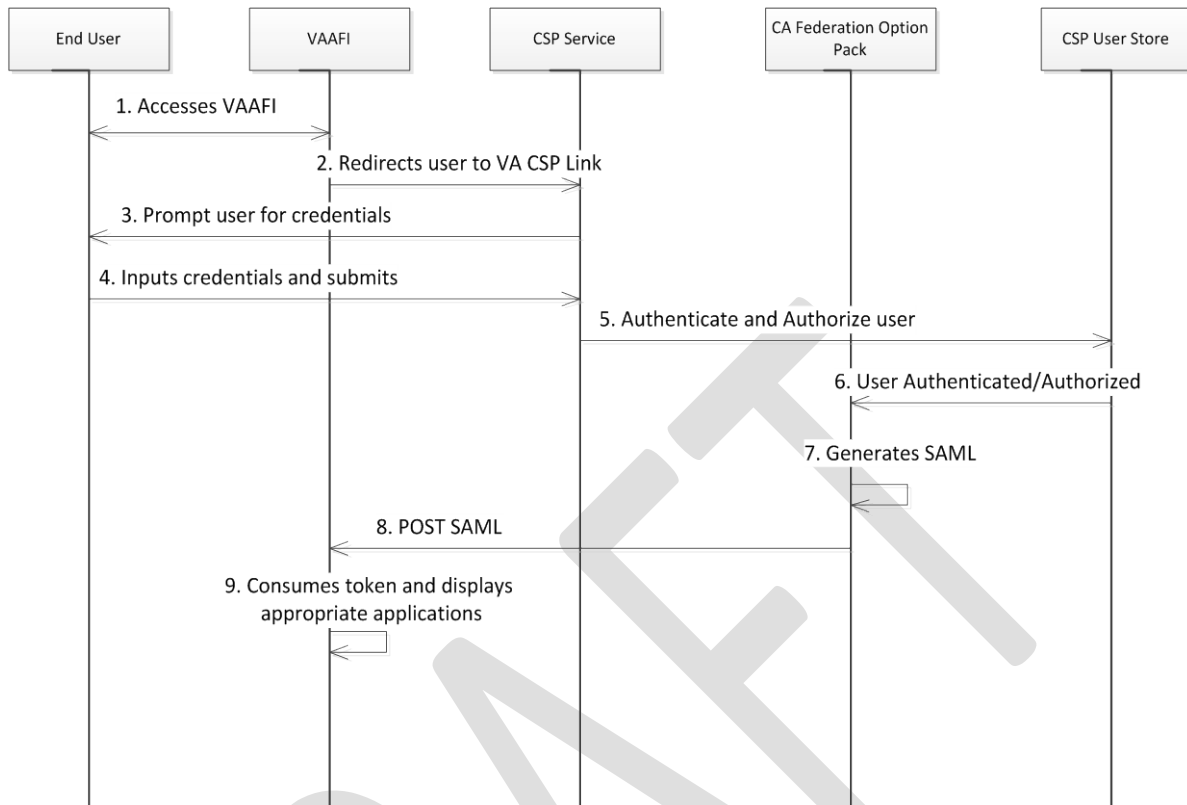


Figure 39: Federation with Consuming Application Sequence Diagram

Table 45: Federation with Consuming Application

Field	Description
Use Case Name	Federation with Consuming Application
Description	This workflow describes the technical activities and associated data exchanges through which a CSP user who poses LOA 1/ 2 credential, federate to VAAFI, to access the application behind VAAFI.
Actors	1. CSP Service 2. CSP User 3. CA SiteMinder Federation Service
Pre-Conditions	CSP user have a valid LOA 1 or LOA 2 credential
Trigger	A CSP user wants to access applications behind VAAFI

Field	Description
Actions	<ol style="list-style-type: none"> 1. CSP user access VAAFI, for accessing application behind VAAFI 2. VAAFI redirects the user to VA CSP link, which is a protected federation link by CA SiteMinder 3. The SiteMinder agent prompts the user for user credentials 4. CSP user type in the credentials and submit the request 5. The CSP service authenticate and authorize the user against the CSP user store is 6. The user is successfully authenticated and authorized. 7. SiteMinder federation option pack generated a SAML 2.0 token with assurance level of the user as an attribute 8. The option pack redirects the user with a SAML POST to VAAFI 9. VAAFI consumes the SAML token and based on the assurance level (LOA 1 or LOA2) it displays the list of application the user can access
Main Success Scenarios	Successfully single sign on to VAAFI application
Main Failure Scenarios	Failure to Single Sign on to VAAFI application

6.2.2. Specific Requirements

This SDD provides the foundational detailed design for AcS activities under VA Development Support program. VA AcS components leverage the installation and configuration of COTS products to meet the technical requirements that sufficiently meet the detailed functional requirements. The design applies specific configurations and customizations made to the base infrastructure to create the technical solution necessary to meet the business requirements provided in requirements documents listed in Table 5 above.

6.2.2.1. Database Repository

N/A

6.2.2.2. System Features

Please refer to the AcS i5 RSD located at: [AcS 2.0 i5 RSD.PDF](#)

6.2.2.3. Design Element Tables

N/A

6.2.2.3.1. Routines (Entry Points)

N/A

6.2.2.3.2. Templates

N/A

6.2.2.3.3. Bulletins

N/A

6.2.2.3.4. Data Entries Affected by the Design

N/A

6.2.2.3.5. Unique Record(s)

N/A

6.2.2.3.6. File or Global Size Changes

N/A

6.2.2.3.7. Mail Groups

N/A

6.2.2.3.8. Security Keys

CSP consumes 2 integrations /interfaces with SiteMinder:

CSP consumes SSOi as a service to protect CSP by requiring a login; for this purpose CSP employs the siteminder web agent "pattern" similar to any other application that wants to be protected by SSOi. CSP also produces data for consumption by SiteMinder from the CSP data store; this is the CSP authentication information to the LDAP directory.

6.2.2.3.9. Options

N/A

6.2.2.3.10. Protocols

Within the integration effort between the VA CSP Credential Service Provider and VAAFI as a Service Provider, the Web Browser SSO Profile in conjunction with HTTP POST Binding is utilized.

6.2.2.3.11. Remote Procedure Call (RPC)

N/A

6.2.2.3.12. Constants Defined in Interface

N/A

6.2.2.3.13. Variables Defined in Interface

N/A

6.2.2.3.14. Types Defined in Interface

N/A

6.2.2.3.15. GUI

N/A

6.2.2.3.16. GUI Classes

N/A

6.2.2.3.17.	Current Form
N/A	
6.2.2.3.18.	Modified Form
N/A	
6.2.2.3.19.	Components on Form
N/A	
6.2.2.3.20.	Events
N/A	
6.2.2.3.21.	Methods
N/A	
6.2.2.3.22.	Special References
N/A	
6.2.2.3.23.	Class Events
N/A	
6.2.2.3.24.	Class Methods
N/A	
6.2.2.3.25.	Class Properties
N/A	
6.2.2.3.26.	Uses Clause
N/A	
6.2.2.3.27.	Forms
N/A	
6.2.2.3.28.	Functions
N/A	
6.2.2.3.29.	Dialog
N/A	
6.2.2.3.30.	Help Frame
N/A	
6.2.2.3.31.	HL7 Application Parameter
N/A	
6.2.2.3.32.	HL7 Logical Link
N/A	

6.2.2.3.33. COTS Interface

N/A

6.3. Network Detailed Design

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

6.4. Service Oriented Architecture / ESS Detailed Design

CSP has a web service interface to facilitate integration with other VA applications. The task that is exposed via web service is an update to the status for a CSP record that matches the submitted criteria. The web service is defined using the SOAP protocol, and web service messages are conveyed using HTTPS. The CSP web service is enabled through configuration of the CA Identity Manager product. The web service is described by an XML document named a Web Services Description Language (WSDL) file.

Business applications which use the web service to communicate with CSP submit a remote task as an HTTP 1.x POST request to the designated web service URL. The body of the POST request is a SOAP document that conforms to the interface designed in the task-specific WSDL document. The WSDL document describes the metadata that the client application requires to prepare and submit a task request. Calls made to the web service will be SOAP messages submitted over HTTPS.

The CSP/IP application allows a business application to submit a status update in order to update a status for a person in the CSP application. This task occurs via web service. This task is described in

Note: Additional information about the TEWS tasks types and client implementations can be found on the vendor's support site. The client application submits an Identity Manager request through a generated proxy. The proxy transforms the request into a SOAP document that the CSP/IP Web Service can understand, and then submits the request. Identity Manager processes the request and returns a SOAP response to the client application.

The client application submits an Identity Manager request through a generated proxy. The proxy transforms the request into a SOAP document that the CSP/IP Web Service can understand, and then submits the request. Identity Manager processes the request and returns a SOAP response to the client application.

The user interface enables Level 1 and Level 2 credentialing, credential upgrades and subscriber self-service. The Federated (SAML 2.0) Interface enables the verification of CSP issued credentials as part of user authentication and Single Sign-On. The interfaces available to support these functions are identified in Figure 40 below:

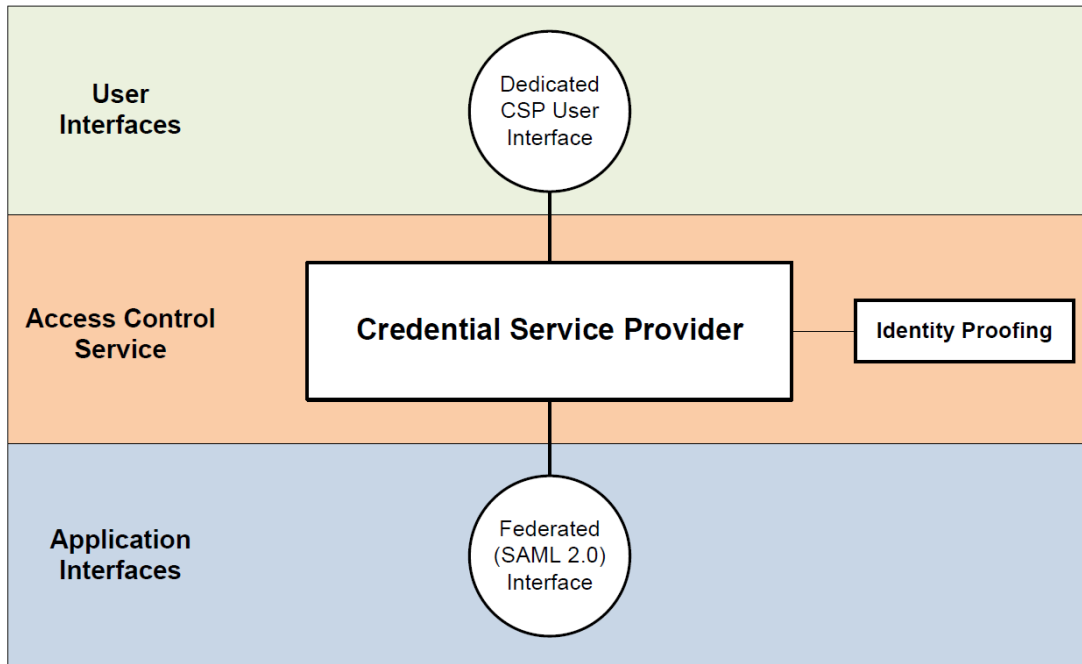


Figure 40: Federated (SAML 2.0) Interfaces

User Interfaces:

- For the self-service, issuance, upgrade, and lifecycle management of CSP credentials, there is a dedicated user web interface that is part of the CSP service. The dedicated User CSP User Interface provides Applicants with the ability to request and generate Level 1 credentials, request Level 2 credentials, and allows Applicants / Subscribers to perform self-service functions, such as password reset. It allows Security Officers to generate and issue Level 2 credentials, upgrade a Level 1 credential to a Level 2 credential, and produce management reports.

Application Interfaces:

- CSP supports a Federated (SAML 2.0) Interface to support authentication using the credential. In order to accept CSP credentials, applications have two options: (1) integrate with the CSP SAML 2.0 Interface directly or (2) leverage the SSOe SAML Service Provider. All VA hosted applications will leverage SSOe (see the SSOe section), as the external identity provider broker to the VA, for consumption of CSP credentials. However, there may be external applications, otherwise known as Service Providers (SP), which may request direct integration with the CSP. It provides applications the ability to verify CSP-issued credentials through the use of SAML. This is the interface leveraged internally with AcS to integrate the CSP with SSOe.

CSP provides the following web services:

- Generate L1 Credential:** The first step in using the CSP Service is obtaining a CSP credential, consisting of a User ID and password. The user is not currently registered with CSP. The User ID can be based on a specified format, but in this version will allow the user to create their own. The password is provided by the user during the initial

registration and is required to meet VA policy for password strength. This service provides an applicant ability to register for a Level 1.

- **Generate L2 Credential:** The first step in using the CSP Service is obtaining a CSP credential, consisting of a User ID and password. The user is not currently registered with CSP. The User ID can be based on a specified format, but in this version will allow the user to create their own. The password is provided by the user during the initial registration and is required to meet VA policy for password strength. This service provides an applicant ability to register for a Level 2 Credential.
- **Upgrade from L1 to L2 Credential:** Once a user authenticates to CSP self-service interface using their Level 1 credential, the user can select to Upgrade to Level 2. The user is prompted to enter additional identity information as required for a Level 2 credential.
 - The user account is updated in appropriate data store and the user is instructed to follow up with IP process to obtain a Level 2 credential. Once the user completes in-person proofing and once approved through IP process, user's Level 2 credential is created in the appropriate data store and user is notified via email.
- **Perform Self Service:** Provides the processes for users to edit their CSP account information without intervention from an external support persons assistance. The User can update their CSP profile information including personal information, password and modify challenge questions.
 - The CSP Service also provides the user's ability to retrieve forgotten user ID or password via the CSP interface.
- **Authenticate Credential:** Authentication to the CSP Service increases the assurance that only approved authorized users are logging into the service to perform self-service functions.
 - Federated authentication is supported via VAAFI to provide CSP credential holder's ability to log in to VAAFI integrated VA applications.
 - CSP integrates with VAAFI Solution to provide federated authentication of both Level 1 and Level 2 credentials to VA application using Security Assertion Markup Language (SAML) mechanisms. VAAFI Solution is responsible for integrating VA applications to utilize the CSP credential.

6.4.1. Service Description for CSP

N/A

6.4.2. Service Design for CSP

N/A

6.4.2.1. Introduction

N/A

6.4.2.1.1. Purpose and Scope of Service

N/A

6.4.2.1.2. Links to Other Documents

N/A

6.4.2.2. Service Details

N/A

6.4.2.2.1. Service Identification

N/A

6.4.2.2.2. Service Versions

N/A

6.4.2.2.3. Summary of Design and Platform Details

N/A

6.4.2.2.3.1. SOA Pattern(s) Implemented

N/A

6.4.2.2.3.2. COTS Platform vendor names and versions for hosting platform

N/A

6.4.2.3. Dependencies

N/A

6.4.2.4. Service Design Details

N/A

6.4.2.4.1. Interface Technical Specs

N/A

6.4.2.4.1.1. Service Invocation Type

N/A

6.4.2.4.1.2. Service Interface Type

N/A

6.4.2.4.1.3. Service Name

N/A

6.4.2.4.1.4. Interface

N/A

6.4.2.4.1.5. End Points

N/A

6.4.2.4.1.6.	Operations or Methods
N/A	
6.4.2.4.1.7.	Message Schemas
N/A	
6.4.2.4.2.	Information Model
N/A	
6.4.2.4.2.1.	Class Diagram and Description of Entities Involved
N/A	
6.4.2.4.2.2.	Mappings from ELDM to Standards Based Schemas
N/A	
6.4.2.4.3.	Behavior Model (AKA Use Case Realization)
N/A	
6.4.2.4.3.1.	Use Cases (Use Case Model)
N/A	
6.4.2.4.3.2.	Interaction Diagrams
N/A	
6.4.2.5. Gap Analysis	
N/A	
6.4.2.5.1.	Variances from Enterprise Target Architecture
N/A	
6.4.2.5.2.	Variances from SLDs
N/A	
6.4.2.5.3.	Variances from Standards and Policies
N/A	
6.4.2.5.4.	Justification for Exceptions and Mitigation
N/A	

7. External System Interface Design

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

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

Refer to Section 4.1 which describes the external system interface design in detail.



CSP
Integrations.docx

7.1. Interface Architecture

7.1.1.VA CSP Federation with VAAFI

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

In Figure 41: CSP to VAAFI Interface Flow, VAAFI is the Service Provider; CSP using SSOi is the Identity Provider; the User Agent is the web browser of the user accessing the VAAFI protected applications.

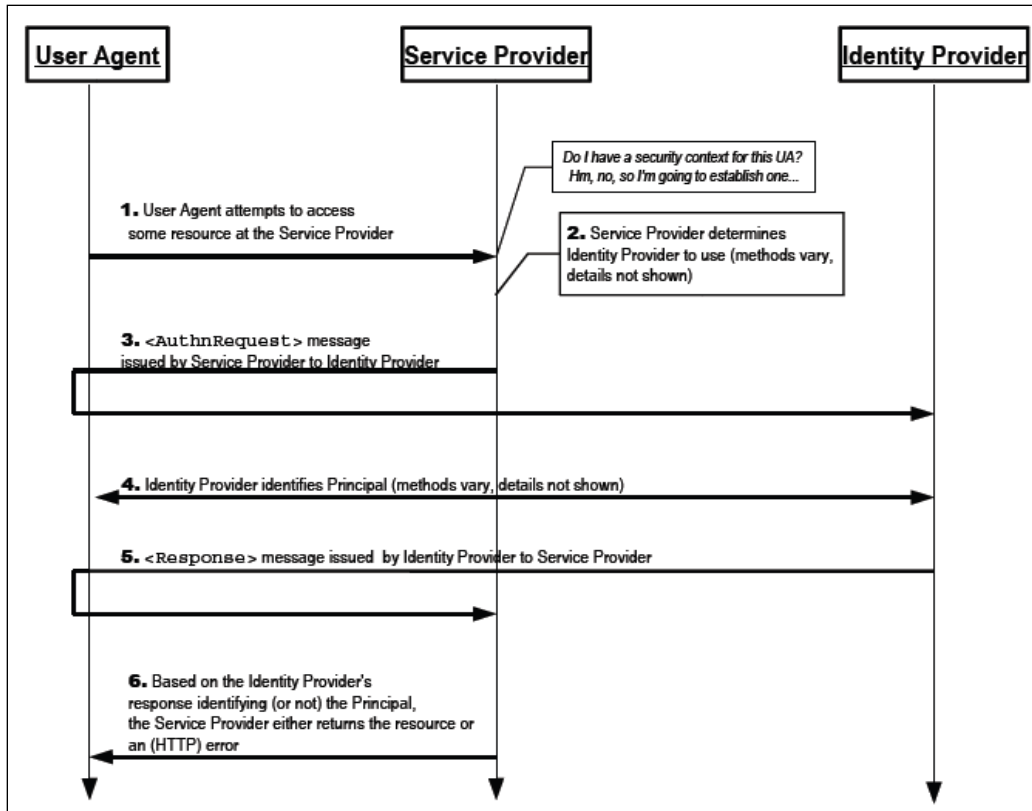


Figure 41: CSP to VAAFI Interface Flow

7.2. Interface Detailed Design

7.2.1.VA CSP Federation with VAAFI

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

Table 46: VA CSP (as CSP/IdP) Sending SAML to VAAFI

Field	Description
SPID:	
SiteMinder Affiliate Domain:	CSPFederationDomain
NameID:	UID
Authn Director:	CSP User Directory
Encryption Algorithm:	

Field	Description
SLO:	N/A
Attribute Details:	<div> <div></div> <div></div> <div></div> <div></div> </div>
Signature Algorithm:	<div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div>

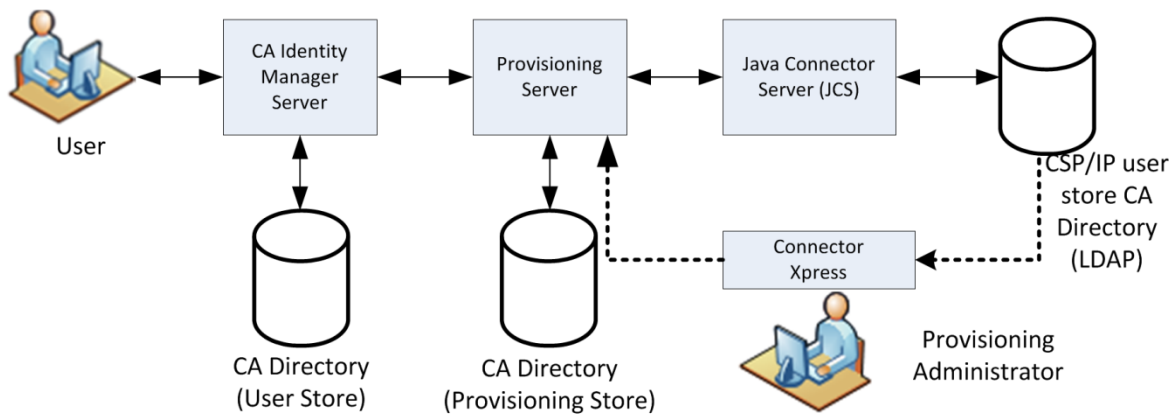
7.2.2. Provisioning - CSP Connector

The CSP service and Provisioning Service integration enables more effective access enablement for CSP Security Officers. The user population of CSP application is both internal to VA as well as external users such as veterans and their dependents. In context of Provisioning Service it is focused on internal users who need to access the CSP application as CSP Security Office. The intent of the Provisioning integration is to automate the provisioning of aforementioned users into the CSP system through the approval process.

As CSP Service is using CA IDM with backend user store as CA Directory. CA Identity Manager Connector Xpress tool is used to create and to deploy dynamic connector to allow provisioning and management of CSP CA Directory (LDAP). The primary input into Connector Xpress is the native schema of the endpoint system. Provisioning administrator use Connector Xpress to connect to the LDAP, retrieve the schema of the LDAP instance for CSP and construct mappings from those parts of the native schema that are relevant to identity management and provisioning. The mapping describes how the provisioning layer represents an element of the native schema. Connector Xpress generates metadata that describes, to a dynamic connector, the runtime mappings to a target system. The output of Connector Xpress is a metadata document produced when mapping is completed. The metadata is an XML file that describes the structure of the connector to the Java Connector Server (CS). The output describes the provisioning server classes and attributes and how they are mapped to the native schema. The dynamic connector maps the user attributes and assigns them to appropriate groups for each role on CSP CA Directory to provide appropriate access.

The diagram below shows the high level communication of the Provisioning components with CSP CA Directory user instance.

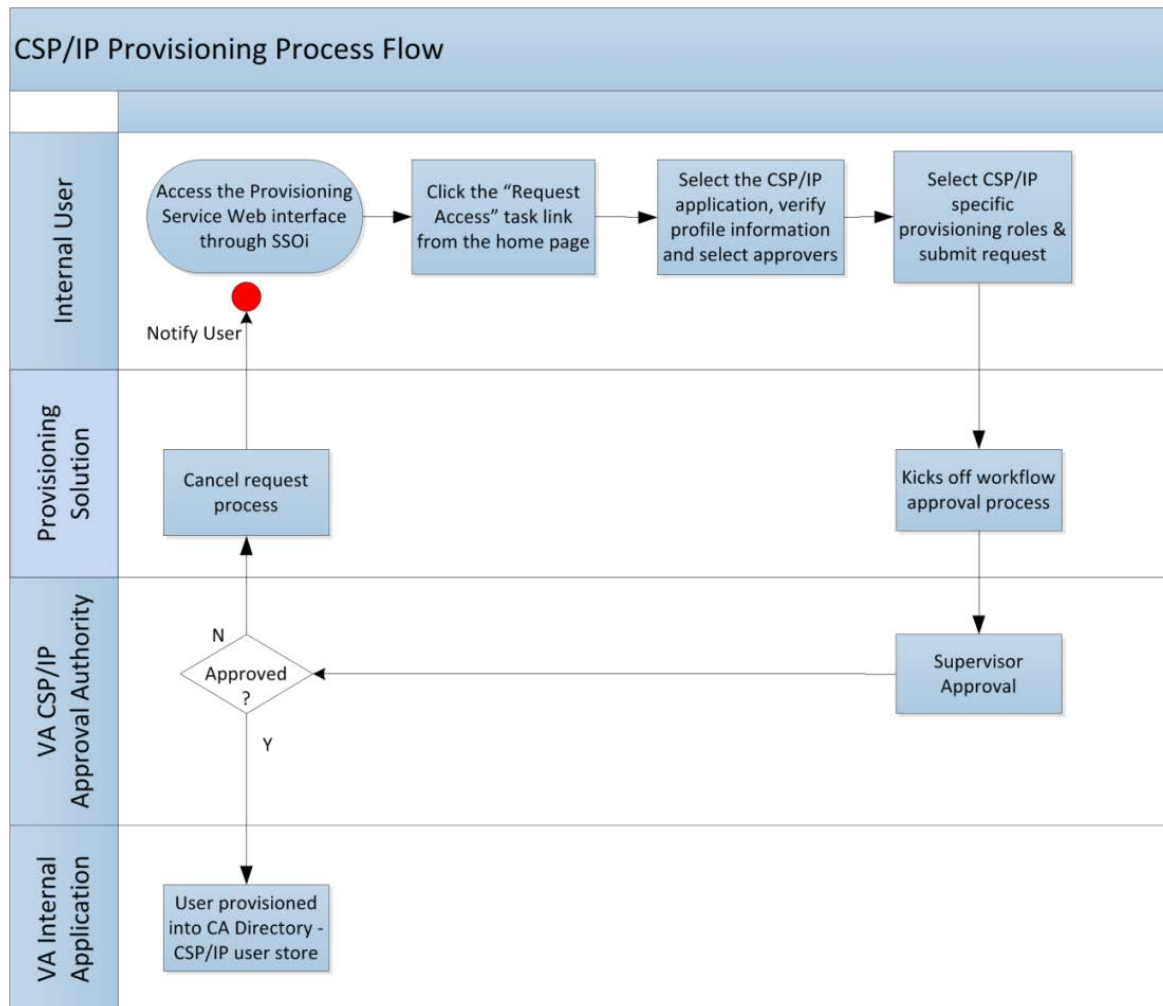
Figure 42 High Level Communication of Provisioning



7.2.2.1. Processing

The figure below shows the steps where a user submits request access for the CSP application, which is followed by the approval process and after approval; the user is provisioned into the CSP application CA Directory.

Figure 43 CSP Provisioning Process Flow



User accesses the Provisioning service web interface through SSO desktop authentication and lands directly on the homepage. If SSO is not enabled for the user, he / she may authenticate to the Provisioning Service interface using their AD credentials. From the home page, the user selects the "Request Access" task. On the "Request Access" task screen, user selects the CSP application tab. The user profile information is pre-populated on the profile page. User validates the information and provides other required information such as the supervisor approval. The user then submits the task. The Provisioning Service initiates the workflow approval process and sends email notification to the appropriate approver(s). Once the request is approved by the request is finally processed and user is provisioned into the CSP CA Directory user store.

7.2.2.2. Local data structures

The below table provides attribute mapping for CSP endpoint and provisioning service.

Table 47: CSP Attribute Mapping

CA IDM Corporate Store	Provisioning Attribute	ESR Attributes
uid	eTGlobalUserName	uid
userPassword	eTPassword	userPassword
cn	eTFullName	cn
givenName	eTFirstName	givenName
Initials	eTInitials	initials
Sn	eTLastName	sn
Title	eTTitle	title
Mail	eTEmailAddress	eTEmailAddress
VAAssuranceLevel	eTCustomField04	VAAssuranceLevel
VAAffiliation	eTCustomField05	VAAffiliation
VAPersonID	eTCustomField06	VAPersonID
VAIDProofStatus	eTCustomField07	VAIDProofStatus

8. Human-Machine Interface

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

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

The below section outlines the interfaces utilized to interact with the VA's CSP solution. The interfaces may be categorized based on users as follows:

- **CSP Users:** The web interface / screens used by the end users for registration, user record management and for authentication /login.
- **CSP Administrators:** The web interfaces used by the administrators to manage user records or to grant permissions or to add new administrators to the CSP system.
- **CSP ID Proofer:** The web interfaces used by the ID Proofer to update user records with ID Proofing information.
- The HMIs for the CSP application are contained in the User's Guide.

8.1. Interface Design Rules

The following design rules are applicable to the user interfaces for the CSP 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 web interface provides necessary validation checks such as blanks for mandatory fields, special characters, and invalid email id format before form submission.
-

8.2. Inputs

The CSP activity is a web page, accessible via VA standard web-browsers. Navigation and data entry require no special devices beside mouse and keyboard, while meeting Section 508 compliance where appropriate.

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

8.3. Outputs

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

- PDF
- Comma Separated File (CSF)
- Excel

8.4. Navigation Hierarchy

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

8.4.1. CSP

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

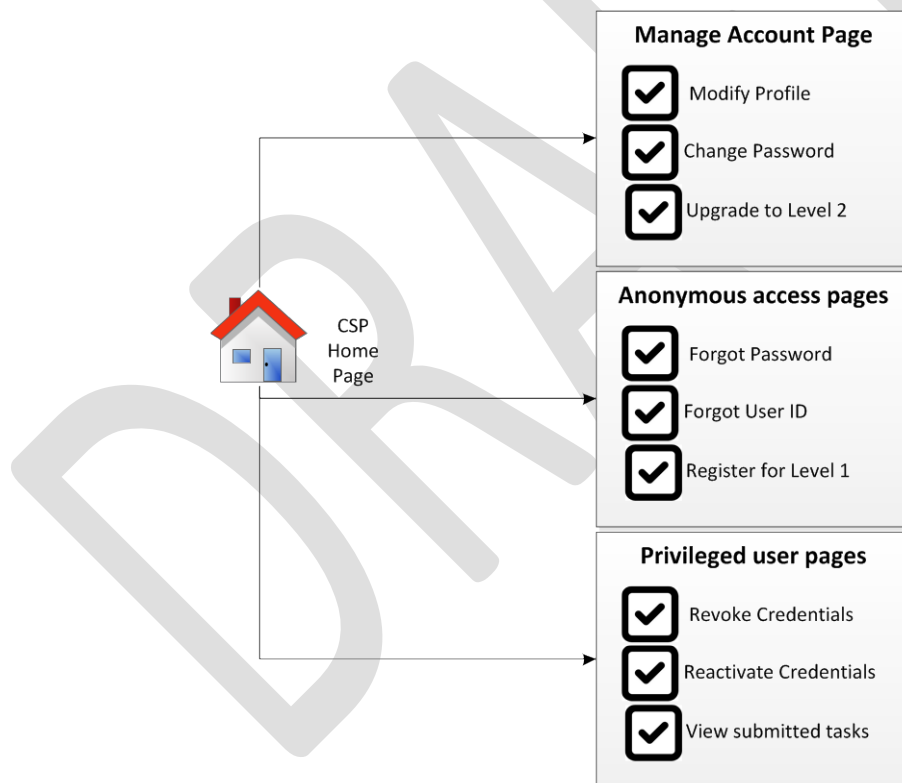


Figure 44: CSP Navigation Hierarchy

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.

9. Security and Privacy

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

Data in Motion:

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

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

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

Data at Rest:

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

Table 48: 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.

Data Points	Data Type	Explanation
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 reset are managed through the encryption of sensitive attributes at the directory level for the AcS 2.0. The FIPS 140-2 encryption is applied on the identified PII and sensitive attributes stored in the AcS 2.0 directory attributes. The following table provides the data types (refer to section A.8 below for data type groupings) and who can make updates accordingly.

Table 49: Data Type and Updates

Type	CSP System
Identity Information	End User
User Information	End User
CSP Information	Privileged Users CSP System

9.1. Security

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

9.1.1. Confidentiality of Sensitive Information

The CSP solution stores user record information required for Level 1 & Level 2 credentials. 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 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 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 solution does not allow duplicate identification values. Users are required to confirm their accounts by following instructions emailed to them. Therefore, the CSP users have their e-mail addresses verified prior to getting a Level 1 or Level 2 credential. The CSP components have appropriate roles established to address each facet of the associated business processes. These roles clearly provide separation of duties. Additionally, due to full auditing of transactions, any misuse of authority is discernible and traceable in the audit logs and reports.

9.1.4. eSig Controls

CSP solution uses eSig to minimize system failures, and access control to minimize man made failures. 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 1 or above user.

9.2. Privacy

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

Attachment A – Approval Signatures

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

Signed: _____

_____ Integrated Project Team Chair and Business Sponsor Date

Signed: _____

_____ OIS Business Sponsor Date

Signed: _____

_____ IAM Program Manager Date

Signed: _____

_____ AcS Program Manager Date

Signed: _____

_____ Chief Architect Date

Signed: _____

_____, SDE Date

A. Additional Information

A.1. RTM

Refer to section 1.10 for a complete list of requirements documents that are applicable to the AcS 2.0

A.2. Packaging and Installation

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

A.3. Design Metrics

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



VA CSP User
Population Estimates.

A.4. Acronym List and Glossary

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

A.5. Required Technical Documents

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

A.6. Attach Documents

Once the SDD is approved, submit the AERB Design Compliance Decision Certificate as an attachment to the completed and approved SDD.

A.7. CSP Class Documents

The CSP.NET wrapper class diagram is shown below.

Figure 45: CSP Class Diagram A

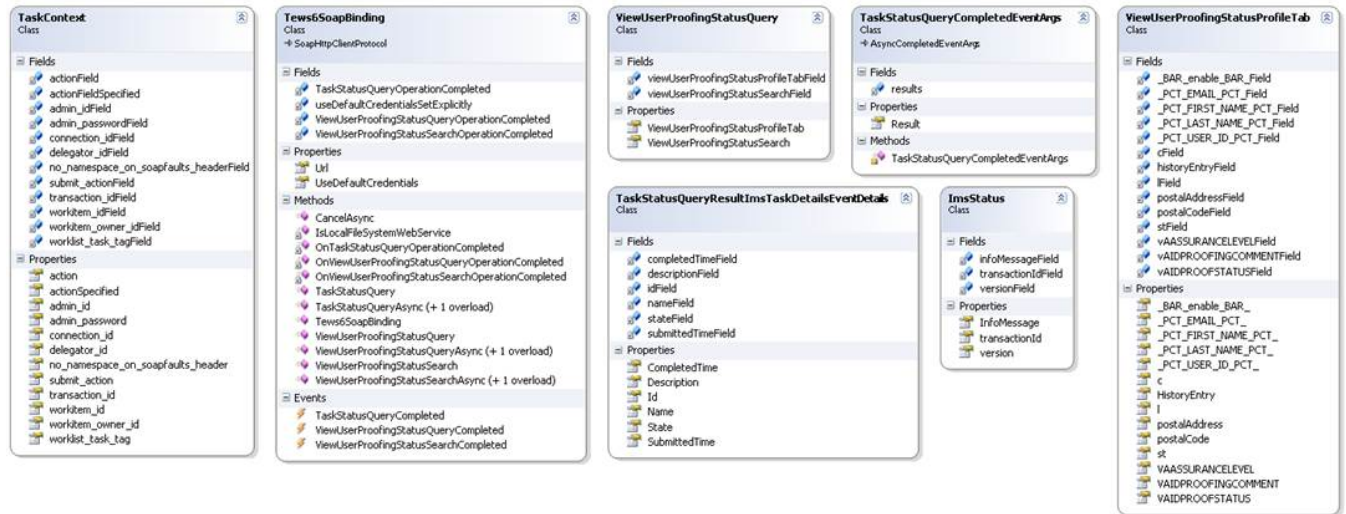


Figure 46: CSP Class Diagram B

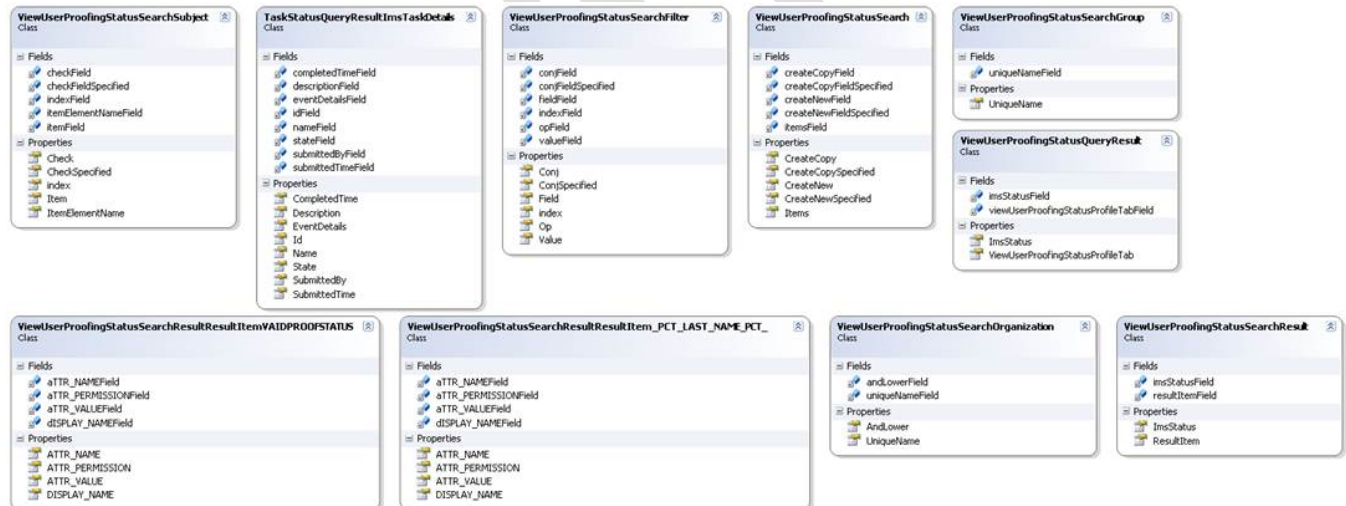


Figure 47: CSP Class Diagram C

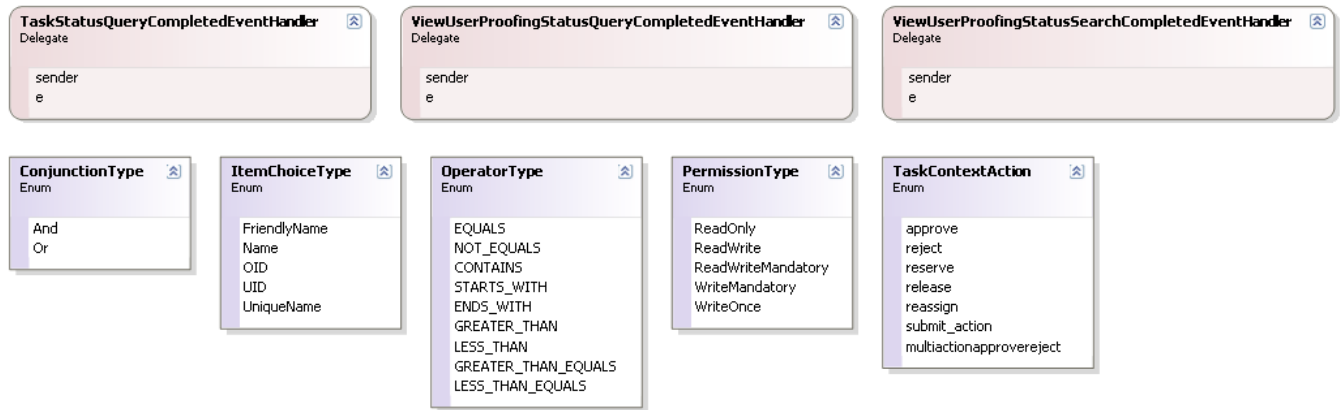
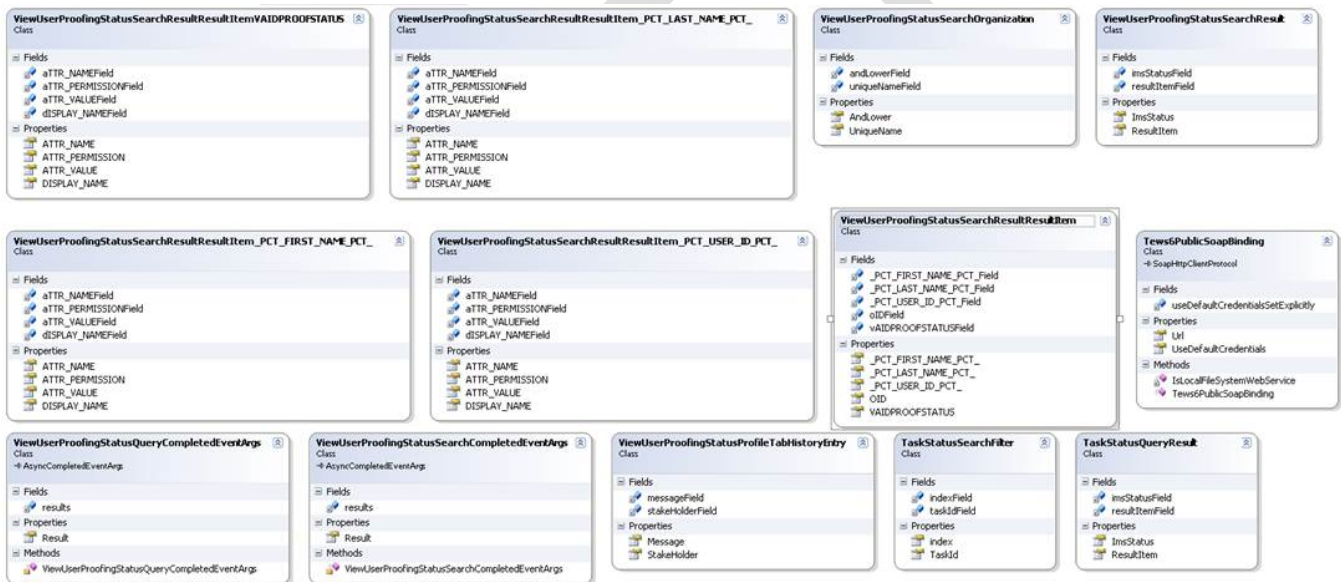


Figure 48: CSP Class Diagram D



A.8. Data Dictionary

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



ACS Data
Elements.xlsx

Template Revision History

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

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