

**Identity and Access Management  
Access Services 2.0 Increment 5  
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
04/17/2015	1.1	Updated per anomalies	[REDACTED]
03/25/2015	1.0	Updated to new ProPath template and applied CAR specific details	[REDACTED]

## Artifact Rationale

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

## Table of Contents

<b>1. Introduction .....</b>	<b>7</b>
1.1. Purpose of the SDD .....	7
1.2. Identification .....	7
1.3. Scope .....	8
1.3.1. Increment 5 CAR Scope .....	8
1.4. Constraining Policies, Directives and Procedures .....	8
1.5. User Characteristics .....	11
1.6. Relationship to Other Documents and Plans .....	11
1.7. Definitions, Acronyms, and Abbreviations .....	11
1.8. References .....	12
<b>2. Background .....</b>	<b>12</b>
2.1. Overview of the System .....	12
2.2. Overview of the Business Process .....	12
2.3. Business Benefits .....	13
2.4. Assumptions and Constraints .....	14
2.4.1. Design Assumptions .....	14
2.4.2. Design Constraints .....	14
2.4.3. Design Trade-offs .....	15
2.5. Overview of the Significant Requirements .....	15
2.5.1. Overview of Significant Functional Requirements .....	15
2.5.2. Overview of Functional Workload/Performance Requirements .....	20
2.5.3. Overview of Operational Requirements .....	20
2.5.4. Overview of the Technical Requirements .....	21
2.5.5. Overview of the Security or Privacy Requirements .....	21
2.5.6. Overview of System Criticality and High Availability Requirements .....	22
2.5.7. Single Sign-on Requirement .....	22
2.5.8. Requirement for Use of Enterprise Portals .....	22
2.5.9. Special Device Requirements .....	22
2.6. Legacy System Retirement .....	22
<b>3. Conceptual Design .....</b>	<b>22</b>
3.1. Conceptual Application Design .....	23
3.1.1. Application Context .....	23
3.1.1.1. Compliance Audit and Reporting .....	24
3.1.2. High-Level Application Design .....	27
3.1.3. Application Locations .....	28
3.2. Conceptual Data Design .....	29
Project Conceptual Data Model .....	29

3.2.1.	29
3.2.2.	Database Information ..... 30
3.2.3.	User Interface Data Mapping ..... 33
3.2.3.1.	CAR Screen Interface ..... 33
3.2.3.2.	Report Interface ..... 33
3.2.3.3.	Unmapped Data Element..... 33
3.3.	Conceptual Infrastructure Design ..... 33
3.3.1.	System Criticality and High Availability..... 34
3.3.2.	Special Technology ..... 35
3.3.3.	Technology Locations..... 35
3.3.4.	Conceptual Infrastructure Diagram..... 38
3.3.4.1.	Location of Environments and External Interfaces ..... 39
3.3.4.2.	Conceptual Production String Diagram ..... 40
4.	System Architecture ..... 40
4.1.	Hardware Architecture ..... 42
4.2.	Software Architecture..... 43
4.3.	Network Architecture..... 45
4.4.	Service Oriented Architecture/ESS ..... 46
4.5.	Enterprise Architecture ..... 46
5.	Data Design ..... 47
5.1.	DBMS Files ..... 47
5.2.	Non-DBMS Files ..... 47
5.3.	Data View ..... 48
6.	Detailed Design ..... 49
6.1.	Hardware Detailed Design..... 49
6.2.	Software Detailed Design..... 50
6.2.1.	Conceptual Design ..... 50
6.2.1.1.	Product Perspective..... 50
6.2.1.1.1.	User Interfaces ..... 50
6.2.1.1.2.	Hardware Interfaces ..... 50
6.2.1.1.3.	Software Interfaces ..... 50
6.2.1.1.4.	Communications Interfaces..... 50
6.2.1.1.5.	Memory Constraints..... 51
6.2.1.1.6.	Special Operations ..... 51
6.2.1.2.	Product Features ..... 51
6.2.1.3.	User Characteristics..... 52
6.2.1.4.	Dependencies and Constraints ..... 52
6.2.2.	Specific Requirements ..... 52
6.2.2.1.	Database Repository ..... 52
6.2.2.2.	System Features..... 53
6.2.2.3.	Design Element Tables..... 53
6.2.2.3.1.	Routines (Entry Points)..... 53
6.2.2.3.2.	Templates ..... 53

6.2.2.3.3.	Bulletins .....	53
6.2.2.3.4.	Data Entries Affected by the Design.....	53
6.2.2.3.5.	Unique Record(s) .....	53
6.2.2.3.6.	File or Global Size Changes.....	53
6.2.2.3.7.	Mail Groups .....	53
6.2.2.3.8.	Security Keys .....	53
6.2.2.3.9.	Options .....	54
6.2.2.3.10.	Protocols.....	54
6.2.2.3.11.	Remote Procedure Call (RPC) .....	54
6.2.2.3.12.	Constants Defined in Interface.....	54
6.2.2.3.13.	Variables Defined in Interface .....	54
6.2.2.3.14.	Types Defined in Interface.....	54
6.2.2.3.15.	GUI .....	54
6.2.2.3.16.	GUI Classes.....	54
6.2.2.3.17.	Current Form.....	54
6.2.2.3.18.	Modified Form .....	54
6.2.2.3.19.	Components on Form.....	54
6.2.2.3.20.	Events.....	54
6.2.2.3.21.	Methods.....	54
6.2.2.3.22.	Special References .....	54
6.2.2.3.23.	Class Events .....	54
6.2.2.3.24.	Class Methods.....	54
6.2.2.3.25.	Class Properties.....	55
6.2.2.3.26.	Uses Clause .....	55
6.2.2.3.27.	Forms .....	55
6.2.2.3.28.	Functions.....	55
6.2.2.3.29.	Dialog.....	55
6.2.2.3.30.	Help Frame.....	55
6.2.2.3.31.	HL7 Application Parameter .....	55
6.2.2.3.32.	HL7 Logical Link.....	55
6.2.2.3.33.	COTS Interface .....	55
<b>6.3.</b>	<b>Network Detailed Design.....</b>	<b>56</b>
<b>6.4.</b>	<b>Service Oriented Architecture/ESS Detailed Design .....</b>	<b>56</b>
<b>6.4.1.</b>	<b>Service Description for CAR.....</b>	<b>56</b>
<b>6.4.2.</b>	<b>Service Design for CAR.....</b>	<b>56</b>
6.4.2.1.	Introduction.....	56
6.4.2.1.1.	Purpose and Scope of Service .....	56
6.4.2.1.2.	Links to Other Documents .....	56
6.4.2.2.	Service Details.....	56
6.4.2.2.1.	Service Identification .....	56
6.4.2.2.2.	Service Versions .....	56
6.4.2.2.3.	Summary of Design and Platform Details .....	56
6.4.2.2.3.1.	SOA Pattern(s) Implemented .....	56
6.4.2.2.3.2.	COTS Platform vendor names and versions for hosting platform .....	56
6.4.2.3.	Dependencies.....	56
6.4.2.4.	Service Design Details.....	56
6.4.2.4.1.	Interface Technical Specs .....	56
6.4.2.4.1.1.	Service Invocation Type .....	56
6.4.2.4.1.2.	Service Interface Type .....	57

6.4.2.4.1.3.	Service Name .....	57
6.4.2.4.1.4.	Interface .....	57
6.4.2.4.1.5.	End Points .....	57
6.4.2.4.1.6.	Operations or Methods.....	57
6.4.2.4.1.7.	Message Schemas .....	57
6.4.2.4.2.	Information Model .....	57
6.4.2.4.2.1.	Class Diagram and Description of Entities Involved.....	57
6.4.2.4.2.2.	Mappings from ELDM to Standards Based Schemas.....	57
6.4.2.4.3.	Behavior Model (AKA Use Case Realization) .....	57
6.4.2.4.3.1.	Use Cases (Use Case Model) .....	57
6.4.2.4.3.2.	Interaction Diagrams .....	57
6.4.2.5.	Gap Analysis .....	57
6.4.2.5.1.	Variances from Enterprise Target Architecture .....	57
6.4.2.5.2.	Variances from SLDs.....	57
6.4.2.5.3.	Variances from Standards and Policies.....	57
6.4.2.5.4.	Justification for Exceptions and Mitigation .....	58
<b>7.</b>	<b>External System Interface Design.....</b>	<b>59</b>
7.1.	Interface Architecture.....	59
7.2.	Interface Detailed Design .....	60
<b>8.</b>	<b>Human-Machine Interface .....</b>	<b>61</b>
8.1.	Interface Design Rules .....	61
8.2.	Inputs .....	61
8.3.	Outputs .....	61
8.4.	Navigation Hierarchy.....	62
8.4.1.	Screen Shots.....	62
<b>9.</b>	<b>Security and Privacy.....</b>	<b>62</b>
9.1.	Security.....	62
9.2.	Privacy .....	64
9.2.1.	CAR .....	64
9.2.2.	Confidentiality of Sensitive Information .....	64
9.2.3.	Privacy of Personal Information .....	64
9.2.4.	Process Integrity.....	64
	<b>Attachment A – Approval Signatures.....</b>	<b>65</b>
<b>A.</b>	<b>Additional Information.....</b>	<b>66</b>
A.1.	RTM.....	66
A.2.	Packaging and Installation.....	66
A.3.	Design Metrics .....	66
A.4.	Acronym List and Glossary .....	66
A.5.	Required Technical Documents .....	66
A.6.	Attach Documents .....	66

# 1. Introduction

The subject of this System Design Document (SDD) is Compliance, Audit, and Reporting (CAR); a commercial off-the-shelf (COTS) product providing centralized monitoring, alerting, and auditing, as well as compliance reports in association with Access Services 2.0 (AcS). CAR establishes a common compliance auditing framework; providing protections and security for audit data, as required.

## 1.1. Purpose of the SDD

The purpose of the System Design Document (SDD) is to describe the supporting mechanics of the CAR 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 CAR developers and teams who will assist in the establishment of the infrastructure, as well as the following stakeholders:

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

This document provides the solution architecture and detailed design of the CAR 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**

<b>Name</b>	<b>Description</b>	<b>Abbreviation</b>	<b>Version</b>	<b>Release</b>
Compliance Audit and Reporting	Provides audit and reporting capability based on data made available to the Access Services.	CAR	V 2.5.X	N/A

### 1.3. Scope

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

**Table 2: Scope Inclusions**

<b>Includes</b>
Integrates with the AcS 2.0 activities such as provisioning, SSOi (CA SiteMinder), SSOe, Provisioning, CSP,IP,SAC and e-Sig to provide audit reports based on agreed upon data and alerts for daily reports

**Table 3: Scope Exclusions**

<b>Excludes</b>
The scope of the CAR Service only includes the reporting of activity associated with integrated IAM Services. As such, the CAR Service does not report on any business application activity.

#### 1.3.1. Increment 5 CAR Scope

There are no CAR Enterprise Requirements for AcS 2.0 in Increment 5.

### 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"> <li>• Directive Information Security Program.</li> <li>• Defining overall Security Framework for VA.</li> </ul>
2	VA	VA 6501 Directive	<ul style="list-style-type: none"> <li>• VA Identity Verification In-Person Proofing (IPP) Process.</li> <li>• Defining overall Identity Proofing Methodology for VA IAM.</li> </ul>
3	VA	VA 6300 Directive	<ul style="list-style-type: none"> <li>• Directive Records and Information Management.</li> <li>• Defines information management framework for VA Access Services.</li> </ul>
4	NIST	SP 800-53-4	<ul style="list-style-type: none"> <li>• Special Publication – Recommended Security Controls for Federal Information Systems and Organizations.</li> <li>• Defines the required security controls for IT systems under the Federal Information Security Management Act (FISMA).</li> </ul>
5	NIST	SP 800-63-2	<ul style="list-style-type: none"> <li>• Special Publication – Electronic Authentication Guideline.</li> <li>• Defines levels of assurance in user identities presented to IT systems over open networks.</li> <li>• Defines the data and procedural requirements for VA Access Services.</li> </ul>
6	NIST	FIPS-201-2	<ul style="list-style-type: none"> <li>• Federal Information Processing Standards Publication – PIV of Federal Employees and Contractors.</li> <li>• Provides Identity Proofing, credentialing and chain of trust requirements and processes.</li> <li>• Defines the method for secure administrative interaction and control.</li> </ul>
7	NIST	FIPS-140-2	<ul style="list-style-type: none"> <li>• Federal Information Processing Standards Publication (FIPS) – Security Requirements for Cryptographic Modules.</li> <li>• Defines the cryptographic standards and requirements.</li> </ul>
8	NIST	SP 800-122	<ul style="list-style-type: none"> <li>• Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).</li> <li>• Provides technical procedures for protecting PII in information systems.</li> <li>• Defines the information which can be used to distinguish or trace an individual's identity.</li> </ul>

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
9	US Congress	Section 508 Amendment to the Rehabilitation Act of 1973	<ul style="list-style-type: none"> <li>Section 508 Electronic and information technology requirements for Federal departments and agencies.</li> <li>Accessibility, development, procurement maintenance, or use of electronic and information technology.</li> <li>Defines the “Human-Machine Interface” accessibility requirements.</li> </ul>
10	OMB	M-04-04	<ul style="list-style-type: none"> <li>Memorandum to the Heads of All Department and Agencies – E-Authentication Guidance for Federal Agencies.</li> <li>Defines the E-Authentication requirement.</li> </ul>
11	OMB	M-11-11	<ul style="list-style-type: none"> <li>Requirements for Accepting Externally-Issued Identity Credentials.</li> <li>FICAM architecture and procedures for federal agencies.</li> </ul>
12	GSA	FICAM	<ul style="list-style-type: none"> <li>Federal Identity, Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance.</li> <li>Provides the common segment architecture and implementation guidance for federal ICAM programs.</li> </ul>
13	White House	NSTIC	<ul style="list-style-type: none"> <li>National Strategy for Trusted Identities in Cyberspace (NSTIC) – Provides guidance for identity trust in cyberspace.</li> </ul>
14	US Congress	FISMA	<ul style="list-style-type: none"> <li>FISMA of 2002, Public Law 107-347</li> </ul>
15	US Congress	E-Government Act of 2002	<ul style="list-style-type: none"> <li>Federal Management and Promotion of Electronic Government Services.</li> <li>Defines the requirements for electronic services.</li> </ul>
16	US Congress	The Privacy Act of 1974	<ul style="list-style-type: none"> <li>§ 552a. Records maintained on individuals.</li> <li>Defines VA Access Services Privacy assessment and control requirements.</li> </ul>
17	National Archives and Records Administration (NARA)	Federal Records Act	<ul style="list-style-type: none"> <li>Establishes the framework for records management programs in Federal Agencies.</li> </ul>

#	Issuing Agency	Policy, Directive, or Procedure	Purpose
18	VA	VA D 0735	<ul style="list-style-type: none"> <li>Homeland Security Presidential Directive 12 (HSPD-12) Program</li> <li>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.</li> </ul>
19	OMB	M-05-24	<ul style="list-style-type: none"> <li>Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.</li> </ul>

## 1.5. User Characteristics

The user community for the CAR activities consists of internal users including VA employees, contractors and affiliates. All users identified above are internal users. At this point none of the CAR reports and functionalities are external or Veteran facing.

## 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.

The following plans and other documents relate to this SDD:

- Requirements Specification Document (RSD) is developed from the system's original System Requirements Specification (SRS) along with the additional requirements that led to the changes to the system over the years since the original SRS was developed.
- Contingency Plan is developed according to the VA templates and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, which describes the processes and personnel required to operate the system when the system's primary site is not functional.
- Production Operations Manual (POM) contains the information required to successfully operate and maintain the system.
- Installation and Configuration Guide contains detailed information about how the products are installed and configured.
- Interface Control Documents (ICDs) contain information about specific interfaces with external systems.

## 1.7. Definitions, Acronyms, and Abbreviations

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

## **1.8. References**

The document references are listed in Section 1.6 above.

## **2. Background**

### **2.1. Overview of the System**

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.

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

The CAR Service provides the ability to proactively monitor and mitigate various potential compliance infractions and incidents. It provides a common compliance auditing and reporting framework to be leveraged throughout the VA. It sets the foundation to support adherence to applicable government policies and regulations and provides the capability to monitor IAM services to produce reports and generate alerts triggered by events or breach of predetermined thresholds. The focus of this IAM activity is to consolidate and to lessen the occurrence of redundancies, where possible, while reducing the administrative burden of compliance reporting for the VA.

### **2.2. Overview of the Business Process**

Compliance Audit and Reporting (CAR), based on the CA User Activity Reporting Module (UARM) product, provides centralized monitoring, alerting, and auditing as well as compliance reporting in association with the AcS 2.0. It establishes a compliance auditing framework that will provide the protections and security for the audit data as required. The CAR Service is integrated with Specialized Access Control (SAC), Credential Service Provider (CSP), Identity Proofing (IP), Single Sign-On internal (SSOi), Provisioning (Prov), e-Signature (e-Sig) and Single Sign-On external (SSOe) activities as well as Enrollment Services (ES). The CAR service provides the unique ability to proactively monitor, mitigate, and recover from potential compliance infractions and incidents, a common compliance auditing framework to be leveraged throughout the VA to provide the foundation for adherence within applicable government policy and regulation and the capability to monitor AcS services to produce reports and generate alerts triggered by events or breach of predetermined thresholds.

**Table 5: Business Processes**

<b>Business Process ID</b>	<b>Business Process Name</b>	<b>Owner</b>	<b>Description</b>
1	Manage Auditable Events	VA IAM AuthR/CAR PM	Provides ability for Privileged Users to define and configure auditable events.
2	Generate Standard Reports	VA IAM AuthR/CAR PM	Provides ability for Privileged Users to generate standard reports.
3	Define and Generate Ad-Hoc Reports	VA IAM AuthR/CAR PM	Provides ability for Privileged Users to define and generate ad-hoc reports using data elements available to CAR.
4	Define and Generate Alerts	VA IAM AuthR/CAR PM	Provides ability for Privileged Users to define parameters which will initiate alerts.
5	Manage User Access	VA IAM AuthR/CAR PM	Provides ability for CAR privileged user to manage user access to reporting features.

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

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

**Table 6: Business Process**

<b>Business Process ID</b>	<b>Business Process Name</b>	<b>Type</b>	<b>Owner</b>	<b>Description</b>
1	<a href="#">VA IAM SAC Use Case Model</a>	SAC Use Cases and Use Case Model	PD OIT	Use Cases to support SAC System
1	<a href="#">VA 2.0 Increment 2 Use Case Model Document</a>	Use Cases	PD OIT	Use Case Model Document
2	<a href="#">VA i4 Use Case Model</a>	Use Cases	PD OIT	I4 Use cases
3	<a href="#">CAR Use Case Model</a>	Use Cases	PD OIT	I4 CAR Use cases

## 2.3. Business Benefits

The CAR System also provides service integrity while reducing exposure to excess expense and audit activities. CAR is a common compliance auditing framework to be leveraged throughout the VA to provide the foundation for adherence within applicable government policy and regulation. The VA AcS 2015 Business Requirements Document, [BRD VA IAM Access Services 2015 4-24-14 SignatureReady.pdf](#), provides additional information to support the business benefits of the CAR solution.

## 2.4. Assumptions and Constraints

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

### 2.4.1. Design Assumptions

The end of life of the CAR application is 12/31/2017. The only changes that can be made are configuration changes on the application. Any requests for enhancements made to the underlying COTS product will be rejected. This is due to the vendor only addressing bug fixes.

**Table 7: Assumptions**

Assumption
UARM is currently nearing its end of life. Any future enhancements of the product will be limited.

### 2.4.2. Design Constraints

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

#### AcS Service - CAR

- **CA User Activity Reporting Module:** Version 12.5.1 or greater must be used and be configured and operated in FIPS Mode. FIPS Mode is required to provide FIPS-certified security algorithms for event transport and other communications between the CA User Activity Reporting Module and the CA Embedded Entitlements Manager (EEM). Per CA, the product is slated for end of life by year 2014 but active support will be until year 2017.
- **Operating Systems:** The CAR product only supports CentOS System which is a closed vendor provided Virtual Appliance. All the Subscription patches for the CentOS system are provided by the Vendor itself.
- **SSOi integrations:** The CAR product (UARM) does not support integration with the current integration patterns offered by SSOi. Therefore, SSO with CAR at this point is not supported.

**Table 8: Constraints**

Constraints
<ul style="list-style-type: none"><li>• UARM does not store actual authoritative audit logs so it does not have the capability, nor is it intended, to protect the integrity of the authoritative audit data.</li><li>• UARM does not support PIV authentication. Since it is a flash-based application, it also cannot be integrated with CA SSO.</li></ul>

### 2.4.3. Design Trade-offs

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

- Since CAR (CA UARM) cannot integrate with SSOi, it will continue to use EEM for maintaining user information and authentication.

## 2.5. Overview of the Significant Requirements

The material in this section is not to replace either the existing functional or technical requirements documents, nor serve as the basis for the Requirements Traceability Matrix, but only to inform non-project personnel reading this document of the basis for the design.

### 2.5.1. Overview of Significant Functional Requirements

**Table 9: Functional Requirements**

<b>AUDITING AND REPORTING</b>				
<b>Audit Trail</b> – Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.			<b>Medium</b>	<b>FY14 8/15/2013</b>
23.01	The CAR Service will provide a single point of auditing and reporting capability (only user & access mgmt. data) for all IAM services.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.02	The CAR Service will provide a single point of auditing and reporting capability (only user & access mgmt. data) for business applications (including applications not integrated with IAM).	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.03	The CAR Service will provide applications with the ability to request integration with the CAR service (via governance process) for their respective auditing and reporting capabilities (only user and access mgmt. data).	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.04	The CAR Service will provide applications with a standard set of guidelines and interface specifications to allow for seamless integration	FICAM v2, Section 9.4	Medium	FY14 8/15/2013

<b>AUDITING AND REPORTING</b>				
<b>Audit Trail</b> – Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.			<b>Medium</b>	<b>FY14 8/15/2013</b>
	with CAR.			
23.05	The CAR Service will support integration with various auditing data stores (e.g. flat files, databases, and directories).	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.06	The CAR Service will provide integrated applications with the ability to request standard and custom reports on available access management data for their respective application.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.07	The CAR Service scope and functionality shall be limited to the IAM functionality/services being rolled out in particular release iteration.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.08	The CAR Service shall provide the capability for a VA Requestor to define auditable events to be recorded.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.09	The CAR Service shall store the auditable events defined by a VA Requestor.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.10	The CAR Service shall provide a means to identify the IAM systems and services from which to collect the auditable events.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.11	The CAR Service shall store the list of IAM systems and services from which to collect the auditable events.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013



<b>AUDITING AND REPORTING</b>				
<b>Audit Trail</b> – Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.			<b>Medium</b>	<b>FY14 8/15/2013</b>
23.12	The CAR Service shall securely interface/communicate with the IAM systems and services to collect the audit data.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.13	The CAR service shall map all collected audit data into a standardized nomenclature.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
23.14	The CAR Service shall store the audit data collected from the IAM systems and services.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.01	The CAR Service shall provide the means for a VA Requestor to define standard reports.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.02	The CAR Service shall provide the means to run standard reports at the scheduled times.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.03	The CAR Service shall generate standard reports from the data collected from subscribing IAM systems and services and stored in the CAR reporting log.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.04	The CAR Service shall provide a means to preview standard reports upon request.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.05	The CAR Service shall provide a means to store standard reports for later retrieval.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.06	The CAR Service shall deliver standard reports to the appropriate recipients.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.07	The CAR Service shall provide the means for a VA Requestor to define and run ad hoc reports.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013

<b>AUDITING AND REPORTING</b>				
<b>Audit Trail</b> – Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.			<b>Medium</b>	<b>FY14 8/15/2013</b>
24.08	The CAR Service shall provide the means to store ad hoc reports and define them as new standard reports.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.09	The CAR Service shall generate ad hoc reports from the data collected from subscribing IAM systems and services and stored in the CAR reporting log.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.10	The CAR Service shall provide a means to preview ad hoc reports upon request.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.11	The CAR Service shall provide a means to store ad hoc reports for later retrieval.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
24.12	The CAR Service shall deliver ad hoc reports to the appropriate recipients.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
25.01	The CAR Service shall present a means for a VA Requestor to define alerts and alert thresholds.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
25.02	The CAR Service shall store the alert and threshold attributes defined by a VA Requestor.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
25.03	The CAR Service shall provide a means to identify the subscribing IAM systems and services for which to monitor compliance and audit alert attributes.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
25.04	The CAR Service shall store the list of subscribing IAM systems and services for which to monitor	FICAM v2, Section 9.4	Medium	FY14 8/15/2013

<b>AUDITING AND REPORTING</b>				
<b>Audit Trail</b> – Provide a capability to capture and maintain a chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific event in a security relevant transaction from inception to final result.			<b>Medium</b>	<b>FY14 8/15/2013</b>
	compliance and audit alert attributes.			
25.05	The CAR Service shall securely interface/communicate with the IAM systems and services to monitor alert attributes.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
25.06	The CAR Service shall provide the means to identify when alert conditions are met or alert thresholds are exceeded.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
25.07	The CAR Service shall generate alerts when alert conditions are met or alert thresholds are exceeded and deliver them to NSOC.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
26.01	The CAR Service shall provide a means for a CAR administrator to add and delete users/requestors.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
26.02	The CAR Service shall provide a means for a CAR administrator to modify the permissions of users/requestors	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
26.03	The CAR Service shall maintain a list of approved service users with access to reports.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
26.04	The CAR Service shall maintain a list of permissions assigned to service users.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013
26.05	The CAR Service shall provide a means to generate summary reports of the status of CAR service users and their permissions.	FICAM v2, Section 9.4	Medium	FY14 8/15/2013

## 2.5.2. Overview of Functional Workload/Performance Requirements

**User Profile:** VA Employee or Contractor accessing CAR to run standard and ad hoc reports

The CAR service for this increment shall support the following:

**Table 10: Workload and Performance Requirements**

Operation	
<b>Name</b>	CAR
Usage Profile (Log Entries)	
Mean Daily volume	1,000,000
Projected Growth	250,000/year
Peak Daily volume	2,000,000
Projected Growth	500,000/year
Peak Hourly volume	100,000
Days of operation	Sunday-Saturday
Hours of operation	24/7
Peak Hours	9am-7p.m.Eastern
Maximum Response Time	Data must be returned at no more than 1 minute for every 10,000 records

## 2.5.3. Overview of Operational Requirements

The AcS 2.0 is available within the Terremark environment as required by VA. Terremark is responsible for reliability and monitoring while the AcS 2.0 is operational. The tools, methods, and specifications for monitoring the reliability of the AcS 2.0 are the responsibility of Terremark.

**Table 11: Service Availability Level 4**

<b>*Standards adopted from specification created by Application Structure and Integration Services (ASIS)</b>	
<b>Description</b>	Mission Critical Information
<b>Minimum Availability</b>	99.99%
<b>Maximum Downtime Per Month</b>	4.4 minutes
<b>Business Value</b>	Essential to fundamental business operations – outage seriously impairs functioning of business.
<b>System Response</b>	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.

<b>*Standards adopted from specification created by Application Structure and Integration Services (ASIS)</b>	
<b>Operational Hours</b>	Required 24 hours a day, every day.
<b>Significant Outage</b>	More than five minutes of downtime is considered significant at any time and requires an ANR to be sent out to the appropriate teams.
<b>Outage Impact</b>	Interruption of service may result in severe financial, regulatory, patient safety, patient health, or other business issues.
<b>Scheduled Maintenance</b>	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

Applicable requirements to support CAR within i5 can be found in the i5 RSD: [AcS 2.0 i5 RSD.PDF](#)

**Table 12: Technical Requirements**

<b>ID</b>	<b>Requirement</b>
[FEAT461961]	The Role Engineering and Compliance tool and the CAR Service shall integrate to produce reports on policy violations data.
[FEAT461962]	The Role Engineering and Compliance tool and the CAR Service shall integrate to produce reports on provisioning and de-provisioning activities.

## 2.5.5. Overview of the Security or Privacy Requirements

Per Section 2.13 of the AcS 2.0 i5 RSD, the applicable security specifications include the following:

- CAR is deployed inside the VA firewall.
- CAR conforms to the VA security standards detailed in VA Handbook 6500 Information Security Program.
- CAR meets all Veterans Health Administration (VHA) security, privacy, and identity management requirements and those listed in VA Handbook 6500 (Enterprise Requirements Appendix).

- The system must store and transmit Personally Identifiable Information (PII) or sensitive information such as passwords in an encrypted or one-way hashed format and on the SSL channel.
- The web servers providing access to VA applications for external users over the Internet must reside in the demilitarized zone (DMZ).

### **2.5.6. Overview of System Criticality and High Availability Requirements**

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

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

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

### **2.5.7. Single Sign-on Requirement**

Per the Vendor of the CA solution, CA UARM requires explicit authentication to its system. Given that CA UARM is a flash based application it inherently resists accepting custom HTTP headers (In this case, headers pertinent to SSOi); The CAR product (UARM) does not support integration with the current integration patterns offered by SSOi. Therefore, SSO with CAR is not supported at this point.

### **2.5.8. Requirement for Use of Enterprise Portals**

N/A

### **2.5.9. Special Device Requirements**

N/A

## **2.6. Legacy System Retirement**

N/A

## **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 CAR solution. The overall AcS design is shown in Figure 1 below.

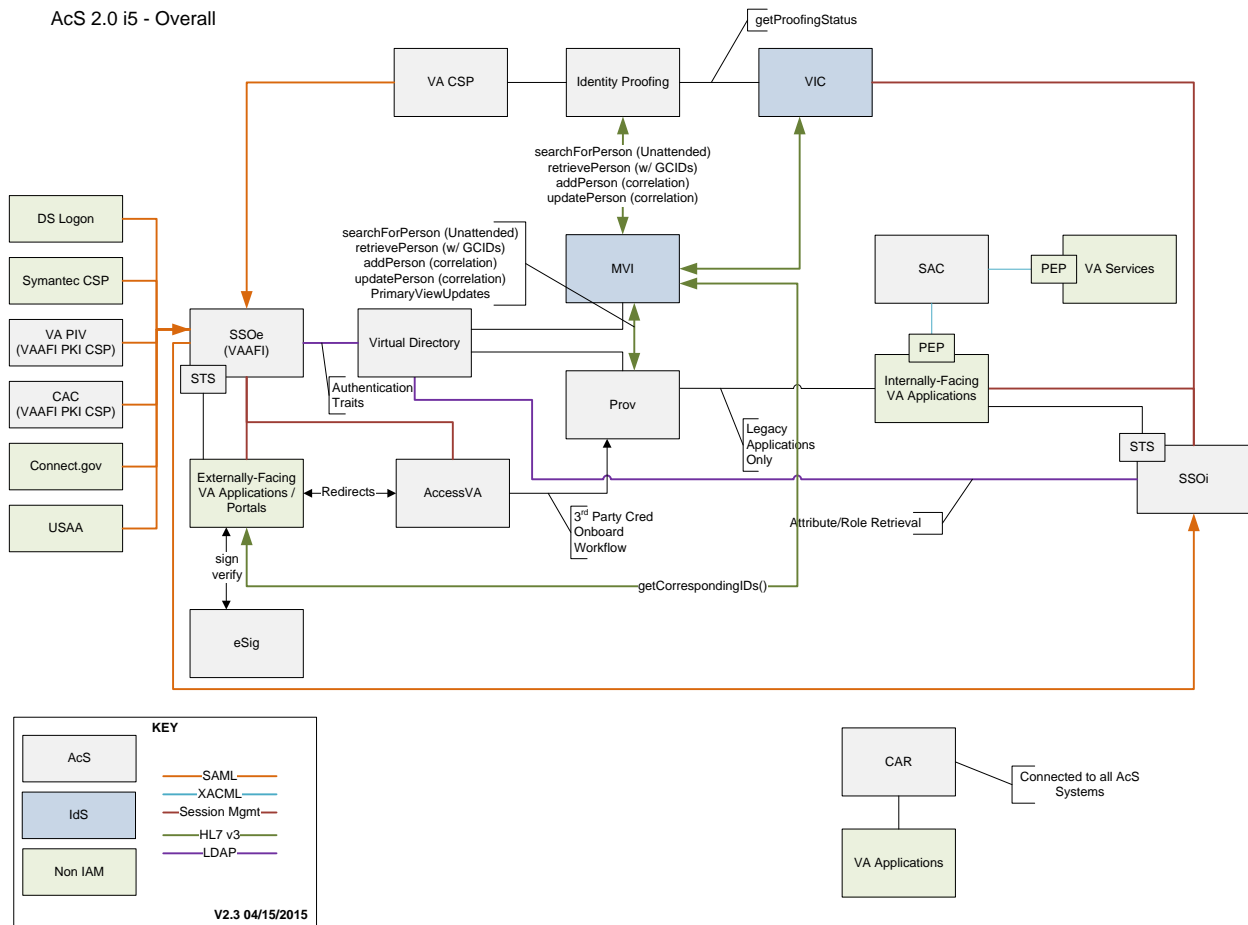


Figure 1: AcS 2.0 Overview

#### 3.1.1. Application Context

This section provides context for each of the activities developed for VA AcS 2.0. The aim of the AcS 2.0 is to deploy a cohesive and consistent foundational AcS architecture that is flexible, modular, extensible, and scalable in VA's infrastructure. VA AcS foundation infrastructure enables internal users, external users and VA business partners to access various AcS activities such as:

- Credential Service Provider (CSP)
- Identity Proofing (IP)
- Electronic Signature (eSig)

- Specialized Access Control (SAC)
- Provisioning (PROV)
- Single Sign-On – Internal (SSOi)
- Single Sign-On – External (SSOe)
- Compliance Audit and Reporting Service (CAR)

#### **3.1.1.1. Compliance Audit and Reporting**

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

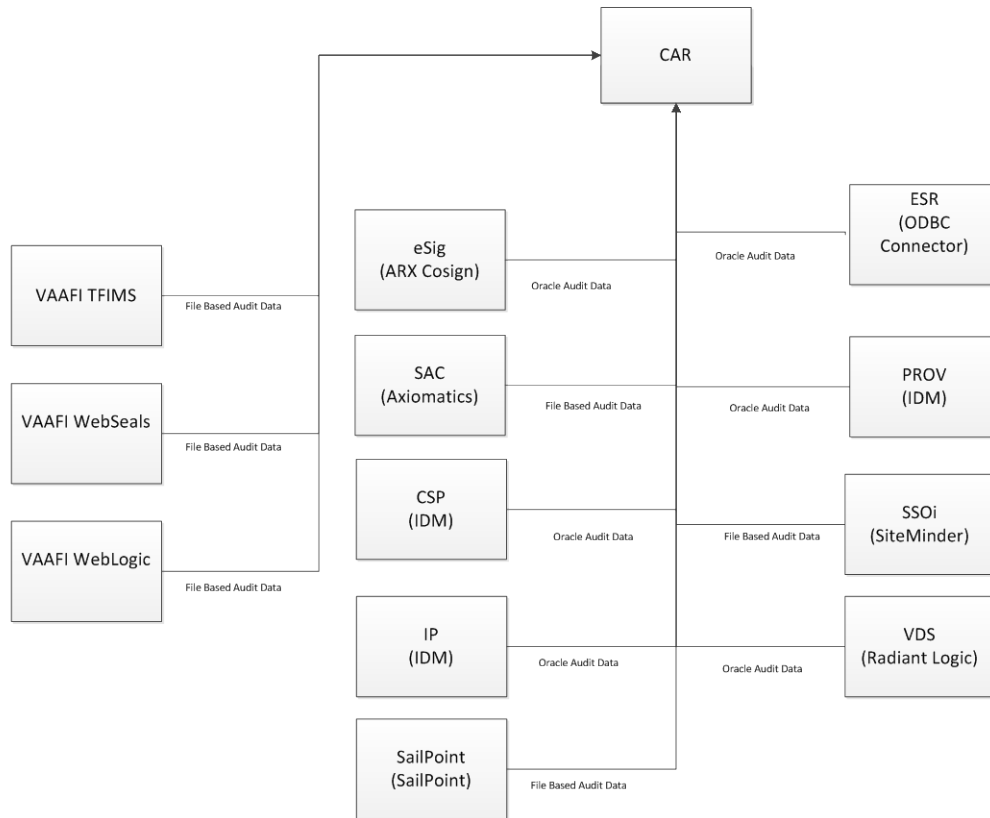
The primary actors interacting with the CAR application are the following:

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

The CAR Service is based on the User Activity Reporting Module (UARM) COTS provided by CA Technologies (CA). The UARM is a HA solution. The CAR Service interacts with SAC and CSP/IP by listening to the changes that occur within these services. The CAR Service integrates with the following Services:

- Specialized Access Control (SAC)
- Identity Proofing (IP)
- Credential Service Provider (CSP)
- Single Sign on internal (SSOi)
- Single Sign on internal (SSOi)/VAAFI
- Electronic Signature (E-Sig)
- Provisioning (including VDS and SailPoint)
- Enrollment Services (ES)





**Figure 2: CAR Context Diagram**

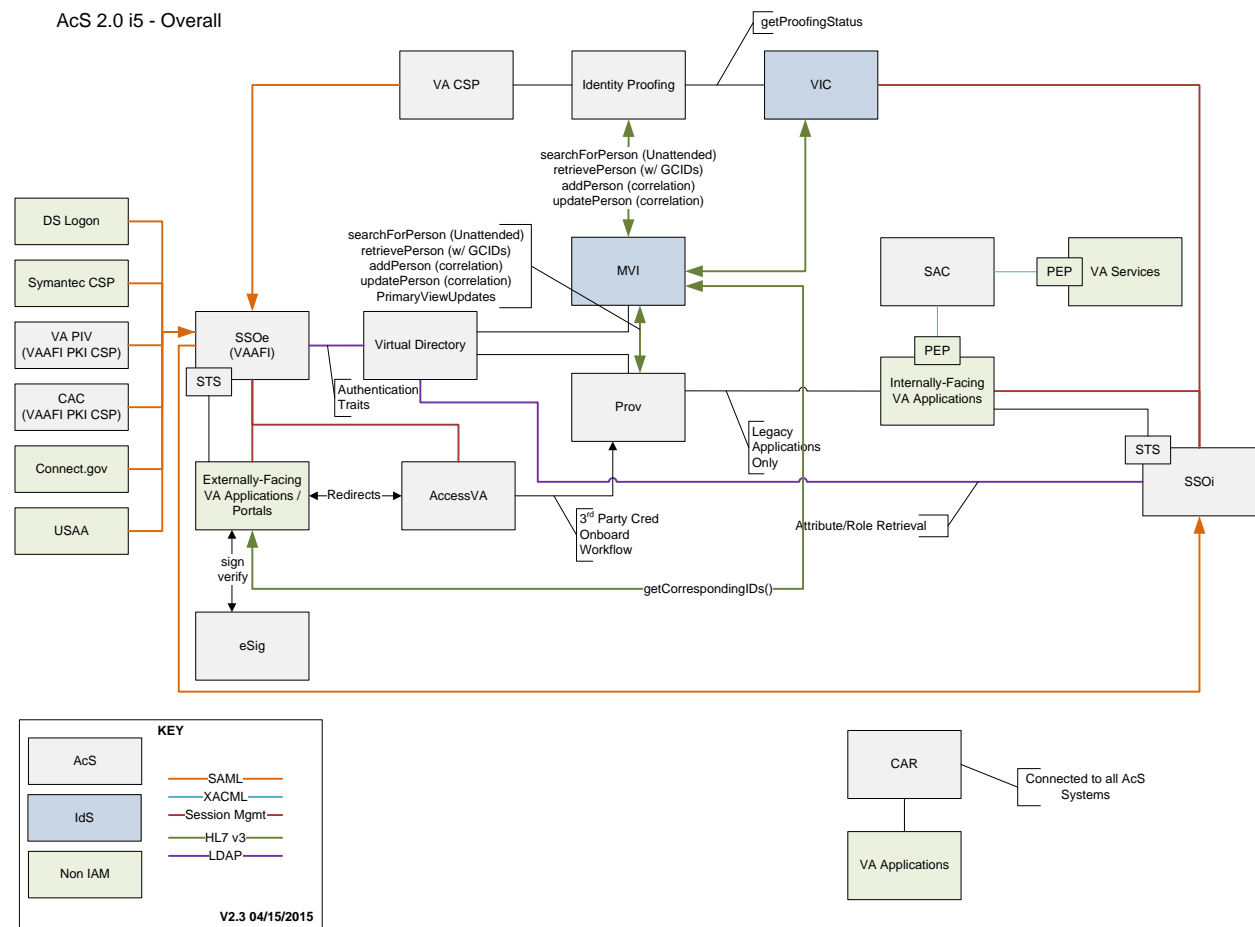
**Table 13: (Grouping): Application Context Description**

**Interfaces Internal to OIT**

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

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

Figure 3 below provides a high-level application design for the CAR and identifies the major AcS activities and/or relationships with VA applications.



### Figure 3: CAR Application Design

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

### Table 14: Activities in the High-Level Application Design

ID	Name	Description	Service or Legacy Code	External Interface Name	Internal Interface Name
1	CSP	CSP provides external user's credentials to VA applications that are not eligible for another VA approved credential.	Service	Self Service and Registration	VAAFI, IP, CAR

ID	Name	Description	Service or Legacy Code	External Interface Name	Internal Interface Name
2	IP	IP facilitates evaluating and validating a user's identity to be true and unique to the degree (level) of confidence required by VA.	Service	N/A	MVI, CSP, CAR
3	eSig	eSig provides the ability to sign documents electronically.	Service	N/A	CAR
4	SAC	SAC provides the ability to maintain and process granular access decisions based on a set of business rules and user attributes.	Service	N/A	CAR
5	Provisioning	Provisioning associates an identity to one or more application accounts and the associated entitlements to the identity. Provisioning also provides the capabilities for managing roles and certifying entitlements.	Service	TMS	AD, CAR, EDR, MVI, PIV, VDS, IP
6	SSOi	SSOi provides the desktop sign-on capability to internal VA users. SSOi also provides authentication and access to VA business applications for both internal and external user populations. External credentials are brokered by the VAAFI service and are a federated partner with SSOi.	Service	Federation	AD, IP, CSP, Provisioning, SAC
7	CAR	CAR provides the ability to proactively monitor, mitigate, and recover from potential compliance infractions and incidents.	Service	N/A	SSOi, Provisioning, CSP, IP, eSig, SAC

### 3.1.3. Application Locations

Table 13: Application Locations

Application Component	Description	Production /PreProd Hosting Facility	Type	SQA
CA UARM	User Audit and Reporting Module.	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)	N/A	AITC

<b>Application Component</b>	<b>Description</b>	<b>Production /PreProd Hosting Facility</b>	<b>Type</b>	<b>SQA</b>
Management/Reporting Server	Managing the UARM interface to the user	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)	Presentation Service	AITC
Collection Server	Repository for normalized UARM logs	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)	Data Layer	AITC
Oracle	Repository for CSP/IP audit events	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)	Data Layer	AITC
DataPower Audit Logs	The output consisting of the events for SAC	Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery)	Data Layer	AITC

**Table 15: Application Users**

<b>Application Component</b>	<b>Location</b>	<b>User</b>
CAR	Performs administrative functions including management of UARM reports dashboard, generation of reports, and creating other users in UARM	CAR Administrator
CAR	Read Only Users	Auditor
CAR	Runs reports and tracks audit records to verify continual system conformance with security and policy with some edit capabilities	Analyst

## 3.2. Conceptual Data Design

The CAR data model aligns the necessary data attributes to meet the functional requirements, as well as standard, FIPS compliant technologies to secure sensitive data types. The CAR data model design leverages the default schema used by CSP and IP, as well as flat file structure of SAC log files and is imported into the default schema for UARM product using the default normalization. The default schema is internal to the COTS and is not visible to the end user.

### 3.2.1. Project Conceptual Data Model

CAR is based on a closed system (CA UARM) which does not interact with any separate repositories for its functions and therefore follows data model which is provided out of the box with the product. CAR is a COTS based application; please refer to the CA UARM documentation for the applicable data model.

### 3.2.2. Database Information

The CAR Service stores the event data in the UARM logs. Table 18 below defines the UARM schema designed to meet the needs of the CAR Service and associated functional and technical requirements.

Note: The end user may choose the attributes selected for display within the report. Selecting a particular event will display the following attributes:

**Table 16: UARM Attributes**

Index	Attribute	Attribute Description	Data Format
1	source_address	The source address for the event	Any Text <sup>1</sup>
2	source_hostdomainname	The host domain name for the source	Any Text
3	source_hostname	The hostname for the source	Any Text
4	source_objectname	The object name for the event	Any Text
5	source_processname	The process name	Any Text
6	dest_hostname	The destination hostname	Any Text
7	event_action	Action	Any Text
8	event_category	Category of the event	Any Text
9	event_class	Class of the event	Any Text
10	event_count	Count for the event	Any Text
11	event_datetime	Date and time for the event	Any Text
12	event_day_datetime	The day	Any Text
13	event_hour_datetime	Hour	Any Text
14	event_logname	The logname	Any Text
15	event_minute_datetime	Minute	Any Text
16	event_month_datetime	Month	Any Text
17	event_quarterhour_datetime	Quarterhour	Any Text

---

<sup>1</sup> Any Text is nomenclature specific to UARM. Any text supports dynamic length alphanumeric characters.

Index	Attribute	Attribute Description	Data Format
18	event_sequence	Sequence	Any Text
19	event_summarized	Summary	Any Text
20	event_time_gmt	Time	Any Text
21	event_time_hour	Hour	Any Text
22	event_time_minute	Minute	Any Text
23	event_time_month	Month	Any Text
24	event_time_monthday	Day of the Month	Any Text
25	event_time_weekday	Weekday info	Any Text
26	event_time_year	Year of the event	Any Text
27	event_year_datetime	Datetime of the event	Any Text
28	ideal_model	The model	Any Text
29	event_result	The event result string	Any Text
30	result_string	The detailed result string	Any Text
31	event_source_address	Event source address	Any Text
32	event_source_hostdomainname	The host domain name for the source	Any Text
33	event_source_hostname	The hostname for the source	Any Text
34	agent_address	The address of the agent	Any Text
35	agent_connector_name	The connector name for the agent	Any Text
37	agent_group	The group of the agent	Any Text
38	agent_hostdomainname	The host domain name for the agent	Any Text
39	agent_hostname	The hostname of the agent	Any Text
40	agent_name	The name of the agent	Any Text

<b>Index</b>	<b>Attribute</b>	<b>Attribute Description</b>	<b>Data Format</b>
41	agent_version	The version number for the agent	Any Text
42	raw_event	The raw event string	Any Text
43	receiver_hostaddress	The hostaddress for the receiver	Any Text
44	receiver_hostname	The hostname of the receiver	Any Text
45	receiver_name	The name of the receiver	Any Text
46	receiver_port	The port for the receiver	Any Text
47	receiver_time_gmt	The GMT time for the receiver	Any Text
48	receiver_timezone	The timezone for the receiver	Any Text
49	receiver_version	The version number for the receiver	Any Text



### **3.2.3. User Interface Data Mapping**

This section describes and defines the data that will be available for users of the CAR solution. Out-of-the-box screens are not shown.

#### **3.2.3.1. CAR Screen Interface**

N/A

#### **3.2.3.2. Report Interface**

N/A

#### **3.2.3.3. Unmapped Data Element**

N/A

## **3.3. Conceptual Infrastructure Design**

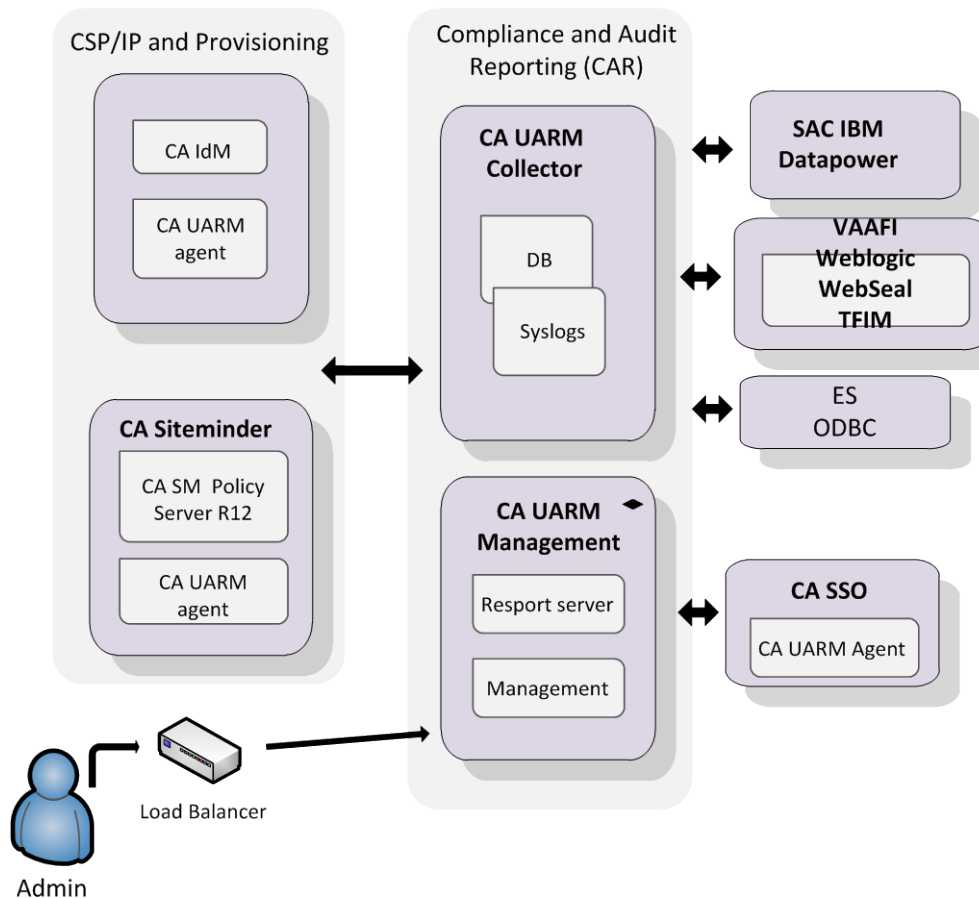
CAR is the central reporting authority for the IAM service for the VA. The following list describes the event sources for various IAM services.

- CSP, IP, and Provisioning provide the information through the CA Identity Manager and SiteMinder connections. These events are captured in the Oracle instance as explained earlier in this section and in turn transfer the information into UARM logs.
- The IBM DataPower is the underlying backbone for the SAC system and the CAR system pulls in the data events in form of log files and parses them appropriately.

Figure 4 presents the conceptual representation from CAR.

**Figure 4: Conceptual Infrastructure Design**

Internal VA Network



The Internal Administrator will access the load balanced admin URL to view the reports. The load balancer will route the request to the report server where the user may view different compliance reports.

In conjunction with the integration contained herein, the IAM components (Identity Manager, SiteMinder and CA SSO) will have UARM agent installed. The agent will transfer the logs into UARM Collector server. The Report server will collect the data from the collector server and display it to the end user.

### 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.

The CAR architecture maintains two (2) Collector Servers and one (1) Reporting Server. The Collector Servers are the main actors that collect the data events and are designed to have an instant failover. The agents for the collectors would failover to the appropriate collector, which will reduce the likelihood of data loss in transit.

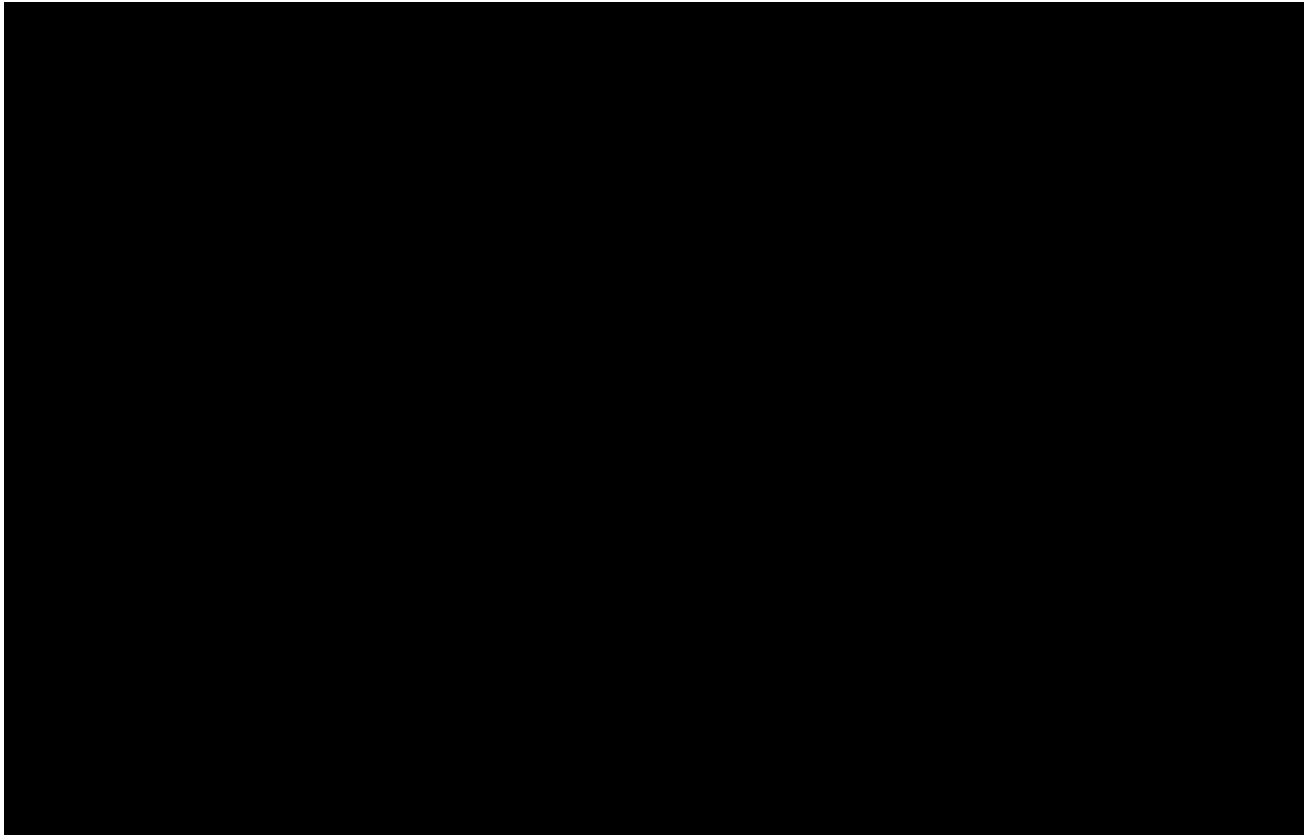
The reporting servers are designed with a hot and cold instance. Since the reporting server is not responsible for any data collection, the hot and cold instance addresses HA requirements in that the collector server will be switched to the cold instance in case of a failure.

### **3.3.2. Special Technology**

N/A

### **3.3.3. Technology Locations**

Please refer to the Application Locations Section for the additional details of the Technology Locations.



**Figure 5**

### **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**

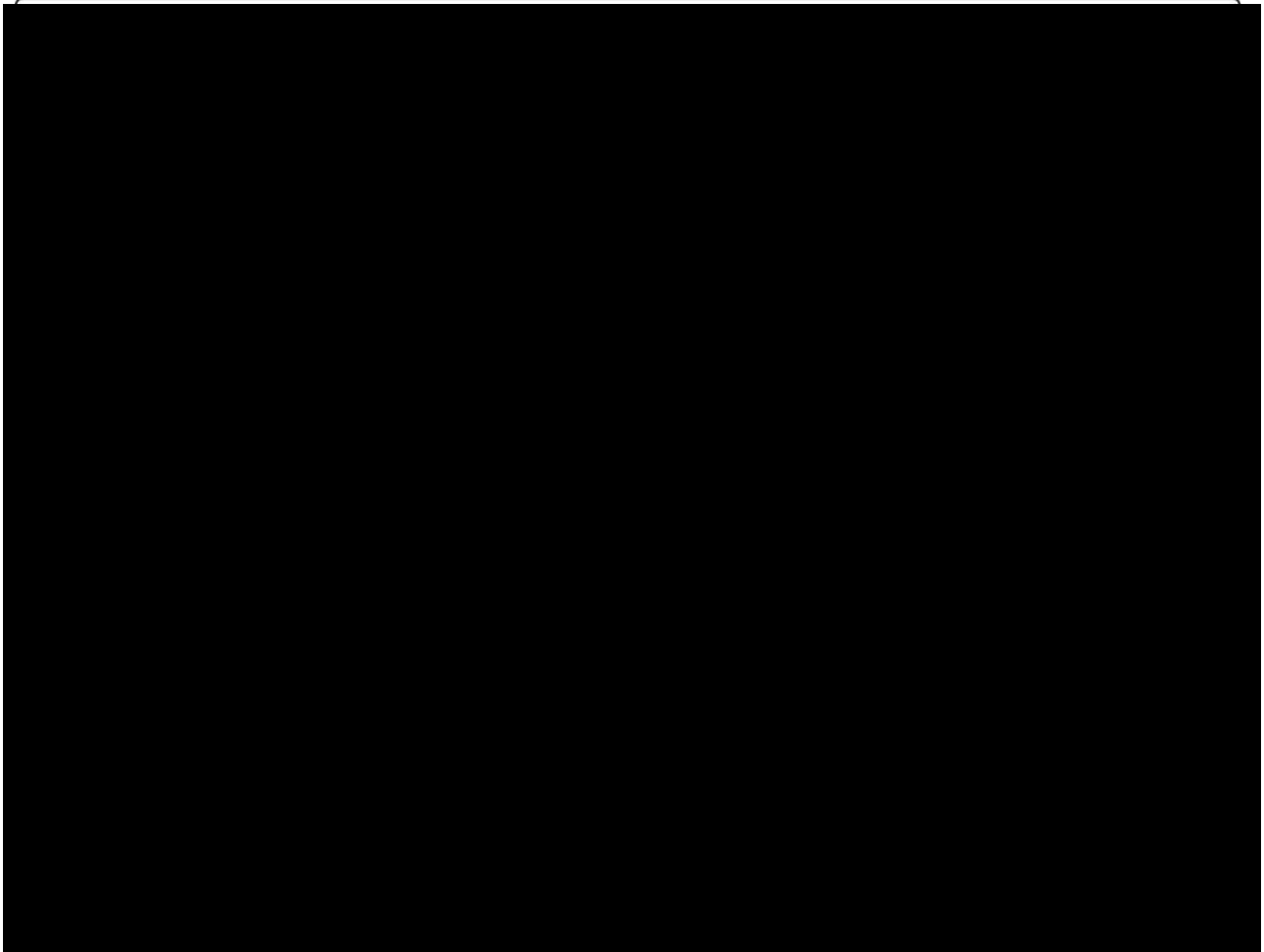
- This site provides hot failover capability so that services and data are maintained in the event of a failure in Production.
- This environment is identical to the Production environment.

- 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 CAR infrastructure. Each component of the infrastructure will be described in the next sections of this document. In each section, these connections will be described and an internal breakdown of the components will also be shown.

#### 3.3.4.1. Location of Environments and External Interfaces



**Figure 6: Sample Conceptual Networks and Environments**

### 3.3.4.2. Conceptual Production String Diagram

The following diagram, Figure 7, provides a logical view of CAR

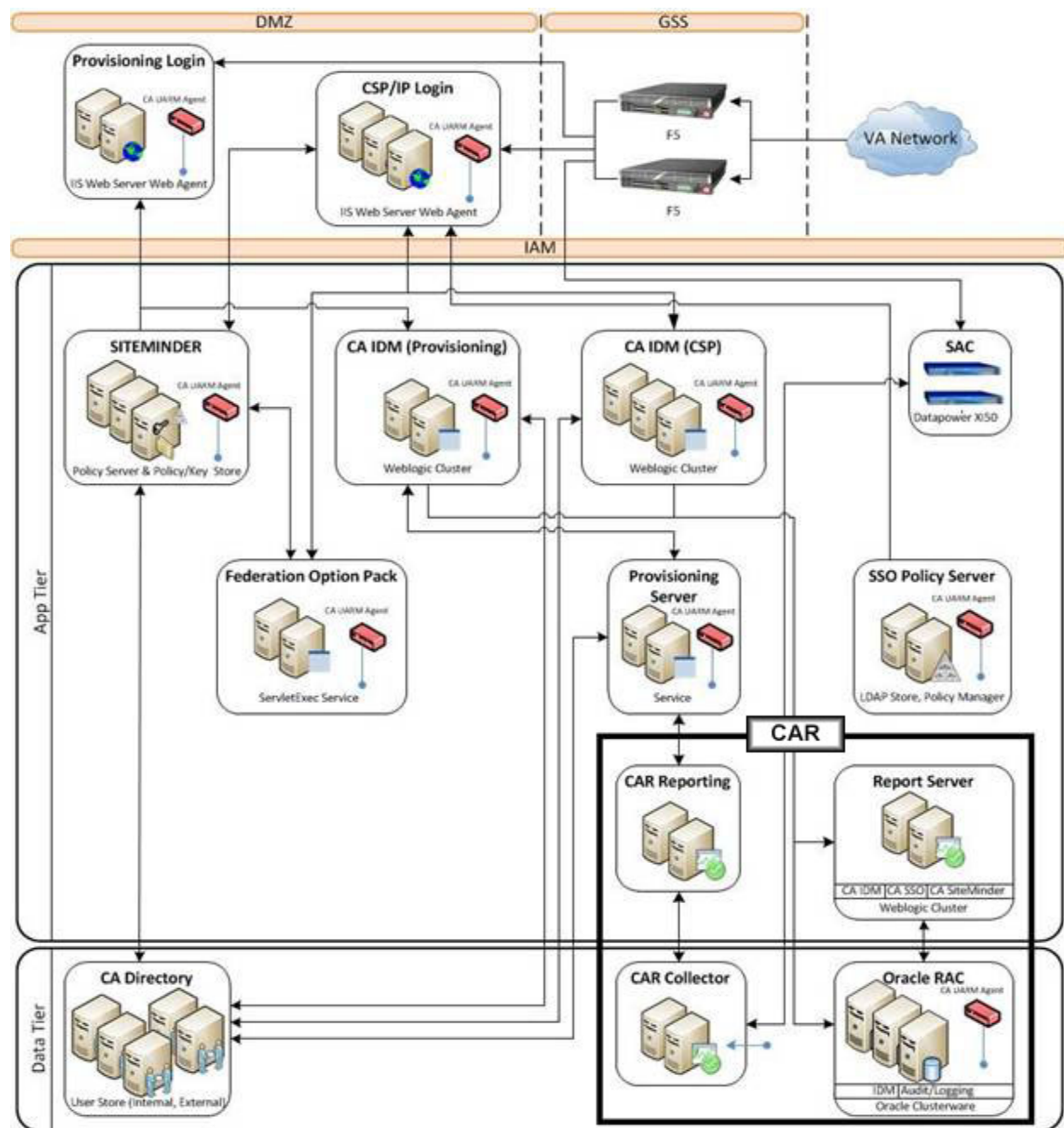


Figure 7: Logical Network String Diagram

## 4. System Architecture

The following section describes the overall solution architecture along with hardware and software architecture view of the CAR solution. This section provides an overview of the various components involved in the solution and their interaction both internally and externally. An



abstract operational view of the solution is depicted in the conceptual design above. The Hardware Architecture and Software Architecture sections elaborate the CAR solution system architecture.

**Figure 8: CAR System Architecture**

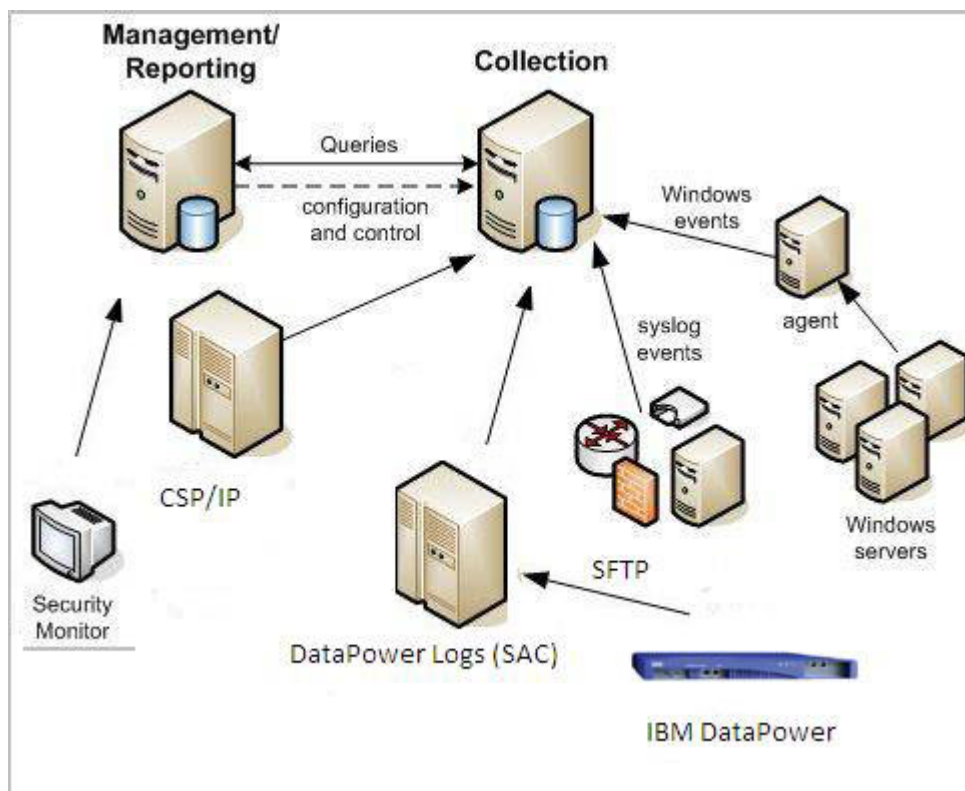


Table 20 describes each components of the CAR Architecture.

**Table 17: CAR Components**

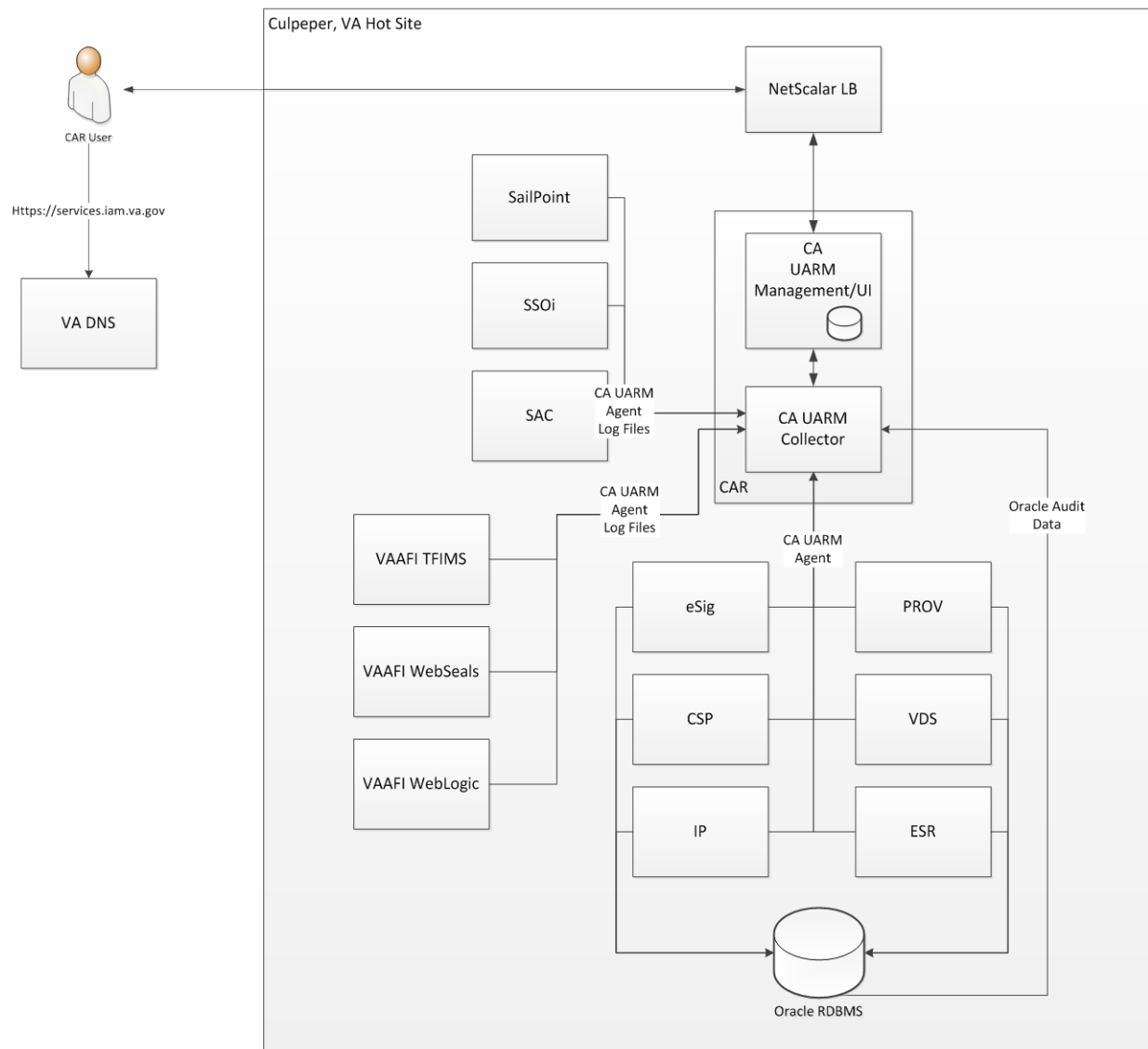
Component	Definition/Description
Management Server	The Management server presents the GUI to the end user and aggregates reports from the Collection server.
Collection Server	The Collection server is the main engine of the CAR system. It aggregates event information from CSP/IP and SAC. The Collection Server also contains the UARM logs that store the event information for CAR.
Agents	Various agents are deployed across IAM activities and Windows servers to poll the events that need to be recorded. Agent details are documented in section 3.1.2

## 4.1. Hardware Architecture

The CAR Service architecture is composed of following components:

- UARM Report and Management Server
- UARM Collector
- UARM Agent and Connector

The following diagram, Figure 9, shows the AcS 2.0 hardware architecture.



**Figure 9: Hardware Architecture**

The uniform resource locators (URLs) for CAR for production, pre-production and SQA are provided in the table below. The following table provides details on the CAR server such as ports, URLs, protocols hostnames for each application in every environment.

**Table 18: Virtual Machines and Appliances  
SQA (AITC)**

Application	Number of VMs	Number of Physical Servers	Hostname
CA UARM (Tomcat)	4	N/A	[REDACTED]

**Pre-Production (Terremark Culpeper, VA)**

Application	Number of VMs	Number of Physical Servers	Hostname
CA UARM	3	N/A	[REDACTED]

**Production (Terremark Culpeper, VA)**

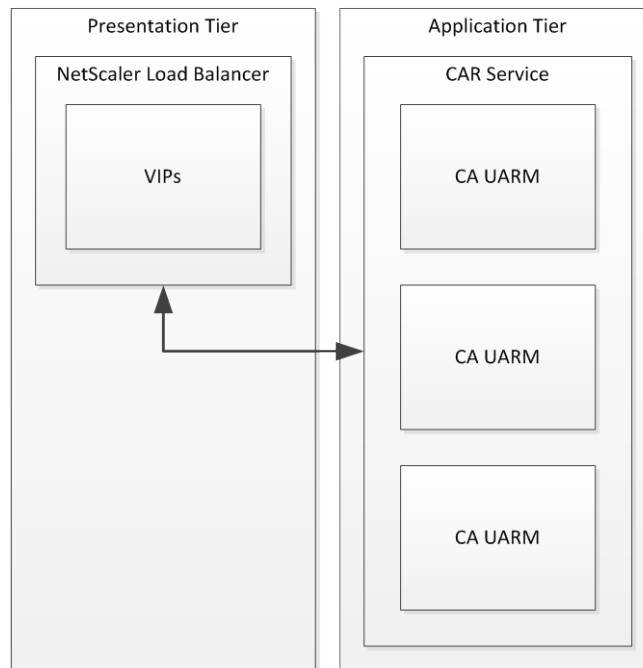
Application	Number of VMs	Number of Physical Servers	Hostname
CA UARM	3	N/A	[REDACTED]

**DR (Terremark Miami, FL)**

Application	Number of VMs	Number of Physical Servers	Hostname
CA UARM	3	N/A	[REDACTED]

## 4.2. Software Architecture

The Management and Collection server form the backbone for the CAR system. The figure below describes the software architecture for CAR users:



**Figure 10: Software Architecture**

The end of life of the CAR application is 12/31/2017. The only changes that can be made are configuration changes on the application. Any requests for enhancements made to the underlying COTS product will be rejected.

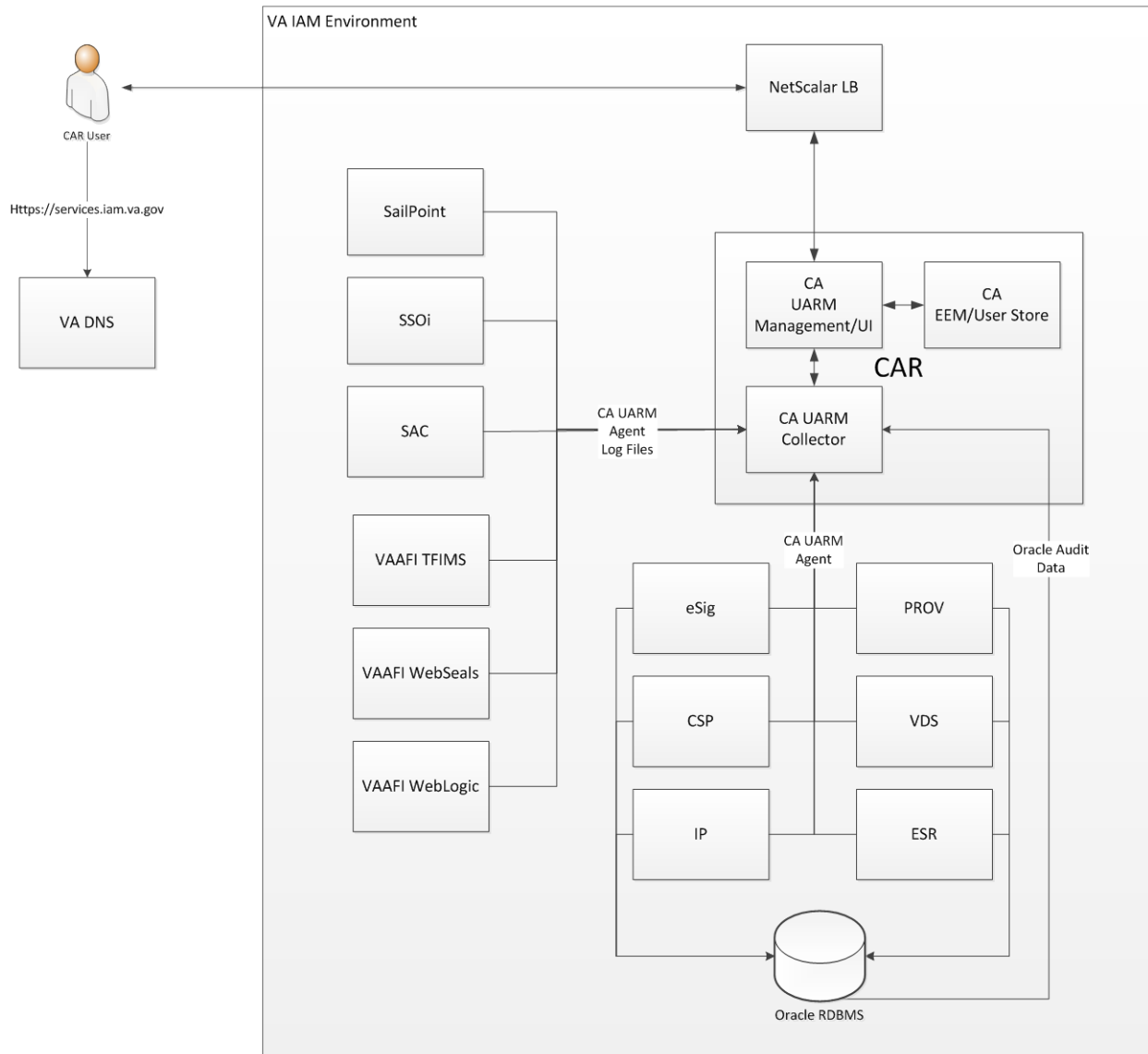
The Management server provides the GUI to the user and sends the query to the Collector Server and presents it to the user.

- The CAR Service deploys agents for CSP, IP and SAC Services.
  - The agents are deployed using the UARM administrator console.
  - There are two agents that are deployed for CSP and IP on the CSP and IP server. These agents poll the audit event changes to SiteMinder and Identity Manager. As mentioned later, the agents forward the events to the Collector server. The Collector server are configured for failover so no data is lost in transition
  - There is no agent deployed for SAC as the events are captured in a log file which is transferred via SFTP to the Collector server
  - In addition to the aforementioned agents for CSP and IP, there is a self-monitoring agent which comes pre-bundled and preconfigured with UARM.
- The connectors capture events in the CSP and IP Services and store them in the Oracle database.
- The CAR Service utilizes a built in Oracle connector to gather audit data, normalize the audit events, and store them in the UARM collector server.
- The DataPower logs are transferred using the SFTP protocol to the UARM server. The Custom file log connector parses the events and stores them in the UARM collector store.

- The Management and Reporting server uses the internal UARM logs to provide the ad-hoc and standard reports/alerts.

### 4.3. Network Architecture

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



**Figure 11: CAR Network Security Topology**

## 4.4. Service Oriented Architecture/ESS

CAR is self a contained system but is not an SOA service because it does not offer a Service interface and thus this section is Not Applicable.

## 4.5. Enterprise Architecture

The end of life of the CAR application is 12/31/2017. The only changes that can be made are configuration changes on the application. Any requests for enhancements made to the underlying COTS product will be rejected.

**Table 19: Compliance Audit and Reporting (CAR)**

Products	Abbreviation	Product Version/Release
CA User Activity Reporting Module <sup>2</sup>	CA UARM	12.5 SP3 (12.5)
CA User Activity Reporting Module Agent	CA UARM Agent	12.5 SP3 (12.5)

## 5. Data Design

CA UARM is a COTS solution; please refer to the COTS documentation.

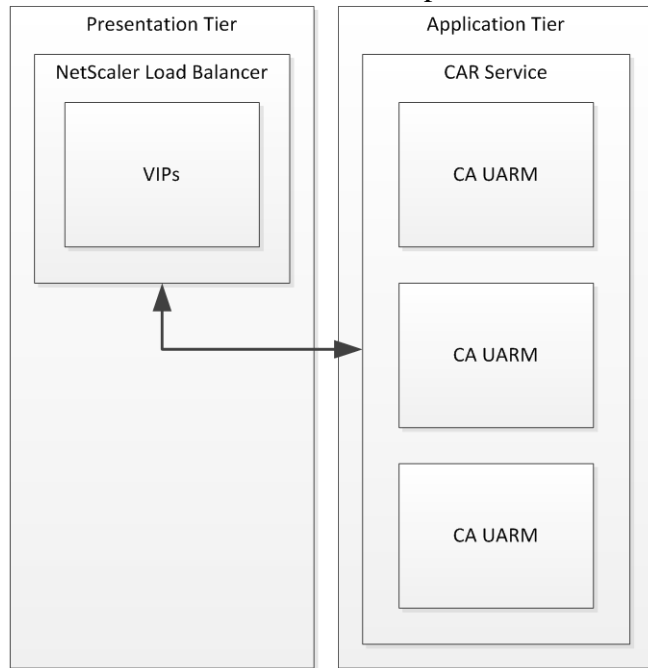


Figure 12

### 5.1. DBMS Files

In order for CAR to collect audit data an agent binary is installed on the servers of integrated applications with access to the relevant audit data for reporting. A connector is configured on the agent for each event source. The connector configuration specifies the data source and the relevant data from that data source that CAR will collect.

Collected events specified by connectors are sent by the agent to a CA User Activity Reporting Module server for processing and initial storage. The events are stored within a SQL based log store that is part of the CA UARM application. These log stores are part of the COTS product and can only be modified by the application. They are then synched up between all three of the UARM Log Manager servers.

The event log store uses a federated system, with each host server maintaining its own local event log store and the ability to contact other stores in the CAR environment. When you query a server for event information, it can search its own local event log store as well as all others connected through the federation. This arrangement allows for data integrity to be maintained even if an issue develops with one of the servers.

### 5.2. Non-DBMS Files

Refer to the ICD for integration related information.

### **5.3. Data View**

N/A



## 6. Detailed Design

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

### 6.1. Hardware Detailed Design

The sections below provide the hardware information for CAR. The following table displays the sizing, network, Operating System, and number of Virtual Machines:

**Table 20: Virtual Machines**

Hostname	Zone	Function	OS	Type	Software Baseline	CPU	RAM	OS GB	APPG BD :	Databases GB E :	Logging GB F :	Page GB G :	Total GB B	Server OS	Server Middleware	IOC Date	Internal IP	NAT IP	FQDN	Gateway	Mask	DNS 1	DNS 2	
Preprod - TFG027-015																								



20131108 - AcS IAM  
TerreMark PreProd ar

## 6.2. Software Detailed Design

The CAR Service is deployed within the VA IAM Infrastructure. CAR leverages the capabilities of the CA UARM COTS suite to minimize software development using out of box features. While every effort will be made to minimize the customization for ease of maintenance in the future, the following customizations are necessary based upon VA requirements:

- The agents will be configured for CSP and IP. The details are provided in the install guide.
- The out of the box connectors is configured to perform the UARM normalization.

### 6.2.1. Conceptual Design

#### 6.2.1.1. Product Perspective

CAR is based on a COTS product; and is independent and self-contained.

##### 6.2.1.1.1. User Interfaces

Refer to Section 3.2.3 for information on user interfaces.

The CA User Activity Reporting Module is incompatible with SSOi and instead must rely on its own internal user store. User accounts are configured manually by an administrator and are solely used for accessing CAR. The three predefined roles included within the UARM COTS product are Administrator, Analyst, and Auditor. Although custom roles are created based on the requirements of individual integrations they all conform to the same basic privileges. Administrators have full access to everything in CAR including configuration changes. Analysts only have access to the reports including the ability to create and modify reports but they cannot access system configurations. Auditors are users that only have read access on reports.

##### 6.2.1.1.2. Hardware Interfaces

N/A

##### 6.2.1.1.3. Software Interfaces

N/A

##### 6.2.1.1.4. Communications Interfaces

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

**Table 21: Port Communications and Protocols**

Application	Network	Port(s)	Reason	Protocol(s)
CA UARM	Internal	████	Administration Port for CA UARM	TCP

Application	Network	Port(s)	Reason	Protocol(s)
CA UARM	Internal	████	SSL Port (reverse proxy to administration port 5250) for CA UARM	HTTPS
CA UARM	Internal	████	Syslog port (UDP) for CA UARM server	TCP
CA UARM	Internal	████	Syslog TCP listening port for CA UARM	TCP
CA UARM	Internal	████	Agent command and control listening port	TCP
CA UARM	Internal	████	Communication port for ODBC /JDBC driver	TCP
CA UARM	Internal	████	Audit client communication with port-mapper	TCP
CA UARM	Internal	████	Dispatcher SME listener	TCP
CA UARM	Internal	████	CA Directory LDAP DXadmin port (CA Directory bundled with CA UARM)	TCP
CA UARM	Internal	████	Dispatcher Service in SSL mode for events from Client Connector	TCP

Please refer to the POM for PreProd and Prod PKI Certificates.

#### 6.2.1.1.5. Memory Constraints

The CA recommended system configuration requires at least 8 gigabytes of RAM per UARM server.

#### 6.2.1.1.6. Special Operations

N/A

#### 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 for the CAR application

**Table 22: CAR Products**

#	Software	Description
1	CA User Activity Reporting Module (UARM)	CA User Activity Reporting Module is a high-performance log management solution.

### 6.2.1.3. User Characteristics

Refer to Section 1.5 and Section 3.2.3 for user-related information.

### 6.2.1.4. Dependencies and Constraints

Refer to section 1.4 and section 2.4 for AcS 2.0 constraints and dependencies.

## 6.2.2. Specific Requirements

This SDD provides the foundational detailed design for CAR activities under the VA Development Support program. CAR is a COTS product that sufficiently meets the detailed functional requirements.

### 6.2.2.1. Database Repository

N/A

The UARM product maintains its own database.

CA User Activity Reporting Module collects logs from a variety of applications and devices using agentless or agent-based methods. It then normalizes the log to CA Common Event Grammar (CEG) and reduces the volume of logs by filtering unwanted events based on pre-defined event filtering policies. Processed events are available for reporting, alerting, and multi-dimensional investigation. Based on log archival policy, CA UARM compresses logs and stores them on external storage systems for long-term storage. The CA UARM component is installed and configured in FIPS only mode as per TRM.

CA UARM only supports CentOS System which is a closed vendor provided Virtual Appliance. This Product is procured and properly licensed to VA. All the Subscription patches for the CentOS system are provided by the Vendor itself. Additionally, according to CA vendor, UARM is near its End-Of-Life, and attempting to migrate from the CentOS Linux to RedHat Enterprise Linux platform in order bring CAR in compliance with TRM is not going to be vendor supported.

Table 23

Characteristic	Description
Subcomponents	<p><b>Management/Reporting Server:</b> There will be one active management server in the User Activity Reporting Module network. The second server will be a failover (inactive) management server. The management server stores predefined and user-defined content and configurations. The management server also authenticates users and authorizes feature access.</p> <p><b>Collection Server:</b> Collection server will be responsible to collect and normalize the log events sent by respective UARM agents. Agent is responsible to failover to respective collector servers in case one of collector servers is not available.</p>

Characteristic	Description
<b>High Availability</b>	<p>The CAR architecture maintains two (2) Collector Servers and one (1) Reporting Server. The Collector Servers are the main actors that collect the data events and are designed to have an instant failover. The agents for the collectors would failover to the appropriate collector, which will reduce the likelihood of data loss in transit.</p> <p>The reporting servers are designed with a hot and cold instance. Since the reporting server is not responsible for any data collection, the hot and cold instance addresses HA requirements in that the collector server will be switched to the cold instance in case of a failure.</p>

CAR does not utilize any programming languages. For the DataPower logs coming from SAC, regular expression (REGEX) parsing is used.

#### **6.2.2.2. System Features**

N/A

#### **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**

N/A

<b>6.2.2.3.9.</b>	<b>Options</b>
N/A	
<b>6.2.2.3.10.</b>	<b>Protocols</b>
N/A	
<b>6.2.2.3.11.</b>	<b>Remote Procedure Call (RPC)</b>
N/A	
<b>6.2.2.3.12.</b>	<b>Constants Defined in Interface</b>
N/A	
<b>6.2.2.3.13.</b>	<b>Variables Defined in Interface</b>
N/A	
<b>6.2.2.3.14.</b>	<b>Types Defined in Interface</b>
N/A	
<b>6.2.2.3.15.</b>	<b>GUI</b>
N/A	
<b>6.2.2.3.16.</b>	<b>GUI Classes</b>
N/A	
<b>6.2.2.3.17.</b>	<b>Current Form</b>
Refer to the <a href="#">AcS Help Desk Training for CAR.</a>	
<b>6.2.2.3.18.</b>	<b>Modified Form</b>
N/A	
<b>6.2.2.3.19.</b>	<b>Components on Form</b>
N/A	
<b>6.2.2.3.20.</b>	<b>Events</b>
N/A	
<b>6.2.2.3.21.</b>	<b>Methods</b>
N/A	
<b>6.2.2.3.22.</b>	<b>Special References</b>
N/A	
<b>6.2.2.3.23.</b>	<b>Class Events</b>
N/A	
<b>6.2.2.3.24.</b>	<b>Class Methods</b>
N/A	

<b>6.2.2.3.25.</b>	<b>Class Properties</b>
N/A	
<b>6.2.2.3.26.</b>	<b>Uses Clause</b>
N/A	
<b>6.2.2.3.27.</b>	<b>Forms</b>
N/A	
<b>6.2.2.3.28.</b>	<b>Functions</b>
N/A	
<b>6.2.2.3.29.</b>	<b>Dialog</b>
N/A	
<b>6.2.2.3.30.</b>	<b>Help Frame</b>
N/A	
<b>6.2.2.3.31.</b>	<b>HL7 Application Parameter</b>
N/A	
<b>6.2.2.3.32.</b>	<b>HL7 Logical Link</b>
N/A	
<b>6.2.2.3.33.</b>	<b>COTS Interface</b>
N/A	

## **6.3. Network Detailed Design**

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

## **6.4. Service Oriented Architecture/ESS Detailed Design**

N/A

### **6.4.1. Service Description for CAR**

N/A

### **6.4.2. Service Design for CAR**

N/A

#### **6.4.2.1. Introduction**

##### **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**

##### **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**

###### **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



<b>6.4.2.4.1.2.</b>	<b>Service Interface Type</b>
N/A	
<b>6.4.2.4.1.3.</b>	<b>Service Name</b>
N/A	
<b>6.4.2.4.1.4.</b>	<b>Interface</b>
N/A	
<b>6.4.2.4.1.5.</b>	<b>End Points</b>
N/A	
<b>6.4.2.4.1.6.</b>	<b>Operations or Methods</b>
N/A	
<b>6.4.2.4.1.7.</b>	<b>Message Schemas</b>
N/A	
<b>6.4.2.4.2.</b>	<b>Information Model</b>
N/A	
<b>6.4.2.4.2.1.</b>	<b>Class Diagram and Description of Entities Involved</b>
N/A	
<b>6.4.2.4.2.2.</b>	<b>Mappings from ELDM to Standards Based Schemas</b>
N/A	
<b>6.4.2.4.3.</b>	<b>Behavior Model (AKA Use Case Realization)</b>
N/A	
<b>6.4.2.4.3.1.</b>	<b>Use Cases (Use Case Model)</b>
N/A	
<b>6.4.2.4.3.2.</b>	<b>Interaction Diagrams</b>
N/A	
<b>6.4.2.5.</b>	<b>Gap Analysis</b>
N/A	
<b>6.4.2.5.1.</b>	<b>Variances from Enterprise Target Architecture</b>
N/A	
<b>6.4.2.5.2.</b>	<b>Variances from SLDs</b>
N/A	
<b>6.4.2.5.3.</b>	<b>Variances from Standards and Policies</b>
N/A	

#### **6.4.2.5.4.**

#### **Justification for Exceptions and Mitigation**

N/A

## 7. External System Interface Design

The CAR Service does not interface with any external systems.  
Interfacing mechanisms for CAR are encompassed within agent architecture.

Please refer to the specific ICD for additional details.

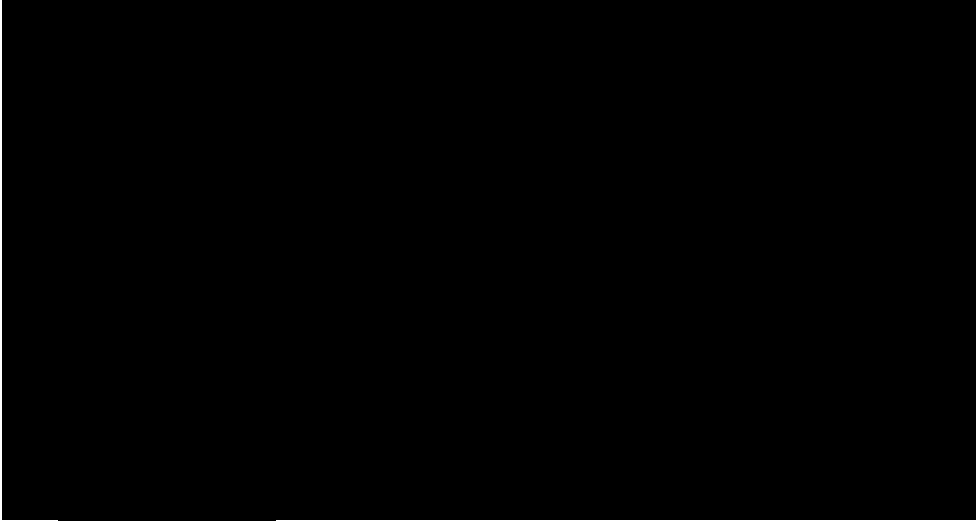
### 7.1. Interface Architecture

The CAR Service does not interface with any external systems.

The table below lists all the server names where a CAR agent is installed along with the names of the connectors configured on those agents and the applications that they connect to.

**Table 24: Car Server**

CAR Agent Server	Agent Connector Names	Integrated Application
		CSP, IP, VDS
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe
		SSOe

CAR Agent Server	Agent Connector Names	Integrated Application
		SSOe
		SailPoint
		SiteMinder
		ESig, ESR
		Provisioning
		SSOi
		SSOi
		SAC
		SAC

## 7.2. Interface Detailed Design

Refer to the ICDs for each integration for additional details.

## 8. Human-Machine Interface

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

- CAR Users: The web interface used by the CAR Users to run standard reports.
- CAR Privileged: The web interfaces used by the administrators to manage CAR Users and generate, view, and schedule ad hoc reports and manage alerts.
- CSP Privileged: The web interfaces used by the CSP Privileged User to manage CSP reports.
- IP Privileged: The web interfaces used by the IP Privileged User to manage IP reports.
- SAC Privileged: The web interfaces used by the SAC Privileged User to manage SAC reports.
- CAR ISSO: The web interfaces used by the VA ISSO for auditing purposes.
- Super User: CAR Super User to create and manage Privileged Users.

### 8.1. Interface Design Rules

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

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

### 8.2. Inputs

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

Refer to section 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 CAR:

- PDF
- Comma Separated File (CSF)
- Excel

## 8.4. Navigation Hierarchy

CAR is based on a COTS product and does not use custom interfaces.

### 8.4.1. Screen Shots

Please reference the [AcS Help Desk Training for CAR](#) to review all navigational screenshots.

## 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.

### 9.1. Security

#### 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 25: Data Points and Security**

Data Points	Data Type	Explanation
Oracle	Sensitive	<ul style="list-style-type: none"><li>• Stores the IdentityMinder objects- sensitive user attributes.</li><li>• Stores the audit log for SiteMinder and needs to be secured, but not encrypted, as there is no PII.</li><li>• Stores the audit log for CA IDM and must be encrypted and secured for PII.</li><li>• See vendor documentation for additional information regarding actual encryption algorithms used.</li></ul>

Data Points	Data Type	Explanation
Directory	Sensitive	<ul style="list-style-type: none"> <li>Stores encrypted SiteMinder policy data.</li> <li>Stores SiteMinder/IdentityMinder user data. Only sensitive user attributes will be encrypted.</li> <li>Provisioning server related objects and sensitive user attributes are encrypted.</li> <li>See vendor documentation for additional information regarding actual encryption algorithms used.</li> </ul>
File Store	Non-Sensitive/ Sensitive	<ul style="list-style-type: none"> <li>IM is stored in a JMS data in file system and contains transactional data. It does not contain any sensitive information.</li> <li>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.</li> </ul>
VDS	Sensitive	<ul style="list-style-type: none"> <li>Stores PII data and other user data in clear text. VDS will store PII data in the format that the source system transmits. Both Provisioning and MVI will have to encrypt/one-way hash the data and VAAFI will have to decrypt the data upon receipt.</li> <li>Vendor does not support encryption/de-encryption of data.</li> </ul>

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 and who can make updates accordingly.

**Table 26: Data Type and Updates**

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

## **9.2. Privacy**

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.

### **9.2.1. CAR**

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

### **9.2.2. Confidentiality of Sensitive Information**

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

### **9.2.3. Privacy of Personal Information**

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

### **9.2.4. Process Integrity**

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



## Attachment A – Approval Signatures

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

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

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 RSD and Rational Tool Composer for the AcS 2.0 RTM.

### **A.2. Packaging and Installation**

N/A

### **A.3. Design Metrics**

N/A

### **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.

---