

**Identity and Access Management
Access Services 2.0 Increment 5
Specialized Access Control (SAC)
System Design Document**



Department of Veterans Affairs

March 2015

Version 1.2

Revision History

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

| Date | Version | Description | Author |
|------------|---------|---|------------|
| 04/17/2015 | 1.1 | Updated per anomalies | [REDACTED] |
| 03/24/2015 | 1.0 | Updated to new template; added additional language and diagrams for SAC | [REDACTED] |

Artifact Rationale

The System Design Document (SDD) is a dual-use document that provides the conceptual design as well as the as-built design. This document will be updated as the product is built, to reflect the as-built product. Per the Project Management Accountability System (PMAS) Guide, the SDD with conceptual design is required prior to the Milestone 1 Review. The as-built for each delivery must be incorporated prior to the Milestone 2 Review.

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

Table of Contents

| | |
|--|-----------|
| 1. Introduction | 8 |
| 1.1. Purpose of the SDD | 8 |
| 1.2. Identification | 9 |
| 1.3. Scope | 9 |
| 1.3.1. Increment 5 SAC Scope | 9 |
| 1.4. Constraining Policies, Directives and Procedures | 9 |
| 1.4.1. Constraints | 9 |
| 1.4.2. Policies and Directives | 9 |
| 1.5. User Characteristics | 12 |
| 1.5.1. User Problem Statement | 12 |
| 1.6. Relationship to Other Documents and Plans | 12 |
| 1.7. Definitions, Acronyms, and Abbreviations | 13 |
| 1.8. References | 13 |
| 2. Background | 13 |
| 2.1. Overview of the System | 13 |
| 2.2. Overview of the Business Process | 14 |
| 2.3. Business Benefits | 16 |
| 2.4. Assumptions and Constraints | 16 |
| 2.4.1. Design Assumptions | 16 |
| 2.4.2. Design Constraints | 16 |
| 2.4.3. Design Trade-offs | 17 |
| 2.5. Overview of the Significant Requirements | 17 |
| 2.5.1. Overview of Significant Functional Requirements | 17 |
| 2.5.2. Overview of Functional Workload/Performance Requirements | 17 |
| 2.5.3. Overview of Operational Requirements | 18 |
| 2.5.4. Overview of the Technical Requirements | 19 |
| 2.5.5. Overview of the Security or Privacy Requirements | 27 |
| 2.5.6. Overview of System Criticality and High Availability Requirements | 27 |
| 2.5.7. Single Sign-on Requirement | 28 |
| 2.5.8. Requirement for Use of Enterprise Portals | 28 |
| 2.5.9. Special Device Requirements | 28 |
| 2.6. Legacy System Retirement | 28 |
| 3. Conceptual Design | 28 |
| 3.1. Conceptual Application Design | 28 |
| 3.1.1. Application Context | 29 |
| 3.1.2. High-Level Application Design | 32 |
| 3.1.3. Application Locations | 34 |

| | |
|---|-----------|
| 3.2. Conceptual Data Design..... | 34 |
| 3.2.1. Project Conceptual Data Model | 34 |
| 3.2.2. Database Information | 36 |
| 3.2.3. User Interface Data Mapping | 36 |
| 3.2.3.1. Application Screen Interface | 36 |
| 3.2.3.2. Application Report Interface..... | 36 |
| 3.2.3.3. Unmapped Data Element..... | 36 |
| 3.3. Conceptual Infrastructure Design | 36 |
| 3.3.1. System Criticality and High Availability..... | 37 |
| 3.3.2. Special Technology | 38 |
| 3.3.3. Technology Locations..... | 38 |
| 3.3.4. Conceptual Infrastructure Diagram..... | 39 |
| 3.3.4.1. Location of Environments and External Interfaces | 39 |
| 3.3.4.2. Conceptual Production String Diagram | 41 |
| 4. System Architecture | 41 |
| 4.1. Hardware Architecture | 42 |
| 4.2. Software Architecture..... | 45 |
| 4.3. Network Architecture..... | 49 |
| 4.4. Service Oriented Architecture/ESS | 49 |
| 4.5. Enterprise Architecture | 49 |
| 5. Data Design | 50 |
| 5.1. DBMS Files | 50 |
| 5.2. Non-DBMS Files | 51 |
| 5.3. Data View | 51 |
| 6. Detailed Design | 51 |
| 6.1. Hardware Detailed Design..... | 51 |
| 6.2. Software Detailed Design..... | 51 |
| 6.2.1. SAC Design | 51 |
| 6.2.1.1. Product Perspective..... | 53 |
| 6.2.1.1.1. User Interfaces | 53 |
| 6.2.1.1.2. Hardware Interfaces | 53 |
| 6.2.1.1.3. Software Interfaces | 53 |
| 6.2.1.1.4. Communications Interfaces..... | 53 |
| 6.2.1.1.5. Memory Constraints..... | 54 |
| 6.2.1.1.6. Special Operations | 54 |
| 6.2.1.2. Product Features | 54 |
| 6.2.1.3. User Characteristics..... | 54 |
| 6.2.1.4. Dependencies and Constraints | 55 |
| 6.2.1.5. Security Policy Authoring | 56 |
| 6.2.1.6. Manage Access Control Policies..... | 58 |
| 6.2.1.7. Make Access Control Decisions..... | 59 |
| 6.2.1.8. Make Access Control Decisions..... | 60 |
| 6.2.2. Specific Requirements | 61 |

| | | |
|---------------|---|-----------|
| 6.2.2.1. | Database Repository | 61 |
| 6.2.2.2. | System Features..... | 61 |
| 6.2.2.3. | Design Element Tables..... | 61 |
| 6.2.2.3.1. | Routines (Entry Points)..... | 61 |
| 6.2.2.3.2. | Templates | 62 |
| 6.2.2.3.3. | Bulletins | 62 |
| 6.2.2.3.4. | Data Entries Affected by the Design..... | 62 |
| 6.2.2.3.5. | Unique Records | 62 |
| 6.2.2.3.6. | File or Global Size Changes..... | 62 |
| 6.2.2.3.7. | Mail Groups | 62 |
| 6.2.2.3.8. | Security Keys | 62 |
| 6.2.2.3.9. | Options | 62 |
| 6.2.2.3.10. | Protocols..... | 62 |
| 6.2.2.3.11. | Remote Procedure Call (RPC) | 62 |
| 6.2.2.3.12. | Constants Defined in Interface..... | 62 |
| 6.2.2.3.13. | Variables Defined in Interface | 62 |
| 6.2.2.3.14. | Types Defined in Interface..... | 62 |
| 6.2.2.3.15. | GUI | 62 |
| 6.2.2.3.16. | GUI Classes..... | 62 |
| 6.2.2.3.17. | Current Form..... | 62 |
| 6.2.2.3.18. | Modified Form | 63 |
| 6.2.2.3.19. | Components on Form..... | 63 |
| 6.2.2.3.20. | Events..... | 63 |
| 6.2.2.3.21. | Methods..... | 63 |
| 6.2.2.3.22. | Special References | 63 |
| 6.2.2.3.23. | Class Events | 63 |
| 6.2.2.3.24. | Class Methods | 63 |
| 6.2.2.3.25. | Class Properties..... | 63 |
| 6.2.2.3.26. | Uses Clause | 63 |
| 6.2.2.3.27. | Forms | 63 |
| 6.2.2.3.28. | Functions..... | 63 |
| 6.2.2.3.29. | Dialog..... | 63 |
| 6.2.2.3.30. | Help Frame..... | 63 |
| 6.2.2.3.31. | HL7 Application Parameter | 63 |
| 6.2.2.3.32. | HL7 Logical Link..... | 63 |
| 6.2.2.3.33. | COTS Interface | 63 |
| 6.3. | Network Detailed Design | 64 |
| 6.4. | Service Oriented Architecture/ESS Detailed Design | 64 |
| 6.4.1. | Service Description | 64 |
| 6.4.2. | Service Design | 64 |
| 6.4.2.1. | Introduction..... | 64 |
| 6.4.2.1.1. | Purpose and Scope of Service | 64 |
| 6.4.2.1.2. | Links to Other Documents | 64 |
| 6.4.2.2. | Service Details..... | 64 |
| 6.4.2.2.1. | Service Identification | 64 |
| 6.4.2.2.2. | Service Versions | 64 |
| 6.4.2.2.3. | Summary of Design and Platform Details | 64 |
| 6.4.2.2.3.1. | SOA Pattern(s) Implemented | 64 |
| 6.4.2.2.3.2. | COTS Platform vendor names and versions for hosting platform..... | 64 |

| | | |
|---|---|-----------|
| 6.4.2.3. | Dependencies..... | 64 |
| 6.4.2.4. | Service Design Details..... | 64 |
| 6.4.2.4.1. | Interface Technical Specs | 64 |
| 6.4.2.4.1.1. | Service Invocation Type | 65 |
| 6.4.2.4.1.2. | Service Interface Type | 65 |
| 6.4.2.4.1.3. | Service Name | 65 |
| 6.4.2.4.1.4. | Interface | 65 |
| 6.4.2.4.1.5. | End Points | 65 |
| 6.4.2.4.1.6. | Operations or Methods..... | 65 |
| 6.4.2.4.1.7. | Message Schemas | 65 |
| 6.4.2.4.2. | Information Model | 65 |
| 6.4.2.4.2.1. | Class Diagram and Description of Entities Involved..... | 65 |
| 6.4.2.4.2.2. | Mappings from ELDM to Standards Based Schemas..... | 65 |
| 6.4.2.4.3. | Behavior Model (AKA Use Case Realization) | 65 |
| 6.4.2.4.3.1. | Use Cases (Use Case Model) | 65 |
| 6.4.2.4.3.2. | Interaction Diagrams | 65 |
| 6.4.2.5. | Gap Analysis | 65 |
| 6.4.2.5.1. | Variances from Enterprise Target Architecture | 65 |
| 6.4.2.5.2. | Variances from SLDs..... | 65 |
| 6.4.2.5.3. | Variances from Standards and Policies..... | 66 |
| 6.4.2.5.4. | Justification for Exceptions and Mitigation | 66 |
| 7. | External System Interface Design..... | 66 |
| 7.1. | Interface Architecture..... | 66 |
| 7.2. | Interface Detailed Design | 66 |
| 8. | Human-Machine Interface | 66 |
| 8.1. | Interface Design Rules | 66 |
| 8.2. | Inputs | 66 |
| 8.3. | Outputs | 66 |
| 8.4. | Navigation Hierarchy..... | 67 |
| 8.4.1. | Screen Shots..... | 67 |
| 8.4.1.1. | Application Screen Interface | 67 |
| 8.4.1.1.1. | PAP Authoring Page | 67 |
| 9. | Security and Privacy..... | 68 |
| 9.1. | Security..... | 68 |
| 9.2. | Privacy | 69 |
| 9.2.1. | Confidentiality of Sensitive Information | 69 |
| 9.3. | SAC | 69 |
| 9.3.1. | Confidentiality of Sensitive Information | 69 |
| 9.3.2. | Privacy of Personal Information..... | 69 |
| 9.3.3. | Process Integrity..... | 70 |
| 9.3.4. | System Availability | 70 |
| Attachment A – Approval Signatures | | 71 |
| A.1. | RTM..... | 72 |

| | |
|--|-----------|
| A.2. Packaging and Installation..... | 72 |
| A.3. Design Metrics | 72 |
| A.4. Acronym List and Glossary | 72 |
| A.5. Required Technical Documents | 72 |
| A.6. Attach Documents | 72 |

DRAFT

1. Introduction

The SAC Activity is designed to provide an enterprise-wide capability for enforcing dynamic fine-grained attribute based access control (ABAC). Software applications in need for such access control behavior can benefit by consuming this standards based enterprise solution as opposed to natively implementing one.

Specialized Access Control (SAC) is an element of an IAM Authorization service that provides the ability to receive requests for access to VA systems, and return a decision to permit or deny access based on evaluation of attributes applicable to each request. In this context, “attributes” might include, for example, patient preferences, provider roles, organizational responsibilities, geographies, etc. SAC provides a granular policy-based access decision service to future applications capable of consuming them.

1.1. Purpose of the SDD

The purpose of the System Design Document (SDD) is to describe the supporting mechanics of the SAC architecture. 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 SAC 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 SAC solution as well as details for understanding the specific system configurations, interfaces, workflow, Graphical User Interfaces (GUI), and data models.

This document also describes the SAC design and implementation and is the technical response to realize the business requirements put forth by the Identity and Access Management (IAM) Business Program Management Office (BPMO) in the [BRD](#) and the [Access Services increment 5.0 Requirements Specification Document \(RSD\)](#). This document is restricted to the current requirements and the approach to provide access functionality to stakeholders and users

including Veterans, Active Duty Members, Business Partners, and Service Providers. This SDD identifies the capabilities included in the AcS Increment 5 release delivery.

1.2. Identification

The information contained herein applies to SAC, a dynamic fine grained attribute based access control service. SAC is based off a COTS product, and is a part of the overarching IAM AcS Solution (version 2.5.0). The key underlying standard leveraged by SAC is OASIS XACML 3.0.

1.3. Scope

This section establishes boundaries of the IAM AcS SAC (version 1.0) SDD. The table below lists the governing business needs and features for SAC.

Table 1: SAC Scope Inclusions

| Includes |
|--|
| Provides a Policy Decision Point (PDP) and Policy Administration Point (PAP) according to the OASIS eXtensible Access Control Markup Language (XACML) 3.0 standard |
| Provides available Software Development Kits (SDKs) for VA applications to perform Policy Enforcement Point (PEP) capabilities |

Table 2: Scope Exclusion

| Excludes |
|---|
| SAC does not provide a virtual directory such as the Policy Information Point (PIP) |

1.3.1. Increment 5 SAC Scope

There are no SAC requirements for AcS 2.0 increment 5.

1.4. Constraining Policies, Directives and Procedures

1.4.1. Constraints

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

IAM AcS SAC shall enforce privacy and security policies that best serve interest of Veterans and the VA, under purview of application owners, IAM BPMP, IT Security Program managers and VA Privacy and Security group. The system shall comply and follow OASIS XACML 3.0 for standardization, interoperability and computability.

1.4.2. Policies and Directives

This design complies with the following policies, directives, and procedures (as applicable).

Table 3: Applicable Policies, Directives, and Procedures

| # | Issuing Agency | Policy, Directive, or Procedure | Purpose |
|---|----------------|---------------------------------|---|
| 1 | VA | VA 6500 Handbook | <ul style="list-style-type: none"> • Directive Information Security Program. • Defining overall Security Framework for VA. |
| 2 | VA | VA 6501 Directive | <ul style="list-style-type: none"> • VA Identity Verification In-Person Proofing (IPP) Process. • Defining overall Identity Proofing Methodology for VA IAM. |
| 3 | VA | VA 6300 Directive | <ul style="list-style-type: none"> • Directive Records and Information Management. • Defines information management framework for VA Access Services. |
| 4 | NIST | SP 800-53-4 | <ul style="list-style-type: none"> • Special Publication – Recommended Security Controls for Federal Information Systems and Organizations. • Defines the required security controls for IT systems under the Federal Information Security Management Act (FISMA). |
| 5 | NIST | SP 800-63-2 | <ul style="list-style-type: none"> • Special Publication – Electronic Authentication Guideline. • Defines levels of assurance in user identities presented to IT systems over open networks. • Defines the data and procedural requirements for VA Access Services. |
| 6 | NIST | FIPS-201-2 | <ul style="list-style-type: none"> • Federal Information Processing Standards Publication – PIV of Federal Employees and Contractors. • Provides Identity Proofing, credentialing and chain of trust requirements and processes. • Defines the method for secure administrative interaction and control. |
| 7 | NIST | FIPS-140-2 | <ul style="list-style-type: none"> • Federal Information Processing Standards Publication (FIPS) – Security Requirements for Cryptographic Modules. • Defines the cryptographic standards and requirements. |
| 8 | NIST | SP 800-122 | <ul style="list-style-type: none"> • Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). • Provides technical procedures for protecting PII in information systems. • Defines the information which can be used to distinguish or trace an individual's identity. |

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

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

1.5. User Characteristics

1.5.1. The SAC service is not consumed by an end user, but rather by other applications requiring access control. User Problem Statement

This section is not applicable as SAC is a middleware component to provide authorization decisions to external policy enforcement points.

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

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 applications. Authorization capabilities provide coarse and fine-grained application access, while providing workflow for self-service account requests, approvals, and user life cycle management.

Many VA applications follow the Role Based Access Control (RBAC) paradigm where roles are created to encapsulate entitlements and are then associated statically with users to facilitate access control. Frequently applications are in need of a more dynamic approach where Privacy and Security policies are enforced at runtime based on granular fine grained user, resource, transaction and environmental authorization attributes, as opposed to statically established roles and entitlements. Additionally, such access control logic is native to most applications at the VA. The SAC Policy Decision Point (PDP) Service is designed to provide an enterprise-wide capability for enforcing dynamic fine grained attribute based access control (ABAC). Software applications in need for such access control behavior can benefit by consuming this standards based enterprise service as opposed to natively implementing one.

The SAC function within the IAM program will provide an enterprise authorization service that enables a centralized policy decision engine to support access control decisions based on real-time evaluation of user attributes, resources, context and environmental constraints.

2.1. Overview of the System

At its core SAC maintains a decision engine, the policy decision point (PDP), that generates authorization decisions under the governance of organizational policies, patient specified policies and authorization attributes such as subject's identity, environment, transaction and resource attributes. Below is high level overview of the System:

- Policy Decision Point (PDP): PDP is an eXtensible Access Control Markup Language (XACML) 3.0 policy evaluation engine that receives authorization decision requests from the consuming application Policy Enforcement Points (PEPs). The PDP evaluates these requests against Organizational, patient policies/attributes and other authorization attributes and renders an authorization decision
- Policy Administration Point (PAP): The PAP facilitates the creation of organizational policies and policy sets and registers them in policy stores with the intent of making them available to the PDP

- Patient Policies/Attributes: SAC does not yet offer a mechanism for capturing patient policies/attributes. For the eHealth Policy enforcement scenario, PDP receives patient preference information from an external VLER system called VAP.
- Authorization Attributes: These could be passed in by the consuming application PEP and/or integrated into a Policy Information Point (PIP) that the PDP can access. Various types of Authorization attributes are:
 - User or subject attributes: identity or access attributes associated with the user.
 - Resource Attributes: attributes inherent in the data itself such as Confidentiality or Sensitivity indicators for Sickle Cell Anemia in clinical data
 - Transaction Attributes: that reflect entitlements for the business transaction requiring protection
 - Contextual constraints: attributes inherent in the environment, like location, time, day of week, etc.

SAC events are captured for auditing and reporting purposes through the integration with Compliance Audit and Reporting (CAR) service.

2.2. Overview of the Business Process

The capability to manage access to systems, applications, and data based on resource, subject, and environmental attributes across the VA and VA constituents via a common Enterprise Policy, will directly and indirectly impact a veteran's experience. This capability will aid in the reduction of enforcement points, cumbersome and inconsistent access controls, and provide the foundation for on-demand access to benefit services based on need.

Historically, the VA has relied on local security procedures to control and provide access to facilities, resources, and information. Access is provided to users through multiple and varying manual or self-service registrations that require approving authorities and system administrators to control access to computer systems, networks, and information these systems provide. In addition to the manpower burdens, the registration process has been found to have inherent weaknesses and can be susceptible to exploitation. New and existing systems will be required to evolve their current identification, authentication, authorization, and audit capabilities to support both anticipated and unanticipated VA application stakeholders¹. As the VA continues to realize the importance of information sharing and protection to the successful delivery of Veteran benefits and enterprise security, it is critical that VA enhance its access control mechanisms to achieve the fine-grained control levels necessary to protect valuable information assets.

The business benefits of the SAC service will be:

- Accommodate diverse user populations (e.g., veterans, beneficiaries, and providers).
- Putting policy management into the hands of the business, rather than application developers.
- Authorize unanticipated user with legitimate need for application access, in real-time, without the overhead of lengthy and costly workflow and provisioning processes.

¹ An unanticipated user is a user that does not have an account in the resource identity store and has not pre-registered for access to the resource. They may be trusted based on verified attributes or organizational affiliation.

- Reduce the cost of change management as business rules change by reducing or eliminating hard-coded application logic. When a policy changes, it does not require the SDLC typical in today applications.
- Enable access for unanticipated users with no pre-registration required based on user attributes (e.g. citizenship, organizational affiliations, operational roles, privacy needs, environmental conditions, training, and security clearances).
- Share information with a broad set of users employing a diverse and complex set of access control restrictions that require fine-grained digital policies.

Ultimately, the primary relevance of SAC is in its ability to ensure that accurate and trusted information is shared and available where it is needed, when it is needed, and to those who needs it most.

SAC enables the provision of policy-based access control decision support to a core capability, the Policy Decision Point (PDP). The benefits of the Service are discussed in Section 2.3.

The critical components of an actual policy decision support capability, the attributes themselves, are not retrieved from their authoritative sources when requested, but instead are hard-coded into the test cases. In the full SAC Service, these attributes would be retrieved upon request of the PDP, based on the request from the originating applications, including client preferences (opt-in/opt-out consent) and other future applications.

Table 4: Business Process

| Business Process ID | Business Process Name | Type | Owner | Description |
|---------------------|--|----------------------------------|--------|---------------------------------|
| 1 | VA IAM SAC Use Case Model | SAC Use Cases and Use Case Model | PD OIT | Use Cases to support SAC System |
| 2 | VA 2.0 Increment 2 Use Case Model Document | Use Cases | PD OIT | Use Case Model Document |
| 3 | VA i4 Use Case Model | Use Cases | PD OIT | I4 Use cases |
| 4 | SAC Enforce Access Control | Use Case | PD OIT | Enforce Access Use Case |
| 5 | SAC Generate Access Control | Use Case | PD OIT | Generate Access Use Case |
| 6 | SAC Manage Access Control | Use Case | PD OIT | Manage Access Use Case |
| 7 | SAC Obtain Attributes | Use Case | PD OIT | Obtain Attributes Use Case |

2.3. Business Benefits

The SAC Service allows an application to request an authorization decision based on the real-time attributes of a person requesting the access. This policy-based access control decision process allows the application and data owners to offload the details of the information flows, identity management, and access control logic that would otherwise have to be implemented within the applications, thus an application can benefit by consuming this standards based enterprise solution as opposed to natively implementing one. In addition to simplifying the applications themselves, the policy-based access control process reduces the need for duplicative identity stores that are hard to maintain and synchronize with “authoritative” sources over time.

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 content.*

2.4. Assumptions and Constraints

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

2.4.1. Design Assumptions

- SAC has a High System Baseline for Confidentiality, Integrity, and Availability.
- The XACML 3.0 standard has been released 22 Jan 2013. All new consumers should be following the XACML 3.0 standards.
- Protected applications provide authorization of users for content appropriate for the users’ credential assurance level based on NIST SP 800-63 and OMB M04-04.
- SAC should be able to serve as a ubiquitous, enterprise-wide solution for dynamic fine grained access control based on Organizational and Patient specified Privacy and Security Policies and additional authorization attributes from a variety of sources
- SAC should be able to offer stewardship of Organizational policies that reflect Organizational and Legal Privacy and Security priorities for all Lines of Business
- The Organizational policies stored in SAC should be standards based for interoperability and computability

2.4.2. Design Constraints

- Organizational Policies stored in SAC are to be authored per the XACML 3.0 specification
- Consuming application PEPs are required to transact with SAC using HTTPS/SOAP/XACML 3.0 messaging
- Consuming application PEPs are required to support TLS based mutual authentication with the IAM Data Power XML Gateway, the reverse proxy to SAC services
- Consuming application PEPs are required to enforce Authorization Decisions returned by SAC PDP

2.4.3. Design Trade-offs

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

- SAC does not offer a Policy Enforcement Point (PEP) service. Offering a PEP would enable SAC to intercept resource access requests and render access control. Currently SAC requires integrated applications to deploy their own XACML 3.0 aware PEP which would explicitly reach out to the SAC PDP to obtain an authorization decision, prior to carrying out its business transaction.
- Since the SAC administrative UI does not support direct PIV authentication, an alternative is that the administration console links may be provided in the CA Single Sign-On system and rely on the Desktop PIV login. However, a username and password will still be required for the administration consoles.

2.5. Overview of the Significant Requirements

This section provides an overview of the requirements that are within the scope for SAC increment 5.

2.5.1. Overview of Significant Functional Requirements

Table 5: Functional Requirements

| ID | Requirement |
|-----|--|
| N/A | Per the Business Requirements, SAC shall establish an XACML-conformant Policy Decision Point (PDP) to return access control decisions based on evaluation of supplied attributes against a defined Master Policy |

2.5.2. Overview of Functional Workload/Performance Requirements

This section provides a list of functional workload and performance requirements within the scope of SAC increment 5.

- There are no i5 Requirements to support SAC.

User Profile: Users of an External System that checks SAC to determine whether a Veteran has given permission to see their health information

- The target end state for the SAC service should support 325,000 transactions per day.
- The SAC service for this increment shall support the following:

Table 6: Workload and Performance Requirements

| | |
|---|------------------|
| Operation | |
| Name | SAC |
| Usage Profile (Webservice Calls) | |
| Mean Daily volume | 200 |
| Projected Growth | 200/year |
| Peak Daily volume | 300 |
| Projected Growth | 300/year |
| Peak Hourly volume | 25 |
| Days of operation | Sunday-Saturday |
| Hours of operation | 24/7 |
| Peak Hours | 9am-7p.m.Eastern |
| Maximum Response Time | 5 seconds |

2.5.3. Overview of Operational Requirements

The Operational Requirements or Reliability Specifications listed in Section 2.11 of the [AcS 2.0 Version 1.6 RSD](#) include the following:

The AcS solution is hosted within the Terremark environment as required by VA which encompasses SAC. 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 7: 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. |

| *Standards adopted from specification created by Application Structure and Integration Services (ASIS) | |
|---|---|
| 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](#).

Table 8 specifies the operational requirements that drive this design for SAC.

Table 8: i5 SAC Operational Requirements

| ID | Requirement |
|-----------|--------------------|
| 1 | None |

2.5.4. Overview of the Technical Requirements

Table 9: Technical Requirements

| ID | Requirement |
|-----------|---|
| 1A | The SAC service shall provide the ability to manage approved Client Preference attributes. The SAC service shall provide the ability to make authorization decisions based on the following attribute categories. <ul style="list-style-type: none"> - Client Preference - Data Restriction - User Security - Contextual Constraints - Application Function |
| 1A.1 | The SAC service shall provide the ability for a SAC System Administrator to indicate (add) Client opt-in/opt-out and other Client data restriction preferences on behalf of a Client. SAC does not directly manage attributes. It provide the ability to make authorization decisions based on the attributes outlined in 1A |
| 1A.2 | The SAC service shall interface with other services/applications to allow a Client to indicate (add) their opt-in/opt-out and other Client data restriction preferences. |
| 1A.2a | The SAC service shall interface with other services/applications to allow a Client to indicate (add) their Client data restriction preferences for individuals. |
| 1A.3 | The SAC service shall save the opt-in/opt-out and other Client data restriction preferences entered by a SAC System Administrator or provided by the Client. |
| 1A.4 | The SAC service shall provide the ability for a SAC System Administrator to modify the opt-in/opt-out and other Client data restriction preferences entered by a SAC System Administrator or provided by the Client. |
| 1A.5 | The SAC service shall provide the ability for a SAC System Administrator to review the established Client data restriction preferences. |
| 1A.6 | The SAC service shall provide the ability for a SAC System Administrator to revoke (remove) the opt-in/opt-out and other Client data restriction preferences entered by a SAC System Administrator or provided by the Client without deleting the original record from the data store. |

| ID | Requirement |
|-------|---|
| 1B | The SAC service shall provide the ability to manage Data Restriction attributes. Authorization services typically do not directly manage attributes. If IAM does manage authoritative attributes (not yet identified), it will do so via Provisioning. SAC manages the lifecycle of authorization policies used to make decisions on resource operations by means of the subject, their attributes, and environmental context. The attribute types must be made available to the policy author. |
| 1B.1 | The SAC service shall provide the ability for a SAC System Administrator to enter (add) data restriction attributes. |
| 1B.2 | The SAC service shall save the data restriction attributes entered by a SAC System Administrator. |
| 1B.3 | The SAC service shall provide the ability for a SAC System Administrator to modify the data restriction attributes entered. |
| 1B.4 | The SAC service shall provide the ability for a SAC System Administrator to revoke (remove) the data restriction attributes entered without deleting the original record from the data store. |
| 1B.5 | The SAC service shall provide the ability for a SAC System Administrator to review the established data restrictions. |
| 1B.5a | The SAC service shall provide the ability for a SAC System Administrator to filter the established data restrictions by attributes. |
| 1C | The SAC service shall provide the ability to manage User Security Attributes. Authorization services typically do not directly manage attributes. If IAM does manage authoritative attributes (not yet identified), it will do so via Provisioning. SAC manages the lifecycle of authorization policies used to make decisions on resource operations by means of the subject, their attributes, and environmental context. The attribute types must be made available to the policy author. |
| 1C.1 | The SAC service shall provide the ability for a SAC System Administrator to enter (add) User Security Attributes. |
| 1C.1a | The SAC service shall provide the ability for a SAC System Administrator to assign a User Security Attribute value to data. |
| 1C.1b | The SAC service shall provide the ability for a SAC System Administrator to assign a User Security Attribute value to Users. |
| 1C.2 | The SAC service shall save the User Security attributes entered by a SAC System Administrator. |
| 1C.3 | The SAC service shall provide the ability for a SAC System Administrator to modify the User Security attributes entered. |
| 1C.4 | The SAC service shall provide the ability for a SAC System Administrator to revoke (remove) the User Security attributes entered without deleting the original record from the data store. |
| 1C.5 | The SAC service shall provide the ability for a SAC System Administrator to review the established User Security restrictions. |
| 1C.5a | The SAC service shall provide the ability for a SAC System Administrator to filter the established User Security restrictions by attributes. |
| 1D | The SAC service shall provide the ability to manage Contextual Constraints. Authorization services typically do not directly manage attributes. If IAM does manage authoritative attributes (not yet identified), it will do so via Provisioning. SAC manages the lifecycle of authorization policies used to make decisions on resource operations by means of the subject, their attributes, and environmental context. The attribute types must be made available to the policy author. |
| 1D.1 | The SAC service shall provide the ability for a SAC System Administrator to enter (add) Contextual Constraints. |

| ID | Requirement |
|-------|---|
| 1D.2 | The SAC service shall save the Contextual Constraints entered by a SAC System Administrator. |
| 1D.3 | The SAC service shall provide the ability for a SAC System Administrator to modify the Contextual Constraints entered. |
| 1D.4 | The SAC service shall provide the ability for a SAC System Administrator to revoke (remove) the Contextual Constraints entered without deleting the original record from the data store. |
| 1D.5 | The SAC service shall provide the ability for a SAC System Administrator to review the established Contextual Constraint restrictions. |
| 1D.5a | The SAC service shall provide the ability for a SAC System Administrator to filter the established Contextual Constraint restrictions by attributes. |
| 1E | The SAC service shall provide the ability to manage Application Function attributes. Authorization services typically do not directly manage attributes. If IAM does manage authoritative attributes (not yet identified), it will do so via Provisioning. SAC manages the lifecycle of authorization policies used to make decisions on resource operations by means of the subject, their attributes, and environmental context. The attribute types must be made available to the policy author. |
| 1E.1 | The SAC service shall provide the ability for a SAC System Administrator to enter (add) Application Function attributes. |
| 1E.2 | The SAC service shall save the Application Function attributes entered by a SAC System Administrator. |
| 1E.3 | The SAC service shall provide the ability for a SAC System Administrator to modify the Application Function attributes entered. |
| 1E.3a | The SAC service shall provide the ability to specify scheduled periods of system un-availability. |
| 1E.3b | The SAC service shall provide the ability to specify ad-hoc (emergency) periods of system un-availability. |
| 1E.3c | The SAC service shall provide the application function attributes after modifications have been verified. |
| 1E.4 | The SAC service shall provide the ability for a SAC System Administrator to revoke (remove) the Application Function attributes entered without deleting the original record from the data store. |
| 1E.5 | The SAC service shall provide the ability for a SAC System Administrator to review the established Application Function restrictions. |
| 1E.5a | The SAC service shall provide the ability for a SAC System Administrator to filter the established Application Function restrictions by attributes. |
| 2A | The SAC service shall interface with Identity services as required to facilitate the SAC processes. |
| 2B | The SAC service shall interface with Authentication services as required by SAC processes. |
| 2C | The SAC service shall interface with the Provisioning service as required to facilitate the SAC processes. The SAC service shall interface with the Provisioning service to provision SAC Privileged Users to facilitate the SAC processes. |
| 2D | The SAC service shall interface with SSO services as required to facilitate the SAC processes. The SAC Service shall interface with SSOi Service as required to provide privileged user access to the policy management interface. |

| ID | Requirement |
|---------|--|
| 2E | The SAC service shall determine if content restrictions exist for each user session within a subscribing application. The SAC Service shall determine content restrictions based on available user attributes and pre-defined authorization policies. |
| 2E.1 | The SAC service shall have the ability to provide the user a 'Fail PERMIT' or 'Fail DENY' based on pre-defined authorization policy. |
| 2E.2 | If access restrictions exist, the SAC service shall prevent end-user access to the resource requested. |
| 2E.2a | The SAC service shall manage system and data access based on approved Client Preference attributes. |
| 2E.2a.1 | In the absence of Client Preferences, the SAC service shall allow end-user access to the resource requested. |
| 2E.2a.2 | If Client Preferences exist, the SAC service shall prevent end-user access to the resource requested based on the stored Client Preferences. |
| 2E.2b | The SAC service shall manage system and data access based on Data Restriction attributes. |
| 2E.2b.1 | In the absence of Data Restrictions, the SAC service shall allow end-user access to the resource requested. |
| 2E.2b.2 | If Data Restrictions exist, the SAC service shall prevent end-user access to the resource requested. |
| 2E.2c | The SAC service shall manage system and data access based on User Security Attributes. |
| 2E.2c.1 | In the absence of User Security Attributes, the SAC service shall allow end-user access to the resource requested. |
| 2E.2c.2 | If User Security Attributes exist, the SAC service shall prevent end-user access to the resource requested. |
| 2E.2d | The SAC service shall manage system and data access based on Contextual Constraints. |
| 2E.2d.1 | In the absence of Contextual Constraints, the SAC service shall allow end-user access to the resource requested. |
| 2E.2d.2 | If Contextual Constraints exist, the SAC service shall prevent end-user access to the resource requested. |
| 2E.2e | The SAC service shall manage system and data access based on Application Function attributes. |
| 2E.2e.1 | In the absence of Application Function attributes, the SAC service shall allow end-user access to the resource requested. |
| 2E.2e.2 | If Application Function attributes exist, the SAC service shall prevent end-user access to the resource requested. |
| 2K | The SAC service shall interface with legacy and other external applications as required to facilitate the SAC processes. |
| 2K.1 | The SAC service shall communicate the absence of access restrictions to legacy and external applications to allow end-user access to resources The SAC service shall communicate the access decision to permit/deny access to integrated legacy and external applications. If a policy is not found for the requesting application, the XACML standard specifies the response that must be levied. |
| 3A | The SAC Reporting feature shall allow the definition and scheduling of standard management reports. The SAC Reporting feature within Compliance and Audit Reporting (CAR) Service will provide the privileged user ability to define and schedule standard management. |

| ID | Requirement |
|------|--|
| 3A.1 | The SAC Reporting feature shall provide the ability to establish data parameters for the generation of standard management reports. The SAC Reporting feature within CAR Service shall provide the approved privileged users ability to establish data parameters for the generation of standard management reports. |
| 3A.2 | The SAC Reporting feature shall provide the ability to establish schedule (date) parameters for the generation of standard management reports. The SAC Reporting feature within CAR Service shall provide the ability to establish schedule (date) parameters for the generation of standard management reports. |
| 3B | The SAC Reporting feature shall allow the customization and generation of ad hoc and custom management reports. The SAC Reporting feature within CAR Service shall allow the privileged user ability to customize and generate ad hoc and custom management reports based on available data parameters. |
| 3B.1 | The SAC Reporting feature shall provide the ability to modify data parameters for the generation of custom/ad hoc management reports. The SAC Reporting feature within CAR Service shall provide the privileged user ability to modify available data parameters for the generation of custom/ad hoc management reports. |
| 3B.2 | The SAC Reporting feature shall provide the ability to modify schedule (date) parameters for the generation of custom/ad hoc management reports. The SAC Reporting feature within CAR Service shall provide the ability to modify schedule (date) parameters for the generation of custom/ad hoc management reports. |
| 3C | The SAC Reporting feature shall support the storage and output of reports in a variety of formats. The SAC Reporting feature within CAR Service shall support the storage and output of reports in a variety of formats. |
| 3C.1 | The SAC Reporting feature shall support the storage and output of reports in portable document format (PDF). The SAC Reporting feature within CAR Service shall support the storage and output of reports in portable document format (PDF). |
| 3C.2 | The SAC Reporting feature shall support the storage and output of reports in comma separated value (CSV) format. The SAC Reporting feature within CAR Service shall support the storage and output of reports in comma separated value (CSV) format. |
| 3C.3 | The SAC Reporting feature shall support the storage and output of reports in text (ASCII) format. The SAC Reporting feature within CAR Service shall support the storage and output of reports in Rich Text Format (RTF) format. |
| 4A | The SAC Reporting feature shall provide the ability to select and configure the collection parameters of the auditable events to be captured. The SAC Reporting feature within CAR Service shall provide the privileged user ability to select and configure the collection parameters of the auditable events to be captured. |
| 4A.1 | The SAC Reporting feature shall comply with the audit requirements applicable per the VA cross-cutting requirements as defined in the OI&T ERR. The SAC Reporting feature within CAR Service shall comply with the audit requirements applicable per the VA cross-cutting requirements as defined in the OI&T ERR. |
| 4A.2 | The SAC Reporting feature shall interface with the Compliance and Audit Reporting (CAR) service to accept the identified set of auditable events required. The SAC Reporting feature shall interface with the CAR Service to provide reporting attributes for identified set of auditable events required. |

| ID | Requirement |
|------|--|
| 4A.3 | The SAC Reporting feature shall provide a means to display the current set of auditable events to be stored. The SAC Reporting feature within CAR Service shall provide privileged users a means to display the current set of auditable events to be stored. |
| 4A.4 | The SAC Reporting feature shall provide a means for the user to add, delete, and modify the collection parameters of auditable events. The SAC Reporting feature within CAR Service shall provide privileged user means to add, delete, and modify the data parameters of auditable events. |
| 4A.5 | The SAC Reporting feature shall confirm to the user the successful addition, deletion, or modification of auditable events. The SAC Reporting feature within CAR Service shall confirm to the privileged user the successful addition, deletion, or modification of auditable events. |
| 4B | The SAC Reporting feature shall capture each event configured as auditable. The SAC Reporting feature within CAR Service shall capture each event configured as auditable. |
| 4B.1 | When a SAC event occurs, the SAC Reporting feature shall refer to the auditable event and configuration record to determine if the event should be captured. When a SAC event occurs, the SAC Reporting feature within CAR Service shall refer to the auditable event and configuration record to determine if the event should be captured. |
| 4B.2 | If the SAC Reporting feature determines the event should be captured, the event shall be stored in the SAC Reporting data store. If the SAC Reporting feature within CAR Service determines the event should be captured, the event shall be stored in the CAR Reporting data store. |
| 4C | The SAC Reporting feature shall interface with the CAR service to make available the audit event data collected and stored. The SAC Reporting feature shall interface with the CAR service to provide data parameters collected and stored within log files. |
| 5A | The SAC service shall provide a Policy Enforcement Point (PEP), Policy Decision Point (PDP), Attribute Service (AS), Policy Information Point (PIP), and Policy Administration Point (PAP) to make and enforce authorization decisions. |
| 5A.1 | The SAC service shall have the capability to request and retrieve access control policies and user attributes. |
| 5A.3 | The SAC service shall verify that the transaction is in an approved format, each mandatory field is provided, each field has a value that is within the approved schema for that transaction, and protections are intact. |
| 5A.4 | The SAC service shall have the capability to customize and apply additional workflow controls used to enforce constraints and obligations contained in the authorization decision. |
| 5A.5 | The SAC service shall use exceptions for emergency and temporary access authorization based on established policies. |
| 5B | The SAC service shall provide a policy enforcement point (PEP) to enforce access control decisions. |
| 5B.1 | The Policy Enforcement Point (PEP) shall have the capability to enforce access control decisions including any obligations contained in the access decision. |
| 5B.2 | The Policy Enforcement Point (PEP) shall have the capability to intercept access requests from an authenticated requestor of a requesting application. |
| 5B.3 | The Policy Enforcement Point (PEP) shall have the capability to forward access requests to the Policy Decision Point (PDP). |

| ID | Requirement |
|------|--|
| 5B.4 | The Policy Enforcement Point (PEP) shall have the capability to receive access control decisions from the Policy Decision Point (PDP). |
| 5B.5 | The Policy Enforcement Point (PEP) shall have the capability to enforce access control decisions. |
| 5C | The SAC service shall have a policy decision point (PDP) with the ability to make access control decisions. |
| 5C.1 | The Policy Decision Point (PDP) shall utilize user attributes and policies to determine authorization decisions. |
| 5C.2 | The Policy Decision Point (PDP) shall provide the following access decision responses: Permit, Deny, Indeterminate, or Not Applicable to the Policy Enforcement Point (PEP). |
| 5C.3 | The Policy Decision Point (PDP) shall have the capability to receive access control requests from the Policy Enforcement Point (PEP). |
| 5C.4 | The Policy Decision Point (PDP) shall have the capability to send access control decisions to the Policy Enforcement Point (PEP). |
| 5C.5 | The Policy Decision Point (PDP) shall have the capability to obtain user attributes from the Attribute Service (AS). |
| 5C.6 | The Policy Decision Point (PDP) shall have the capability to obtain decision attributes from a Policy Information Point (PIP). |
| 5C.7 | The Policy Decision Point (PDP) shall have the capability to obtain authorization policies from a Policy Store. |
| 5D | The SAC service shall provide a Policy Administration Point (PAP) that will be used by Privileged User to manage access control policies. |
| 5D.1 | The Policy Administration Point (PAP) shall utilize authoritative policy stores that serve as repositories for access control policies. |
| 5D.2 | The Policy Administration Point (PAP) shall allow Privileged User the capability to add/modify authorization policies. |
| 5E | The SAC service shall provide an Attribute Service (AS) that will obtain user attributes from an external Policy Information Point (PIP). |
| 5E.1 | The Attribute Service (AS) shall have access to approved and authoritative attribute stores/directories for users. |
| 5E.2 | The Attribute Service (AS) shall have ability to receive requests from the Policy Decision Point (PDP) for user attributes. |
| 5E.3 | The Attribute Service (AS) shall have ability to provide user attributes to the Policy Decision Point (PDP). |
| 5E.4 | The Attribute Service (AS) shall not make attributes available in response to improperly formed messages. |
| 5F | If there is a need to store attributes locally, the SAC service shall validate data is current by synchronizing local data automatically or periodically with the external authoritative source. |
| 5G | The SAC service shall have the ability to provide adequate information to Compliance, Audit & Reporting (CAR) service in order for CAR to create reports. |
| 5H | The SAC service shall satisfy security and privacy policies for passing information (requests, decisions, attributes). |
| 5H.1 | The SAC service shall perform the security checks necessary to verify that transactions have the requisite protections. |
| 5H.2 | The SAC service shall determine that the data-in-transit (DIT) and data-at-rest (DAR) are protected using appropriate mechanisms. |
| 5H.3 | The SAC service shall enforce separation of duties through business rules. |

| ID | Requirement |
|------|--|
| 5H.4 | The SAC service shall verify that the content of the transaction has not been subjected to modification by an unauthorized source. |
| 5H.5 | The SAC service shall provide a Policy Service (PS) that will obtain access control policies from external Policy Store. |
| 5C.6 | The Policy Decision Point (PDP) shall have the capability to obtain decision attributes from a Policy Information Point (PIP). |
| 5C.7 | The Policy Decision Point (PDP) shall have the capability to obtain authorization policies from a Policy Store. |
| 5D | The SAC service shall provide a Policy Administration Point (PAP) that will be used by Privileged User to manage access control policies. |
| 5D.1 | The Policy Administration Point (PAP) shall utilize authoritative policy stores that serve as repositories for access control policies. |
| 5D.2 | The Policy Administration Point (PAP) shall allow Privileged User the capability to add/modify authorization policies. |
| 5E | The SAC service shall provide an Attribute Service (AS) that will obtain user attributes from an external Policy Information Point (PIP). |
| 5E.1 | The Attribute Service (AS) shall have access to approved and authoritative attribute stores/directories for users. |
| 5E.2 | The Attribute Service (AS) shall have ability to receive requests from the Policy Decision Point (PDP) for user attributes. |
| 5E.3 | The Attribute Service (AS) shall have ability to provide user attributes to the Policy Decision Point (PDP). |
| 5E.4 | The Attribute Service (AS) shall not make attributes available in response to improperly formed messages. |
| 5F | If there is a need to store attributes locally, the SAC service shall validate data is current by synchronizing local data automatically or periodically with the external authoritative source. |
| 5G | The SAC service shall have the ability to provide acceptable information to Compliance, Audit & Reporting (CAR) service in order for CAR to create reports. |
| 5H | The SAC service shall satisfy security and privacy policies for passing information (requests, decisions, attributes). |
| 5H.1 | The SAC service shall perform the security checks necessary to verify that transactions have the requisite protections. |
| 5H.2 | The SAC service shall determine that the data-in-transit (DIT) and data-at-rest (DAR) are protected using appropriate mechanisms. |
| 5H.3 | The SAC service shall enforce separation of duties through business rules. |
| 5H.4 | The SAC service shall verify that the content of the transaction has not been subjected to modification by an unauthorized source. |

2.5.5. Overview of the Security or Privacy Requirements

The security specifications in Section 2.13 of the [AcS 2.0 Version 1.6 RSD](#) 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).

The SAC Specific Requirement is listed below:

Table 10: Security Requirements

| ID | Requirement |
|----|---|
| 1 | Encryption of transport between consuming application PEP and SAC PDP - Mutual Auth/TLS/FIPS 140-2 etc. |

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

External application users (“End Users”) will not have any direct interaction with SAC, so user interfaces are not required. SAC is primarily a machine-to-machine service within IAM.

End Users authenticate to an externally-managed application that establishes a machine-to-machine connection between the application’s PEP and the SAC service when a fine-grained access control decision is required therefore SSOi is not a supportable function for SAC.

2.5.8. Requirement for Use of Enterprise Portals

SAC is a system-to-system web service thus this section is not applicable.

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 SAC 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 SAC solution. There are no design updates within Increment 5 to support SAC. The overall AcS design is shown in Figure 1 below.

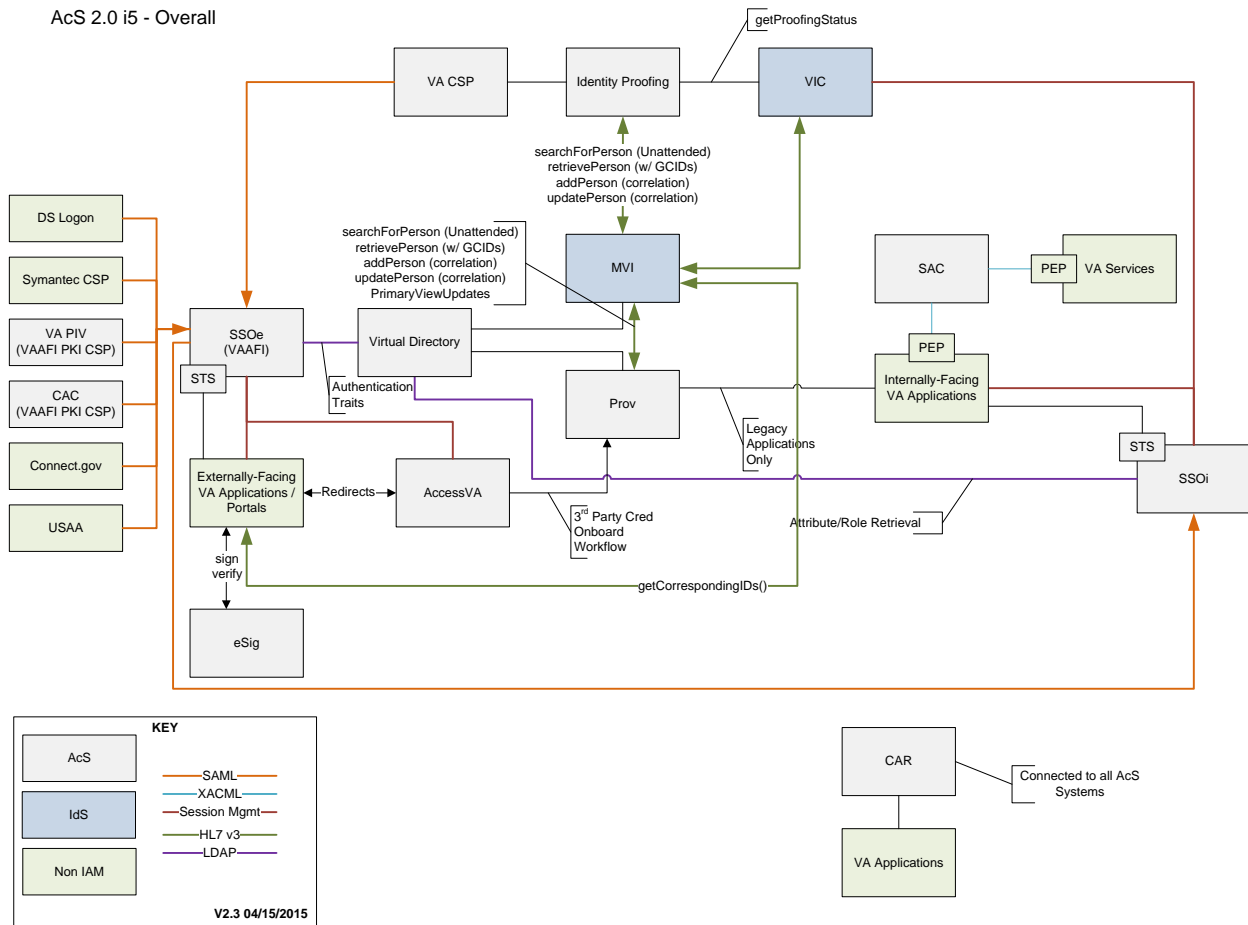


Figure 1: AcS 2.0 Overview

3.1.1. Application Context

SAC offers an enterprise level ABAC (Attribute Based Access Control) capability to generate fine grained access control decisions based on requestor, resource, transaction and environment authorization attributes, under the purview of Privacy and Security Policies.

SAC leverages OASIS eXtensible Access Control Markup Language 2.0 (XACML 2.0) standards for backwards compatibility. SAC uses XACML 3.0 standards for:

- Policy representation
- Messaging with consuming applications

The following figure is the application context diagram for SAC.

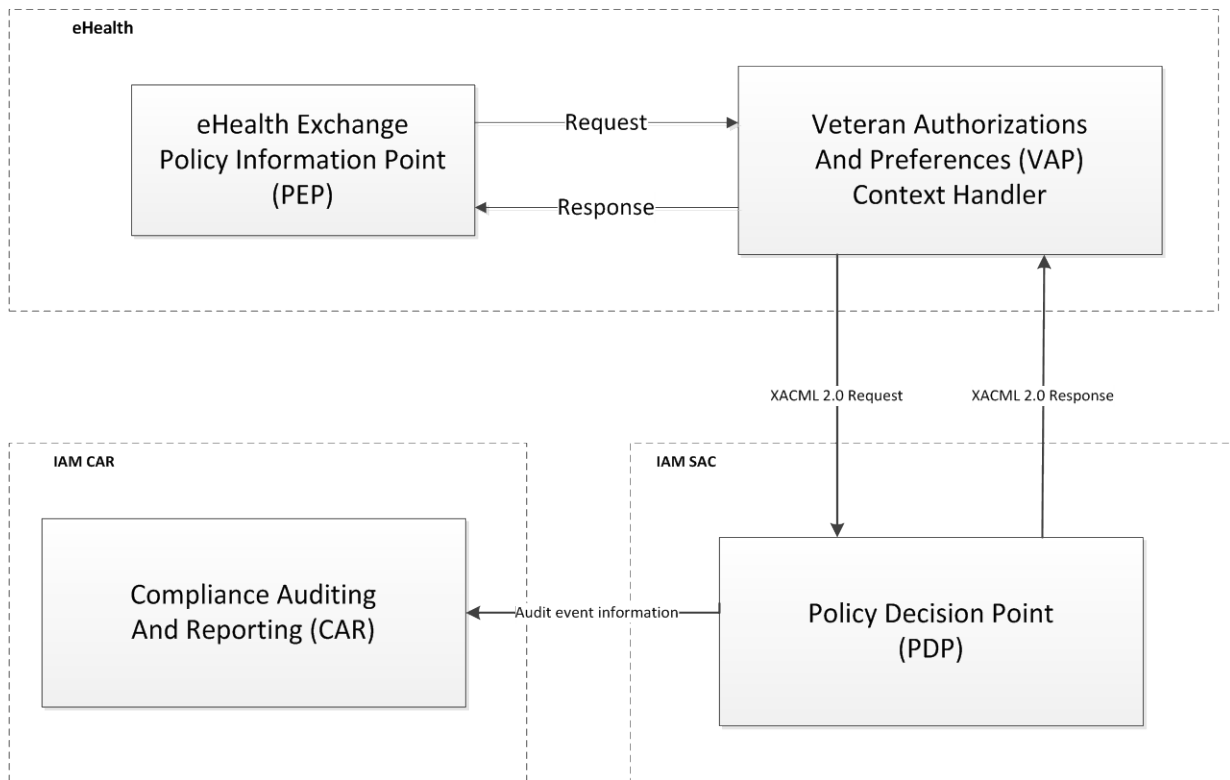


Figure 2: SAC Application Context Diagram

Table 11: Application Context Description

| Objects | | | | | | |
|----------------------------|------------------|--|---|---------------------------------|---------------------|------------------|
| ID | Name | Description | | | Interface Name | Interface System |
| 1 | eHealth | eHealth will send a XACML request to SAC. The purpose of this request is for SAC to evaluate the request against a master policy and to recommend an access control decision to EHealth. | | | XACML <Request/> | eHealth |
| 2 | VAP | Veteran Authorization and Preferences | | | XACML <Request/> | VAP |
| 3 | CAR | Auditing and Reporting Service | | | | CAR |
| Interfaces External to OIT | | | | | | |
| ID | Interface Name | Related Object | Input Messages | Output Messages | External Party | |
| 1.1 | XACML <Request/> | eHealth Pilot Site | XACML <Request/> sent via a SOAP envelop over HTTP(s) | Authorization Decision Response | EHealth | |

3.1.2. High-Level Application Design

These are applications external to SAC that require access control decisions in order to proceed with their respective business workflows

eHealth Veterans Authorization Preferences (VAP) is a live system, that consumes SAC access control decisions, to enforce data sharing constraints, during eHealth transactions between VA and its partners

The SAC service, as a middleware component without a human interface, has a simplified application architecture and design. However, in order to adequately document the steps involved in an authorization policy evaluation and decision, the SAC service has been decomposed into the following application components and data flows.

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

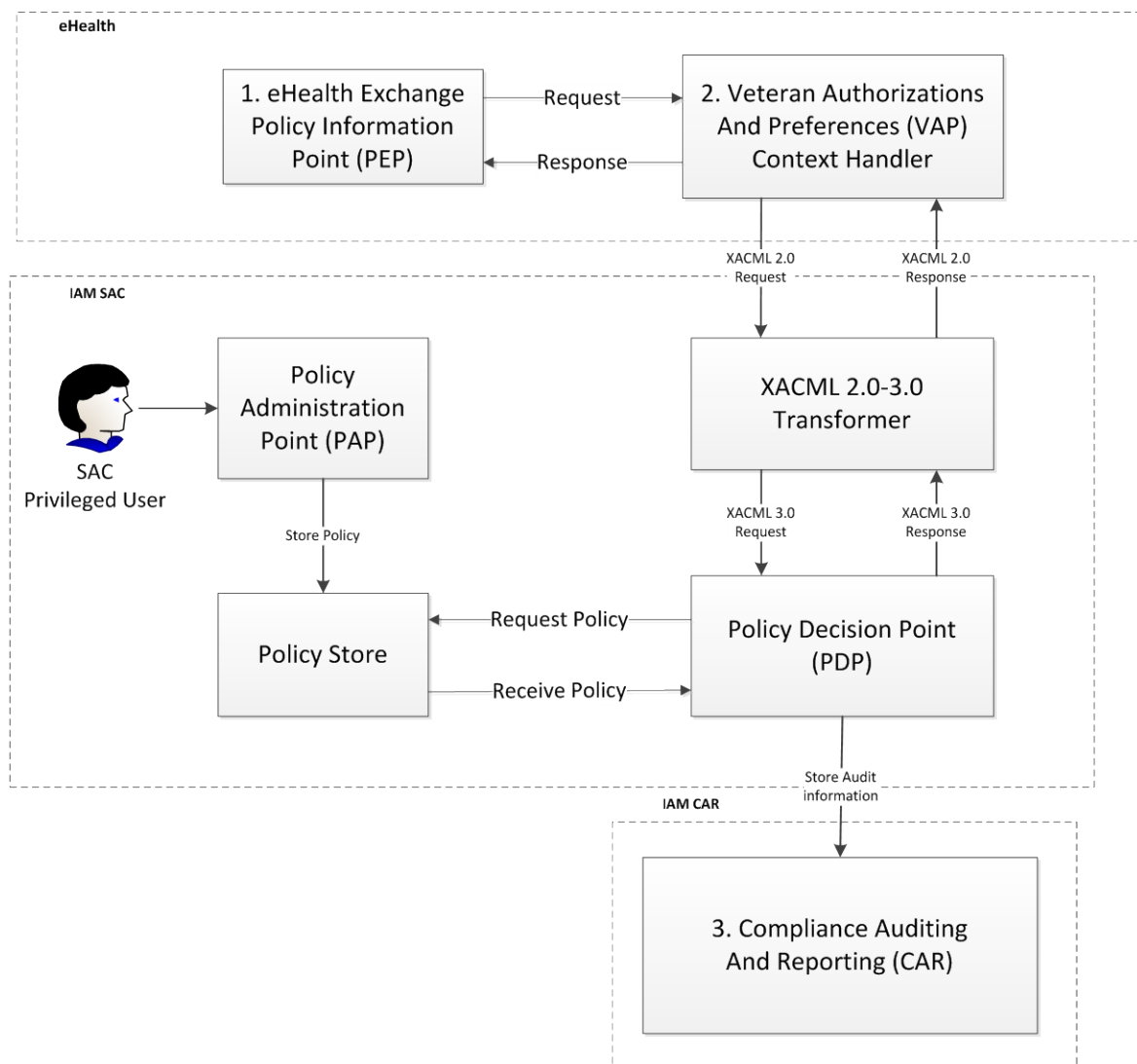


Figure 3: SAC High Level Application Design

Table 12: SAC Application Objects High Level 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 |
| Policy Decision Point | | Entry point for all authorization decisions required by EHealth | No | XACML <Request/> | 1.1 | N/A | N/A | |
| AAA Policy | | Primary container responsible for authentication and applying the master policy as part of the PDP. | No | N/A | N/A | PDP | | |
| Policy Evaluation | | Component responsible for evaluating inbound XACML Request to Master Policy | No | N/A | N/A | AAA Policy | | |
| Response Transformation | | Transforms Policy Evaluation results to XAXML response | No | N/A | N/A | Policy Evaluation | | |
| Internal Data Stores | | | | | | | | |
| Name | ID | Data Stored | | | Steward | | Access | |
| Policy Information Point | | A single XML file (see data design) that contains the EHealth Master Policy | | | EHealth Business Owners | | Read – During evaluation of policy Update – During administrative updates to the Master Policy | |
| Log | | Internal Log file that audits each application object functions | | | N/A – Internal to DataPower appliance | | Write | |

3.1.3. Application Locations

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

Table 13: Solution Application Locations

| Application Component | Description | Location at Which Component is Run | Type |
|-----------------------|---|---|------|
| Axiomatics ASM | The components of Axiomatics are managed from a central point, the Axiomatics Services Manager (ASM). Via ASM, policies and configurations are distributed to the authorization services and PDPs, which are deployed, managed, and monitored via the management interface. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) | |
| Axiomatics PAP | Policy Administration Point, an application for managing policies used by the policy decision point (PDP). | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) | |
| Axiomatics PDP | Policy Decision point for fine-grained authorization decision requests. | Terremark Culpeper, VA (Primary) Terremark Miami, FL (Disaster Recovery) | |

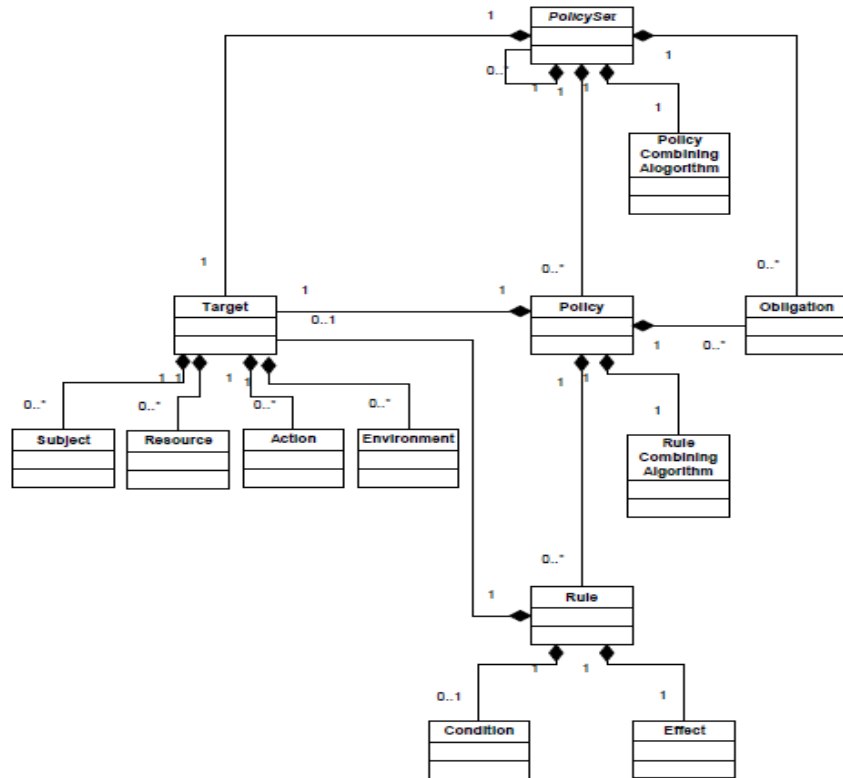
3.2. Conceptual Data Design

The SAC service does not store any transactional data, nor does it query any internal or external data. SAC does evaluate incoming decision requests against a static XACML policy file. This file is loaded at development time to the DataPower appliance and stored within the internal DataPower flash memory storage.

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 policies that can be stored in SAC should correspond to the XACML 3.0 model shown below.



CPPeEHealth.CPPEeHealth

Figure 4: XACML Policy Data Model

All SAC PDP requests are based on the Request element of the XACML 3.0 context schema.

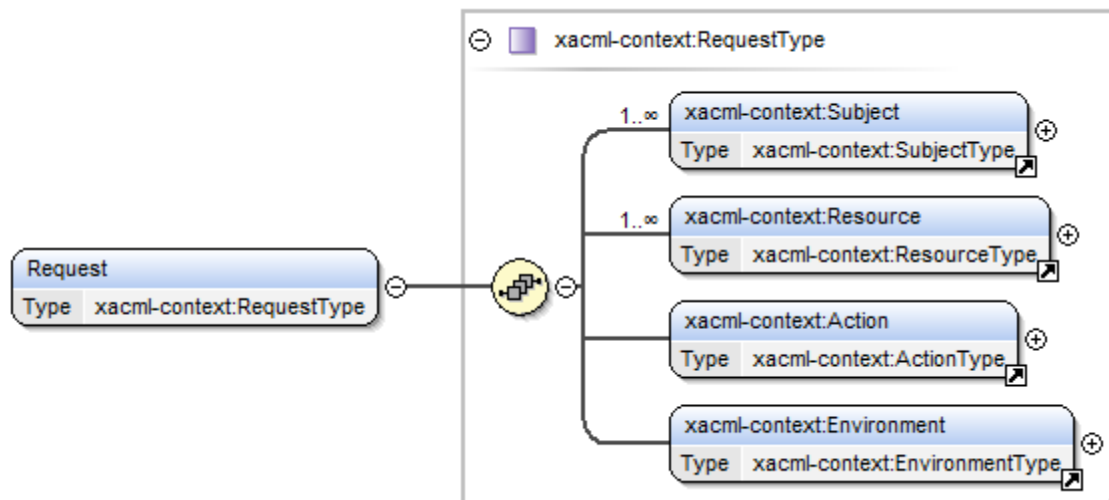


Figure 5: XACML 3.0 Request Data Model

All SAC PDP responses are based on the Response element of the XACML 3.0 context schema.

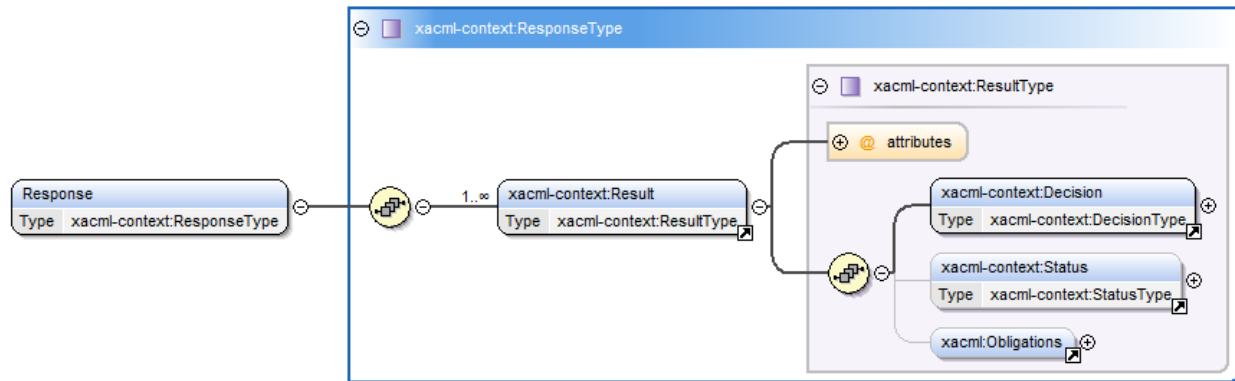


Figure 6: XACML Response Data Model

3.2.2. Database Information

As part of the AcS 2.0, the following table identifies the Oracle Database instances that will be interfaced.

SAC is based on a COTS product; refer to the applicable Axiomatics documentation for pertinent Database information.

3.2.3. User Interface Data Mapping

SAC is based on a COTS product; therefore, there are no Custom UIs.

3.2.3.1. Application Screen Interface

N/A

3.2.3.2. Application Report Interface

SAC Integrates with the Compliance Audit and Reporting (CAR) service to support expanded compliance audit and reporting capabilities.

3.2.3.3. Unmapped Data Element

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



3.3. Conceptual Infrastructure Design

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



Figure 7: SAC Infrastructure Design

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 that support SAC is shown in Figure 8 below.

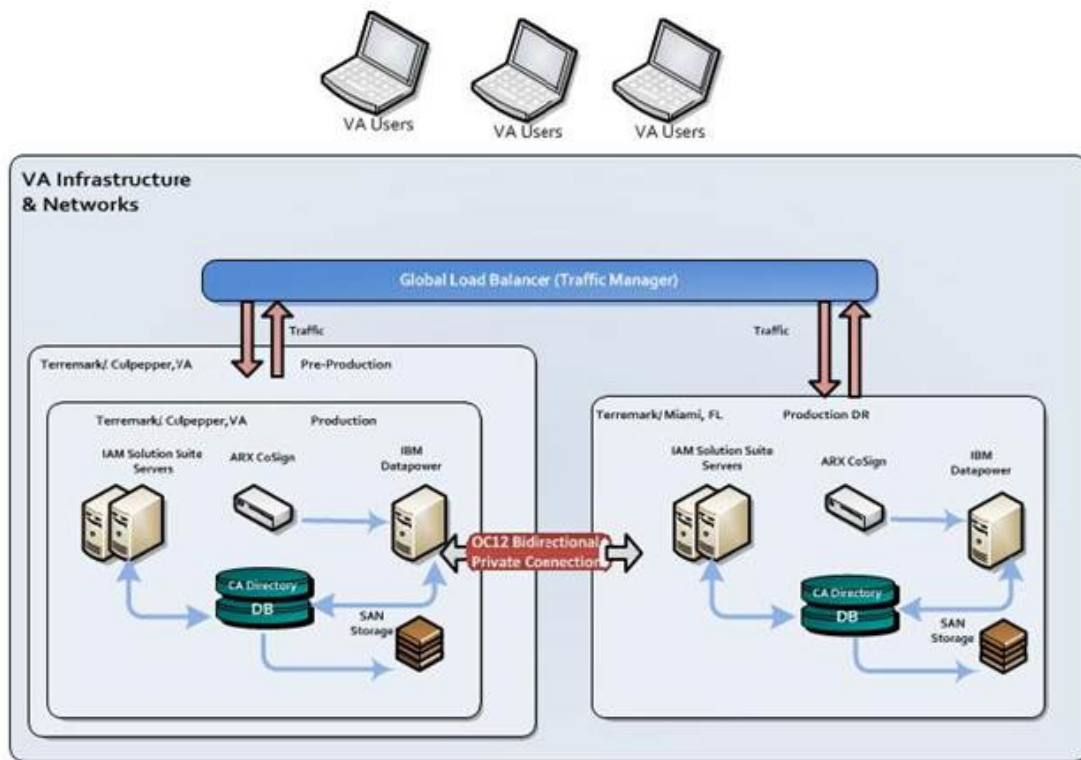


Figure 8: AcS Production Environments

3.3.4. Conceptual Infrastructure Diagram

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

3.3.4.1. Location of Environments and External Interfaces

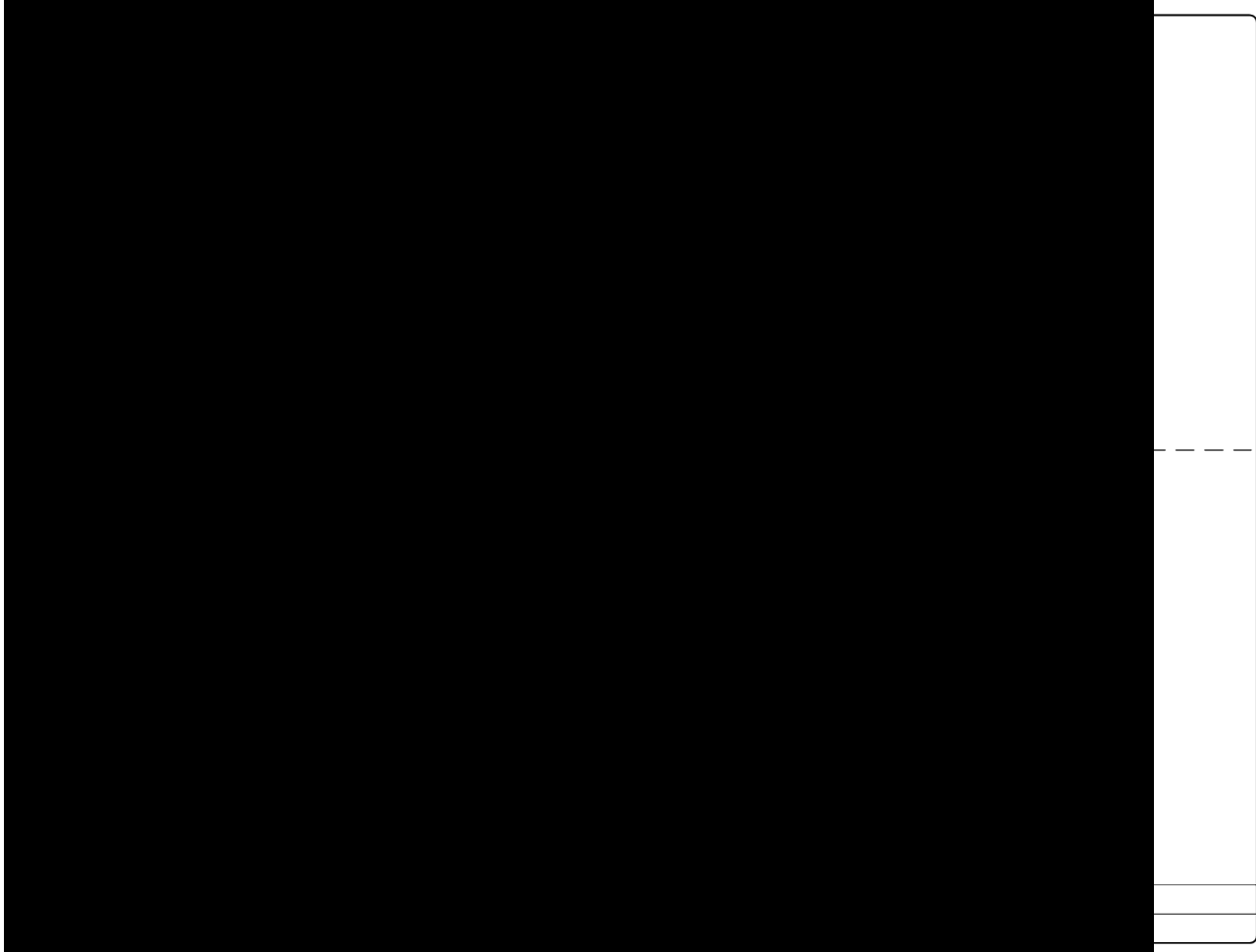


Figure 9: Sample Conceptual Networks and Environments

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.
- There will be a directory and database synchronized across a private OC-12 connection between both sites. Multiple instances of CA Directory are deployed locally at Terremark Culpeper, VA and remotely at Terremark Miami, FL data centers in a multi-write replication mode. Multi-write replication is a mechanism for replicating updates to a number of instances to maintain that the user stores are synchronized for internal and external users.
- Oracle Data Guard is utilized for database replication from the Production data center at Terremark Culpeper, VA to the disaster recovery data center at Terremark Miami, FL sending the archive logs at an incremental time span asynchronously down to as low as 1 second.

3.3.4.2. Conceptual Production String Diagram

The following diagram, Figure 10 provides a logical view of the SAC components.

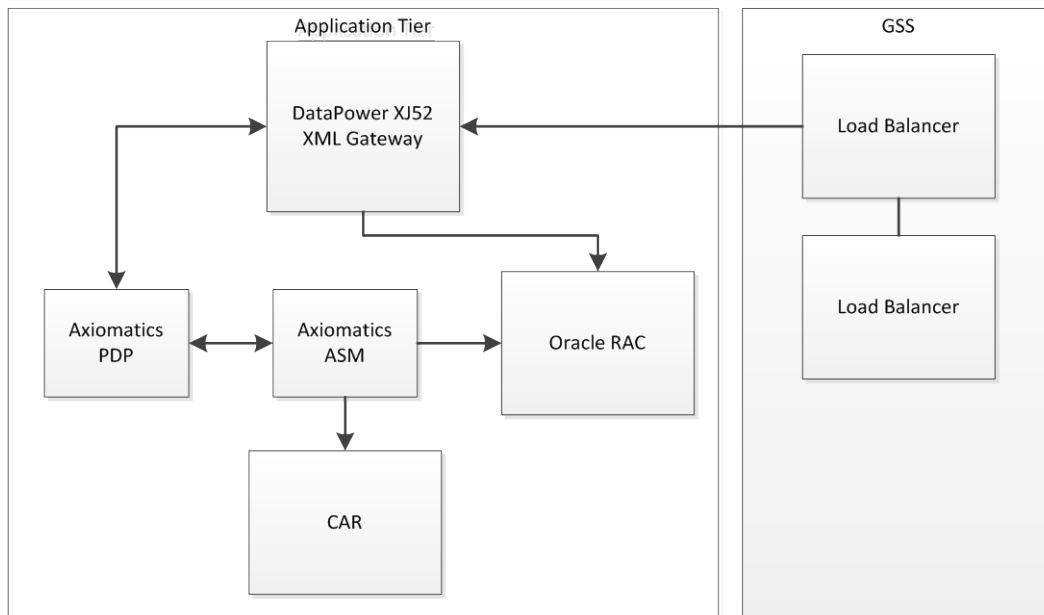


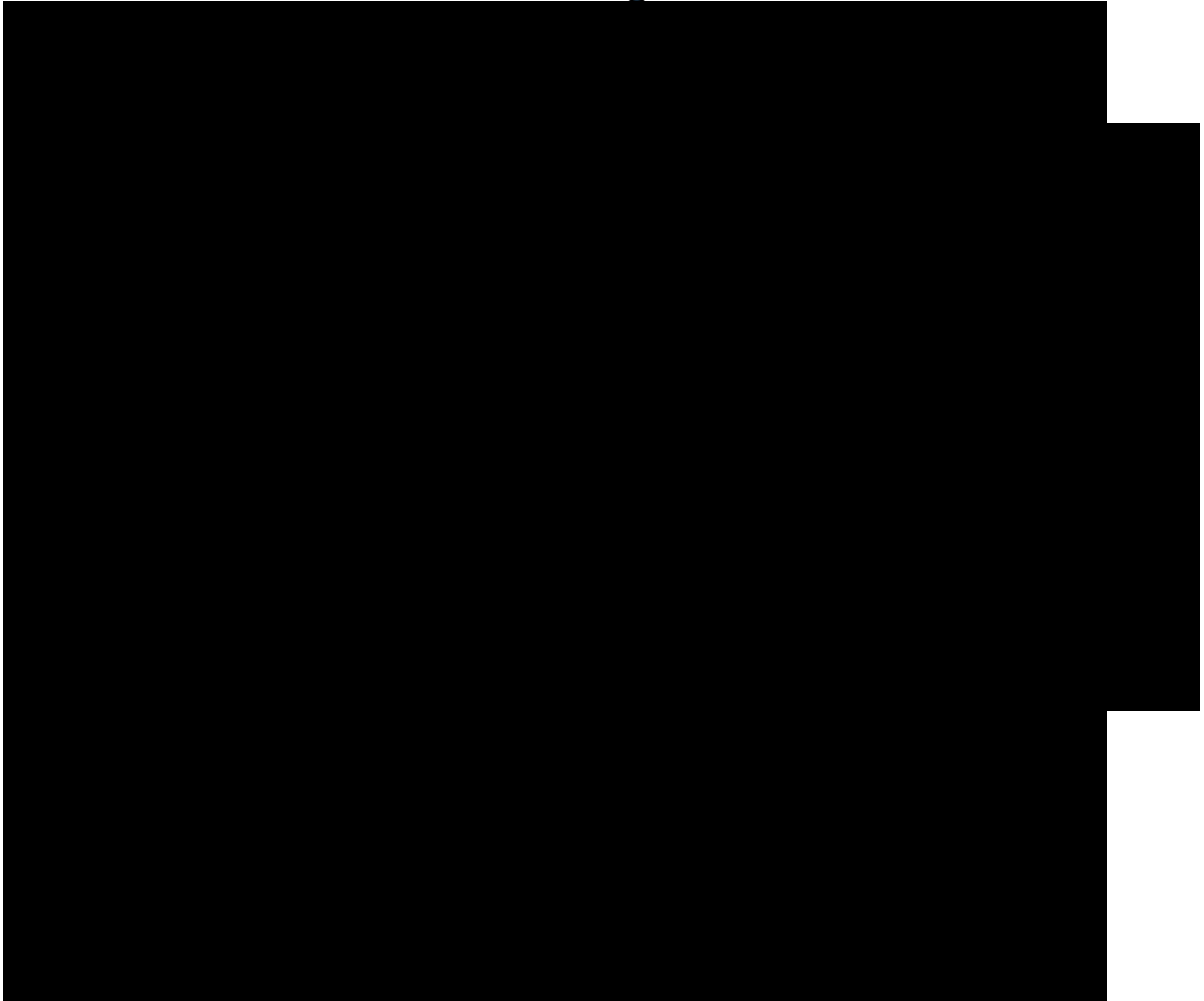
Figure 10: Logical Network String Diagram

4. System Architecture

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

4.1. Hardware Architecture

The following diagram, Figure 11, shows the AcS 2.0 hardware architecture and network topology.



The following table provides information for the hardware appliances used for the VA AcS 2.0.

Notes:

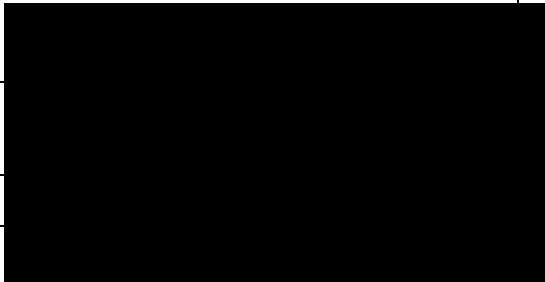
- X150 DataPower is currently being used in lower environment and will be upgraded.
- Production and DR are using X152 DataPower.

Table 14: Hardware Appliance

| Hardware Appliance | Descriptions | High Availability (HA) |
|--------------------|---|---|
| IBM DataPower | A critical component of AcS infrastructure to securing web service message flows as a proxy using IBM DataPower Appliance | For High Availability configuration, the DataPower X152 appliances will reside behind a Citrix Netscaler. This setup will have no effect on the existing DataPower configurations, as each transaction will be independent and processed separately by each DataPower appliance. The load balancer will serve as a reverse-proxy to distribute network traffic. The goal is to improve the overall burden of a single machine by enabling an industry standard algorithm. |

The uniform resource locators (URLs) for SAC for production, pre-production and SQA are provided in the table below. The AcS components residing in the DMZ are the external facing web servers that contain the CSP pages and federation components. These components will be load balanced by the Citrix Netscalers located in the Terremark GSS. DataPower, along with the remaining AcS application components, will reside in the GSS. The following table provides details on the AcS 2.0 machines such as ports, URLs, protocols hostnames for each application in every environment.

**Table 15: Virtual Machines and Appliances
SQA (AITC)**

| Application | Number of VMs | Number of Physical Servers | Hostname |
|-----------------------------|---------------|----------------------------|--|
| Axiomatics PDP (Tomcat) | 1 | N/A |  |
| Axiomatics ASM/PAP (Tomcat) | 1 | N/A | |
| Axiomatics Policy Auditor | 1 | N/A | |

Pre-Production (Terremark Culpeper, VA)

| Application | Number of VMs | Number of Physical Servers | Hostname |
|-----------------------------|----------------------|-----------------------------------|-----------------|
| Axiomatics PDP (Tomcat) | 2 | N/A | |
| Axiomatics ASM/PAP (Tomcat) | 1 | N/A | |

Production (Terremark Culp

| Application | Number of VMs | Number of Physical Servers | |
|-----------------------------|----------------------|-----------------------------------|--|
| Axiomatics PDP (Tomcat) | 2 | N/A | |
| Axiomatics ASM/PAP (Tomcat) | 1 | N/A | |

DR (Terremark Miami,

| Application | Number of VMs | Number of Physical Servers | |
|-----------------------------|----------------------|-----------------------------------|--|
| Axiomatics PDP (Tomcat) | 2 | N/A | |
| Axiomatics ASM/PAP (Tomcat) | 1 | N/A | |

4.2. Software Architecture

The following diagram shows the complete software architecture for SAC.

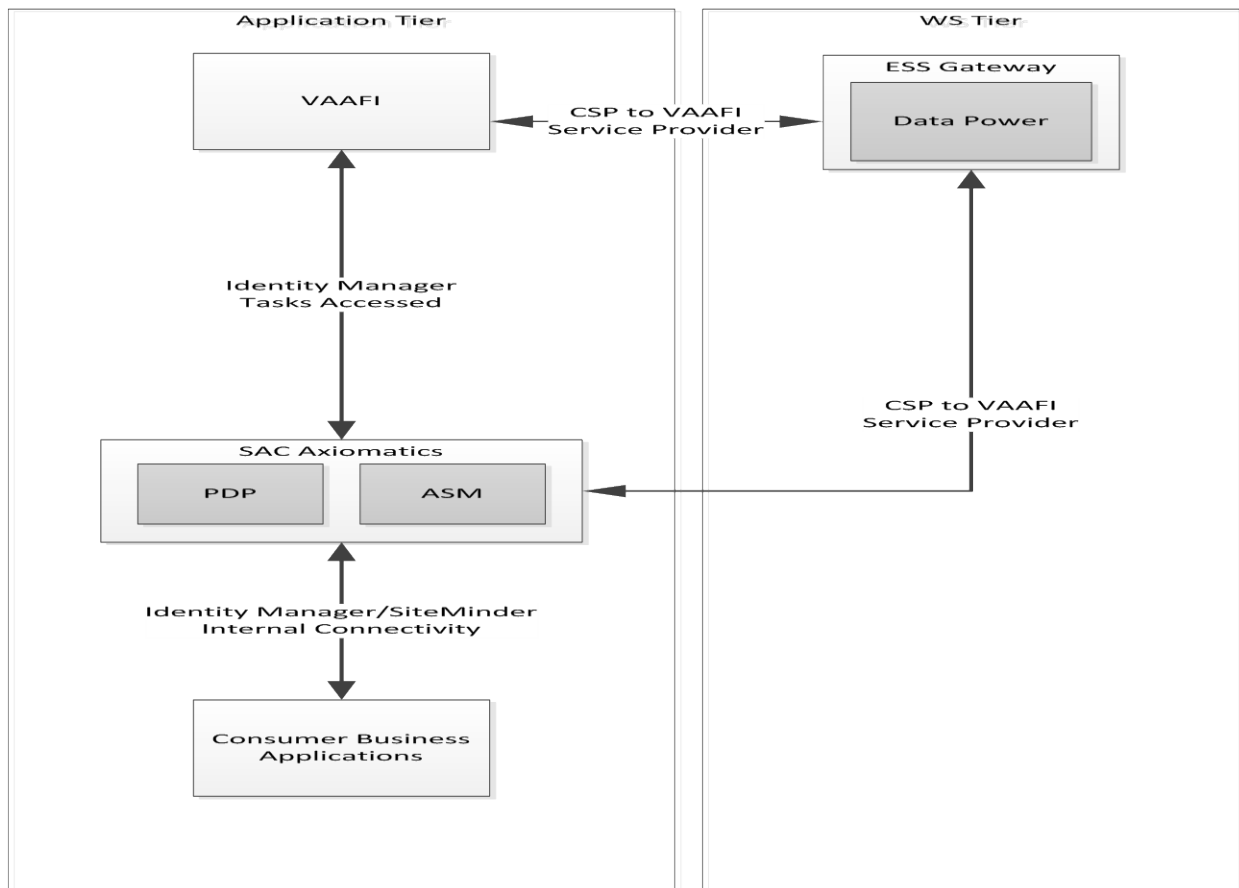


Figure 12: Software Architecture

The following table describes the AcS 2.0 SAC product versions.

Table 16: SAC Products and Versions

| Products | Abbreviation | Product Version/Release |
|-----------------|-------------------------------|--------------------------------|
| Axiomatics PDP | Policy Decision Point | 5.2.1 |
| Axiomatics ASM | Services Manager | 5.2.1 |
| Axiomatics PAP | Policy Administration Point | 5.2.1 |
| Axiomatics APA | Axiomatics Policy Auditor | 1.1.3 |
| Apache Tomcat | Axiomatics Application Server | 7.0.42 |

The following table provides information about the software components.

Table 17: 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 | 4 Data Table spaces: PROVIDM_DATA, CSPIPIDM_DATA, CASMAUDIT_DATA,ESIGAUDIT_DATA,VDSAUDIT_DATA, SACASM_DATA 3 Index Table spaces: PROVIDM_INDX, CSPIPIDM_INDX, CASMAUDIT_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 the AcS 2.0. The CA Directory infrastructure will be configured in a multi-master replication configuration. The CA Directory comprises of various instances elaborated as follows.

Application Tier –Tomcat Application Server

The application tier for the SAC solution is comprised of Tomcat application servers. The Application Tier is a shared environment for hosting application components. The AcS related applications hosted are listed below. The Axiomatics PDP and ASM components are hosted on the Tomcat application servers.

| Characteristic | Description |
|--------------------------|---|
| Tomcat Instances | Axiomatics ASM Axiomatics PDP Axiomatics APA |
| High Availability | Tomcat will not be configured as an application cluster. Tomcat is used to as an applications container for the Axiomatics product. No other applications will be deployed to the container. High Availability will be provided through load balancing of the service requests via DataPower and F5 VIP. Each TCP connection will be alternated between application nodes without a sticky bit. Each connection is stateless. |

Axiomatics

The Axiomatics components are integral to the specialized access control solution. It provides the necessary components for externalizing authorization. Axiomatics is comprised of the following components.

| Characteristic | Description |
|-------------------|---|
| Subcomponents | <p>Axiomatics Services Manager: System for managing an APS installation from a central point by providing for the deployment, configuration, and monitoring of PDPs, as well as for the management of attributes and audit services. ASM makes possible the remote management of PDP configurations, including policies, attribute sources and various other run-time configurations. ASM provides functionality for declaring attribute sources and also allows users to create and maintain attribute definitions for use in the Axiomatics PAP Client. In addition, ASM monitors the operational status of PDPs. Applicable data needed by ASM is stored in an external database.</p> <p>Policy Decision Point: Service that provides XACML-based authorization to Policy Enforcement Points (PEPs). The Axiomatics PDP provides externalized authorization and runs as a service on the network, exposing a web service interface that is secured by SSL/TLS.</p> <p>Policy Administration Point: Development environment for XACML 3 policies is used in the Axiomatics authorization infrastructure. Provides graphical XACML policy editor, attribute dictionary, and simulating and tracing policies. Policies will check in to RTC JAZZ when finalized and can be checked out by an administrator when policy updates are needed.</p> <p>Policy Auditor: Simplifies the analysis and validation process of XACML policies. Provides a user-friendly web-based graphical interface.</p> |
| High Availability | The PDPs are stateless and will use the F5 for high availability. |

The following table defines the programming languages used for development within the VA AcS 2.0.

Table 18: Programming Languages

| Programming Languages | Definition/Description |
|-----------------------|--|
| Java | Java language was used to develop custom class/jar file for IdentityMinder Business Logic Task Handler BLTH. |
| XML | Common configurations are stored as XML files. |
| XACML | XML-based language for development of privileges/role management. |
| JavaScript | Scripting language. |

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

Table 19: 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 AcS components and protocols used.

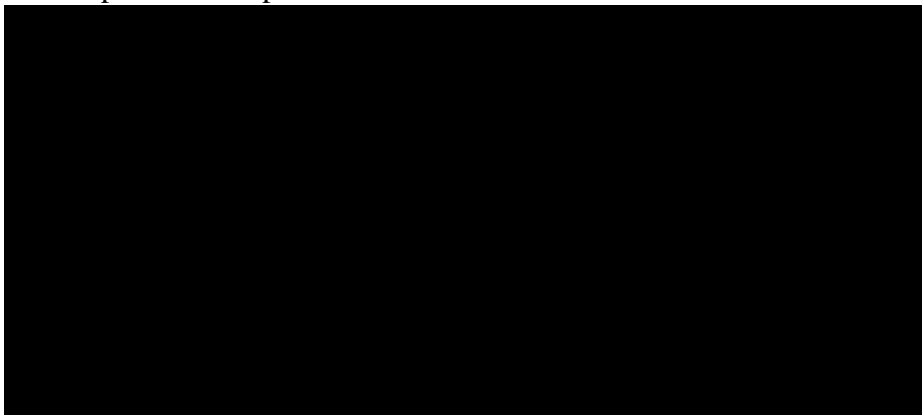


Figure 13: AcS Network Security Topology

4.4. Service Oriented Architecture/ESS

The approach for implementing SAC using Axiomatics' software suite in conjunction with the existing DataPower appliances integrations follow the generally accepted SOA paradigms and implement industry accepted protocols for communication and data processing.

SAC offers an enterprise level Attribute based Access Control (ABAC) capability to generate fine grained access control decisions. These decisions are based on requestor, resource, transaction, and environment authorization attributes, under the purview of Privacy and Security Policies. The key capability of this service that is exposed to consumers corresponds to the "Generate Authorization Decision" use case.

The SAC PDP is a SOAP based web-service. While this service is consumed within the larger healthcare SOA initiative (exchange), the service itself is inherently agnostic to the consumer's domain and could be leveraged within other SOA contexts.

4.5. Enterprise Architecture

The SAC technical solution is based on a One-VA TRM approved product – Axiomatics. Axiomatics, and SAC as a whole, leverages OASIS eXtensible Access Control Markup Language

(XACML 3.0) for policy representation and messaging with external applications, such as VAP and VDS. As of this writing, VDS is not yet in production use with Axiomatics.

SAC is a technical solution that offers an enterprise level Attribute based Access Control (ABAC) capability to generate fine grained access control decisions. The PDP service offered by Axiomatics helps protect business function from unauthorized access based on user entitlements, resource and contextual constraints under purview of organization and individual security and privacy policies. This technical solution can be leveraged in the existing VA environment to move away from individual application access control and towards a centralized authorization decision based on pre-configured policies and run-time policy decisions.

Privileged users can add and test policies through Axiomatics' Services Manager. Axiomatics PDP can also retrieve attributes through Policy Information Points, such as VDS in the future, to make run-time authorization decisions.

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

Table 20: Port Communications and Protocols

| Application | Network | Port(s) | Reason | Protocol(s) |
|-------------|----------|---------|----------------------|-------------|
| Axiomatics | Internal | ████ | HTTP Connector Port | HTTP |
| Axiomatics | Internal | ████ | AJP Connector Port | TCP |
| Axiomatics | Internal | ████ | Server Shutdown Port | TCP |
| Axiomatics | Internal | ████ | HTTPS Connector Port | HTTPS |

PreProd and Prod PKI Certificates can be found in the [POM](#).

5. Data Design

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

SAC is a COTS solution; please refer to the Axiomatics Installation documentation for DB related information.

5.1. DBMS Files

The AcS 2.0 uses Oracle 11gR2 Database and CA Directory for persistent data storage.

Table 21: SAC Database File System

| Table Spaces | Data Files |
|--------------|--------------------------------------|
| SACASM_DATA | +ORADATA/acsdbs/datafile/sacasm_data |

5.2. Non-DBMS Files

Non-DBMS files are not used for SAC.

5.3. Data View

N/A

6. Detailed Design

6.1. Hardware Detailed Design

The sections below provide the hardware information for the SAC service. The following table displays the sizing, network, Operating System, and number of Virtual Machines required to be deployed for SAC:



The DataPower is a hardened appliance, already provisioned with an Operating System, CPU, Memory, and Network interfaces. No hardware configuration is required.

6.2. Software Detailed Design

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

6.2.1. SAC Design

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

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

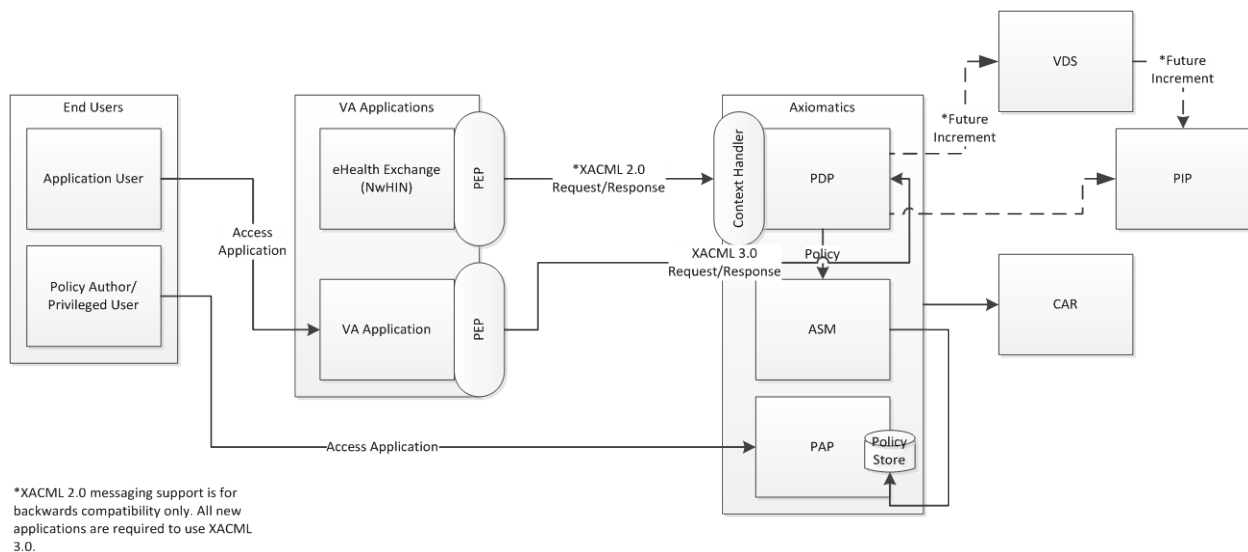


Figure 14: SAC Detailed Design

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

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

Axiomatics:

- Policy Enforcement Point (PEP):** PEP intercepts requests for protected resources and defers to the PDP for access control decisions; which it subsequently enforces, upon receipt from the PDP. SAC does not offer a PEP service yet. Custom PEPs can be built using the Software Development Kit (SDK) provided by Axiomatics, and may be implemented in the future. Currently, SAC expects consuming applications to implement their own PEPs. The PEPs must conform to XACML 3.0 in order to integrate with the SAC enterprise PDP.
- Policy Decision Point (PDP):** The PDP is an XACML engine that receives requests from PEPs containing authorization attributes and evaluates these requests against cached XACML 3.0 Privacy and Security policies. The PDP then determines the applicable security policy to use and the attributes needed for decision generation. When SAC integration with VDS is complete, the PDP will be able to obtain additional authorization attributes from numerous attribute sources front-ended by VDS. The generated access control decision is then sent back to the PEPs for enforcement. The Axiomatics PDP has

two web service interfaces used for communication. The ASM communicates with the PDP through the management web service interface. PEPs communicate with the PDP through the PDP endpoint address web service.

- **Context Handler Functionality:** PDP has backwards compatibility with XACML 2.0 standard and currently the SAC implementation has a separate endpoint, configured for handling legacy application requests.
- **Policy Administration Point (PAP):** The PAP facilitates creation of policies and policy sets and retains these policies in policy stores with the intent of making them available to the PDP. Axiomatics PAP is a stand-alone Java application providing a full-featured graphical XACML 3.0 policy editor. The interface provides administrators authoring, testing, and troubleshooting capabilities. The PAP is used in the SAC solution for authoring XACML 3.0 security policies. The security policies represent the business rules for access control that restrict access based on client preferences, data restrictions, user security, and contextual constraints. The policies are exported from the PAP as policy packages.
- **Axiomatics Services Manager (ASM):** Axiomatics ASM is a web based application that provides a centralized configuration management interface for the PDPs. It provides the capability to manage and provision configurations to remotely managed PDPs. The PDPs can be grouped logically for easier management. New and updated XACML 3.0 policies can be pushed to individual PDPs or to PDPs within groups for easier policy management.
- **Axiomatics Policy Auditor (APA):** Axiomatics APA is a web-based application that provides a tool for analyzing the behavior of XACML policies. This analysis and process provides compliance with consumers business rules, increases policy controls, and supports accountability. It can also help determine unexpected policy behavior.
- **Policy Information Point (PIP):** The PIP is a source of authoritative information attributes that can be consumed by the PDP during policy evaluation. Numerous PIPs can be integrated into the VDS product, for consumption by the PDP.

SAC is an enterprise service that will be consumed by numerous entities within the VA for fine-grained access control. SAC is based on a COTS product and is independent and self-contained. SAC may leverage an attribute service, such as VDS, in the future.

6.2.1.1. Product Perspective

6.2.1.1.1. User Interfaces

There are no custom UIs for SAC, as it is based on a COTS product. Refer to for SAC GUIs.

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

The Table below lists the established memory constraints for Axiomatics.

Table 22: Memory Constraints

| Stack | Not Set | Not Set | Not Set |
|---------------------------|---------|---------|---------|
| Heap Space | Not Set | Not Set | Not Set |
| JVM Config for Axiomatics | 3GB | 3GB | 3GB |

- Stack
- Heap Space
- What's being used in Production
- JVM Configuration for Axiomatics

6.2.1.1.6. Special Operations

N/A

6.2.1.2. Product Features

SAC uses the Axiomatics Policy Server (APS), which is a powerful access control system allowing users to manage, simulate, and enforce fine-grained policies written in the eXtensible Access Control Markup Language (XACML). The Axiomatics Policy Server (APS) provides a full-fledged, XACML-based authorization service. The components are managed from a central point, the Axiomatics Services Manager (ASM).

6.2.1.3. User Characteristics

Refer to section 1.4 and section 1.5 for user-related information.

6.2.1.4. Dependencies and Constraints

Refer to section 1.6 and section 2.3 for AcS 2.0 constraints and dependencies.

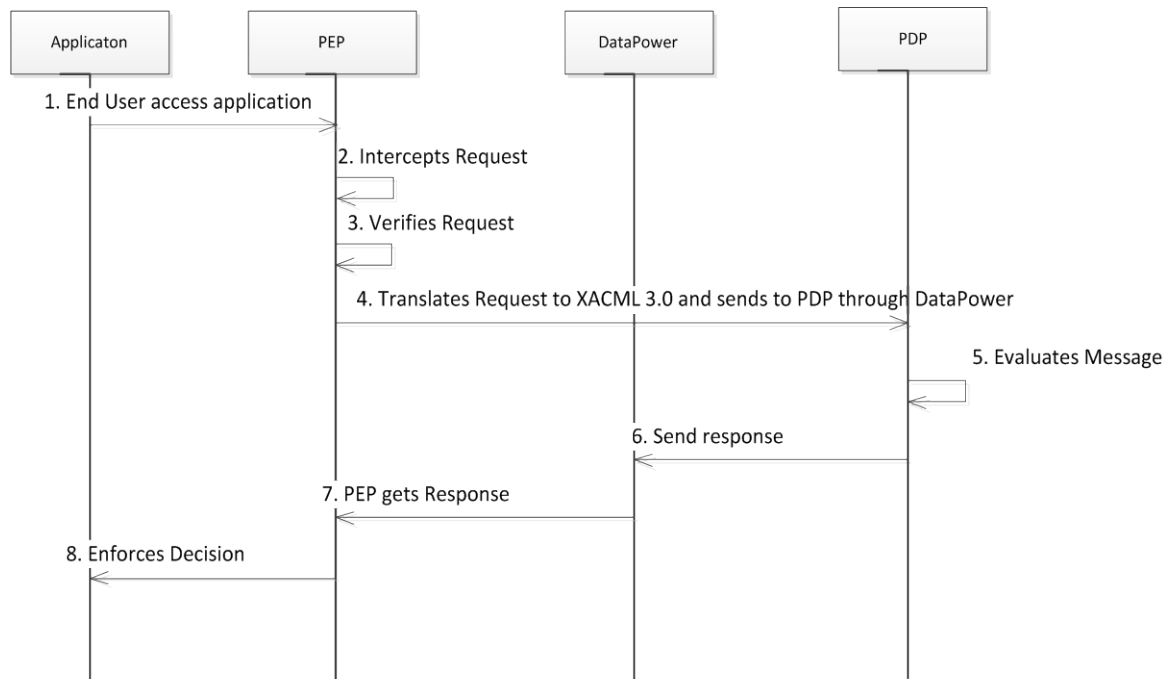


Figure 15: Enforce Access Control Decision Sequence Diagram

Table 23: Enforce Access Control Decision

| Field | Description |
|----------------|---|
| Use Case Name | Enforce Access Control Decision |
| Description | This use case describes the process by which a Policy Enforcement Point (PEP) interacts with a consuming application and the SAC service to facilitate an authorization request and enforce an access control decision. |
| Actors | 1. Application 2. PEP 3. DataPower 4. PDP |
| Pre-Conditions | 1. Enter User has authenticated session with Application 2. TLS session is established between the Application and PEP |
| Trigger | The PEP receive a request for an authorization from an application |
| Actions | 1. End-User attempts to access protected application 2. PEP intercepts access request 3. The PEP can reside between the end user and the application 4. The PEP can reside within the application itself 5. PEP verifies request is valid and contains authentication attributes that can be used to uniquely identify the user |

| Field | Description |
|------------------------|---|
| | 6. PEP translates access request to XACML 3.0 7. Includes authentication attributes (SECID, ICN, unique identifier) 8. May include client preferences, data restrictions, user security, contextual constraints 9. Forwards XACML 3.0 (2.0 if eHealth) request to DataPower 10. DataPower performs XML threat reduction and forwards request to PDP 11. PDP evaluates appropriate policy(s) and attributes (within XACML request and from PIPs (VDS)) and generates an access control decision. *Note – ‘eHealth’ initiated requests are first transformed from 2.0 to 3.0. PIP is not consulted. 12. The PDP response is sent to DataPower 13. DataPower sends PDP response to the PEP. PEP receives XACML 3.0 (2.0 if eHealth) access control decision response from the PDP 14. PEP enforces access control that it received from PDP |
| Main Success Scenarios | 1. If Decision is Permit, access is granted to the user to access the protected resource 2. If Decision is Deny, access is denied. The user is not allowed to access the protected resource 3. The processing of Indeterminate or Not Applicable is determined by the application requirements |
| Main Failure Scenarios | 1. Message format/contents are not valid 2. PDP is non-responsive and decision is not provided to application |

6.2.1.5. Security Policy Authoring

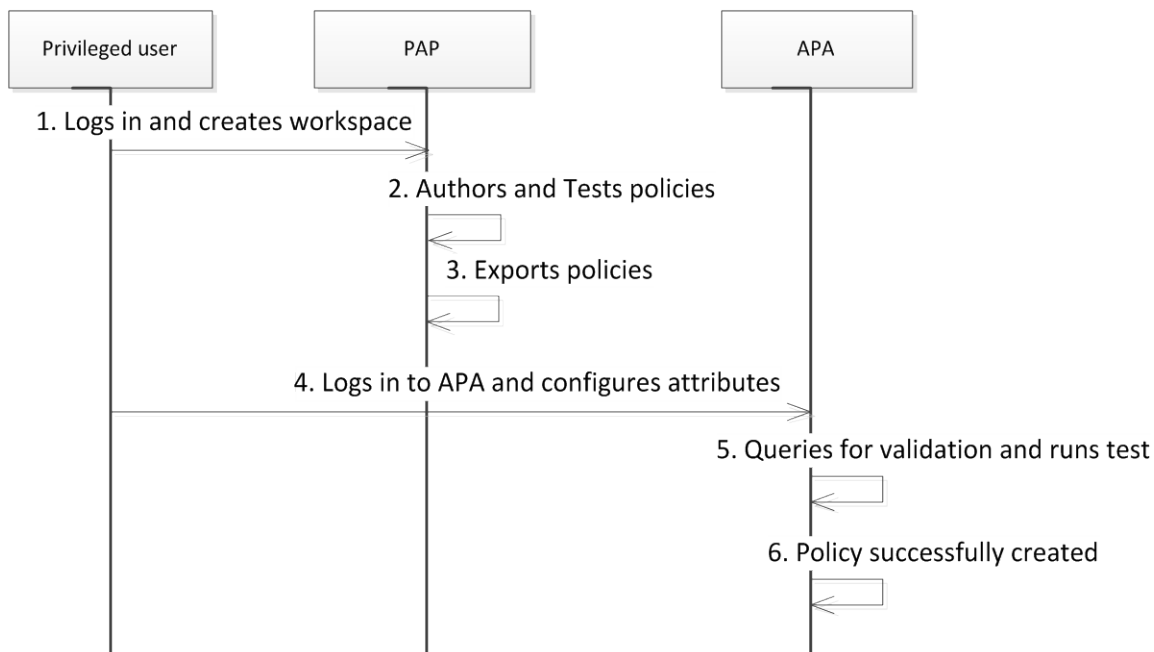


Figure 16: Security Policy Authoring Sequence Diagram

Table 24: Security Policy Authoring

| Field | Description |
|------------------------|---|
| Use Case Name | Security Policy Authoring |
| Description | This use case describes the process through which a SAC Privileged User authors security control policies. |
| Actors | <ol style="list-style-type: none">1. Privileged User2. PAP3. APA |
| Pre-Conditions | Privileged user has access to PAP. |
| Trigger | The privileged user starts up Axiomatics Policy Administration Point thick client GUI interface to author and test XACML 3.0 policies. |
| Actions | <ol style="list-style-type: none">1. Privileged User creates workspace to organize and store policies2. The policies and configurations are stored locally3. Privileged User authors and tests XACML 3.0 policies4. Once completed, the privileged user exports policy package to dedicated file location5. Privileged User logs into APA and configures attributes from the PEP perspective6. Privileged User creates queries for validation and runs validation tests7. Policy is authorized successfully upon successful testing |
| Main Success Scenarios | Policy is created successfully. |
| Main Failure Scenarios | Policy creation fails and user has to start over. |

6.2.1.6. Manage Access Control Policies

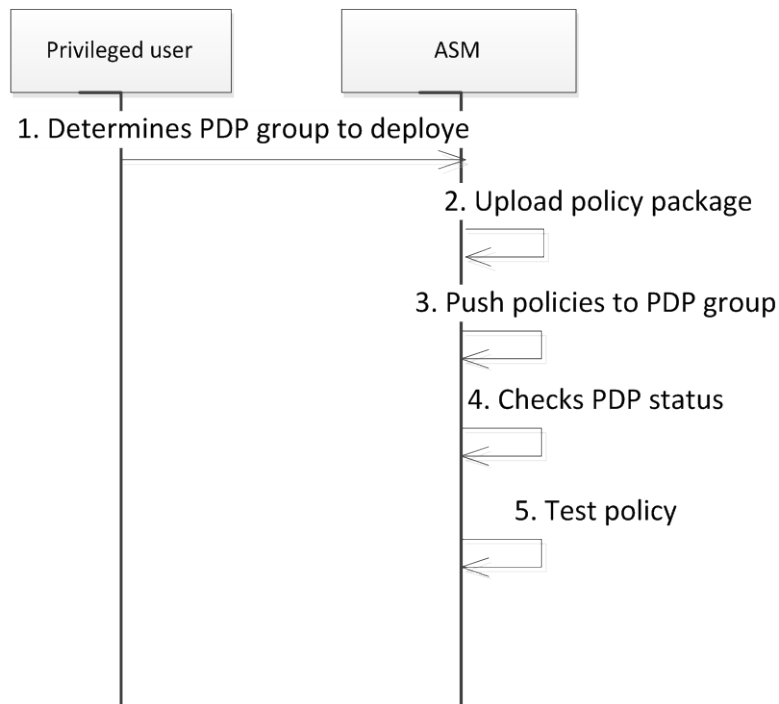


Figure 17: Manage Access Control Policies

Table 25: Manage Access Control Policies

| Field | Description |
|------------------------|--|
| Use Case Name | Manage Access Control Policies |
| Description | This use case describes the process through which a SAC Privileged User manages access control policies across PDPs. |
| Actors | 1. Privileged User 2. ASM |
| Pre-Conditions | Privileged user has access to ASM component. |
| Trigger | The privileged user is logged in to ASM and is ready to deploy policy package. |
| Actions | 1. Privileged User determines proper PDP group to deploy policy package 2. Upload validated policy package 3. Push policies to managed PDP within PDP group 4. Policies are pushed via web service call over TLS 5. Privileged user checks PDP status and pushes policies 6. Privileged user tests PDP with XACML requests to verify policy |
| Main Success Scenarios | Policy is pushed to PDP successfully |

| Field | Description |
|------------------------|---|
| Main Failure Scenarios | Policy upload fails and user has to start over. |

6.2.1.7. Make Access Control Decisions

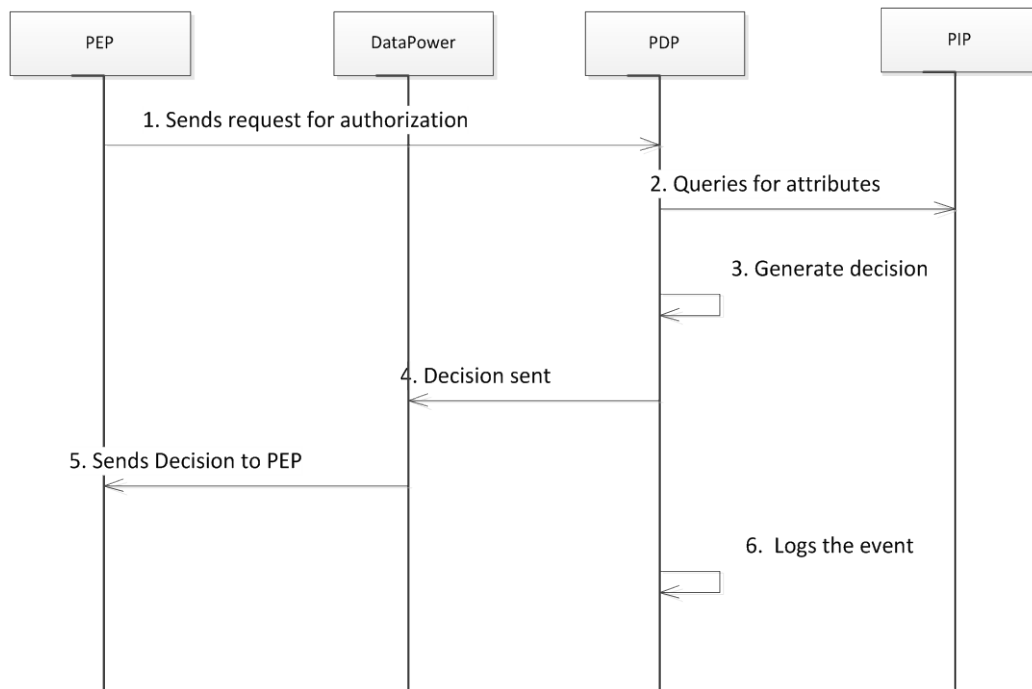


Figure 18: Make Access Control Decisions Sequence Diagram

Table 26: Make Access Control Decisions

| Field | Description |
|----------------|--|
| Use Case Name | Make Access Control Decisions |
| Description | This use case describes the process through which a Policy Decision Point (PDP) gathers and evaluates the necessary information (access control policy (s) and attributes) and makes an access control decision. |
| Actors | 1. PEP 2. DataPower 3. PIP 4. PDP |
| Pre-Conditions | The application authorization policy and needed attributes exist |
| Trigger | PDP receives XACML request from PEP via DataPower |
| Actions | 1. PEP request is received and PDP examines the request attributes to determine the correct policy to apply 2. Once the correct policies have been determined the PDP queries the PIP for |

| Field | Description |
|------------------------|--|
| | <p>attributes required by policy(s)</p> <p>3. The PDP uses the attributes found in the XACML 3.0 request, the attributes retrieved from the PIP, and the XACML 3.0 security policies to generate an access control decision</p> <p>4. The XACML 3.0 response/access control decision is sent to DataPower</p> <p>5. DataPower sends the XACML 3.0 response/access control decision to the requested PEP</p> <p>6. PDP logs the access request and response</p> |
| Main Success Scenarios | Decision is generated and passed to PEP |
| Main Failure Scenarios | Policy is not found or attributes are missing and decision is not generated |

6.2.1.8. Make Access Control Decisions

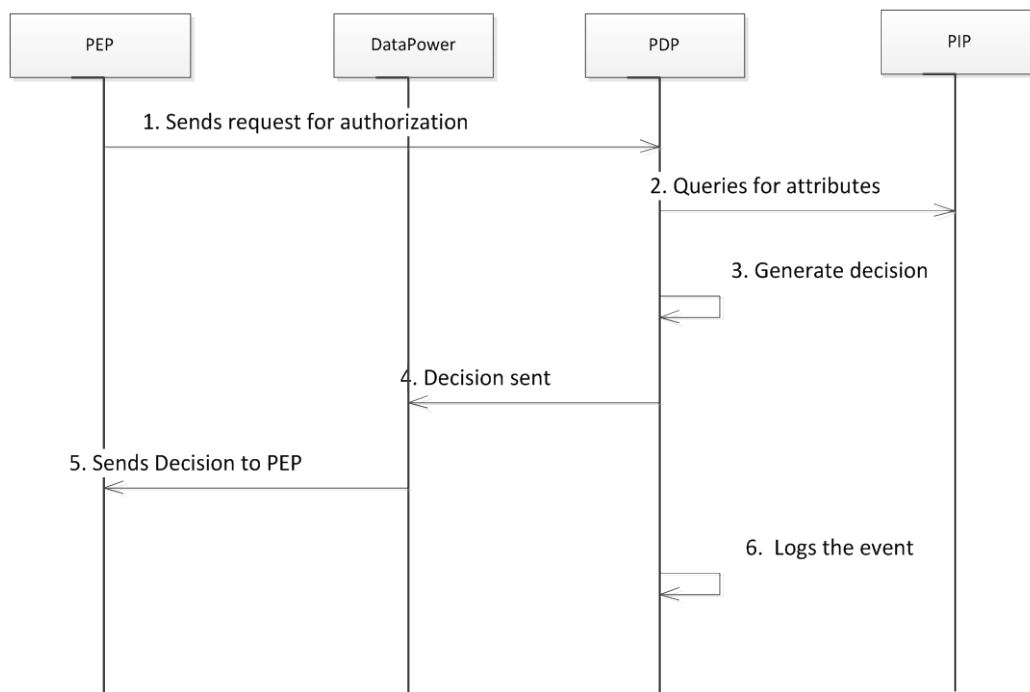


Figure 19: Make Access Control Decisions Sequence Diagram

Table 27: Make Access Control Decisions Using XACML 2.0 Request/Response

| Field | Description |
|---------------|---|
| Use Case Name | Make Access Control Decisions using XACML Request/Response |
| Description | This use case describes the process through which a Policy Decision Point (PDP) gathers and evaluates the necessary information (access control policy(s) and attributes) and makes an access control decision. |

| Field | Description |
|------------------------|--|
| Actors | <ol style="list-style-type: none"> 1. PEP 2. DataPower 3. PIP 4. PDP |
| Pre-Conditions | The application authorization policy and needed attributes exist |
| Trigger | PDP receives XACML request from PEP via DataPower |
| Actions | <ol style="list-style-type: none"> 1. PEP request is received and PDP examines the request attributes to determine the correct policy to apply 2. Once the correct policies have been determined the PDP queries the PIP for attributes required by policy(s) 3. The PDP uses the attributes found in the XACML request, the attributes retrieved from the PIP, and the XACML security policies to generate an access control decision 4. The XACML response/access control decision is sent to DataPower 5. DataPower sends the XACML response/access control decision to the requested PEP 6. PDP logs the access request and response |
| Main Success Scenarios | Decision is generated and passed to PEP |
| Main Failure Scenarios | Policy is not found or attributes are missing and decision is not generated |

6.2.2. Specific Requirements

Specific Requirements this SDD provides are the foundational detailed design for SAC activities under VA Development Support program. SAC is a COTS products used to meet the technical requirements that sufficiently meet the detailed functional requirements. The design applies specific configurations and customizations made to create the technical solution necessary to meet the business requirements provided in requirements documents listed in section 1.6.

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 Records |
| 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 | |
| 6.2.2.3.9. | Options |
| N/A | |
| 6.2.2.3.10. | Protocols |
| N/A | |
| 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 SAC solution.

6.4. Service Oriented Architecture/ESS Detailed Design

6.4.1. Service Description

Add WSDL for PDP

6.4.2. Service Design

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

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

7.1. Interface Architecture

N/A

7.2. Interface Detailed Design

N/A

8. Human-Machine Interface

SAC provides a web service and does not utilize an end user UI.

SAC provides an Admin UI to configure and enable integrations to the SAC service.

- Please refer to the [SAC Configuration Guide](#) for additional content.
- For user interface information related to COTS administrator functions, refer to the product documentation available at the following websites:
- Axiomatics site: <http://www.axiomatics.com> Refer to section 3.2.3, which provides the interfaces that are used by AcS activities as appropriate for the end users.

8.1. Interface Design Rules

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

- The user and administrator interfaces comply with VA's branding specifications.

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.

8.2. Inputs

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 SAC:

- PDF
- Comma Separated File (CSF)

- Excel

8.4. Navigation Hierarchy

8.4.1. Screen Shots

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

8.4.1.1. Application Screen Interface

This section provides the screens of the Graphical User Interface (GUI) that the SAC users will have access within the SAC application.

8.4.1.1.1. PAP Authoring Page

Once a workspace is opened or created by the privileged user, the following screen, Figure 6, displays in which the SAC privileged user creates/edits XACML 3.0 policies.

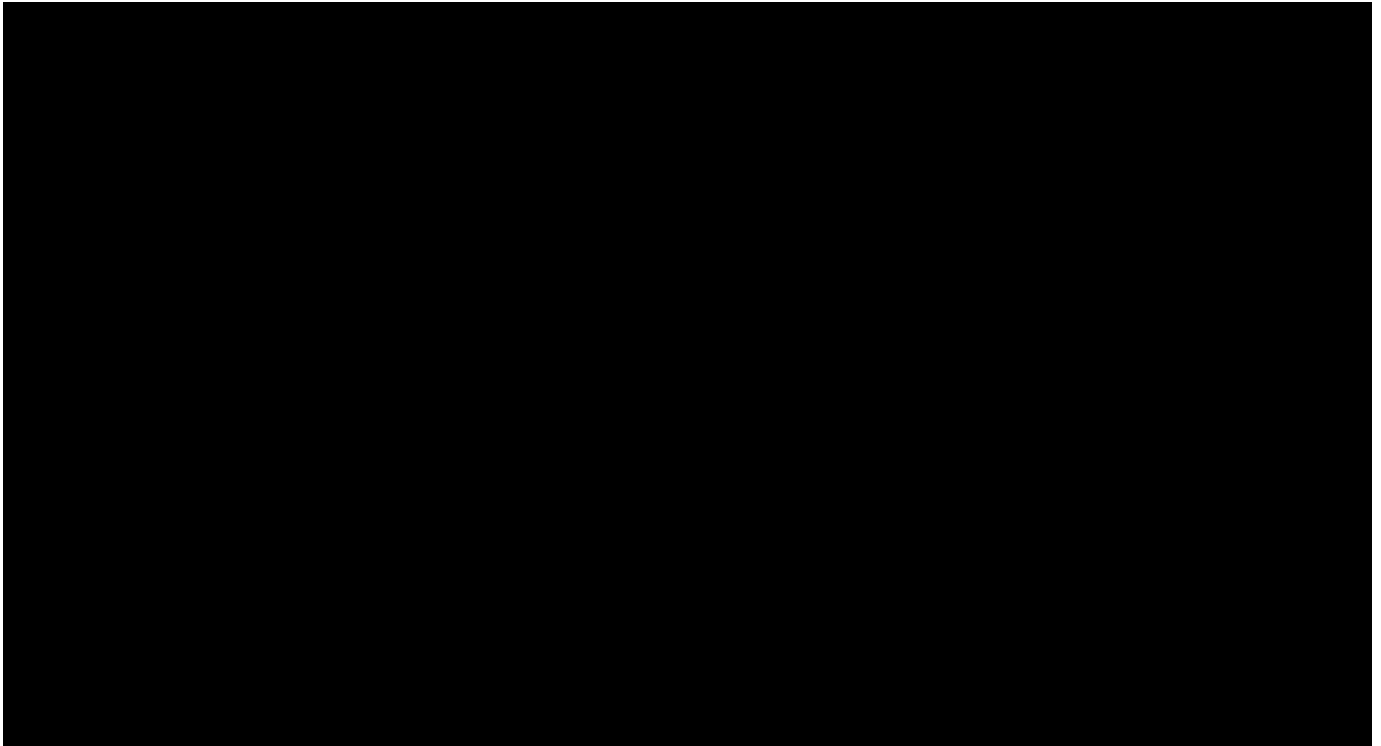


Figure 20: SAC PAP Landing Page

9. Security and Privacy

9.1. Security

Data security is critical for VA to safeguard user information and ensure that data in motion as well as rest is secured properly. For SAC, 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.

Data at Rest:

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

Table 28: 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. |
| File Store | File Store | Non-Sensitive/ Sensitive | <ul style="list-style-type: none">• IM is stored in a JMS data in file system and contains transactional data. It does not contain any sensitive information.• A FIPS encryption key file is stored in the file system. Access to the file should be restricted and enforced by setting the directory/file access permissions for specific groups and/or users. |

The security controls for the data at rest are managed through the encryption of sensitive attributes at the directory level for the AcS 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.1 below for data type groupings) and who can make updates accordingly.

Table 29: 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 |

| Type | Provisioning System | CSP System | IP 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. Confidentiality of Sensitive Information

N/A

9.3. SAC

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

9.3.1. Confidentiality of Sensitive Information

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

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

9.3.2. Privacy of Personal Information

The SAC service does not store any sensitive PII of the users. Privacy is maintained through the security measures described in Section 9.1.

9.3.3. Process Integrity

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

9.3.4. System Availability

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

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

A.1. RTM

Refer to the AcS RSD/or the Rational Requirements Manager (RRM) to obtain the AcS RTM for increment 5.

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.