Department of Veterans Affairs

Identity and Access Management (IAM)

Access Services (AcS) Solution 2.0 Increment 7 (i7) -

Specialized Access Control (SAC)

System Design Document (SDD)



July 2016

Version 2.7

Revision History

| Date | Version | Description | Author |
| --- | --- | --- | --- |
| 7/7/2016 | 2.7 | Update for i7 increment: authorization data storage in MVI and added PR authz policy, updated PDP endpoints, included message format for VDT request/response, updated VDT diagram. | ByLight |
| 2/24/2016 | 2.6.0 | Final AcS 2.0 i6 version | AcS Tech Lead |
| 02/10/2016 | 2.5.3 | Updated post-release | Insignia |
| 11/18/2015 | 2.5.2 | Updated per anomaly log | Insignia |
| 11/02/2015 | 2.5.1 | Updated for AcS i6 and new ProPath template | Insignia |
| 6/27/2015 | 0.5 | Completed a quality review | xxxxxxxxxxx |
| 5/11/2015 | 0.4 | Finalized | xxxxx  xxxxx  xxxxx  xxxxx |
| 5/01/2015 | 0.3 | Updated per re-opened anomalies | xxxxx  xxxxx  xxxxx  xxxxx |
| 4/17/2015 | 0.2 | Updated per anomalies | xxxxx  xxxxx  xxxxx  xxxxx |
| 3/24/2015 | 0.1 | Updated to new template; added additional language and diagrams for SAC | xxxxx  xxxxx  xxxxx  xxxxx |

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..

When to Complete Each Section of the SDD

| Section | Completed On or Before PMAS Phase | Rationale |
| --- | --- | --- |
| 1 – Introduction | MS 0 Review; updated thereafter | Conceptual design should inform evaluation of investments |
| 2 - Background | MS 0 Review; updated thereafter | Conceptual design should inform evaluation of investments |
| 3 – Conceptual Design | MS 0 Review; updated thereafter | Conceptual design should inform evaluation of investments |
| 4 – System Architecture | MS 0 Review; updated thereafter | Conceptual design should inform evaluation of investments |
| 5 – Data Design | MS 1 Review; updated thereafter | Design details should be elaborated upon during PMAS Planning phase and prior to development |
| 6 – Detailed Design | MS 1 Review; updated thereafter | Design details should be elaborated upon during PMAS Planning phase and prior to development |
| 7 – External System Interface Design | MS 1 Review; updated thereafter | Design details should be elaborated upon during PMAS Planning phase and prior to development |
| 8 – Human Machine Interfaces | MS 1 Review; updated thereafter | Design details should be elaborated upon during PMAS Planning phase and prior to development |
| Attachments | MS 1 Review; updated thereafter | Design details should be elaborated upon during PMAS Planning phase and prior to development |

A product’s system design should be defined conceptually prior to the allocation of personnel and resources that occur at project initiation. This gives the enterprise an opportunity to evaluate IT investments before project teams are stood up and funding is allocated. Sections 1- 4 which discuss the high level design should be completed prior to MS 0. All sections should be completed and updated before MS 1. Projects will need to address all SDD approval constraints prior to the MS 2 review. In addition, the SDD should reflect the as-built product going into the MS 2 review.

Table of Contents

[1. Introduction 1](#_Toc450655994)

[1.1. Scope 1](#_Toc450655995)

[1.2. User Profiles 1](#_Toc450655996)

[2. Background 1](#_Toc450655997)

[2.1. Overview of the System 2](#_Toc450655998)

[2.2. Overview of the Business Process 3](#_Toc450655999)

[2.3. Overview of the Significant Requirements 4](#_Toc450656000)

[3. Conceptual Design 5](#_Toc450656001)

[3.1. Conceptual Application Design 5](#_Toc450656002)

[3.1.1. Application Context 6](#_Toc450656003)

[3.1.2. High-Level Application Design 9](#_Toc450656004)

[3.1.3. Application Locations 13](#_Toc450656005)

[3.2. Conceptual Data Design 13](#_Toc450656006)

[3.2.1. Project Conceptual Data Model 13](#_Toc450656007)

[3.2.2. Database Information 15](#_Toc450656008)

[3.2.3. User Interface Data Mapping 15](#_Toc450656009)

[3.2.3.1. Application Screen Interface 15](#_Toc450656010)

[3.2.3.2. Application Report Interface 15](#_Toc450656011)

[3.2.3.3. Unmapped Data Element 15](#_Toc450656012)

[3.3. Conceptual Infrastructure Design 15](#_Toc450656013)

[3.3.1. System Criticality and High Availability 16](#_Toc450656014)

[3.3.2. Special Technology 17](#_Toc450656015)

[3.3.3. Technology Locations 17](#_Toc450656016)

[3.3.4. Conceptual Infrastructure Diagram 17](#_Toc450656017)

[3.3.4.1. Location of Environments and External Interfaces 18](#_Toc450656018)

[3.3.4.2. Conceptual Production String Diagram 20](#_Toc450656019)

[4. System Architecture 20](#_Toc450656020)

[4.1. Hardware Architecture 21](#_Toc450656021)

[4.2. Software Architecture 24](#_Toc450656022)

[4.3. Network Architecture 27](#_Toc450656023)

[4.4. Service Oriented Architecture/ESS 27](#_Toc450656024)

[4.5. Enterprise Architecture 27](#_Toc450656025)

[5. Data Design 28](#_Toc450656026)

[5.1. DBMS Files 28](#_Toc450656027)

[5.2. Non-DBMS Files 28](#_Toc450656028)

[5.3. Data View 28](#_Toc450656029)

[6. Detailed Design 29](#_Toc450656030)

[6.1. Hardware Detailed Design 29](#_Toc450656031)

[6.2. Software Detailed Design 29](#_Toc450656032)

[6.2.1. SAC Design 29](#_Toc450656033)

[6.2.1.1. Product Perspective 36](#_Toc450656034)

[6.2.1.1.1. User Interfaces 36](#_Toc450656035)

[6.2.1.1.2. Hardware Interfaces 36](#_Toc450656036)

[6.2.1.1.3. Software Interfaces 36](#_Toc450656037)

[6.2.1.1.4. Communications Interfaces 36](#_Toc450656038)

[6.2.1.1.5. Memory Constraints 36](#_Toc450656039)

[6.2.1.1.6. Special Operations 37](#_Toc450656040)

[6.2.1.2. Product Features 37](#_Toc450656041)

[6.2.1.3. User Characteristics 37](#_Toc450656042)

[6.2.1.4. Dependencies and Constraints 37](#_Toc450656043)

[6.2.1.4.1. Design Assumptions 37](#_Toc450656044)

[6.2.1.4.2. Design Constraints 38](#_Toc450656045)

[6.2.1.4.3. Design Trade-offs 38](#_Toc450656046)

[6.2.2. Specific Requirements 38](#_Toc450656047)

[6.2.2.1. Database Repository 38](#_Toc450656048)

[6.2.2.2. System Features 38](#_Toc450656049)

[6.2.2.3. Design Element Tables 39](#_Toc450656050)

[6.2.2.3.1. Routines (Entry Points) 39](#_Toc450656051)

[6.2.2.3.2. Templates 39](#_Toc450656052)

[6.2.2.3.3. Bulletins 39](#_Toc450656053)

[6.2.2.3.4. Data Entries Affected by the Design 39](#_Toc450656054)

[6.2.2.3.5. Unique Records 39](#_Toc450656055)

[6.2.2.3.6. File or Global Size Changes 39](#_Toc450656056)

[6.2.2.3.7. Mail Groups 39](#_Toc450656057)

[6.2.2.3.8. Security Keys 39](#_Toc450656058)

[6.2.2.3.9. Options 39](#_Toc450656059)

[6.2.2.3.10. Protocols 40](#_Toc450656060)

[6.2.2.3.11. Remote Procedure Call (RPC) 40](#_Toc450656061)

[6.2.2.3.12. Constants Defined in Interface 40](#_Toc450656062)

[6.2.2.3.13. Variables Defined in Interface 40](#_Toc450656063)

[6.2.2.3.14. Types Defined in Interface 40](#_Toc450656064)

[6.2.2.3.15. GUI 40](#_Toc450656065)

[6.2.2.3.16. GUI Classes 40](#_Toc450656066)

[6.2.2.3.17. Current Form 40](#_Toc450656067)

[6.2.2.3.18. Modified Form 40](#_Toc450656068)

[6.2.2.3.19. Components on Form 40](#_Toc450656069)

[6.2.2.3.20. Events 41](#_Toc450656070)

[6.2.2.3.21. Methods 41](#_Toc450656071)

[6.2.2.3.22. Special References 41](#_Toc450656072)

[6.2.2.3.23. Class Events 41](#_Toc450656073)

[6.2.2.3.24. Class Methods 41](#_Toc450656074)

[6.2.2.3.25. Class Properties 41](#_Toc450656075)

[6.2.2.3.26. Uses Clause 41](#_Toc450656076)

[6.2.2.3.27. Forms 41](#_Toc450656077)

[6.2.2.3.28. Functions 41](#_Toc450656078)

[6.2.2.3.29. Dialog 41](#_Toc450656079)

[6.2.2.3.30. Help Frame 42](#_Toc450656080)

[6.2.2.3.31. HL7 Application Parameter 42](#_Toc450656081)

[6.2.2.3.32. HL7 Logical Link 42](#_Toc450656082)

[6.2.2.3.33. COTS Interface 42](#_Toc450656083)

[6.3. Network Detailed Design 42](#_Toc450656084)

[6.4. Security and Privacy 42](#_Toc450656085)

[6.4.1. Security 42](#_Toc450656086)

[6.4.1.1. Security Policy Authoring 43](#_Toc450656087)

[6.4.1.2. Manage Access Control Policies 44](#_Toc450656088)

[6.4.2. Privacy 47](#_Toc450656089)

[6.4.2.1. Confidentiality of Sensitive Information 47](#_Toc450656090)

[6.4.2.2. Privacy of Personal Information 47](#_Toc450656091)

[6.4.2.3. Process Integrity 47](#_Toc450656092)

[6.4.2.4. System Availability 47](#_Toc450656093)

[6.5. Service Oriented Architecture (SOA)/ESS Detailed Design 47](#_Toc450656094)

[6.5.1. Service Description for AMS 48](#_Toc450656095)

[6.5.2. Service Design for SAC PDP 48](#_Toc450656096)

[6.5.2.1. Introduction 48](#_Toc450656097)

[6.5.2.1.1. Purpose and Scope of Service 48](#_Toc450656098)

[6.5.2.1.2. Links to Other Documents 48](#_Toc450656099)

[6.5.2.2. Service Details 48](#_Toc450656100)

[6.5.2.2.1. Service Identification 48](#_Toc450656101)

[6.5.2.2.2. Service Versions 49](#_Toc450656102)

[6.5.2.2.3. Summary of Design and Platform Details 49](#_Toc450656103)

[6.5.2.2.4. SOA Pattern(s) Implemented 49](#_Toc450656104)

[6.5.2.2.5. COTS Platform Vendor Names and Versions for Hosting Platform 50](#_Toc450656105)

[6.5.2.3. Dependencies 50](#_Toc450656106)

[6.5.2.4. Service Design Details 50](#_Toc450656107)

[6.5.2.4.1. Interface Technical Specs 50](#_Toc450656108)

[6.5.2.4.2. Service Invocation Type 50](#_Toc450656109)

[6.5.2.4.2.1. Service Interface Type 50](#_Toc450656110)

[6.5.2.4.3. Service Name 50](#_Toc450656111)

[6.5.2.4.3.1. Interface 51](#_Toc450656112)

[6.5.2.4.4. End Points 58](#_Toc450656113)

[6.5.2.4.5. Operations or Methods 58](#_Toc450656114)

[6.5.2.4.5.1. Message Schemas 58](#_Toc450656115)

[6.5.2.4.6. Information Model 61](#_Toc450656116)

[6.5.2.4.7. Class Diagram and Description of Entities Involved 61](#_Toc450656117)

[6.5.2.4.8. Mappings from ELDM to Standards Based Schemas 61](#_Toc450656118)

[6.5.2.4.9. Behavior Model (Use Case Realization) 61](#_Toc450656119)

[6.5.2.4.9.1. Use Cases (Use Case Model) 61](#_Toc450656120)

[6.5.2.4.9.2. Interaction Diagrams 62](#_Toc450656121)

[6.5.2.5. Gap Analysis 64](#_Toc450656122)

[6.5.2.5.1. Variances from Enterprise Target Architecture 64](#_Toc450656123)

[6.5.2.5.2. Variances from SLDs 64](#_Toc450656124)

[6.5.2.5.3. Variances from Standards and Policies 65](#_Toc450656125)

[6.5.2.5.4. Justification for Exceptions and Mitigation 65](#_Toc450656126)

[7. External System Interface Design 65](#_Toc450656127)

[7.1. Interface Architecture 65](#_Toc450656128)

[7.2. Interface Detailed Design 65](#_Toc450656129)

[8. Human-Machine Interface 65](#_Toc450656130)

[8.1. Interface Design Rules 65](#_Toc450656131)

[8.2. Inputs 66](#_Toc450656132)

[8.3. Outputs 66](#_Toc450656133)

[8.4. Navigation Hierarchy 66](#_Toc450656134)

[8.4.1. Screen Shots 66](#_Toc450656135)

[8.4.2. Application Screen Interface 66](#_Toc450656136)

[8.4.3. PAP Authoring Page 66](#_Toc450656137)

[Attachment A – Approval Signatures 68](#_Toc450656138)

[A. Additional Information 70](#_Toc450656139)

Table of Figures

[Figure 1: AcS 2.0 Overview 6](#_Toc450656553)

[Figure 2: SAC Application Context Diagram 7](#_Toc450656554)

[Figure 3: SAC High-Level Application Design 10](#_Toc450656555)

[Figure 4: XACML Policy Data Model 14](#_Toc450656556)

[Figure 5: XACML 3.0 Request Data Model 14](#_Toc450656557)

[Figure 6: XACML Response Data Model 15](#_Toc450656558)

[Figure 7: SAC Infrastructure Design 16](#_Toc450656559)

[Figure 8: Production Environment 18](#_Toc450656560)

[Figure 9: Logical Network String Diagram 20](#_Toc450656561)

[Figure 10: Network Communication Architecture 21](#_Toc450656562)

[Figure 11: Software Architecture 24](#_Toc450656563)

[Figure 12: SAC Detailed Design 30](#_Toc450656564)

[Figure 13: SAC PDP and AMS Integration 32](#_Toc450656565)

[Figure 14: Security Policy Authoring Sequence Diagram 43](#_Toc450656566)

[Figure 15: Manage Access Control Policies 44](#_Toc450656567)

[Figure 16: Enforce Access Control Decision Sequence Diagram 45](#_Toc450656568)

[Figure 17: Make Access Control Decisions Sequence Diagram 62](#_Toc450656569)

[Figure 18: Make Access Control Decisions (eHealth Only) Sequence Diagram 63](#_Toc450656570)

[Figure 19: SAC PAP Landing Page 67](#_Toc450656571)

List of Tables

[Table 1: Business Process 3](#_Toc450656572)

[Table 2: Significant Requirement Documents 4](#_Toc450656573)

[Table 3: Application Context Description: Objects 7](#_Toc450656574)

[Table 4: Interfaces External to OIT 8](#_Toc450656575)

[Table 5: Interfaces Internal to OIT 8](#_Toc450656576)

[Table 6: Externally Shared Data Stores 9](#_Toc450656577)

[Table 7: SAC Application Objects in the High-Level Application Design 11](#_Toc450656578)

[Table 8: Internal Data Stores 12](#_Toc450656579)

[Table 9: Solution Application Locations 13](#_Toc450656580)

[Table 10: Application Users 13](#_Toc450656581)

[Table 11: Hardware Appliance 22](#_Toc450656582)

[Table 12: Virtual Machines (VMs) and Appliances − SQA (AITC) 22](#_Toc450656583)

[Table 13: VMs and Appliances − Pre-Production (Terremark Culpeper, VA) 22](#_Toc450656584)

[Table 14: VMs and Appliances − Production (Terremark Culpeper, VA) 23](#_Toc450656585)

[Table 15: VMs and Appliances − DR (Terremark Miami, FL) 23](#_Toc450656586)

[Table 16: Port Communications and Protocols 24](#_Toc450656587)

[Table 17: Application Tier – Tomcat Application Server 25](#_Toc450656588)

[Table 18: Axiomatics 26](#_Toc450656589)

[Table 19: Programming Languages 26](#_Toc450656590)

[Table 20: Operating Systems 27](#_Toc450656591)

[Table 21: SAC Infrastructure Components 28](#_Toc450656592)

[Table 22: SAC Database File System 28](#_Toc450656593)

[Table 23: Memory Constraints 37](#_Toc450656594)

[Table 24: Data Points and Security 42](#_Toc450656595)

[Table 25: Security Policy Authoring 43](#_Toc450656596)

[Table 26: Manage Access Control Policies 45](#_Toc450656597)

[Table 27: Enforce Access Control Decision 46](#_Toc450656598)

[Table 28: RetrieveActiveVAHPAuthForSubjTargetReq.json Error! Bookmark not defined.](#_Toc450656599)

[Table 29: RetrieveActiveVAHPAuthForSubjTargetResponse.json Error! Bookmark not defined.](#_Toc450656600)

[Table 30: Service Identification 48](#_Toc450656601)

[Table 31: Service Versions 49](#_Toc450656602)

[Table 32: Service Name 50](#_Toc450656603)

[Table 33: PDP WSDL for Production 51](#_Toc450656604)

[Table 34: Entities 61](#_Toc450656605)

[Table 35: Make Access Control Decisions 62](#_Toc450656606)

[Table 36: Make Access Control Decisions Using XACML 2.0 Request/Response 63](#_Toc450656607)

[Table 37: System Identification 70](#_Toc450656608)

[Table 38: Applicable Policies, Directives, and Procedures 71](#_Toc450656609)

# Introduction

The Specialized Access Control (SAC) Service is designed to provide an enterprise-wide capability for enforcing dynamic fine-grained attribute-based access control (ABAC). Software services in need of such access control behavior can benefit by consuming this standards based enterprise service, as opposed to one that is natively implemented.

SAC is an Identity and Access Management (IAM) Authorization service that provides the ability to receive requests for access to VA services and return a decision to permit or deny access, based on evaluation of attributes applicable to each request under governance of access control policies. In this context, examples of attributes might include patient preferences, provider roles, organizational responsibilities, geographies, etc. SAC provides a granular policy-based access decision service to future services capable of consuming them.

## Scope

This section establishes boundaries of the IAM AcS SAC SDD. The [IAM AcS Business Requirements Document (BRD) in the Technical Service Project Repository (TSPR)](http://xxxxxxxxxxxxxx/warboard/anotebk.asp?proj=1803&Type=Active#Documentation) lists the governing business needs and features for SAC.

VDT will be integrated with SAC for PR authorization decisions and SAC PDP will use the custom PIP’s to access the data/attributes required by PDP for policy decisions.

The scope also considers a SR from MHV for authorization decisions.

## User Profiles

The SAC service is not consumed by an end user, but rather by other services requiring access control. Privileged users, such as employees, contractors, etc., are given roles such as admins, who can perform administrative tasks using SAC Axiomatics Services Manager (ASM) and Policy Decision Point (PDP) graphical user interfaces (GUI) to include operations, maintenance, and deployment. SAC GUIs (Policy Access Point [PAP]) also allows for privileged users to create and deploy policies.

# Background

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

Many VA services 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 services 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 services at the VA. The SAC PDP Service is designed to provide an enterprise-wide capability for enforcing dynamic fine grained ABAC. Software services 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.

## Overview of the System

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

* **PDP**: A XACML 3.0 policy evaluation engine that receives authorization decision requests from the consuming service PEPs. The PDP evaluates these requests against organizational, patient policies/attributes, and other authorization attributes and renders an authorization decision.
* **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 Virtual Lifetime Electronic Record (VLER)/eHealth service called VAP.
* **Authorization Attributes**: These could be passed in by the consuming service PEP and/or integrated into a PIP that the PDP can access. The various types of Authorization attributes include the following:
* 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: Attributes that reflect entitlements for the business transaction requiring protection
* Contextual Constraints: Attributes inherent in the environment; such as location, time, day of week, etc.

SAC events are captured for auditing and reporting purposes through the integration with CAR service.

## Overview of the Business Process

The capability to manage access to systems, services, 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. SAC will help centralize multi-dimensional fine grained Privacy and Security Policies that can secure numerous services across multiple lines of business from unauthorized access.

Numerous VA services rely on locally implemented security mechanisms to control and provide access to resources and information. These approaches result in proliferation of home grown service specific access services leading to lack of governance, uniformity and standardization across the enterprise. This increases overhead on service owners to maintain security controls. Additionally, this approach has been found to have inherent weaknesses and can be susceptible to exploitation. New and existing services will be required to evolve their current identification, authentication, authorization, and audit capabilities to support both anticipated and unanticipated VA service stakeholders (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). As the VA continues to realize the importance of information sharing and protection to the successful delivery of Veteran services and enterprise security, it is critical that VA services leverage its access control mechanism that is standards based and enterprise scope with requisite course and mechanisms fine-grained control levels necessary to protect valuable information assets.

SAC enables the provision of policy-based fine grained access control decision support through its core capability, the PDP. The benefits of the Service are discussed in Section 2.3.

The critical components of policy-based decision support capability, the attributes themselves, are currently passed in to SAC by the requesting services. In the future, these attributes would also be accessible through authoritative sources that are linked in to the SAC VDS PIP framework.

Table : Business Process

| Business Process ID | Business Process Name | Type | Owner | Description |
| --- | --- | --- | --- | --- |
| 1 | [*xxxxxxx*](http://xxxxx/warboard/ProjectDocs/Access_Services/VA_IAM_SAC_Use_Case_Model.pdf) | SAC Use Cases and Use Case Model | PD OIT | Use Cases to support SAC System |
| 2 | [*xxxxxxxxxxt*](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/VA_AcS_2.0_i2_Solution_UC_Model_SAC.pdf) | Use Cases | PD OIT | Use Case Model Document |
| 3 | [*xxxxxxxxxx*](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/AcS_i4_Use_Case_Model.pdf) | Use Cases | PD OIT | i4 Use Cases |
| 4 | [*xxxxxxxxxxx*](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/SAC_Enforce_Access_Control_Decision_Use_Case.pdf) | Use Case | PD OIT | Enforce Access Use Case |
| 5 | [*xxxxxxxxxxx*](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/SAC_Generate_Access_Control_Decision_Use_Case.pdf) | Use Case | PD OIT | Generate Access Use Case |
| 6 | [*xxxxxxxxxxx*](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/SAC_Manage_Access_Control_Policies_Use_Case.pdf) | Use Case | PD OIT | Manage Access Use Case |
| 7 | [*xxxxxxxxxxx*](http://tspr.vista.med.va.gov/warboard/ProjectDocs/Access_Services/SAC_Obtain_Attributes_Use_Case.pdf) | Use Case | PD OIT | Obtain Attributes Use Case |

For additional information, refer to the Requirements Specification Document (RSD) on the [TSPR](http://xxxxxxxxxxxxxxxx/warboard/anotebk.asp?proj=1803&Type=Active).

## Overview of the Significant Requirements

This version of the SDD meets the high-level requirements described in the following documents.

**Note:** There are no significant functional requirements being implemented for SAC in i7.

Table : Significant Requirement Documents

| Document | Content Description | Location |
| --- | --- | --- |
| AcS Business Requirements Document (BRD) | Identifies the business needs of the customer/business owner; stakeholders; and an overview of the request requirements, constraints, and Information Technology (IT) options considered | [xxxxxxxx](http://tspr.vista.med.va.gov/warboard/anotebk.asp?proj=1803&Type=Active) |
| i7 AcS Requirements Specification Document (RSD) | Summarizes the business and functional requirements that are required for the development and implementation of AcS 2.0 i7. | xxxxxxxxxx |
| SAC Functional Requirements | Overview of significant functional requirements |  |
| SAC Workload/Performance Requirements | Overview of the functional workload/performance requirements |  |
| SAC Operational Requirements | Overview of operational requirements |  |
| SAC pivotal technical requirements | Overview of pivotal technical requirements |  |
| SAC Security and Privacy Requirements | Overview of the security and privacy requirements |  |
| SAC Availability Requirements | Overview of system criticality and high availability requirements |  |
| SAC Single Sign On (SSO) Requirements | Overview of SSO requirements |  |
| SAC Enterprise Portals Use | Overview of use of enterprise portals |  |
| SAC Special Device Requirements | Overview of special device requirements |  |

# Conceptual Design

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

* Conceptual Application Design
* Conceptual Data Design
* Conceptual Infrastructure Design

## Conceptual Application Design

This section provides the conceptual design of the SAC service. There are no design updates within i7 to support SAC.

The overall AcS design is shown in Figure 1, below.

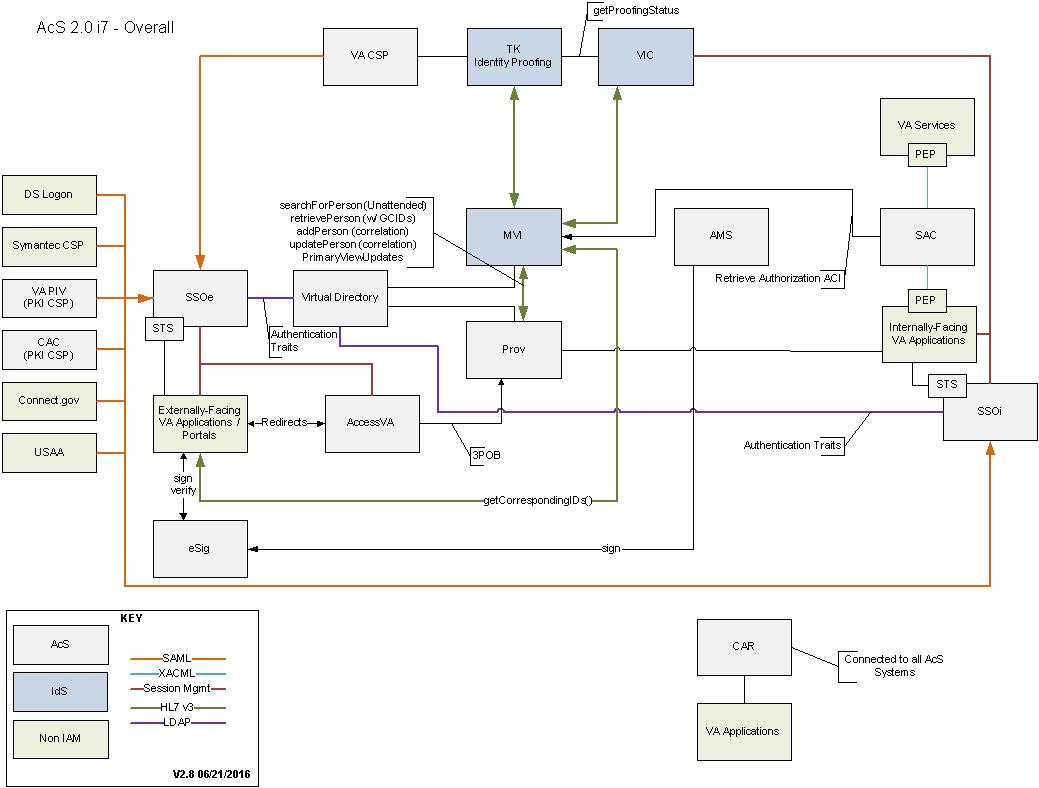


Figure : AcS 2.0 Overview

### Application Context

SAC offers an enterprise level ABAC 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 services

The following figure is the application context diagram for SAC.



Figure : SAC Application Context Diagram

Table : Application Context Description: Objects

| ID | Name | Description | Interface Name | Interface System |
| --- | --- | --- | --- | --- |
| 1 | eHealth/VAP | eHealth sends XACML 2.0 request to SAC for an access control decision | SAC PDP | eHealth VAP |
| 2 | AcS/AMS | SAC will now have the ability to obtain Authorization (Delegation) information from an information point such as AMS. It is shown in dashed line because there is no consumer yet. This information will not be accessed and utilized to support the PDP for generating access control decisions for eHealth | AMS Service | AMS |
| 3 | AcS/CAR | Auditing and Reporting Service – SAC PDP interactions with consumers (eHealth/VAP) are captured in log files | CAR Web Agent deployed on PDP Server | CAR |

Table : Interfaces External to OIT

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Interface Name | Related Object | Input Messages | Output Messages | External Party |
| N/A | N/A | N/A | N/A | N/A | N/A |

Table : Interfaces Internal to OIT

| ID | Name | Related Object | Input Messages | Output Messages | External Party |
| --- | --- | --- | --- | --- | --- |
| 1 | SAC PDP | eHealth/VAP | XACML 2.0 request containing authorization attributes derived from the SAML token on the eHealth Exchange along with patient consent from VAP | XACML 2.0 message indicating Permit or Deny | eHealth/VAP |
| 2 | AMS Service | SAC/PDP | REST/JSON request to retrieve an authorization (delegation) relationship between a Veteran and a Delegate | REST/JSON payload with ACI pertinent to the authorization (delegation) between Veteran and delegate | AcS/AMS |
| 3 | CAR Web Agent deployed on PDP Server | CAR Agent | Audit Record Query | Audit Records (See Schema in Section 5) | AcS/CAR |

Table : Externally Shared Data Stores

| ID | Name | Data Stored | Owner | Access |
| --- | --- | --- | --- | --- |
| N/A | N/A | N/A | N/A | N/A |

### 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 VAP is a live service that consumes SAC access control decisions to enforce data sharing constraints, during eHealth transactions between VA and its partners and as such, provides a high-level application design for SAC. Additionally, it identifies interactions with its subcomponents, activities, and/or relationships with VA applications.

SAC is wired to the Authorization Management System (AMS) and will support decision generation for theconsumer. The Policy governing eHealth decision generation does not require evaluation of authorization ACI from AMS.



Figure : SAC High-Level Application Design

Table : SAC Application Objects in the High-Level Application Design

| Name | ID | Description | Service or Legacy Code | External Interface Name | External Interface ID | Internal Interface Name | Internal Interface ID | SDP Sections 1&2 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Policy Administration Point | 1 | An application for managing policies used by the policy decision point | No | N/A | N/A | PAP | N/A | Approved |
| Policy Store | 2 | Maintains organizational policies and policy sets with the intent of making them available to the PDP | No | N/A | N/A | PDP server | N/A | Approved |
| Policy Decision Point | 3 | Component responsible for evaluating inbound XACML Request to Master Policy.  Transforms Policy Evaluation results to XACML response | No | AMS Service (to obtain Authorization ACI) | N/A | PDP Server | N/A | Being Developed |
| Policy Decision Point | 3 | Component responsible for evaluating inbound XACML Request to Master Policy.  Transforms Policy Evaluation results to XACML response | No | PDP to CAR via agent | N/A | Policy Store on ASM server, Request/Response to DataPower. | N/A | Approved |
| XACML 2.0-3.0 Transformer | 4 | Entry point for all authorization decisions required by EHealth | No | XACML <Request/Response> to eHealth |  | Request/Response to PDP | N/A | Approved |

Table : Internal Data Stores

| Name | ID | Data Stored | Steward | Access |
| --- | --- | --- | --- | --- |
| Log |  | Internal Log file that audits each application object functions | N/A – Internal to DataPower appliance | Write |

### Application Locations

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

Table : 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 PDP. | Terremark Culpeper, VA (Primary)  Terremark Miami, FL (Disaster Recovery) |  |
| Axiomatics PDP | PDP for fine-grained authorization decision requests. | Terremark Culpeper, VA (Primary)  Terremark Miami, FL (Disaster Recovery) |  |

Table : Application Users

| Application Component | Location | User |
| --- | --- | --- |
| SAC PAP | Internal to VA | AcS SAC Admin User |
| SAC ASM | Internal to VA | AcS SAC Admin User |
| SAC PDP | Internal to VA | AcS SAC Admin User |

## Conceptual Data Design

SAC is based on a COTS product; refer to the applicable Axiomatics documentation for Data Model information. Shown below are XACML 3.0 models for policies stored in SAC along with Messaging models.

### Project Conceptual Data Model

SAC is based on a COTS product. Please refer to Axiomatics documentation on their data model.

The policies that can be stored in SAC (Axiomatics store) should correspond to the XACML 3.0 model shown below.

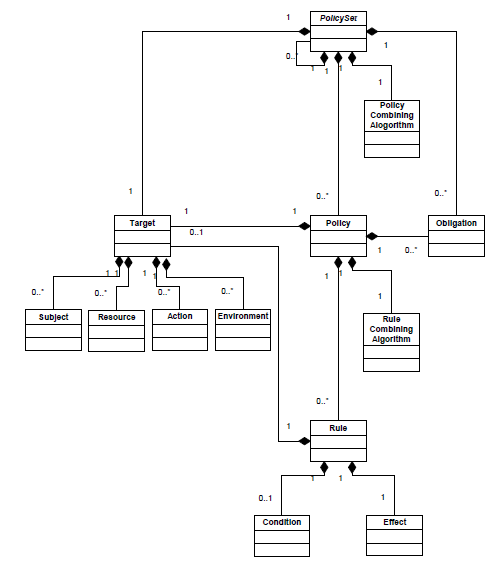


Figure : XACML Policy Data Model

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

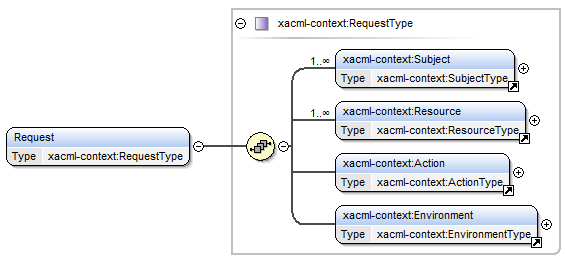


Figure : XACML 3.0 Request Data Model

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

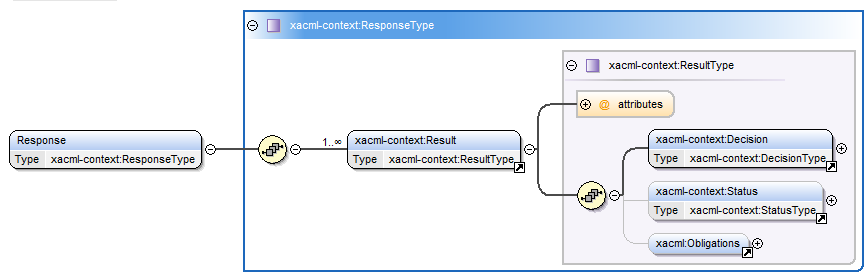


Figure : XACML Response Data Model

### Database Information

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

### User Interface Data Mapping

SAC is based on a COTS product; therefore, there are no custom user interfaces (UIs).

#### Application Screen Interface

N/A

#### Application Report Interface

N/A

#### Unmapped Data Element

N/A

## Conceptual Infrastructure Design

The SAC PDP is a web service that serves as the core engine for generating fine-grained access control decisions. This section provides the technology components and infrastructure needed to implement the SAC PDP Service.

The PDP will be hosted in a Tomcat Container utilizing JRE version 1.7/Java 7 Update 45. The PDP is front-ended by a co-deployed web service, a custom built Context Handler that offers backwards compatibility by accepting XACML 2.0 messaging. Tomcat web containers themselves will be deployed on virtual machines running RHEL 5.3 or Windows Server 2008 R2. Access to the context handler (and PDP) is secured using the IBM DataPower XML Gateway.

The PDP is a COTS service offered by Axiomatics Corporation. This product is managed by the ASM, yet another web service deployed on Tomcat. ASM maintains its processing data such as XACML policies, PDP configurations and Attribute configurations in an Oracle Database. The Oracle Database is in a RAC cluster.

Transactions processed by the PDP are captured within log files on the filesystem. A software called CAR Web Agent monitors the filesystem for event data and relays it to the CAR system for compliance auditing and monitoring.



Figure : SAC Infrastructure Design

### System Criticality and High Availability

The VA AcS infrastructure supports critical business systems. The current availability requirement for mission critical systems is 99.99%. The current data center Service Level Agreement (SLA) with Terremark supports 99.9% availability. Terremark hosts the Production, Pre-Production, and Disaster Recovery (DR) Data Centers in Culpeper, VA, and Miami, FL. Terremark currently does not support an active/active geographic failover and load balancing; thus, failover to the DR site could take between one and eight hours.

**Note:** The 99.9% availability does not include scheduled maintenance for patches, software updates, and related activities.

Terremark does not currently support an active/active geographic failover and load balancing thus failover to the DR site could take between one and eight 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 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, are functions of the hosting facility, Terremark, and the data center operations team. Backups are described more fully in the [Production Operations Manual (POM)](http://xxxxxxxxxxxx/warboard/anotebk.asp?proj=1653&Type=Active), 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

### Special Technology

N/A

### Technology Locations

Refer to Section 3.3.4.1 for technology locations.

### Conceptual Infrastructure Diagram

This section focuses on the primary environments where the SAC service is deployed. It also depicts a diagrammatic representation of SAC infrastructure components in production.

#### Location of Environments and External Interfaces

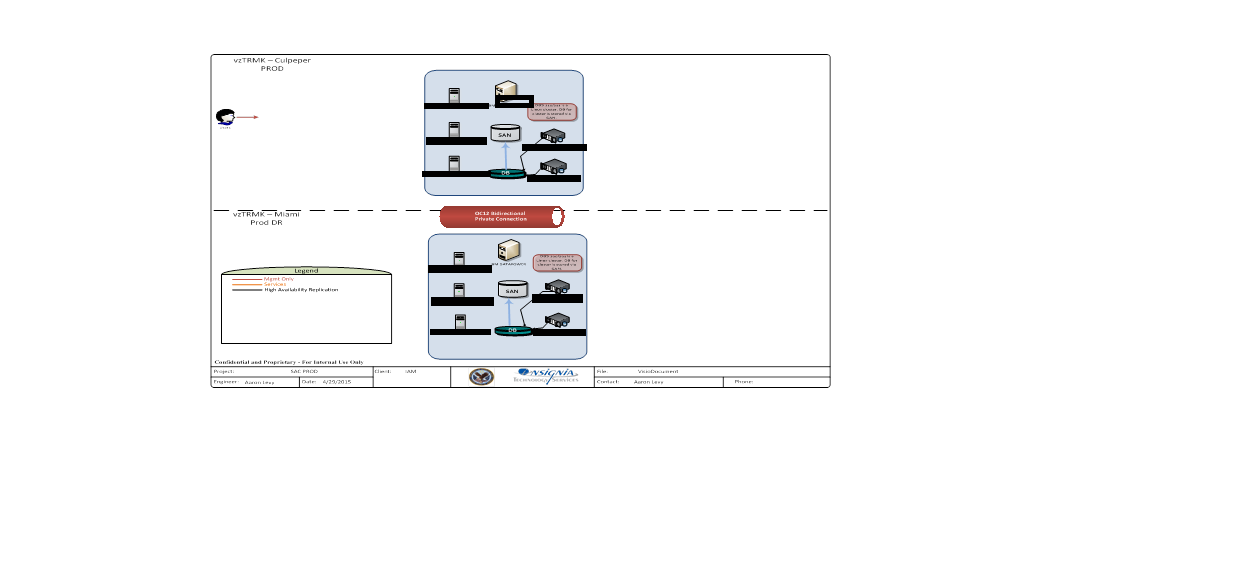


Figure : Production Environment

**Integration Environment (INT) AITC – Austin, TX**

* This is a new environment utilized by the Development team for initial development of service enhancements, 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 services and operating service 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

**Partner Integration Environment (PINT) AITC – Austin, TX**

* This is an old development environment (DEV) which will be repurposed to be utilized by the ACS Partners for initial development of service enhancements, integrations with consuming services, defect resolution, and partner unit testing. This decision was made to limit the impact to the ACS partners who were utilizing the old DEV environment.
* This is a loosely controlled environment for the AcS developers and partners to use. The development team implements and maintains the COTS products, COTS patches, and code.
* System administrators maintain the operating services and operating service patches
* 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 services 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 services 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 SAC 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 one second

#### Conceptual Production String Diagram

Figure 9 depicts a string diagram of the SAC components in production.



Figure : Logical Network String Diagram

# System Architecture

The SAC service architecture includes the hardware, software, and communication architectures. The hardware architecture describes the physical components needed in the service 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.

## Hardware Architecture

The following diagram,

Figure 10, shows the AcS 2.0 hardware architecture and network topology. At a high level, as with other AcS Components, SAC is deployed across two sites to account for DR, per an Active-Passive topology – Terremark, Culpeper, VA serving as the Active/Hot site and Terremark, Miami, FL, serving as the Passive/Warm site.

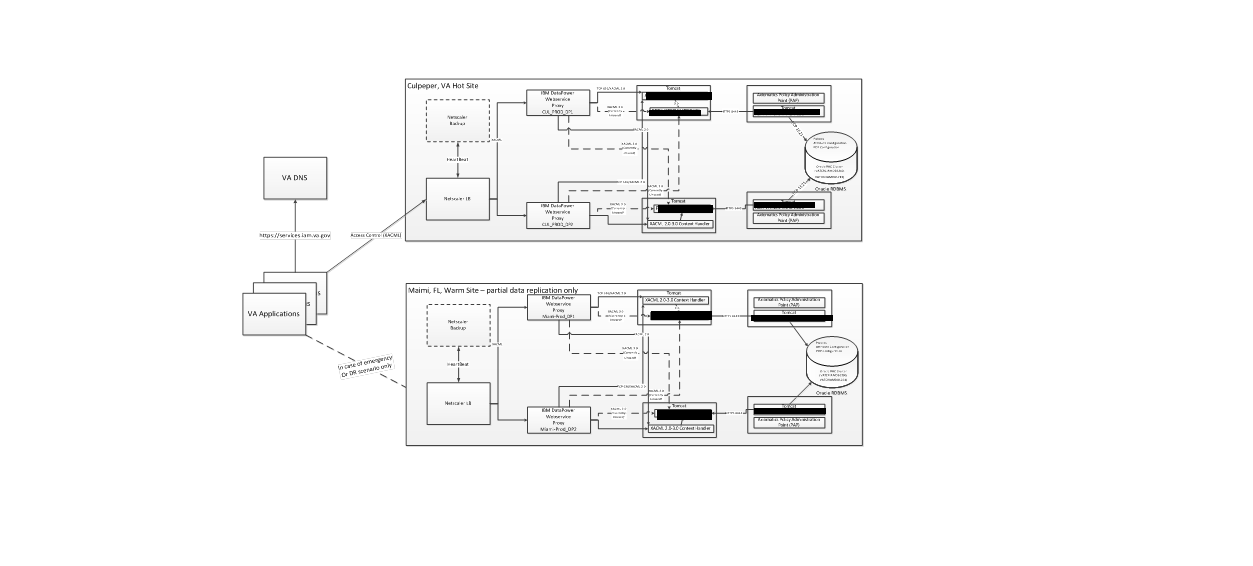


Figure 10: Network Communication Architecture

AcS SAC hardware infrastructure components at each of the sites are tabulated below.

Table : Hardware Appliance

| Hardware Appliance | Descriptions | High Availability (HA) |
| --- | --- | --- |
| IBM DataPower | A critical component of the AcS infrastructure that serves as a secure message proxy for SAC PDP (and Context Handler) web Services. This is the first integration touch point for consuming services accessing SAC | For High Availability configuration, the DataPower XI52 (X150 for DEV and SQA) 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.  **Note:** SAC has no components residing in the DMZ. |

The underpinning technology components for SAC (Axiomatics PDP, Axiomatics ASM, and PAP) are deployed on VMs identified by hostnames and are depicted in the following tables.

Table : Virtual Machines (VMs) and Appliances − SQA (AITC)

| Application | # of VMs | # of Physical Servers | Hostname |
| --- | --- | --- | --- |
| Oracle 11gR2 | 0 | 2 | xxxxx  xxxxx |
| Axiomatics PDP  (Tomcat) | 1 | N/A | xxxxx |
| Axiomatics ASM  (Tomcat)  Axiomatics PAP  (Java Application) | 1 | N/A | xxxxx |
| Axiomatics Policy Auditor | 1 | N/A | xxxxx |

Table : VMs and Appliances − Pre-Production (Terremark Culpeper, VA)

| Application | # of VMs | # of Physical Servers | Hostname |
| --- | --- | --- | --- |
| Oracle 11gR2 | 0 | 2 | xxxxx  xxxxx |
| Axiomatics PDP  (Tomcat) | 2 | N/A | xxxxx  xxxxx |
| Axiomatics ASM  (Tomcat)  Axiomatics PAP  (Java Application) | 1 | N/A | xxxxx |

Table : VMs and Appliances − Production (Terremark Culpeper, VA)

| Application | # of VMs | # of Physical Servers | Hostname |
| --- | --- | --- | --- |
| Oracle 11gR2 | 0 | 2 | xxxxx  xxxxx |
| Axiomatics PDP  (Tomcat) | 2 | N/A | xxxxx  xxxxx |
| Axiomatics ASM  (Tomcat)  Axiomatics PAP  (Java Application) | 1 | N/A | xxxxx |

Table : VMs and Appliances − DR (Terremark Miami, FL)

|  |  |  |  |
| --- | --- | --- | --- |
| Application | # of VMs | # of Physical Servers | Hostname |
| Oracle 11gR2 | 0 | 2 | xxxxx  xxxxx |
| Axiomatics PDP  (Tomcat) | 2 | N/A | xxxx  xxxx |
| Axiomatics ASM  (Tomcat)  Axiomatics PAP  (Java Application) | 1 | N/A | xxxx |

The following table lists the ports and protocols for SAC components.

Table : Port Communications and Protocols

| Application | Network | Port(s) | Reason | Protocol(s) |
| --- | --- | --- | --- | --- |
| Oracle | Internal | xxxx | DB Connector | SQL |
| Axiomatics | Internal | xxxx | HTTPS Connector Port | TLS |
| Axiomatics | Internal | xxxx | HTTP Connector Port | HTTP |
| Axiomatics | Internal | xxxx | AJP Connector Port | TCP |
| Axiomatics | Internal | xxxx | Server Shutdown Port | TCP |

## Software Architecture

The following diagram shows the complete software architecture for SAC.



Figure 11: Software Architecture

Shown above is a 3-tier perspective of the SAC software architecture. The SAC service tier (presentation and middle tiers) is constituted primarily by Axiomatics, a COTS product suite. The only custom component built by IAM is the context handler that facilitates transformation between XACML 2.0 and 3.0 and supports backward compatibility with the eHealth Exchange, SAC’s current consumer. The Application tier is further elaborated below and in Table 17.

The application tier for the SAC service is comprised of Tomcat application servers. The Application Tier is a shared environment for hosting service components. The SAC related services hosted are listed below. The Axiomatics PDP and ASM components are hosted on the Tomcat application servers. The Axiomatics PAP is a standalone Java application.

The AMS application is shown as a part of the SAC software architecture in its integration tier. There is a XACML policy within SAC which references AMS for Personal Representative authorization. AMS/MVI data store is solicited as a policy information point for Authorization ACI. In addition, there are policies for eHealth/VAP authorization currently and MHV delegation authorization in the near future.

Table : Application Tier – Tomcat Application Server

| 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 Citrix NetScaler. Each TCP connection will be alternated between application nodes without a sticky bit. Each connection is stateless. |

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

Table : Axiomatics

| Characteristic | Description |
| --- | --- |
| **Subcomponents** | **ASM:** Service for managing an Axiomatics Policy Server (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.  **PDP:** 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.  **PAP:** Development environment for XACML 3 policies is used in the Axiomatics authorization infrastructure. Provides Java based 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.  **Policy Auditor:** Simplifies the analysis and validation process of XACML policies. Provides a user-friendly web-based graphical interface. |
| **High Availability** | The PDPs are stateless and will use the Citrix NetScaler for high availability. |

Context Handler: This is an IAM AcS SAC custom component that serves as a transformer between XACML 2.0 and XACML 3.0 messaging. It is deployed as a servlet on Tomcat. It receives 2.0 messages from eHealth/VAP and, after transformation to 3.0, redirects them to the PDP. On the return path, a 3.0 response from the PDP is transformed down to 2.0 and then shared with the eHealth PEP.

The following table lists the programming languages used within SAC.

Table : Programming Languages

| Programming Languages | Definition/Description |
| --- | --- |
| Java | Java language was used to develop the custom context handler servlet |
| XML (XACML) | Security and Privacy Policies authored via the PAP are stored as XACML files |

Axiomatics uses a relational repository to store attribute and PDP configuration and XACML3.0 based Security and Privacy Policies. The Relational repository is Oracle-based.

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.

For the AcS 2.0, database high availability is critical. A database outage can cause a multitude of errors to occur on the service side, thereby nullifying the high availability configurations on the service itself. It was planned for Raw Devices to be utilized by Oracle Automatic Storage Management (ASM) file service, working as the volume manager, overseeing the clusterware file services. 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 service storage, mirroring is needed to provide high availability.

The operating services on the Production SAC components are listed below:

Table : Operating Systems

| Operating System | VM/Physical | Purpose |
| --- | --- | --- |
| Windows Server 2008 R2 | VM | Axiomatics |
| Red Hat Enterprise Linux 5.3 | Physical Machines | Oracle RAC Databases |

## Network Architecture

Please refer to Section 4.1 for Hardware/Network architecture.

## Service Oriented Architecture/ESS

SAC offers an enterprise level 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 is the PDP which 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 (eHealth/VAP), the service itself is inherently agnostic to the consumer's domain and could be leveraged within other SOA contexts.

SAC will initiate communication to MVI to get authorization information.

## Enterprise Architecture

SAC is a technical service that offers an enterprise level ABAC capability to generate fine-grained access control decisions. The SAC PDP protects business services and information assets from unauthorized access based on user attributes and, resources and contextual constraints under purview of organization and individual security and privacy policies.

The SAC technical service is based on a One-VA TRM approved products and specifications tabulated below.

Table : SAC Infrastructure Components

| Products/Specifications | Abbreviation | Product Version/Release |
| --- | --- | --- |
| Axiomatics PDP | PDP | 5.34 |
| ASM | ASM | 5.34 |
| Axiomatics PAP | PAP | 5.34 |
| Axiomatics Policy Auditor | APA | 1.1.3 |
| Apache Tomcat | Web Container | 7.0.42 |
| Oracle | RDBMS | 11.0gR2 |
| Windows |  | 2008 Server R2 |
| DataPower |  | X150/X152 |
| XACML |  | 3.0 |

PreProd and Prod PKI Certificates can be found in the [POM](http://xxxxxxxxxxxx/warboard/ProjectDocs/Access_Services/AcS_2.0_i4_Production_Operations_Manual.pdf).

# Data Design

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

## DBMS Files

SAC uses Oracle 11gR2 Database for persistent data storage.

Table : SAC Database File System

| Table Spaces | Data Files |
| --- | --- |
| SACASM\_DATA | +ORADATA/acsdbs/datafile/sacasm\_data |

## Non-DBMS Files

SAC does not use Non-DBMS files.

## Data View

N/A

# Detailed Design

## Hardware Detailed Design

The sections below provide the hardware information for the SAC service. The Server Planning Sheets display the sizing, network, OS, and number of VMs required to be deployed for SAC:

[http:/xxxxxxxxxxxxxxxxxsites/vrm/IAM/IAM%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fvrm%2FIAM%2FIAM%20Documents%2FIAM%20Development%20Documentation%2FByLight%20%2D%20AcS%20Development%20Integration%20i7%2F5%2E4%2E3%2E1%20Solution%20Design%2FUpdated%20Server%20Planning%20Sheets&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence](http://xxxxxxxxxxxxxxxxxsites/vrm/IAM/IAM%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fvrm%2FIAM%2FIAM%20Documents%2FIAM%20Development%20Documentation%2FByLight%20%2D%20AcS%20Development%20Integration%20i7%2F5%2E4%2E3%2E1%20Solution%20Design%2FUpdated%20Server%20Planning%20Sheets&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence)

The DataPower is a hardened appliance, already provisioned with an operating system, CPU, memory, and network interfaces. No hardware configuration is required.

## Software Detailed Design

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

### SAC Design

Numerous services at VA currently have native and proprietary mechanisms for access control. Proliferation of such access control mechanisms is onerous for those services and non-standard from an enterprise perspective, not to mention they add risk to the enterprise. Certain VA services have the additional need for more granular or specialized access controls. The SAC service addresses these concerns by offering an enterprise scoped dynamic fine-grained access control service that evaluates Privacy and Security Policies at runtime against subject, resource, transaction, and contextual authorization attributes, effectively protecting integrated services and data.

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



Figure 12: SAC Detailed Design

SAC leverages the capabilities of Axiomatics and DataPower products to minimize software development. The basic components of Axiomatics are the PEP, PDP, APA, ASM, and PAP. The Radiant Logic product shown is Virtual Directory (VDS) that could serve as the virtual 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 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 service 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 service hosting the PAP tool at the Windows OS level in order for them to be able to use it.

**Axiomatics**

* **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 SDK provided by Axiomatics, and may be implemented in the future. Currently, SAC expects consuming services to implement their own PEPs. The PEPs must conform to XACML 3.0 in order to integrate with the SAC enterprise PDP.
* **PDP:** 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 service requests
* **PAP:** A stand-alone Java service providing a full-featured graphical XACML 3.0 policy editor. The PAP is used in the SAC service 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.
* **ASM:** A web based service 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.
* **APA:** A web-based service 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.
* **Authorization Management System (AMS) PIP:** A PIP is a source of authoritative information attributes that can be consumed by the PDP during policy evaluation. Numerous PIPs can be integrated through the VDS product (a single virtual PIP) for consumption by the PDP. For i7, AMS, which manages Authorization (Delegation) ACI for Veterans, is exposed as a REST/JSON based PIP. It is currently consumed directly and not through VDS. In order to connect with AMS (or any REST service), two custom connectors have been developed – an Http Connector and a JSON Parser Connector.
  + HTTP connector: Can be configured to send an HTTP request (either GET or POST) to a remote service. It then receives the response which it returns as an attribute to the PDP. The SAC PDP sends a REST/POST/JSON request through this Connector to the AMS Service and obtains a JSON response payload that is referenceable by the attribute “pip.payload”. Please see Section 6.5.1 for messaging between the SAC PDP and AMS PIP.
  + The JSON parser connector: Takes in a JSON response payload and uses JSONPath to extract different values from the payload “pip.payload”. Upon receiving a response from AMS, the SAC PDP dereferences to it to extract ACI attributes (delegation status) that help with Policy Evaluation.

Shown below is the architecture depicting the SAC PDP and AMS PIP integration using the aforementioned connectors. In the diagram MHV has been referenced as a notional consumer PEP for the moment. The real consumer/PEP, possibly MHV, requiring policy evaluation using Authorization ACI, would be integrated in the near future.



Figure : SAC PDP and AMS Integration

The configuration aspects of these connectors are summarized below and elaborated further in the SAC PDP deployment guide.

* HTTP Connector key configuration aspects are:
  + - Endpoint URL to resource, in this case, AMS Retrieve Delegation Resource. Section 6.5.1 has the endpoint URL
    - Mapping elements that correspond to response attributes being requested by the PDP from the resource. In this case, the requested attribute is called ‘pip.payload’ which is an attribute to identify the entire response message from AMS.
    - Reference to a request template that contains placeholders for attributes passed in from the PEPs. The template name has been configured to be deployed in the PDP engine’s classpath.

Shown below is the request template for the AMS Resource:

{

"authorization": {

"status": "Active",

"subject": {

"identifier": {

"valueRoot": "@var1",

"valueExtension": "@var2",

"type": "@var3"

}

},

"target": {

"identifier": {

"valueRoot": "@var4",

"valueExtension": "@var5",

"type": "@var6"

}

},

"authorizationType": {

"events": [{

"type": "Create",

"Preferences": [{

"type": "@var7",

"value": "@var8"

}]

}],

"value": "@var9"

}

},

"requestInitiatedBy": {

"system": {

"id": "IAM-AcS-SAC-PDP",

"name": "IAM AcS SAC PDP"

},

"organization": {

"id": "urn:oid:2.16.840.1.113883.4.349",

"name": "Department of Veterans Affairs"

}

}

}

* + - Key elements that correspond to values extracted from the XACML request from the PEP that will complete the request template:

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" AttributeId="subject.identifier.itype" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" AttributeId="subject.identifier.valueRoot" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject" AttributeId="subject.identifier.valueExtension" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" AttributeId="target.identifier.itype" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" AttributeId="target.identifier.valueRoot" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" AttributeId="target.identifier.valueExtension" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" AttributeId="authorizationType.value" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" AttributeId="authorizationType.value.preferences.itype" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

<key>

<xacmlAttribute Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource" AttributeId="authorizationType.value.preferences.value" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer=""/>

</key>

* JSON Parser Connector. Key aspects of this configuration entail:
  + - Payload Elements that correspond to response that has been returned from the PIP. In this case, the requested attribute is called ‘pip.payload’ which is an attribute to identify the entire response message from AMS
    - An expression element, which contains a valid JSON Path expression as defined by Stefan Goessner. It has currently been configured to $.authorizations[0].status to extract the delegation status from the response
* **SAC Policies:**
* Policies are evaluated by PDP in response to access control decision requests from the PEP.

In production, the live policy is to support the VLER initiative and the eHealth Exchange. Shown below is the relevant policy

* A Sample delegation policy has also been incorporated within the PDP. This policy is evaluated when the notional MHV PEP reaches out to the SAC PDP, which in turn obtains ACI from the AMS PIP. Shown below is the relevant policy
* **Sample PR Delegation policy**

**TBD**

#### Product Perspective

SAC is an enterprise scoped service offering that is available for VA business services to leverage to protect itself and its information assets from unauthorized access. SAC is based on the OASIS XACML specification for attribute based access control. The primary benefit of using ABAC, and consequently SAC, is that access control is dynamically established based on authorization attributes associated with the requestor, resource or the environment, under governance of Privacy and Security Policies. This is a divergence from the traditional RBAC approach where users are statically provisioned roles and entitlements for access to resources.

##### User Interfaces

SAC is based on a COTS product. Refer to Axiomatics documentation for information on SAC GUIs.

##### Hardware Interfaces

SAC is a software offering and does not offer any hardware interface.

##### Software Interfaces

The primary software interface is the SOAP/HTTPS based PDP web service for fine-grained access control that works with OASIS XACML payloads. Refer to Section 6.5.2 for details for the software architecture and interfaces of SAC.

##### Communications Interfaces

SAC is a software offering and is available for consumption by VA services using the HTTPS protocol. It does not offer any other communication interfaces.

##### Memory Constraints

The established memory constraints for deployment of the Axiomatics product suite are shown in Table 23.

Table : Memory Constraints

|  | xxxx | xxxxx | xxxx |
| --- | --- | --- | --- |
| Stack | Not Set | Not Set | Not Set |
| Heap Space | 2883 MB | 2883 MB | 2883 MB |
| JVM Config for Axiomatics | 3072 MB | 3072 MB | 3072 MB |

##### Special Operations

N/A

#### Product Features

The key feature of SAC is the PDP webservice. This is a policy decision service that offers access control decisions generated by evaluating authorization attributes from numerous authoritative sources against enterprise privacy and security policies.

#### User Characteristics

The SAC System does not have a front-end for enduser. It has management front ends for the AMS and PDP applications. SAC also offers a product called PAP which is used for authoring policies. PAP users are also typically IAM SAC Admins.

#### Dependencies and Constraints

N/A

##### Design Assumptions

* SAC has a High Service Baseline for Confidentiality, Integrity, and Availability
* The XACML 3.0 standard has been released 22, January 2013. All new consumers should be following the XACML 3.0 standards.
* SAC should be able to serve as a ubiquitous, enterprise-wide service 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

##### Design Constraints

* Organizational Policies stored in SAC are to be authored per the XACML 3.0 specification
* Consuming service PEPs are required to transact with SAC using HTTPS/SOAP/XACML 3.0 messaging
* Consuming service PEPs are required to support TLS based mutual authentication with the IAM Data Power XML Gateway, the reverse proxy to SAC services
* Consuming service PEPs are required to enforce Authorization Decisions returned by SAC PDP
* SAC does not offer a PIP natively PDP

##### Design Trade-offs

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

* SAC does not offer a PEP service. Offering a PEP would enable SAC to intercept resource access requests and render access control. Currently SAC requires integrated services 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 SSO service and rely on the Desktop PIV login. However, a username and password will still be required for the administration consoles. Console does not support PIV directly, but console cannot be accessed except through services that enforce PIV.

### 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 service necessary to meet the business requirements provided in requirements documents listed in Section 2.3.

#### Database Repository

SAC is based on a COTS product and does not have its own logical database repository and schema. Please refer to Axiomatics Documentation for additional information.

#### System Features

Please refer to Section 2.3 for an overview of the key requirements for SAC. Additionally Section 2.2 provides additional documentation links that elaborate on these requirements.

#### Design Element Tables

N/A

##### Routines (Entry Points)

N/A

##### Templates

N/A

##### Bulletins

N/A

##### Data Entries Affected by the Design

N/A

##### Unique Records

N/A

##### File or Global Size Changes

N/A

##### Mail Groups

N/A

##### Security Keys

N/A

##### Options

N/A

##### Protocols

N/A

##### Remote Procedure Call (RPC)

N/A

##### Constants Defined in Interface

N/A

##### Variables Defined in Interface

N/A

##### Types Defined in Interface

N/A

##### GUI

N/A

##### GUI Classes

N/A

##### Current Form

N/A

##### Modified Form

N/A

##### Components on Form

N/A

##### Events

N/A

##### Methods

N/A

##### Special References

N/A

##### Class Events

N/A

##### Class Methods

N/A

##### Class Properties

N/A

##### Uses Clause

N/A

##### Forms

N/A

##### Functions

N/A

##### Dialog

N/A

##### Help Frame

N/A

##### HL7 Application Parameter

N/A

##### HL7 Logical Link

N/A

##### COTS Interface

N/A

## Network Detailed Design

Refer to Section 0 for detailed communication design for the SAC service.

## Security and Privacy

### Security

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

**Data in Motion (DIM):**

DIM 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 (DAR):**

The following table explains the DAR points.

Table : Data Points and Security

| Data Points | Data Type | Explanation |
| --- | --- | --- |
| Oracle | Sensitive | Stores ASM and PDP configurations |

The security controls for the data at rest are managed through the encryption of sensitive attributes at the directory level. The FIPS 140-2 encryption is applied on the identified PII and sensitive attributes stored in the directory attributes.

Additional security examples are shown below:

#### Security Policy Authoring



Figure : Security Policy Authoring Sequence Diagram

Table : Security Policy Authoring

| Field | Description |
| --- | --- |
| Use Case Name | Security Policy Authoring |
| Description | This use case describes the process through which a SAC Privileged User authors security control policies |
| Actors | 1. Privileged User 2. PAP 3. APA |
| Pre-Conditions | Privileged user has access to PAP |
| Trigger | The privileged user starts up Axiomatics Policy Administration Point thick client GUI interface to author and test XACML 3.0 policies |
| Actions | 1. Privileged User creates workspace to organize and store policies   The policies and configurations are stored locally   1. Privileged User authors and tests XACML 3.0 policies 2. Once completed, the privileged user exports policy package to dedicated file location 3. Privileged User logs into APA and configures attributes from the PEP perspective 4. Privileged User creates queries for validation and runs validation tests 5. 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 |

#### Manage Access Control Policies



Figure : Manage Access Control Policies

Table : 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   Policies are pushed via web service call over TLS   1. Privileged user checks PDP status and pushes policies 2. PEP translates access request to XACML 3.0 (2.0 from eHealth PEP) |
| Main Success Scenarios | Policy is pushed to PDP successfully |
| Main Failure Scenarios | Policy upload fails and user has to start over |



Figure : Enforce Access Control Decision Sequence Diagram

Table : Enforce Access Control Decision

| Field | Description |
| --- | --- |
| Use Case Name | Enforce Access Control Decision |
| Description | This use case describes the process by which a PEP interacts with a consuming service 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. End-user has authenticated session with Application 2. TLS session is established between the Application and PEP |
| Trigger | The PEP receives a request for an authorization from a service |
| Actions | 1. End-user attempts to access protected service 2. PEP intercepts access request 3. The PEP can reside between the end-user and the service 4. The PEP can reside within the service itself 5. PEP verifies request is valid and contains authentication attributes that can be used to uniquely identify the user 6. PEP translates access request to XACML 3.0 (2.0 from eHealth PEP) 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.   1. The PDP response is sent to DataPower 2. DataPower sends PDP response to the PEP. PEP receives XACML 3.0 (2.0 if eHealth) access control decision response from the PDP 3. 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 N/A is determined by the service requirements |
| Main Failure Scenarios | 1. Message format/contents are not valid 2. PDP is non-responsive and decision is not provided to service |

### 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.

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, service 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.

#### 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.

#### 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 6.4.1.

#### Process Integrity

The service 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.

#### System Availability

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

## Service Oriented Architecture (SOA)/ESS Detailed Design

SAC consumes the Authorization Management Service (AMS).

### Service Description for AMS

SAC integrates with MVI’s REST based services to retrieve ACI during applicable policy evaluation to generate an access control decision. Resource URI and sample JSON response/request are TBD.

### Service Design for SAC PDP

#### Introduction

##### Purpose and Scope of Service

The purpose of SAC PDP is to offer fine-grained authorization capabilities to consuming services under purview of privacy and security policies

##### Links to Other Documents

No additional SOA documents exist.

#### Service Details

SAC PDP is a SOAP based web-service that uses HTTPS as the transport. Note that SAC consumers actually access DataPower URLS for SAC. DataPower serves as a reverse proxy to the SAC PDP and acts as the SSL terminator. The request and response payloads for the PDP is XACML 3.0. The Attribute profile packaged into these XACML request messages are integration-specific and would be elaborated upon in pertinent ICDs. For example, the eHealth exchange uses Attributes specified by the Healtheway project (<http://healthewayinc.org/>). Response payloads contain Policy Decisions: Permit or Deny.

SAC requires consuming service PEPs to transact using XACML 3.0. The only exception has been made for eHealth exchange which predates SAC. SAC has a one-off context handler that transforms between 2.0 and 3.0 for backward compatibility with eHealth.

##### Service Identification

Table : Service Identification

| Service Attribute | Value |
| --- | --- |
| Name | SAC PDP |
| Overview | SAC PDP offers fine-grained access control capabilities to integrated consumers under purview of Security and Privacy Policies. The authorization attributes that are referenced by these policies need to be made available to SAC either through the consumer request or through integration of the SAC infrastructure with pertinent authoritative sources |
| Version | 1.0 |
| Latest Status | Operation |
| Service Type | Access |
| Architecture Layer | Utility |
| Business Domain | Enterprise Shared Services (ESS) |
| Service Domain | Access Control |
| Business Organization and Owner | Person who approves this service and any changes. Include email. |
| Technical Organization and Owner | Person responsible for provisioning (specifying, acquiring certifying) this service. Include email |
| Development Organization and Owner | Person who is responsible for the development processes and activities for this service. Include email |
| Support Organization and Owner | Person who is responsible for the support of this service while in production. Include email |
| Target Consumer Organization(s) and Owner(s) | Organizations and/or developers roles that service is intended for |

##### Service Versions

Table : Service Versions

|  |  |  |
| --- | --- | --- |
| Version Numbers | Current Status | Change Description |
| Version 1 | Operational | Implemented the PDP Service |

##### Summary of Design and Platform Details

Refer to Section 6.2.1 for a summary of the SAC design and platform details.

##### SOA Pattern(s) Implemented

SAC is based on a Request-Response SOA pattern.

##### COTS Platform Vendor Names and Versions for Hosting Platform

The COTS product that SAC uses is Axiomatics Policy Server. The current version in production is 5.3.4. Axiomatics Policy Server is made by the vendor Axiomatics.

#### Dependencies

SAC interacts with:

* DataPower – Reverse proxy that secures access to SAC PDP
* eHealthVAP – consumer of SAC PDP/NwHIN
* Oracle RAC – Used by the COTS infrastructure that offers the SAC PDP RAC

#### Service Design Details

Refer to Section 6.2.1 for design details.

##### Interface Technical Specs

##### Service Invocation Type

SOAP over TLS

###### Service Interface Type

WSDL via Web Service 2.0

##### Service Name

Table : Service Name

| Service Name | Service Description |
| --- | --- |
| 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. |
| Context Handler | This is a one-off adapter to the SAC PDP for the benefit of the eHealth PEP/VAP. eHealth/VAP transacts using XACML 2.0 and predates SAC. This adapter serves PDP backward compatibility with eHealth and performs requisite transformation between XACML 2.0 and 3.0 messages. This is not meant to be used by any other consumer. |

###### Interface

The PDP WSDL for Production is shown in Table 31.

Table : PDP WSDL for Production

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?>  <!-- Published by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is Metro/2.2.0-4 (tags/2.2.0-4-7595; 2013-05-30T12:51:32+0200) JAXWS-RI/2.2.6-5 JAXWS/2.2 svn-revision#unknown. -->  [<wsdl:definitions name="DelegentPDP" targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5" xmlns:xacml2ctx="urn:oasis:names:tc:xacml:2.0:context:schema:os" xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsdl-soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns="http://schemas.xmlsoap.org/wsdl/" xmlns:ivac="http://axiomatics.com/delegent/pdpsimple/v5/InvalidateAttributeCache" xmlns:titrcap3="http://axiomatics.com/delegent/pdpsimple/v5/TransactionTraceAccessQuery3" xmlns:itrcap3="http://axiomatics.com/delegent/pdpsimple/v5/TraceAccessQuery3" xmlns:tircap3="http://axiomatics.com/delegent/pdpsimple/v5/TransactionAccessQuery3" xmlns:ircap3="http://axiomatics.com/delegent/pdpsimple/v5/AccessQuery3" xmlns:titrcap2="http://axiomatics.com/delegent/pdpsimple/v5/TransactionTraceAccessQuery2" xmlns:itrcap2="http://axiomatics.com/delegent/pdpsimple/v5/TraceAccessQuery2" xmlns:tircap2="http://axiomatics.com/delegent/pdpsimple/v5/TransactionAccessQuery2" xmlns:ircap2="http://axiomatics.com/delegent/pdpsimple/v5/AccessQuery2" xmlns:faults="http://axiomatics.com/delegent/pdpsimple/v5/faults" xmlns:tns="http://axiomatics.com/delegent/pdpsimple/v5"><wsdl:types><xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/faults" elementFormDefault="qualified">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element name="PDPFault" type="xsd:string"/></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/AccessQuery2" elementFormDefault="qualified" xmlns:xacml2-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:import schemaLocation="https://localhost:8443/asm-pdp/pdp?xsd=1" namespace="urn:oasis:names:tc:xacml:2.0:context:schema:os"/><xsd:element name="PDPFault" type="xsd:string"/>[<xsd:element name="AccessQuery2Response"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml2-context:Response"/></xsd:sequence></xsd:complexType></xsd:element>[<xsd:element name="AccessQuery2"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml2-context:Request"/></xsd:sequence></xsd:complexType></xsd:element></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/TransactionAccessQuery2" elementFormDefault="qualified" xmlns:xacml2-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:import schemaLocation="https://localhost:8443/asm-pdp/pdp?xsd=1" namespace="urn:oasis:names:tc:xacml:2.0:context:schema:os"/><xsd:element name="PDPFault" type="xsd:string"/>[<xsd:element name="AccessQuery2Response"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml2-context:Response"/></xsd:sequence></xsd:complexType></xsd:element>[<xsd:element name="TransactionAccessQuery2"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml2-context:Request"/><xsd:element name="transactionId" type="xsd:string" maxOccurs="1" minOccurs="0"/></xsd:sequence></xsd:complexType></xsd:element></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/AccessQuery3" xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" elementFormDefault="qualified">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:import schemaLocation="https://localhost:8443/asm-pdp/pdp?xsd=3" namespace="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"/><xsd:element name="PDPFault" type="xsd:string"/>[<xsd:element name="AccessQuery3Response"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml3:Response"/></xsd:sequence></xsd:complexType></xsd:element>[<xsd:element name="AccessQuery3"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml3:Request"/></xsd:sequence></xsd:complexType></xsd:element></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/TransactionAccessQuery3" xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" elementFormDefault="qualified">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:import schemaLocation="https://localhost:8443/asm-pdp/pdp?xsd=3" namespace="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"/><xsd:element name="PDPFault" type="xsd:string"/>[<xsd:element name="AccessQuery3Response"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml3:Response"/></xsd:sequence></xsd:complexType></xsd:element>[<xsd:element name="TransactionAccessQuery3"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml3:Request"/><xsd:element name="transactionId" type="xsd:string" maxOccurs="1" minOccurs="0"/></xsd:sequence></xsd:complexType></xsd:element></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/TraceAccessQuery2" elementFormDefault="qualified" xmlns:xacml2-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:import schemaLocation="https://localhost:8443/asm-pdp/pdp?xsd=1" namespace="urn:oasis:names:tc:xacml:2.0:context:schema:os"/><xsd:element name="PDPFault" type="xsd:string"/>[<xsd:element name="TraceAccessQuery2Response"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml2-context:Response"/>[<xsd:element name="Trace">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)  <!-- The schema for this will be defined later -->  [<xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:any processContents="skip"/></xsd:sequence></xsd:complexType></xsd:element></xsd:sequence></xsd:complexType></xsd:element>[<xsd:element name="TraceAccessQuery2"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml2-context:Request"/></xsd:sequence></xsd:complexType></xsd:element></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/TransactionTraceAccessQuery2" elementFormDefault="qualified" xmlns:xacml2-context="urn:oasis:names:tc:xacml:2.0:context:schema:os">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:import schemaLocation="https://localhost:8443/asm-pdp/pdp?xsd=1" namespace="urn:oasis:names:tc:xacml:2.0:context:schema:os"/><xsd:element name="PDPFault" type="xsd:string"/>[<xsd:element name="TraceAccessQuery2Response"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml2-context:Response"/>[<xsd:element name="Trace">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)  <!-- The schema for this will be defined later -->  [<xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:any processContents="skip"/></xsd:sequence></xsd:complexType></xsd:element></xsd:sequence></xsd:complexType></xsd:element>[<xsd:element name="TransactionTraceAccessQuery2"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml2-context:Request"/><xsd:element name="transactionId" type="xsd:string" maxOccurs="1" minOccurs="0"/></xsd:sequence></xsd:complexType></xsd:element></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/TraceAccessQuery3" xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" elementFormDefault="qualified">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:import schemaLocation="https://localhost:8443/asm-pdp/pdp?xsd=3" namespace="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"/><xsd:element name="PDPFault" type="xsd:string"/>[<xsd:element name="TraceAccessQuery3Response"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml3:Response"/>[<xsd:element name="Trace">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)  <!-- The schema for this will be defined later -->  [<xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:any processContents="skip"/></xsd:sequence></xsd:complexType></xsd:element></xsd:sequence></xsd:complexType></xsd:element>[<xsd:element name="TraceAccessQuery3"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml3:Request"/></xsd:sequence></xsd:complexType></xsd:element></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/TransactionTraceAccessQuery3" xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" elementFormDefault="qualified">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:import schemaLocation="https://localhost:8443/asm-pdp/pdp?xsd=3" namespace="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"/><xsd:element name="PDPFault" type="xsd:string"/>[<xsd:element name="TraceAccessQuery3Response"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml3:Response"/>[<xsd:element name="Trace">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)  <!-- The schema for this will be defined later -->  [<xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:any processContents="skip"/></xsd:sequence></xsd:complexType></xsd:element></xsd:sequence></xsd:complexType></xsd:element>[<xsd:element name="TransactionTraceAccessQuery3"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element ref="xacml3:Request"/><xsd:element name="transactionId" type="xsd:string" maxOccurs="1" minOccurs="0"/></xsd:sequence></xsd:complexType></xsd:element></xsd:schema>[<xsd:schema targetNamespace="http://axiomatics.com/delegent/pdpsimple/v5/InvalidateAttributeCache" elementFormDefault="qualified"><xsd:element name="InvalidateAttributeCacheResponse">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:complexType> </xsd:complexType></xsd:element>[<xsd:element name="InvalidateAttributeCache"><xsd:complexType><xsd:sequence><xsd:element name="ModuleParameter" maxOccurs="unbounded" minOccurs="0"><xsd:complexType><xsd:sequence>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<xsd:element name="ModuleId" type="xsd:string"/><xsd:element name="Parameter" type="xsd:string"/></xsd:sequence></xsd:complexType></xsd:element></xsd:sequence></xsd:complexType></xsd:element></xsd:schema></wsdl:types>[<wsdl:message name="AccessQuery2Request">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="AccessQuery2Request" element="ircap2:AccessQuery2"/></wsdl:message>[<wsdl:message name="TransactionAccessQuery2Request">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="TransactionAccessQuery2Request" element="tircap2:TransactionAccessQuery2"/></wsdl:message>[<wsdl:message name="AccessQuery2Response">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="AccessQuery2Response" element="ircap2:AccessQuery2Response"/></wsdl:message>[<wsdl:message name="AccessQuery3Request">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="AccessQuery3Request" element="ircap3:AccessQuery3"/></wsdl:message>[<wsdl:message name="TransactionAccessQuery3Request">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="TransactionAccessQuery3Request" element="tircap3:TransactionAccessQuery3"/></wsdl:message>[<wsdl:message name="AccessQuery3Response">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="AccessQuery3Response" element="ircap3:AccessQuery3Response"/></wsdl:message>[<wsdl:message name="TraceAccessQuery2Request">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="TraceAccessQuery2Request" element="itrcap2:TraceAccessQuery2"/></wsdl:message>[<wsdl:message name="TransactionTraceAccessQuery2Request">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="TransactionTraceAccessQuery2Request" element="titrcap2:TransactionTraceAccessQuery2"/></wsdl:message>[<wsdl:message name="TraceAccessQuery2Response">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="TraceAccessQuery2Response" element="itrcap2:TraceAccessQuery2Response"/></wsdl:message>[<wsdl:message name="TraceAccessQuery3Request">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="TraceAccessQuery3Request" element="itrcap3:TraceAccessQuery3"/></wsdl:message>[<wsdl:message name="TransactionTraceAccessQuery3Request">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="TransactionTraceAccessQuery3Request" element="titrcap3:TransactionTraceAccessQuery3"/></wsdl:message>[<wsdl:message name="TraceAccessQuery3Response">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="TraceAccessQuery3Response" element="itrcap3:TraceAccessQuery3Response"/></wsdl:message>[<wsdl:message name="InvalidateAttributeCacheRequest">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="InvalidateAttributeCacheRequest" element="ivac:InvalidateAttributeCache"/></wsdl:message>[<wsdl:message name="InvalidateAttributeCacheResponse">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="InvalidateAttributeCacheResponse" element="ivac:InvalidateAttributeCacheResponse"/></wsdl:message>[<wsdl:message name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:part name="fault" element="faults:PDPFault"/></wsdl:message>[<wsdl:portType name="DelegentPDPPortType"><wsdl:operation name="AccessQuery2">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:AccessQuery2Request"/><wsdl:output message="tns:AccessQuery2Response"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation>[<wsdl:operation name="TransactionAccessQuery2">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:TransactionAccessQuery2Request"/><wsdl:output message="tns:AccessQuery2Response"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation>[<wsdl:operation name="AccessQuery3">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:AccessQuery3Request"/><wsdl:output message="tns:AccessQuery3Response"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation>[<wsdl:operation name="TransactionAccessQuery3">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:TransactionAccessQuery3Request"/><wsdl:output message="tns:AccessQuery3Response"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation>[<wsdl:operation name="TraceAccessQuery2">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:TraceAccessQuery2Request"/><wsdl:output message="tns:TraceAccessQuery2Response"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation>[<wsdl:operation name="TransactionTraceAccessQuery2">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:TransactionTraceAccessQuery2Request"/><wsdl:output message="tns:TraceAccessQuery2Response"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation>[<wsdl:operation name="TraceAccessQuery3">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:TraceAccessQuery3Request"/><wsdl:output message="tns:TraceAccessQuery3Response"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation>[<wsdl:operation name="TransactionTraceAccessQuery3">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:TransactionTraceAccessQuery3Request"/><wsdl:output message="tns:TraceAccessQuery3Response"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation>[<wsdl:operation name="InvalidateAttributeCache">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl:input message="tns:InvalidateAttributeCacheRequest"/><wsdl:output message="tns:InvalidateAttributeCacheResponse"/><wsdl:fault name="PDPFault" message="tns:PDPFault"/></wsdl:operation></wsdl:portType>[<wsdl:binding name="DelegentPDPBinding" type="tns:DelegentPDPPortType">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:binding transport="http://schemas.xmlsoap.org/soap/http" style="document"/>[<wsdl:operation name="AccessQuery2">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="AccessQuery2"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation>[<wsdl:operation name="TransactionAccessQuery2">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="AccessQuery2"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation>[<wsdl:operation name="AccessQuery3">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="AccessQuery3"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation>[<wsdl:operation name="TransactionAccessQuery3">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="TransactionAccessQuery3"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation>[<wsdl:operation name="TraceAccessQuery2">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="TraceAccessQuery2"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation>[<wsdl:operation name="TransactionTraceAccessQuery2">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="TransactionTraceAccessQuery2"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation>[<wsdl:operation name="TraceAccessQuery3">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="TraceAccessQuery3"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation>[<wsdl:operation name="TransactionTraceAccessQuery3">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="TransactionTraceAccessQuery3"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation>[<wsdl:operation name="InvalidateAttributeCache">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:operation soapAction="InvalidateAttributeCache"/>[<wsdl:input>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:input>[<wsdl:output>](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:body encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:output>[<wsdl:fault name="PDPFault">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:fault name="PDPFault" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/" use="literal"/></wsdl:fault></wsdl:operation></wsdl:binding>[<wsdl:service name="DelegentPDP"><wsdl:port name="DelegentPDPPort" binding="tns:DelegentPDPBinding">](file:///C:/Users/Kyle%20Williford/AppData/Local/Temp/pdp%20(2).xml)<wsdl-soap:address location="https://localhost:8443/asm-pdp/pdp"/></wsdl:port></wsdl:service></wsdl:definitions> |

##### End Points

Shown below is a sample endpoint for the PDP: https://VAAUSIAMAPS801.vha.med.va.gov:8443/asm-pdp/pdp

##### Operations or Methods

Axiomatics PDP delivers a decision as either Permit, Deny, Indeterminate, or N/A. A successful evaluation does not return Indeterminate.

###### Message Schemas

Refer to OASIS XACML 3.0 documentation for message schemas.

The message format for the VDT request/response is as follows:

<?xml version=**"1.0"**?>

**-**<xacml-ctx:Request xmlns:xacml-ctx=**"urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"** CombinedDecision=**"false"** ReturnPolicyIdList=**"true"**>

**-**<xacml-ctx:Attributes Category=**"urn:oasis:names:tc:xacml:3.0:attribute-category:resource"**>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"target.identifier.itype"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**ICN**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"target.identifier.valueRoot"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**2.16.840.1.113883.4.349**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"authorizationType.value"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**VAHPDelegation**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"target.identifier.valueExtension"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**0996669990^PN^200PROV^USDVA**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"authorizationType.value.preferences.value"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**Read/Print/Download**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"authorizationType.value.preferences.itype"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**Permission**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

</xacml-ctx:Attributes>

**-**<xacml-ctx:Attributes Category=**"urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"**>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"subject.identifier.valueRoot"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**2.16.840.1.113883.4.349**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"subject.identifier.itype"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**ICN**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

**-**<xacml-ctx:Attribute IncludeInResult=**"true"** AttributeId=**"subject.identifier.valueExtension"**>

<xacml-ctx:AttributeValue DataType=**"http://www.w3.org/2001/XMLSchema#string"**>**0996669990^PN^200PROV^USDVA**</xacml-ctx:AttributeValue>

</xacml-ctx:Attribute>

</xacml-ctx:Attributes>

</xacml-ctx:Request>

Sample messages for VLER/eHX are within the SOAPUI Project below:



Sample messages for Delegation are within the SOAPUI Project below:



##### Information Model

Refer to Section 3.2 and Section 3.2.1 for models of information flow within SAC. The attribute profiles that get packaged into request messages are specific to each integration and would be documented in the ICD pertinent to that integration. The information returned in the response message would always be a policy decision of Permit or Deny.

##### Class Diagram and Description of Entities Involved

Table : Entities

| Entity | Description |
| --- | --- |
| eHealth/VAP | This is the current consumer for SAC. Details on consumer integration with SACs would be available in respective ICDs |
| Context Handler | This is a one-off transformation adapter between eHealth/VAP and the SAC PDP. It transforms XACML messages between versions 2.0 and 3.0. This is not meant to be used by any consumer other than eHealth/VAP. All new consumers of SAC PDP would have to transact using XACML 3.0 messaging and directly connect to the PDPContext Handler. |
| SAC PDP | Decision engine for fine-grained authorization access control |

##### Mappings from ELDM to Standards Based Schemas

SAC PDP uses standard OASIS XACML 3.0 schemas and no native schemas. This section is N/A.

##### Behavior Model (Use Case Realization)

###### Use Cases (Use Case Model)

Refer to Section 6.2.1 for models and use case information.

###### Interaction Diagrams

Make Access Control Decisions



Figure : Make Access Control Decisions Sequence Diagram

Table : 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 (Shown here for context. It is a pass through entity, a reverse proxy that protects the PDP) 3. PDP 4. AMS/PIP (\*Not for eHX) |
| Pre-Conditions | * The service access control policy (XACML 3.0) needs to exist. This would be authored after governance entities have established the Security and Privacy concerns to protect the consuming service * The consuming service should have a PEP * The PEP should be able to transact using XACML 3.0 * The XACML request from the PEP should contain authorization attributes required by the access control Policy (In the future, some of these attributes can be retrieved through authoritative PIPs) * The PEP should be able to communicate with SAC URLs registered with DataPower |
| Trigger | PDP receives XACML 3.0 request from the consuming service 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 AMS PIP for attributes required by policy(s). (**NOTE:** The AMS PIP stores individual authorizations for access to protected data. This is not currently evaluated by existing eHX policies). This is still shown to depict that in an upcoming increment a Consumer and Policy that requires evaluation of Authorization ACI will be integrated. 3. The PDP uses the attributes found in the XACML request (and in the future, the attributes retrieved from the PIP), and the XACML 3.0 security policies, to generate an access control decision 4. PDP logs the access request and response 5. The XACML 3.0 response containing the access control decision (Permit/Deny) is sent to the requesting PEP |
| Main Success Scenarios | Decision is generated and passed to PEP |
| Main Failure Scenarios | Policy is not found or attributes are missing and decision would have a Deny bias |

Make Access Control Decisions (eHealth Only)



Figure : Make Access Control Decisions (eHealth Only) Sequence Diagram

Table : 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 PDP gathers and evaluates the necessary information (access control policy[s] and attributes) and makes an access control decision |
| Actors | 1. PEP (eHealth/VAP) 2. DataPower (Shown here for context. It is a pass through entity, a reverse proxy that protects the PDP and Context Handler). 3. Context Handler – Custom SAC artifact that transforms between XACML 2.0 and 3.0 messaging 4. PDP |
| Pre-Conditions | * The service access control policy/eHealth policy (XACML 3.0) needs to exist * The consuming service should have a PEP * The PEP should be able to transact using XACML 2.0 * The XACML request from the PEP should contain authorization attributes required by the access control Policy * The PEP should be able to communicate with SAC URLs registered with DataPower |
| Trigger | PDP receives XACML request from eHealth/VAP PEP via DataPower |
| Actions | 1. PEP request is received by the Context Handler 2. The context Handler transforms the XACML 2.0 request to XACML 3.0 3. The XACML 3.0 request is forwarded to the PDP 4. The PDP uses the attributes found in the XACML request and the XACML security policies to generate an access control decision 5. PDP logs the access request and response 6. The XACML 3.0 response/access control decision is sent to the context handler 7. The context handler transforms the XACML 3.0 response to XACML 2.0 8. The context handler sends the XACML 2.0 response/access control decision to the requested PEP |
| Main Success Scenarios | Decision is generated and passed to PEP |
| Main Failure Scenarios | Policy is not found or attributes are missing and decision would have a Deny bias |

#### Gap Analysis

N/A

##### Variances from Enterprise Target Architecture

N/A

##### Variances from SLDs

N/A

##### Variances from Standards and Policies

N/A

##### Justification for Exceptions and Mitigation

N/A

# External System Interface Design

## Interface Architecture

N/A

## Interface Detailed Design

PIP will use a REST service from MVI. The AMS service will connect with the PIP so that when PDP gets a call, it will use that web service to pull whatever information it needs to be able to execute the underlying policy. Please see the MVI SDD for detailed design.

MHV is a client to SAC which will need to pull authorization data. Using Axiomatics SDK, MHV will call the PDP, which then calls the PIP to grab authorization data through a REST call. Please see the MHV IAM ICD for detailed design.

.

# Human-Machine Interface

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

* Please refer to the [SAC Configuration Guide](http://xxxxxxxxxxx/sites/vrm/IAM/IAM%20Documents/IAM%20Development%20Documentation/Insignia%20-%20AcS%20Development%20Integration%20i4/5.2.3.4%20Solution%20Release-Deployment/Deployment-Install%20Package/i4VA_IAM_SAC_Configuration_Guide.docx) for additional content
* For user interface information related to COTS administrator functions, refer to the product documentation available at the following website - Axiomatics site: [http://www.axiomatics.com](http://www.axiomatics.com/)

## 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 that are 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.

## Inputs

N/A

## 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 (Portable Document Format)
* Comma Separated File (CSF)
* Microsoft Excel

## Navigation Hierarchy

### Screen Shots

Refer to the [AcS Help Desk Training for SAC](http://xxxxxxxxxxxxxx/warboard/ProjectDocs/Access_Services_Phase_2/VA_AcS_2.0_i5_SAC_Help_Desk_Training.pdf) to review all navigational screenshots.

### Application Screen Interface

This section provides the GUI that the SAC users can access within the SAC application.

### PAP Authoring Page

Once a workspace is opened or created by the privileged user, the following screen, Figure 199, displays in which the SAC privileged user creates/edits XACML 3.0 policies.

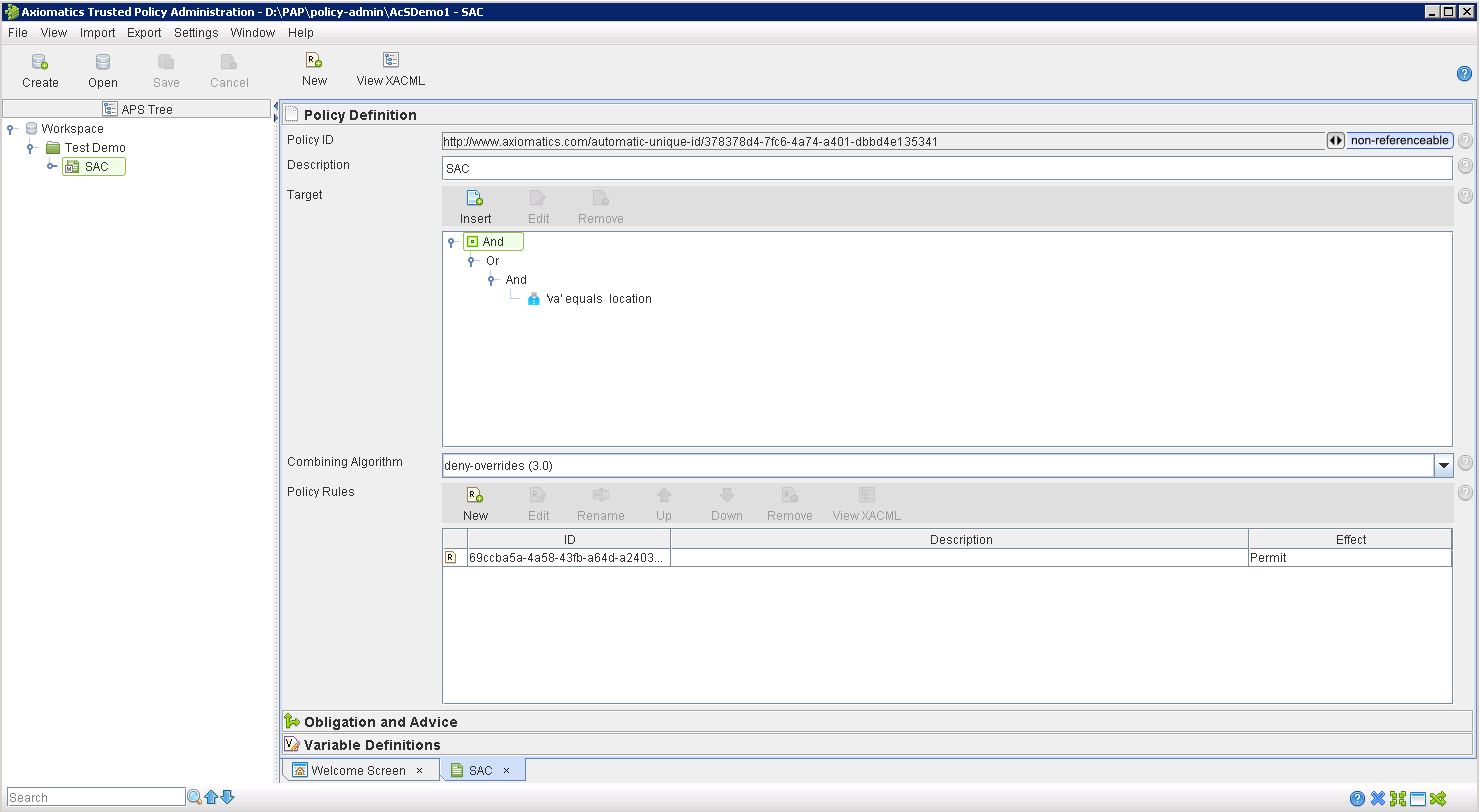


Figure : SAC PAP Landing Page

Attachment A – Approval Signatures

This section is used to document the approval of the SDD. 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, it should be held via LiveMeeting with concurrence captured during the meeting. The Scribe should add names by each position cited. Examples are provided below.

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: Date:

xxxxx,

IAM Program Manager

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: Date:

xxxxx,

AcS Program Manager

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: Date:

xxxxx,

IAM Integrated Project Team (IPT) Chair and Business Sponsor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: Date:

xxxxx,

IAM BPMO Director

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: Date:

xxxxx,

Chief Architect

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed: Date:

xxxxx,

SEDR

1. Additional Information
   1. Identification of Technology Standards

The information contained herein applies to SAC, a dynamic fine-grained ABAC service. SAC is based on 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.

Table : System Identification

| Name | Description | Abbreviation | Version | Release |
| --- | --- | --- | --- | --- |
| VA AcS Solution | Core set of activities to definitively and consistently identify VA stakeholders and to establish supporting processes that provide the appropriate level of security required to protect and manage the identities, information, and interests of the VA stakeholders | AcS | V 2.5.X | Release 6 (i6) |
| SAC | Provides the ability to manage access control policies and generate and enforce access control decisions | SAC | V 2.5.X | N/A |

* 1. Constraining Policies, Directives, and Procedures

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 service owners, ICAM PMO, IT Security Program managers and VA Privacy and Security group. The service shall comply and follow OASIS XACML 3.0 for standardization, interoperability and computability.

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

Table : Applicable Policies, Directives, and Procedures

| # | Issuing Agency | Policy, Directive, or Procedure | Purpose |
| --- | --- | --- | --- |
| 1 | VA | VA 6500 Handbook | * Directive Information Security Program * Defining overall Security Framework for VA |
| 2 | VA | VA 6501 Directive | * VA Identity Verification In-Person Proofing (IPP) Process * Defining overall Identity Proofing Methodology for VA IAM |
| 3 | VA | VA 6300 Directive | * Directive Records and Information Management * Defines information management framework for VA Access Services |
| 4 | NIST | SP 800-53-4 | * Special Publication – Recommended Security Controls for Federal Information Systems and Organizations * Defines the required security controls for IT services under the Federal Information Security Management Act (FISMA) |
| 5 | NIST | SP 800-63-2 | * Special Publication – Electronic Authentication Guideline * Defines levels of assurance in user identities presented to IT services over open networks * Defines the data and procedural requirements for VA Access Services |
| 6 | NIST | FIPS-201-2 | * 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 | * FIPS – Security Requirements for Cryptographic Modules * Defines the cryptographic standards and requirements |
| 8 | NIST | SP 800-122 | * Guide to Protecting the Confidentiality of PII * Provides technical procedures for protecting PII in information services * Defines the information which can be used to distinguish or trace an individual's identity |
| 9 | US Congress | Section 508 Amendment to the Rehabilitation Act of 1973 | * 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 | * 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 | * Requirements for Accepting Externally-Issued Identity Credentials * FICAM architecture and procedures for federal agencies |
| 12 | GSA | FICAM | * Federal Identity, Credentialing and Access Management (FICAM) Roadmap and Implementation Guidance * Provides the common segment architecture and implementation guidance for FICAM programs |
| 13 | White House | NSTIC | * National Strategy for Trusted Identities in Cyberspace (NSTIC) – Provides guidance for identity trust in cyberspace |
| 14 | US Congress | FISMA | * FISMA of 2002, Public Law 107-347 |
| 15 | US Congress | E-Government Act of 2002 | * Federal Management and Promotion of Electronic Government Services * Defines the requirements for electronic services |
| 16 | US Congress | The Privacy Act of 1974 | * § 552a. Records maintained on individuals * Defines VA Access Services Privacy assessment and control requirements |
| 17 | National Archives and Records Administration (NARA) | Federal Records Act | * Establishes the framework for records management programs in Federal Agencies |
| 18 | VA | VA D 0735 | * Homeland Security Presidential Directive 12 (HSPD-12) Program * Defines Department-wide policy, roles, and responsibilities for the creation and maintenance of services 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 | * Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors |

* 1. RTM

Refer to the AcS RSD or the Rational Requirements Manager (RRM) to obtain the AcS RTM for i7.

* 1. Packaging and Installation

N/A

* 1. Design Metrics

N/A

* 1. Acronym List and Glossary

The acronyms and terms used in this SDD are defined in the [Identity and Access Services Master Glossary](http://xxxxxxxxxxxxx/warboard/ProjectDocs/Access_Services/Identity_and_Access_Services_Master_Glossary.pdf).

* 1. Required Technical Documents

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

* 1. Attach Documents

The AERB Design Compliance Decision Certificate is attached upon approval of the SDD.