VA Enterprise Design Patterns
Privacy and Security

Enterprise Authorization

OFFICE OF TECHNOLOGY STRATEGIES (TS)
OFFICE OF INFORMATION AND TECHNOLOGY (OI&T)

VERSION 1.0
DATE ISSUED: JUNE 2016

APPROVAL COORDINATION

Gary E. Marshall 137891

Digitally signed by Gary E. Marshall 137891
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=gary.marshall@va.gov, cn=Gary E. Marshall 137891
Date: 2016.06.15 09:15:14 -04'00'

Gary Marshall
Director, Technology Strategies, ASD

PAUL A. TIBBITS 116858

Digitally signed by PAUL A. TIBBITS 116858
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=paul.tibbits@va.gov, cn=PAUL A. TIBBITS 116858
Reason: I am approving this document.
Date: 2016.06.15 12:52:12 -04'00'

Paul A. Tibbits, M.D.
DCIO Architecture, Strategy, and Design

REVISION HISTORY

Version	Date	Approver	Notes
1.0	6/8/2016	Nicholas Bogden	Updated with scope, problem statement, approach, and use cases, and populated with current and future states. Incorporated stakeholder feedback.

CONTENTS

1 Introduction 4
1.1 Business Need 5
1.2 Approach 5
2 Current Capabilities and Limitations 6
2.1 Lack of Centralized Policy Store 6
2.2 Lack of Standardized Set of Authorization Solutions 7
2.3 Lack of Flexible Standards Profile 7
3 Future Capabilities 8
3.1 Establish the Foundation for Centralized Authorization 8
3.2 Assessing Appropriate Access Controls 9
3.3 Security for the Authorization Infrastructure 12
3.4 Alignment to the One-VA Technical Reference Model (TRM) 13
3.5 Alignment to Veteran-Centric Integration Process (VIP) 14
4 Use Cases 14
4.1 Conditional Data Access Based on Attributes 14
4.1.1 Purpose 14
4.1.2 Assumptions 15
4.1.3 Use Case Description 15
4.2 Restriction of RBAC Using ABAC 16
4.2.1 Purpose 16
4.2.2 Assumptions 16
4.2.3 Use Case Description 16
4.3 External Use Access/Unexpected User 17
4.3.1 Purpose 17
4.3.2 Assumptions 17
4.3.3 Use Case Description 17
Appendix A. Scope 19
Appendix B. Definitions 20
Appendix C. Acronyms 22
Appendix D. References, Standards, and Policies 23
Appendix E. Current Authorization Solutions Profiled 26
Appendix F. Analysis of Smart OAuth Profile 29

Table 1: Authorization Business Benefits 5
Table 2: List of Approved Tools and Standards for Enterprise Authorization 14

Figure 1: Authorization Code Grant Flow Overview 12

QUICK JUMP

Select an icon to skip to a section.

Current Capabilities

Future Capabilities

Use Cases

One-VA Technical Reference Model

The Veteran-Focused Integration Process

Enterprise Design Pattern Scope

1 INTRODUCTION

Within VA there is a complex mesh of internally managed and externally hosted applications. There is also a growing amount of compliance mandates such as FISMA, FIPS, PCI, HIPAA, Health Level 7 (HL7) and others. This creates a challenge to create and administer an appropriate authentication and authorization solution. The Federal Identity, Credential, and Access Management (FICAM) Roadmap calls for the evaluation of attributes as a method of improving access both internally and with external groups. The FICAM Roadmap was created in 2009 to guide federal agencies on logical access control architectures. In 2011, the updated FICAM Roadmap specifically recommended Attribute Based Access Control (ABAC) as a model to achieve this interoperability.

The key issues to be solved include:

- Application owners need for authorization controls that support the granularity of their business requirements.
- An enterprise service that can be used by all application owners.
- A solution that can effectively scale authorization controls to support applications with external users.
- Technical controls to prevent violations and reduce the reliance on manual auditing to detect violations after the fact.
- An enterprise authorization architecture that reduces service overhead through design and policy reusability.

These issues stem from fundamental, systemic problems around authorization at VA (and many other large organizations), such as:

- Lack of a centralized policy store
- Limited governance of standard authorization solutions and attributes
- Lack of a flexible authorization standards profile that applies to all VA projects

1.1 Business Need

VA's responsibility for protecting access to a large amount of sensitive patient information includes moderating access by a number of external business partners as well as its own staff. VA requires an Enterprise Shared Service (ESS) for authorization of internal and external users. A service is needed to manage the availability, vocabulary and use of attributes from multiple sources to implement varying levels of access control. This includes guidance on the creation of a compliant architecture, recommendations for migration to new capabilities and instructions for application owners to integrate with enterprise Identity and Access Management (IAM) services.

TABLE 1: AUTHORIZATION BUSINESS BENEFITS

Business Benefits	Description
Greater ability to meet security requirements through technical controls	In cases where RBAC controls do not meet the application security requirements, IAM is able to provide more granular controls to achieve compliance.
Increased efficiency	Authorization architecture use by multiple stakeholders can be consolidated. Externalization of authorization responds more efficiently by changing authorization policy instead of application code.
A consistent methodology to evaluate access control requirements	Not all applications require the same types of controls. A common methodology will identify the requirements and the most effective means to meet them.
Reduced risk of noncompliance	Reliance on auditing and manual controls often identifies violations after the fact.
Accommodation for the unexpected user	External users will not need to be known in advance. External users will gain the appropriate level of access through the assignment of attributes.

1.2 Approach

The Enterprise Authorization Design Pattern provides a vendor-agnostic approach to authorization including RBAC and ABAC models, lays out the benefits and weaknesses of each

approach and offers a model to address the varying authorization requirements for application owners across VA.

The VA's target Enterprise Authorization solution will provide a consistent process for assessing and providing authorization services across applications. IAM and application owners will work together as described in Section 3 to assess the level of granularity needed by an application. IAM will then support the application owner in selecting the appropriate services to achieve the required level of technical controls by using an approach that leverages RBAC, ABAC or hybrid controls including those inherent to the application.

2 CURRENT CAPABILITIES AND LIMITATIONS

VA OI&T provides multiple services that support authorization. This includes a portfolio of services to include RBAC and ABAC solutions as well as availability of a range of attributes through a Virtual Directory. However, VA projects have historically had limited insight into these available solutions, resulting in challenges adopting an enterprise-wide approach to using a standard set of authorization services. Examples of current authorization services include IAM's Single Sign-On (SSO), Authorization Management Service (AMS), Specialized Access Control (SAC), and access controls set by Microsoft Active Directory domain controllers and middleware platforms such as the Enterprise Messaging Infrastructure (eMI). Each service provides a mixture of role-based and attribute-based access controls along with application-specific access controls that projects consider in designing their solutions. Although IAM provides several enterprise services, some of these are recently deployed and many VA applications have not yet adopted these newer capabilities and have no requirement to do so. A lack of centralization for authorization prevents integrated policy management and compliance. An evaluation of current authorization services (see Appendix E) reveals the following systemic barriers to adopting enterprise authorization services:

- Lack of a centralized policy store
- Limited governance of standard authorization solutions and attributes
- Lack of a flexible authorization standards profile that applies to all VA projects

2.1 Lack of Centralized Policy Store

There are many attribute stores present in VA which are used to authenticate and authorize users. The Virtual Directory Service (VDS), as explained in greater detail in the User Identity Authentication Enterprise Design Pattern, provides a virtualized view of multiple back-end data stores, joining identity information from Active Directory (AD), Provisioning, and the Master Veteran Index (MVI). However, the VDS only focuses on identity information and neglects other

attributes such as resource and contextual data when making an access control decision, which only works well for coarse-grained authorization. For more fine-grained access control, these attributes must be passed to the consuming Policy Enforcement Points (PEP) and/or integrated into a Policy Information Point (PIP) that a Policy Decision Point (PDP) can access.

2.2 Lack of Standardized Set of Authorization Solutions

Within VA, agencies are using their own set of solutions based on their project needs instead of utilizing a standard set of solutions. For example, the Enterprise Health Management Platform (eHMP) uses the VistA Exchange Policy Enforcement Point (PEP) and Policy Decision Point (PDP) to implement authorization, while the larger healthcare Service Oriented Architecture (SOA) initiatives, such as eHealth/Veterans Authorizations Preferences (VAP) utilize the Specialized Access Control (SAC) PDP. VA projects would benefit from having a catalog of approved PEPs and PDPs, which constrain solution architectures to using a standard set of solutions. In addition, there are some stakeholders who use Active Directory for built-in roles along with customized roles to implement RBAC. This is problematic because built-in roles are too high-level for implementing RBAC, except at a broad level, and the creation of custom roles requires manual auditing to add and remove users from the roles. Recent attempts to use existing data to create standardized roles has been hampered by technical challenges and a lack of relevant attributes. VA also uses both manual and semi-automated methods to create and manage user accounts across a myriad of applications and systems that integrate with IAM services. This causes delays associated with VA on-boarding and off-boarding processes for workers and results in inefficiencies and inconsistencies while posing a security risk due to an excessive number of dormant accounts. Standardized authorization solutions would also ensure consistent compliance and reduce the risk of errors in implementation by individual projects interpreting policy.

2.3 Lack of Flexible Standards Profile

The SAC PDP leverages the OASIS eXtensible Access Control Markup Language 3.0 (XACML) standard for policy representation and messaging with consumer services. Many legacy systems do not support XACML 3.0 and eHealth Exchange is the only adopter at this time. The eHealth PEP interacts with SAC using XACML 2.0 and maintains an internal adapter which converts between XACML 2.0 and 3.0 versions. The adapter only exists for backward compatibility and all new applications are required to transact using XACML 3.0. Additionally, many legacy systems support only object-based access control lists (ACL) that do not include XACML profiles externalized from the business logic.

OAuth is another open standard for authorization. It provides delegated access to a third party resource without exposing the authentication credentials used. This is what allows a user to

access a resource on one website by authenticating with their username and password for another. The resource provider can restrict which providers can be used to authenticate. While VA has implemented instances of OAuth for delegated application access, it currently does not have an official standards profile that accommodates OAuth tokens for access control decisions. The improper implementation of this standard is not uncommon and leads to risks of unauthorized access. Compatibility is also a concern as VA provides veterans greater ability to control access to their health information. Use of the OAuth standard does not dictate what attributes must be available to successfully authorize access.

3 FUTURE CAPABILITIES

While IAM offers multiple authorization services now, the future state for VA enterprise authorization services will increase application owner engagement with IAM services to provide consistent authentication, authorization and auditing across VA. This informs the design of authorization services that will cover the following primary goals:

- Define standards for centralized services for RBAC, ABAC and hybrid controls beyond those inherent to the application and guidance for implementation.
- A consistent methodology for assessing application requirements to match the security requirements for appropriate use of RBAC, ABAC and application technical controls.
- Define security considerations for standards and protocols used to support authorization including RBAC, ABAC and others.

3.1 Establish the Foundation for Centralized Authorization

While there are multiple benefits to enforcing policy at runtime, shifting from a RBAC solution is not as simple as procuring an ABAC solution and deploying it. The proper foundation must be established to provide consistent inputs for the authorization architecture. The following are key points to be considered to enable the use of policy for authorization while limiting complexity.

- **Analyze the Existing State** – An analysis of current usage patterns can identify which roles and policies are currently being used and how.
- **Gather Enterprise Policies** – Identify the policies that are applicable across the enterprise and can be reused from one application to another. This would be the area where device information and other contextual information are considered as a possible factor in authorization decisions.
- **Standardize the Authorization Architecture**: The creation of a standard architecture for designing the various types of authorization solutions will reduce complexity and the

deployment of excess PDPs. Avoid proprietary authorization solutions as much as possible. Application owners will engage with IAM in accordance with IAM Access Services (AcS) Integration Patterns for designing the appropriate authorization solutions.

- **Identify the Attributes:** Runtime authorization is dependent on attributes and contextual information to correctly enforce policy. The VA Virtual Directory Service combines attributes from multiple sources. While this increases the ability to create more granular policies, it also increases the need for a defined and predictable structure for naming and defining attributes. Variations from one source to another can lead to authorization errors. Policy authors will need to be able to review all available attributes and know if the attribute values are consistent. Attributes will be governed by a common vocabulary.
- **Policy Organization:** As the amount of policies increases, it becomes more critical to govern and organize the policy. This includes the following areas:
    - Policy creation, distribution and maintenance
    - Policy Naming Convention
    - Mapping of Technical Policy to Business Policy
    - Tracking of Entitlements
    - Determine who will create the policy. Minimize the number of policy management authorities
- **Establish Governance** – Governance of authorization services will be supported by ESS and VA Enterprise Technical Architecture compliance criteria, as aligned to the overall IT vision established in the Enterprise Technology Strategy Plan (ETSP). This includes selecting and prioritizing applications for integration with enterprise authorization services. Adoption initiated by system owners cannot take into account enterprise-wide priorities.
- **Define Success** – The authorization solution and each onboarded application shall have metrics by which the success or the failure of the service can be adequately measured. Service baselines will drive changes within the service. For example, decreases in provisioning timeframes due to increased use of a Self Service portal could trigger accelerated expansion of the service.

3.2 Assessing Appropriate Access Controls

Effective Authorization controls are required to manage risk across the enterprise. Just as with managing other areas of risk, a standardized approach is needed and the level of controls will be matched to the level of risk. Authorization controls can be implemented at two points in time: 1) during Provisioning when account permissions are set and 2) during runtime when the application is accessed. A standardized approach is needed to address both areas.

IAM will serve as a single point of contact for assistance in aligning authorization services to meet business requirements and achieve compliance by transforming business rules into technical authorization policies. It is at this point that each line of business must take into account their specific compliance requirements in addition to internal requirements. This may include enterprise-wide compliance such as FISMA as well as compliance for a specific function such as PCI for financial transactions or HIPAA and HL7 for healthcare. Organizations achieve this by the following process:

- **Identify the Business Requirements**: The business requirements will align with the business model. The process of establishing information system boundaries and the associated risk management implications is an organization-wide activity. This includes taking into account mission and business requirements, technical considerations with respect to information security, and programmatic costs to the organization. Through understanding the business requirements, system owners can determine level of access of certain users, the types of permissions, and isolating authorization credentials to certain applications (e.g., VBMS for Veterans, VAIQ for federal staff users only). Essentially, they serve as the building blocks for creating language in authorization policies that will help map out an effective way to select the optimal access control methods for your lines of business and to govern that access. The key question stakeholders should ask to identify authorization requirements is who should be able to access data, what actions do they perform and under what conditions?
- **Building Natural Language Policies**: These policies will permit users to define policies about the data being shared specifically defining access control rules and describing access requests. This will present implementation requirements based on a policy framework. Defining privacy preferences within the natural language policies should remain simple and straightforward; essentially it must be as expressive as natural language. Access control decisions will be transparent and well explained to users. An example of a method for structuring the natural language policy is through grammatical building blocks:
    - **Subject:** Who is demanding access to the information assets
    - **Action:** The specific function the user wants to perform.
    - **Resource:** Identifying the information asset or object impacted by the action.
    - **Environment***:* Identifying context in which access is requested.
- For example, a business requirement could be to only allow treating doctor's access to the records of patients that reside in the Northeast region of the United States, unless PII is removed. The natural language policy would be "doctors listed as treating patients (subject) can read (action) records (resource) of patients located in the Northeast region

of the United States (Environment). All other users cannot read patient records unless PII is removed."

- **Determining the Level of Granularity Required**: Once basic policies are defined, it becomes easier to determine the authorization type and level of granularity of that authorization. Granularity can stem from different perspectives including subject, object, actions and content. System owners have to consider these perspectives as they document their use cases to look for opportunities to simplify the authorization requirements. For example, a policy can apply to the entire population of a department, such as VHA staff, while some policies may be specific to a limited number of users, such as staff in a specific hospital. Business analysts usually have this perspective when defining business roles to increase granularity for administrative simplicity.
- **Selecting Appropriate Access Controls:** Mapping the policy needs to the required technical controls will help VA implement the correct authorization service. Stakeholders require assistance to make the proper selection. Choosing a service based on simplicity could create excessive privileges while choosing an overly complex solution could create administrative overhead with limited returns. The following are common authorization service types:
    - RBAC - This access control ties people to permissions. They can be used to assign entitlements to users who share similar responsibilities or attributes. This would be a good choice to govern access control over large groups of users who all have the same level of access all the time.
    - ABAC – This access control type binds people to permissions based on specific types of attributes (subject, action, resource and environment). ABAC is a good choice for modeling complex authorization decisions.
    - Hybrid – Utilized when neither RBAC nor ABAC individually can address the complex access management requirements. Many organizations are combining the roles and attribute based access controls for both RBAC and ABAC to provide effective access control for distributed and rapidly changing applications. Combining RBAC and ABAC will uncover opportunities for optimization. When a hybrid model is used, the base permissions will be defined by RBAC and further restricted by ABAC due to the current investment in RBAC solutions at VA. As the policy base within the ABAC solution is matured, IAM will evaluate a transition to an authorization model based on attributes.
- **Implementing the Access Controls:** Once a control has been selected then an authorization service can be matched to the application. Through the Provisioning, AMS, and SAC services, AcS provides flexibility by supporting automation of pre-populated user lists, management of authorizations, as well as RBAC and ABAC. Based on the type of application and the applicable access control policies, VA applications may leverage

Provisioning and/or Specialized Access Control (SAC) for authorizing access to information resources.

3.3 Security for the Authorization Infrastructure

In order to ensure enforcement of policy and the security of application access, VA will centralize the governance of applications. This does not mean that all applications conform to a single solution, but all must follow a minimum set of controls and adopt ESS, whenever possible.

The OAuth 2.0 Authorization framework is increasing in use due to the ability of third party applications to obtain access to an HTTP service by orchestrating an approval interaction between the resource owner and the HTTP service. The improper implementation of the OAuth framework has led to significant unauthorized access risks of services hosted by major commercial organizations. Below is an overview of the Code Grant Authorization Flow.

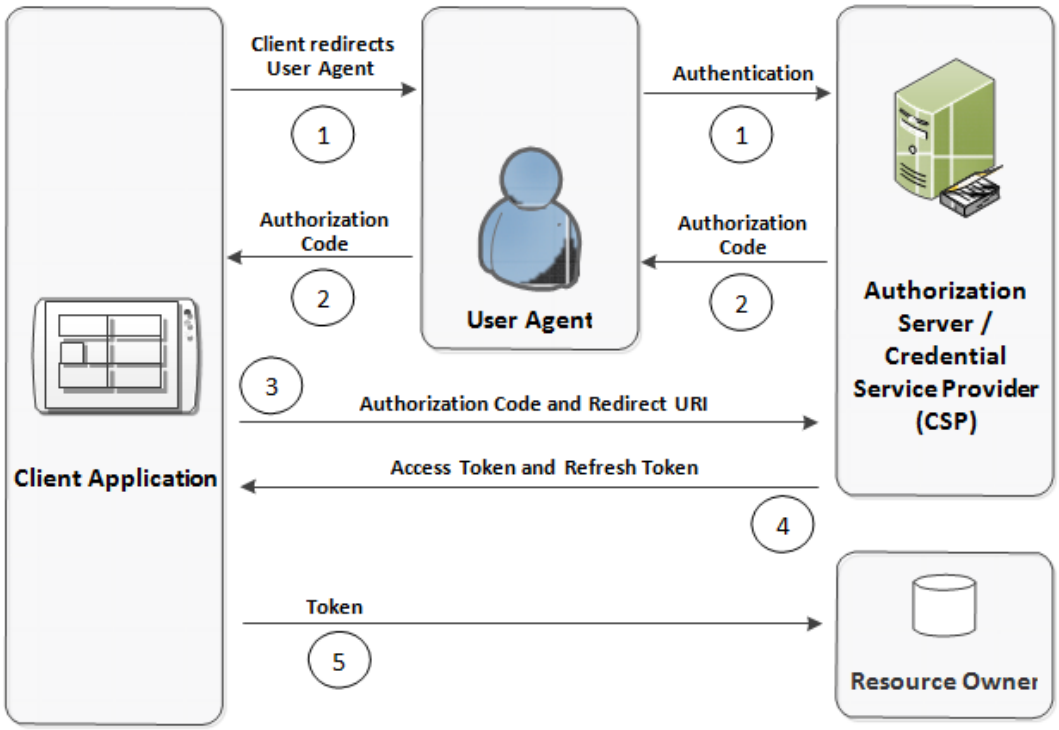

FIGURE 1: AUTHORIZATION CODE GRANT FLOW OVERVIEW

Authorization Code Grant Flow

1. The client application initiates the flow when authorization is required to access a resource by directing the resource owner's user agent to the authorization server. The initial request contains the client identifier, requested scope, local state, and the

redirection URI to which the authorization server will send the user-agent back. The authorization server authenticates the resource owner via the user agent.

2. The authorization server redirects the user-agent back to the client using the redirection URI provided along with the Authorization Code.
3. The client requests an access token using the authentication code and provides the redirect URI.
4. The authorization server validates the authorization code and validates the redirect URI has not changed. The authorization server responds with an access token and optionally a refresh token.
5. The client application presents the access token to the Resource Owner who determines which resources are accessed.

OAuth Security Practices

There are two considerations when using OAuth: Security and Interoperability. RFC6749 describes the OAuth 2.0 framework and RFC6819 describes the OAuth 2.0 Threat Model and Security Considerations. The RFCs provide some insight into potential risks associated with the use of OAuth 2.0. Highly publicized weaknesses surrounding the use of OAuth have primarily revolved around weak or improper implementations of the RFC. The minimum specifications possible using the RFCs may not provide optimal security. It should also be noted that OAuth 2.0 is not meant to be used for authentication.

For interoperability, it is recommended IAM adopt a common profile and contribute to its development to achieve a high level of security while maintaining the ability to share information with external groups. The SMART Health IT profile is one possibility. It is already being evaluated by the National Institutes of Health (NIH) in collaboration with the Office of the National Coordinator for Health IT (ONC) as part of their Sync for Science (S4S) pilot[1] for compliance with Health Level 7's Fast Healthcare Interoperability Resources (FHIR). The SMART Health IT OAuth profile already adheres to a number of OAuth 2.0 best practices. Although the profile is built for healthcare sharing, it demonstrates a secure foundation for use of OAuth in many parameters. However, SMART does not include all best practices and puts some considerations out of scope. A sample set of recommendations to strengthen the practices in that profile is listed in Appendix F.

3.4 Alignment to the One-VA Technical Reference Model (TRM)

The enterprise authorization services provided by IAM leverages approved tools and standards catalogued in the One-VA Technical Reference Model (TRM). The following table includes a

[1] https://www.healthit.gov/buzz-blog/health-innovation/nih-and-onc-launch-the-sync-for-science-pilot/

mapping of technology categories to approved technologies and standards, and mandated ESS required by all VA projects.

TABLE 2: LIST OF APPROVED TOOLS AND STANDARDS FOR ENTERPRISE AUTHORIZATION

Technology Category	Example Technologies	Example Standards	Mandated ESS
Authorization	Axiomatics, Active Directory	XACML, LDAP	IAM Access Services
Messaging	WebSphere SOA Suite	SOAP (legacy interfaces), HTTPS (REST), JMS	eMI
Encryption	FIPS 140-2 compliant Cryptographic modules	WS-*, TLS per FIPS 140-2 requirements	IAM Access Services
Security Gateway	SecureSpan, DataPower	HTTPS	API Gateway

3.5 Alignment to Veteran-Centric Integration Process (VIP)

All projects will integrate with IAM services for authorization and will complete a service request for IAM services prior to Critical Decision 1 in the Veteran-focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely and predictably. VIP is the follow-on framework from Project Management Accountability System (PMAS) for the development and management of IT projects, which will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities.

4 USE CASES

The following sections describe some general use cases that could apply to the use of an Authorization Enterprise Security Service.

4.1 Conditional Data Access Based on Attributes

4.1.1 Purpose

This use case describes a feature of eHealth Exchange that requires advanced or granular access controls to meet compliance with HIPAA and HL7 requirements. Role based access control is not adequate in this situation as the provider is able to access the patient's Electronic Health Record (EHR) only when certain conditions are met. These conditions need to be dynamically

updated to provide efficient patient services. Changing an ACL related to the EHR would require a high level of effort. A more automated solution is desired.

4.1.2 Assumptions

- Application users have been assigned a role. This role may be treated as an attribute for purposes of determining authorization
- The patient has an EHR that is in a system that provides access to both federal and private parties for the purpose of providing the patient medical services
- All parties use the same application or a framework in which the accessing application uses the same attributes and policies to achieve consistent authorization and access controls
- The business requirements related to HIPAA and HL7 compliance have been provided by the application owner
- The provider has made available to the patient an electronic means to record their permission to opt-in to the health information exchange
- The integrity of user actions and the EHR is ensured through identity and access management solutions and other controls outside the scope of this use case

4.1.3 Use Case Description

1. The eHealth Exchange has to comply with Title 38 section 7332 which requires VA to get authorization to exchange health information with non-armed forces organizations when the patient meets certain protected conditions.
2. The current process uses signed authorizations received on paper or scanned. The system owner, acting on feedback from private healthcare providers, desires to improve this by electronically marking a patient's Electronic Health Record (EHR) to opt-in Veterans for health information exchange at the point of care.
3. The system owner has identified the following business requirements that apply:
    a. During the admission process, the patient’s information sharing status must be displayed.
    b. The patient must be able to digitally provide their authorization for sharing at the point of service.
    c. The system must record any changes to the patient’s information sharing status.
4. The system owner contacts IAM and submits a request for assistance by describing the challenge, business requirements and desired outcome.
5. IAM analyses the business requirements and designs the following solution:
    a. IAM provides a service to allow the patient to modify the EHR to record their sharing preference. VAP is used to allow the patient to use their authorized

credentials to authenticate to the system and authorize the configuration of an attribute designed to record the patient's information sharing status.

b. The attribute is imported into VAP to make it accessible for authorization decisions.
c. The SAC service gathers information from eHealth Exchange, through a XACML message to implement an ABAC solution. This externalizes the PDP from the application for this function. Technical policy is created that bases access on the setting of the attribute related to sharing in addition to the normal access control policies.
d. The system owner performs testing to validate that the technical policies have met the business requirements and is compliant. The end goal is met of creating an efficient, digital process while reducing the risk of improper sharing of EHR data with "7332 protected conditions."

4.2 Restriction of RBAC Using ABAC

4.2.1 Purpose

This use case describes a scenario where VA has a new policy going into effect across the enterprise that limits a user's access based on certain conditions. The new policies will go into effect across the enterprise and will provide the conditions for access requirements that will mitigate high risk access scenarios.

4.2.2 Assumptions

- Users have assigned roles which grant elevated privileges on a system or systems
- The attributes related to authorization policy decisions are available
- The provided policy restrictions are for illustrative purposes only and are not indicative of current VA policy
- A directory-based RBAC solution is currently in use for the affected accounts

4.2.3 Use Case Description

1. VA has enacted an insider threat program and has created new policies to mitigate high risk access scenarios. Users with administrator or root level access to systems will continue to have the same level of access based on their role, but the access will be restricted based on the following conditions:
    a. When their public IP address originates outside the US
    b. When geolocation of the user changes unexpectedly
    c. When access to PII or PHI is attempted with an elevated account

2. In response, IAM has implemented an ABAC solution as a gateway through which authorization requests are performed
3. Technical policies are created which meet the business requirements defined by the Office of Information Security (OIS) based on the conditions provided by other VA systems
4. The ABAC gateway applies the policies to restrict the access provided under RBAC when the defined conditions are met

4.3 External Use Access/Unexpected User

4.3.1 Purpose

This use case describes a scenario where National Institutes of Health (NIH) in collaboration with the Office of the National Coordinator for Health IT (ONC) has requested VA to participate in their research project called "Sync for Science". The project will allow veterans the ability to contribute their data to research. The project uses the SMART Health IT OAuth profile to allow participants to authorize access to their data.

4.3.2 Assumptions

- NIH has made a significant investment in the OAuth profile which would prevent the use of other standards
- The CSP validates and records the attributes required for authorization
- The user is not registered in the system before attempting to access the application

4.3.3 Use Case Description

1. NIH has contacted VHA to collaborate on the research project
2. VHA has evaluated the project to establish the business requirements. VHA has applications which can support the research project but lacks a service to connect to NIH for data sharing
3. VHA contacts the IAM service to determine which services are available to allow the two agencies to collaborate and provides their business requirements for interoperability and compliance
4. IAM identifies the following technical solution:
    a. The IAM Single Sign On External (SSOe) will be used to authenticate external users to the application. SSOe already integrates with the DoD DS Logon and other accepted CSPs
    b. IAM evaluates the SMART Health IT OAuth profile being used by NIH. Additional security controls are identified to strengthen the public profile to meet VA

requirements. IAM shares these configurations required for interoperability and recommends they be added to the public profile.

c. IAM creates an OAuth service that integrates with SSOe, meets VA requirements and is interoperable with NIH
d. A mobile app is designed so that the veteran can use their supported CSP to authenticate to the mobile app and grant permission to participate in the project
e. Authorization is forwarded to the SAC service which evaluates the request based on available attributes. Specific PHI VHA does not want to be shared is dynamically blocked by the SAC service based on defined policy

APPENDIX A. SCOPE

The purpose of this document will be to provide strategic direction for VA to establish enterprise-wide authorization services using a common set of standards for attribute-based and role-based access control (ABAC/RBAC). Such a service would allow the VA to define and edit authorizations that determine what resources (e.g., systems, services, and objects/data) can be executed or accessed by an authenticated user or process, ensuring that a user (or process) may only do what he or she has permission to do, thereby increasing data security and protection of sensitive information, including PHI and PII.

- Identify a centralized method for ensuring a consistent authorization process across all VA applications
- Identify best practices for migrating to new authorization processes
- Provide guidance on preparations required by application owners to integrate with the authorization service

Document Development and Maintenance

This Enterprise Design Pattern was developed collaboratively with stakeholders from the ESS Security Group and included participation from VA's Office of Information and Technology (OIT), Product Development (PD), Office of Information Security (OIS), Architecture, Strategy and Design (ASD), and Service Delivery and Engineering (SDE). In addition, the Technology Strategies team engaged industry, external government agencies, and academic experts to review, provide input, and comment on the document. This document contains a revision history and revision approval logs to track all changes. Updates need to be coordinated with the Office of Technology Strategies' lead for this document; they will facilitate stakeholder coordination and subsequent re-approval depending on the significance of the change.

APPENDIX B. DEFINITIONS

This appendix provides definitions for terms used in this document, particularly those related to databases, database management, and data integration.

Key Term	Definition
Access	Interaction with a computer system for instance VistA. Such interaction includes data retrieval, editing (create, update, delete} and may result from a variety of technical mechanisms including traditional user log on, consuming applications exercising middleware based connectivity, SOA service requests, etc.
Accurate, Unambiguous User Identity	Information that represents the actual human that is interacting with a computer system, including the initiation of that interaction.
Application Proxy	Construct involving the use of a generic, non-human "user" entity to represent "machine-to-machine" interaction where appropriate for interactions that do not involve a specific end user.
Auditing	The inspection or examination of an activity based on available information. In the case of computer systems, this is based on review of the events generated by the system or application.
Consuming Application	The application consuming services from a provider system. Generally used when discussing a front-end application supporting a user, but even service providers can themselves be a consumer of other services.
Delegated Access	When an owner authorizes another to serve as his or her representative for access to a particular resource.
Enterprise Shared Service (ESS)	A SOA service that is visible across the enterprise and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions.
Identity Attributes	Characteristics which describe the user (e.g. name, National Provider Identifier, organization, etc.). Establishment of reasonably reliable "unique identity" is generally based on a combination of multiple identity attributes. Specific user identifiers include employee number and email address; may vary from organization to organize ion but identifier types ought to remain constant for all transactions from a specific organization.

Key Term	Definition
Machine-to-Machine Interaction	In some cases, application processes resulting from workflow (not human interaction} will result in interaction with provider systems to download data, initiate background processing, etc. These actions are not directly initiated by a specific human and the interaction would be attributed to an NPE, possibly via a service account.
OAuth 2.0	An open standard for authorization which provides clients a method to delegate access to server resources on behalf of a resource owner without sharing user credentials. OAuth 2.0 is not backwards compatible with OAuth 1.0.
Provider System	A system (e.g. VistA} which *provides* service at the request of a consuming application.
SAML	An XML-based open standard data format for exchanging authentication and authorization data between parties.
System for Cross-Domain Identity Management (SCIM)	The SCIM Protocol is an application- level, REST protocol for provisioning and managing identity data on the web as described by IETF RFC 7642.
Service Oriented Architecture	A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations
User	A person that interacts with a computer system application. In this context, a "user" is not limited to VA staff members and may include persons from external organizations, patients, beneficiaries, designees, etc.
SSO and User Provisioning	A services provided by Identity and Access Management (IAM) for authenticating users and providing user provisioning information to other systems.
User Types	Traditional types including VA staff, staff of non-VA agencies (e.g. DoD), staff of private sector organizations (e.g. Walgreens); nontraditional, non-staff types including patients, beneficiaries, designees, sponsors, caregivers, etc.

APPENDIX C. ACRONYMS

The following table provides a list of acronyms that are applicable to and used within this document.

Acronym	Description
AD	Active Directory
ADFS	Active Directory Federated Services (SSO based on SAML/WS-*)
API	Application Program Interface
ASD	Architecture, Strategy and Design
CSP	Credential Service Provider
eMI	Enterprise Messaging Infrastructure
ESB	Enterprise Service Bus
ESS	Enterprise Shared Service
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol over TLS
IAM	Identity and Access Management
IETF	Internet Engineering Task Force
IdP	Identity Provider
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
PCI	Formally known as Payment Card Industry Data Security Standard (PCI-DSS)
PKI	Public Key Infrastructure
PIV	Personal Identity Verification
REST	Representational State Transfer
RFC	Request for Comment
RPC	Remote Procedure Call
SAML	Security Assertion Markup Language
SCIM	System for Cross-Domain Identity Management
SDD	System Design Document
SPML	Service Provisioning Markup Language
SOA	Service-Oriented Architecture
SSOe/SSOi	Single Sign-On External/Internal
TLS	Transport Layer Security
TRM	Technical Reference Model
VHA	Veteran Health Administration
VistA	Veterans Health Information Systems and Technology Architecture
XML	Extensible Markup Language

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the following VA OI&T references and standards applicable to all new applications being developed in the VA, and are aligned to the VA Enterprise Technical Architecture (ETA):

#	Issuing Agency	Applicable Reference/ Standard	Purpose
1	VA	VA Directive 6551 - http://www.techstrategies.oit.va.gov/docs/designpatterns/6551dir16.pdf	Establishes a mandatory policy for establishing and utilizing Enterprise Design Patterns by all Department of Veterans Affairs (VA) projects developing information technology (IT) systems in accordance with the VA's Office of Information and Technology (OI&T) integrated development and release management process, the Veteran-focused Integration Process (VIP).
2	VA OIS	VA 6500 Handbook	Directive from the OI&T OIS for establishment of an information security program in VA, which applies to all applications that leverage ESS.
3	VA IAM	VA Directive 6051	Department of Veterans Affairs Enterprise Architecture (VA EA), July 12, 2002.
4	NIST	NIST SP 800-162	NIST Guide to Attribute Based Access Control (ABAC), January 2014.
5	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.
6	NIST	SP 800-122	• Guide to protecting the confidentiality of personally identifiable information (PII). • Provides technical procedures for protecting PII in information systems. • Defines the information that can be used to distinguish or trace an individual's identity.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
7	GSA	FICAM	Federal Identity, Credentialing and Access Management roadmap and implementation guidance. Provides the common segment architecture and implementation guidance for federal ICAM programs.
8	US Congress	FISMA	FISMA of 2002, Public Law 107-347.
9	Federal	U.S. CIO, Federal Cloud Computing Strategy	This policy is intended to accelerate the pace at which the Government will realize the value of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.
10	Federal	FIPS 199	FIPS 199 (Federal Information Processing Standard Publication 199).
11	Federal	FIPS 200	Minimum Security Requirements for Federal Information and Information Systems.
12	HL7	HCS	Healthcare Privacy and Security Classification System (HCS), Release 1, August 2014.
13	HHS	Health Insurance Portability and Accountability Act of 1996	Provides national standards for electronic health care transactions and code sets, unique health identifiers, and security.
14	HHS	HIPAA Privacy Rule	This Rule set national standards for the protection of individually identifiable health information by three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically, August 2002.
15	HHS	HIPAA Security Rule	This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information, April 2005.
16	HL7	HL7 Version 3 Standard	Privacy, Access and Security Services; Security Labeling Service, Release 1, June 2014.
17	Oasis	eXtensible Access Control Markup Language (XACML) Version 3.0	Policy language standard for access control requirements.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
18	VA	VA Memorandum Consideration of Open Source Software (VAIQ#7532631)	Establishes requirements to evaluate Open Source Software solutions and consider OSS development practices for VA-developed software.

APPENDIX E. CURRENT AUTHORIZATION SOLUTIONS PROFILED

Sponsor: SDE

Solution: Microsoft Active Directory

Type: RBAC

Description: VA has a single forest Active Directory with multiple domains. Many stakeholders use the built-in roles along with customized roles to implement RBAC solutions. Non-Windows systems can use LDAP lookups. Integrated applications are numerous.

Limitations: Built-in roles are too high level for more implementing RBAC except at a broad level. The creation of custom roles can be time consuming and still requires manual auditing to add and remove users from roles.

Sponsor: IAM

Solution: Provisioning/Sailpoint

Type: RBAC

Description: The IAM AcS provides a solution that associates an identity with one or more accounts and default privileges on IT systems in an automated and programmatic fashion. It provides an automated system account management to create, terminate, and change access rights across all applications that integrate with IAM services. The IAM's provisioning capability supports gathering and maintaining authorization data in an enterprise level authorization repository, where VA operators and administrators can manage accounts, access rules, user privileges, and attributes. The provisioning service maps authorized roles, individuals, or objects with the appropriate access to resources. It also provides account management for consuming applications based on their user role by gathering and analyzing access control information to manage the role life cycle and support enforcement of role based policies.

Limitations: Sailpoint is currently limited to role analysis and provisioning of users access rights. Technical challenges have inhibited the use of current data for a bottom-up approach to role creation.

Sponsor: VHA

Solution: Enterprise Messaging Infrastructure (eMI)

Type: RBAC

Description: The Enterprise Messaging Infrastructure (eMI) Service Oriented Architecture (SOA) is designed to mediate data exchanges between VA and DoD via the Defense Medical Information Exchange (DMIX). This includes access to applications such as Virtual Lifetime Electronic Record (VLER), eHealth Exchange, VISTA Exchange and Bi-Directional Health Exchange (BHIE). eMI relies on the Enterprise Health Management Platform (eHMP). eHMP uses the VistA Exchanges Policy Enforcement Point (PEP) and Policy Decision Point (PDP) to implement Authorization.

Limitations: Authorization is highly dependent on the identification and use of specific attributes. Attributes may not be centralized and exist in each VistA host. System to system access may not pass user attributes for use in restricting access.

Sponsor: IAM

Solution: Specialized Access Control (SAC)/Axiomatics

Type: ABAC

Description: IAM SAC offers a Policy Decision Point (PDP) service for purposes of dynamic, fine-grained, Attribute Based Access Control (ABAC) in order to protect integrated consuming applications and their data assets. Consuming applications need to transact with them using XACML 3.0 using SOAP/HTTPS.

Limitations: Applications may not support XACML 3.0 and as a middleware solution, policy options may be limited in scope. eHealth Exchange is the only adopter at this time. A few stakeholder concerns have been raised with the current approach:

- Many legacy applications will not support XACML.
- Latency between the application and PDP may affect performance.
- The Policy Administration Point (PAP) tool requires an upgrade to enable access control for policy authoring. The current implementation of the SAC service relies on OS-level authentication/access controls to allow or disallow access to the PAP.
- Potential impact of sharing PDPs with other applications.

Sponsor: IAM

Solution: Authorization Management Service (AMS)

Type: RBAC

Description: Authorization Management Service (AMS) is designed to provide an enterprise-wide capability for managing individual authorizations for access to protected information. Delegations are a type of authorization whereby a "delegator" (Veteran or Beneficiary) can request specific access privileges to a "delegate" (Caregivers, Family members, Legal guardians, etc.). AMS can serve as a source of Access Control Information (ACI), Policy Information Point (PIP) for the Specialized Access Control (SAC) service to consume for policy decisions. The Personal Representative Delegation (PR Delegation) and VA Healthcare Proxy Delegation (VAHP Delegation) represent two examples of AMS services in VA.

Limitations: This is a custom solution and currently supports the delegation of authority to access a veteran's record. Other authorization services are planned, but no yet available through this solution.

APPENDIX F. ANALYSIS OF SMART OAUTH PROFILE

The table below does not address all OAuth 2.0 specifications, particularly those that are required by the RFC, but reviews areas where the RFC allows flexibility and identifies areas where the SMART OAuth profile could be strengthened. Information on the SMART OAuth profile can be found here: http://docs.smarthealthit.org/authorization/.

Area	SMART Requirement	Recommendation	Purpose
Authentication	Authentication is out of scope.	Access should not be granted to clients that are not authenticated.	Provides protection against Denial of Service and unauthorized access.
		OAuth 2.0 shall not be used to authenticate clients. The OAuth 2.0 framework is not designed for secure authentication and shall rely on a compliant authentication method to validate the client's identity.	Provides protection against unauthorized access.
		Clients shall not be authenticated automatically using certificates or other methods that don't require user interaction.	Automated authentication increases the risk for manipulation of the authorization process by a malicious client through client impersonation or resource owner impersonation. It could also increase the risk of a Denial of Service attack.
		SAML shall be used to support the authentication process.	SAML provides audience restrictions which reduce the risk of an attacker using a malicious app to social engineer a user to authenticate and then substitute their own

Area	SMART Requirement	Recommendation	Purpose
Authorization Grant	Parameter "grant_type=authorization code". Indicates use of the Authorization Code Grant, although not explicitly.	Only the Authorization Code Grant flow shall be used. Implicit, Resource Owner Password Credentials and Client Credentials flows shall not be used.	Weaknesses in the design of other Authorization Grant methods create risks for impersonation and credential theft. This method also does not expose user credentials to other parties.
Client Secret	Not specified.	Deployment-specific client secrets shall be used when OAuth 2.0 is the intended communication protocol.	Use of a common client secret contained in the code use by all clients creates two risks: The secret can be obtained by reverse engineering the source code. If the client secret is revoked it affects all instances of the client. Use of a client secret unique to each client resolves this issue. The method of issuing the client secret is beyond the scope of OAuth 2.0.
Token Expiration	1 hour recommended.	Access Tokens shall have short expiration times not to exceed 15 minutes. (Implicit practice applied to Token Grant)	Access tokens are often bearer tokens which provide weak security and can't be revoked. A short lifetime limits the window of a compromise.
	Not specified.	The Authorization Server shall support revocation of a client secret.	The authorization server may need to revoke a client secret that is compromised and used to gain unauthorized access.

Area	SMART Requirement	Recommendation	Purpose
Resource Binding	"aud" parameter specifies the URL of the EHR resource server from which the app wishes to retrieve FHIR data.	Tokens shall be bound to the target resource server. The resource server shall validate the target server value.	Protects against malicious resource server use and the impact of replay attempts
Code/Token Thresholds	Not specified.	A threshold shall be established to block clients that issue more than the threshold of invalid codes or tokens.	Reduces the risk of Denial of Service by an attacker by submitting invalid content.
Token/ Client Secret Storage	Apps should persist tokens and other sensitive data in app-specific storage locations only, not in system-wide-discoverable locations. An app should NEVER store bearer tokens in cookies that are transmitted in the clear.	Client Secrets, Access and Refresh tokens shall be stored using FIPS 140-2 compliant encryption to maintain confidentiality. The storage location shall be protected by same-origin policy and client-specific storage locations only, not in system-wide-discoverable locations.	Protects from credential theft.
	Not specified.	Access tokens shall not be stored on the Authorization Server except as hashes.	Protects against an attacker gaining unauthorized access to the Authorization Server database and using it to acquire access tokens.

Area	SMART Requirement	Recommendation	Purpose
Token Integrity	Bearer tokens can be mitigated by digitally signing the token as specified in RFC7515 or by using a Message Authentication Code (MAC)	Tokens shall be digitally signed.	Prevents guessing, modification or spoofing of tokens.
	Not specified.	Tokens shall associate the Session ID with the authentication token	Prevents manipulation of the token on the client side (OWASP)
Nonce	The app MUST use an unpredictable value for the state parameter with at least 128 bits of entropy.	Informational Only. A JSON Web Token may be used to meet this requirement.	Provides confidentiality and integrity protection.
API Security/Token Proof	Not specified.	API calls from the application client shall provide the appsecret_proof parameter. This parameter is generated as a sha256 hash of the access token, using the app secret as the key.	This practice started by Facebook binds the access token to the client secret to prevent use of access tokens by parties besides the original requestor.
Access Token Use	Resource server must support bearer tokens passed in Authentication header.	Informational Only. The Access Token shall be sent in an HTTP authorization header and not as URI query-string parameters.	Prevents data leakage. URI parameters can end up in log files.

Area	SMART Requirement	Recommendation	Purpose
Redirect URI	Redirect uri must be registered.	Informational Only. A list of allowed Redirect URIs shall be registered with the Authorization Server to restrict redirects to authorized CSPs only. Customization by the client shall not be allowed.	Prevents Cross Site Request Forgery (CSRF).
	Requires TLS.	Redirect URIs shall use FIPS 140-2 compliant encryption in transport	This is connected to the requirement for all OAuth communication to use encryption for communications
	The authorization server shall ensure that the redirection URI	Informational Only. It shall also be declined if the Redirect URI is not registered.	Prevents redirection to an unauthorized URI.
	Requires fixed, fully-specified URL.	Informational Only. Subdirectories shall not be allowed to be set by the client.	Protects against using subdirectory variations to redirect to unauthorized URIs.
Browser Use	Allows use of iframes.	Native applications shall not use a browser embedded within the application to display the authorization request. The Authorization Server shall use an "x-frame-options" header with a value of “deny” to restrict the use of iframes and provide protection against clickjacking.	Protection against clickjacking although it may not work for all browsers.
Input Validation	An app should NEVER treat any inputs it receives as executable code	Informational Only. The Authorization Server shall sanitize values received to prevent the injection of unintended commands	Protection against code injection attacks.

Area	SMART Requirement	Recommendation	Purpose
Scope	The app then can declare its launch context requirements by adding specific scopes to the request it sends to the EHR's authorization server.	Informational Only. OAuth shall not be used to grant broad scopes such as would be granted to an administrator role.	Protection against arbitrary scope requests and excess permissions. Proper token definition may resolve issues such as introspection described by RFC7662.
User Education	Not specified.	VA users shall be educated on which redirects are legitimate for use by VA and warning signs of attempted social engineering.	The use of web redirects for authorizations can create a weakness in user behavior. User education aids in protection against social engineering.

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.