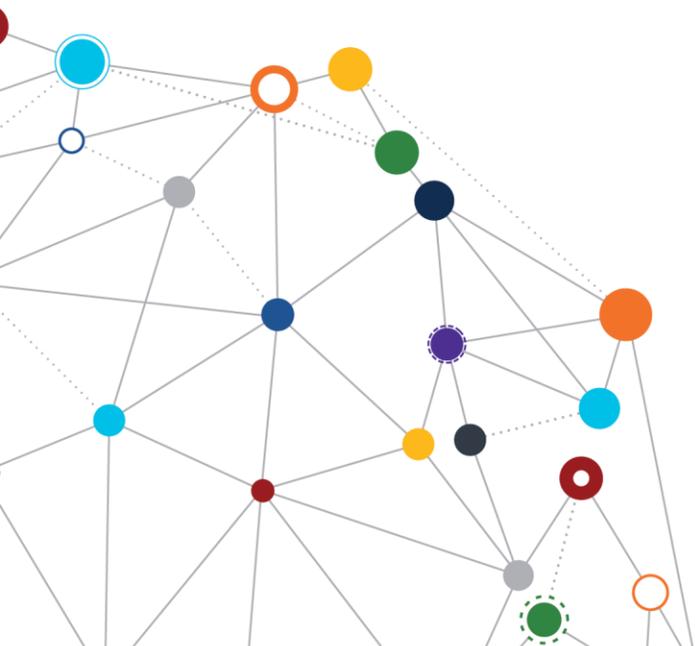


OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

Authorization Planning

September 2018 | Demand Management Division



VA



U.S. Department of Veterans Affairs
Office of Information and Technology



Table of Contents

- 1 Context 3**
- 2 Challenge 3**
- 3 Guidance..... 4**
 - 3.1 Establish the Foundation for Authorization..... 5
 - 3.2 Privacy Requirements for Collecting Attributes 6
- 4 Application of Practices 7**
 - 4.1 Conditional Data Access Based on Attributes..... 7
 - 4.1.1 Purpose 7
 - 4.1.2 Assumptions..... 7
 - 4.1.3 Use Case Description 7
 - 4.2 Key Practices 9
- 5 Impacts 9**
- Appendix A: References 10**

Figure 1: Overview of IAM Future Progression..... 4

Table 1: Change Matrix 2

Table 2: Key Practices Authorization Planning EDP 9

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	9/20/18	IAM EDP Authorization Planning Segment document approved



1 Context

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate secure access to VA resources for both internal and external users. IAM services are guided by the Office of Management and Budget (OMB) M 11-11, the Federal Information Processing Standard (FIPS) 200, the National Institute of Standards and Technology (NIST) Guidelines (800-63 and 800-53 per Appendix D), and the Federal Identity, Credential, and Access Management (FICAM) initiative.

VA has two general populations of users who require access: (1) internal users include employees, contractors, trainees, and volunteers, and (2) external users, comprised of Veterans, beneficiaries, and health partners, including employees and contractors from other Government agencies. All require varying levels of access to interact with VA services.

2 Challenge

There is a complex mesh of internally managed and externally hosted applications within VA. There is also a growing number of compliance mandates through FISMA, FIPS, the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), Health Level 7 (HL7), and others. Thus, it is a challenge to create and administer an appropriate authentication and authorization solution.

The FICAM Roadmap calls for the evaluation of attributes as a method for 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.¹

Application owners require guidance on how to plan for IAM integration to meet business goals for designing authorization within the application. Figure 1 shows the progression required from both the user and system owner to gain access to resources using IAM services. The area addressed in this document is highlighted in red.

¹ The FICAM Roadmap can be referenced at https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf.

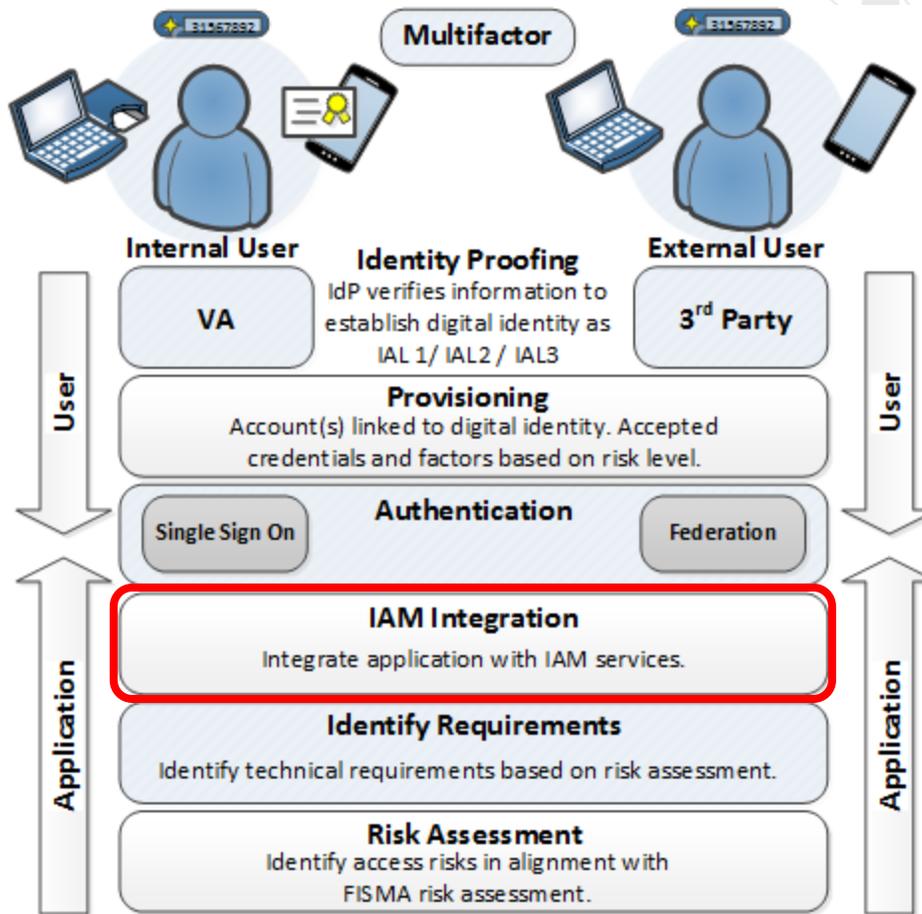


Figure 1: Overview of IAM Future Progression²

3 Guidance

This document provides a consistent process for assessing and designing authorization services across applications. The application owner will assess the business requirements for accessing functions within the 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 Role-Based Access Control (RBAC), ABAC, or hybrid controls; including those inherent to the application.

² Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) Enterprise Design Pattern (EDP) Team from information obtained from VA OIT IAM Subject Matter Experts (SMEs) and the National Institute of Standards and Technology (NIST) Special Publication 800-63A at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.



3.1 Establish the Foundation for Authorization

Effective authorization controls are required to manage risk across the enterprise. Just as with managing other areas of risk, the level of controls must 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.

- **Identify the Business Requirements:** Through understanding the business requirements, system owners can determine the level of access of all users, the types of permissions, and isolation of authorization credentials to certain applications.
 - Use natural language policies³ to define authorization roles in business terms. An example of a method for structuring the natural language policy is through grammatical building blocks:
 - **Subject:** Who is requesting access?
 - **Action:** What is the specific function the user wants to perform?
 - **Resource:** Identify the information asset or object impacted by the action.
 - **Environment:** Identify the context in which access is requested.
 - For example, a business requirement could be to only allow a treating physician, a doctor who provides medical treatment on an ongoing basis, 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.”
- **Select Appropriate Access Controls:** The correct authorization service is enabled by mapping the policy needs to the required technical controls. Selected controls shall align to the assurance levels (ALs) determined during the RMF process. Refer to the *Identity and Access Management (IAM) Risk Assessment Enterprise Design Pattern* (EDP) for more information on AL.⁴ The following are available authorization service types:

³ Refer to *Implementing and Managing Policy Rules in Attribute Based Access Control*, V Hu, National Institute of Standards and Technology (NIIST) and Computer Science & Engineering, University of Texas at Arlington, at https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=919151.

⁴ Refer to the *Identity and Access Management (IAM) Risk Assessment* EDP at https://www.oit.va.gov/library/files/edp/iams/IAM_RiskManagement_v1.pdf.

- **RBAC** -- This access control uses roles or groups to assign permissions. This is an appropriate choice to govern access control when many users will have the same level of access at all times.
- **ABAC** – This access control uses attributes to assign permission. ABAC is an appropriate choice for conditional access that is based on attributes that may change, or combinations of attributes.
- **Hybrid** – This service type is used when a combination of groups and attributes must be assessed to determine authorization. When a hybrid model is used, the base permissions may be defined by RBAC, and further restricted by ABAC.
- **Implement the Access Controls:** Once a control has been selected, an authorization strategy can be matched to the application. The application owner shall coordinate with the VA IAM service, as shown in Figure 1, to review existing roles and attributes and to determine the level of support required.

3.2 Privacy Requirements for Collecting Attributes

A credential service provider (CSP) uses attributes collected at the time of identity proofing to make authentication and authorization decisions. According to NIST, if a CSP processes attributes for purposes other than identity proofing, authentication, or attribute assertion (collectively “identity service”); related fraud mitigation; or to comply with law or legal process; the CSP must complete an assessment to determine the privacy impact of collecting the additional personally identifiable information (PII).⁵

If additional PII is collected as attributes to support project authorization design:

- The Privacy Office shall be contacted to perform a Privacy Impact Assessment (PIA) to determine if a System of Records Notice (SORN), or additional actions, are required.
- Measures *may* include providing clear notice, obtaining subscriber consent, or enabling selective use, or disclosure of, attributes.
 - If subscriber consent is selected, the CSP *shall not* make the consent for additional processing a condition of the identity service.

⁵ Refer to the National Institute of Standards and Technology (NIST) Special Publication 800-63-3, Section 4.4, *Identity Assurance Level Requirements*, at https://pages.nist.gov/800-63-3/sp800-63b/sec4_aal.html.

4 Application of Practices

The following use case relates to applying the described authorization planning principles to solution development.

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. RBAC is not adequate in this situation, since 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 access control list (ACL) that is 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 to provide 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 the permission to opt-in to the health information exchange (HIE).
- The integrity of user actions and the EHR is ensured through IAM solutions and other controls that are outside the scope of this use case.

4.1.3 Use Case Description

1. The eHealth Exchange must comply with Title 38, Section 7332, which requires VA to acquire authorization to exchange health information with non-armed forces organizations when the patient meets certain protected conditions.⁶
2. The current process uses signed authorizations that are received on paper or scanned. The system owner, acting on feedback from private healthcare providers, desires to

⁶ Title 38, Section 7332 can be referenced at <https://www.gpo.gov/fdsys/pkg/USCODE-2011-title38/pdf/USCODE-2011-title38-partV-chap73-subchapIII-sec7332.pdf>.

improve this by electronically marking a patient's EHR to opt-in Veterans for HIE 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 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 analyzes 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. Veterans Authorization and Preferences (VAP) is used to allow the patient to use authorized credentials to authenticate to the system and authorize the configuration of an attribute that is designed to record the patient's information sharing status.⁷
 - b. The attribute is imported into VAP to make it accessible for authorization decisions.
 - c. The security access control (SAC) service gathers information from eHealth Exchange, through a XACML message to implement an ABAC solution. This externalizes the policy decision point (PDP) from the application for this function. In addition to the normal access control policies, technical policy is created that is based on the access setting of the attribute that is related to sharing.
 - d. The system owner performs testing to validate that the technical policies have met the business requirements and is compliant. The end goal is to create an efficient, digital process, while reducing the risk of improperly sharing EHR data with "7332 protected conditions."

⁷ The VAP User Guide can be referenced at [https://www.va.gov/VDL/documents/Clinical/Veterans_Authorization_and_Preferences_\(VAP\)/vape_user_guide_2_7_0_20170427.pdf](https://www.va.gov/VDL/documents/Clinical/Veterans_Authorization_and_Preferences_(VAP)/vape_user_guide_2_7_0_20170427.pdf).

4.2 Key Practices

The following table highlights key practices identified in this EDP.

Table 2: Key Practices Authorization Planning EDP

Category	Area	Description
Identity and Access Management	Access Control/Authorization Planning	Business requirements for access to the service shall use natural language policies to define authorization roles in business terms.
Identity and Access Management	Access Control/Authorization Planning	Appropriate controls shall be selected in compliance with the assurance level (AL) implementation to enforce access control, using Role Based Access Control (RBAC), Attribute Based Access Control (ABAC), or a hybrid of these approaches.
Identity and Access Management	Access Control/Authorization Planning	The VA IAM service shall provide information on available roles and attributes and review proposed controls for integration with IAM services.
Identity and Access Management	Access Control/Authorization Planning	If additional attributes are required beyond what already exists in the VA Identity Store, the VA Privacy Office shall be contacted to perform a Privacy Impact Assessment (PIA); the Privacy Office will then determine if a System of Records Notice (SORN), or additional actions, are required.

5 Impacts

If authorization planning is not used to define technical requirements for IAM components of VA solutions, the following risks are increased:

- Delays to projects that encounter authorization scenarios that are not able to be supported by available solutions
- Privacy violations due to unauthorized capture, or storage, of PII
- Excessive or inadequate permissions that affect delivery of the business service

Appendix A: References

- DEA User Stories: <https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx>
- FISMA User Stories: <https://vaww.portal2.va.gov/sites/asd/AERB/FISMA Security Compliance/SitePages/Home.aspx>
- TRM: <http://trm.oit.va.gov/>
- NIST 800-63-3: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>
- NIST SP 800-162: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf>
- VA 6500.3: http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=733&FType=2
- VA 6510 (under revision): http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2

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.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.