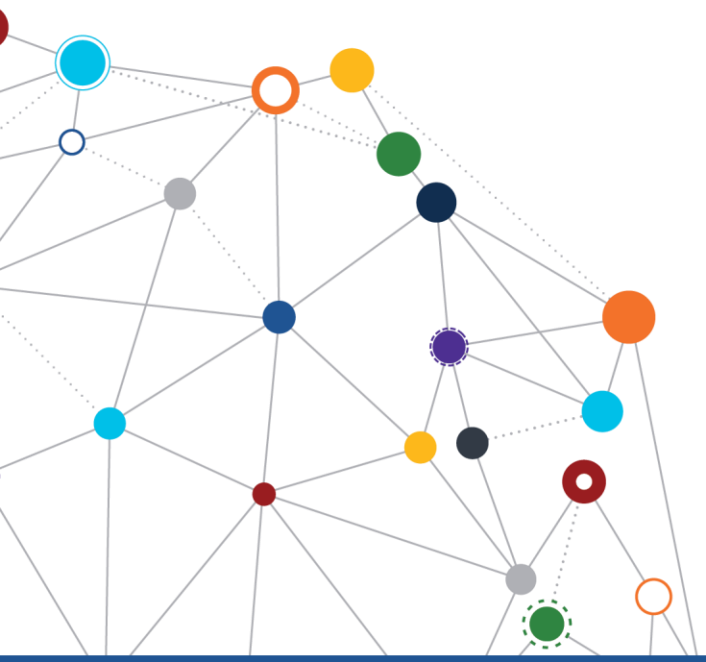
OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

Identity Provisioning

November 2018 | Enterprise Program Management Office



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

Table of Contents

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	11/5/2018	IAM EDP Identity Provisioning 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,[1] 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

Once identity proofing is completed, accounts must be provisioned to provide users with logical access to resources. The goal of identity provisioning is to automate user account management activities, thereby allowing access to services in a secure and efficient manner. In addition to account provisioning and deprovisioning, capabilities include the full identity lifecycle management, such as attribute management, credential management, and self-service functions.

Provisioning has been historically challenged by manual processes, which can delay the onboarding of new staff, offboarding of existing staff, and increase the support needed to execute this service. This may include the creation of custom code that requires review and integration with IAM services. Simple Provisioning Markup Language (SPML) is the current identity provisioning standard at VA and has been widely adopted since version 1.0 was published in 2003; however, the last major SPML update in 2006, SPML 2.0, did not show continued improvements in the standard.

Identity provisioning can benefit from increased automation, especially in response to increased deployment of systems in the cloud. The progression of how IAM services are engaged by users and system owners can be seen in Figure 1. This document focuses on the area highlighted in red.

[1] M 11-11 is a pending rescission. A draft OMB policy aligned with NIST 800-63 can be found at https://policy.cio.gov/identity-draft/.

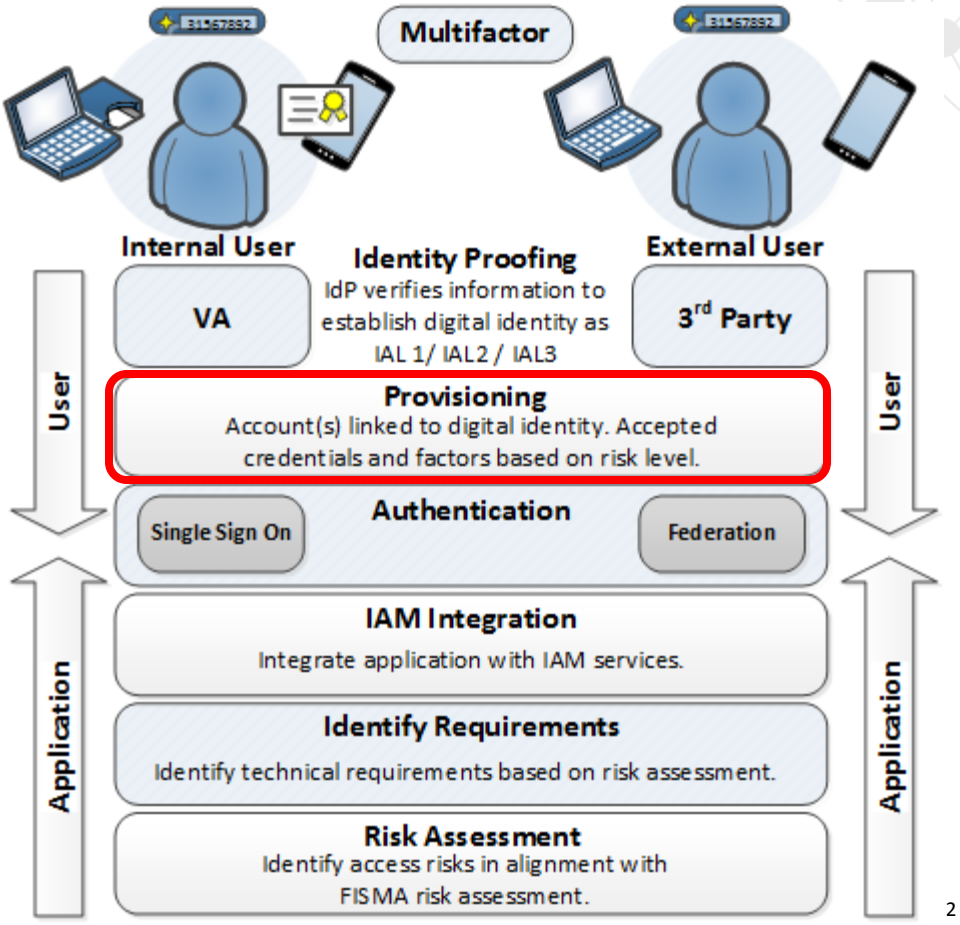


Figure 1: Overview of IAM Progression

3 Guidance

The design of identity provisioning services must support the VA Strategic Plan.[3] That support is provided through:

- Increased user productivity. This is primarily achieved by quickly providing users the appropriate level of access to applications. Delays in either connecting the application to IAM services, or in provisioning user accounts, can counteract efforts to improve productivity.

[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 Identity and Access Management (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] Refer to *VA FY 2018-2024 Strategic Plan*, Business Strategies 4.3.2, 4.3.5, 4.3.6, and 4.3.7, at https://vaww.ea.oit.va.gov/wp-content/uploads/2018/02/VA2018-2024strategicPlan.pdf.

- Creating administrative efficiencies. The increase in the number of applications used emphasizes the need for interoperability, automation, and self-service to maintain a growing portfolio of on-premise and cloud-based applications.
- Supporting security and compliance. Security and alignment to VA policies is achieved through central management of policy, enterprise visibility, and reliable execution of access decisions. Provisioning and de-provisioning services enhance security and meet account management compliance.

This document explains how technical decisions concerning available services can impact business workflow and the ability to meet VA business goals.

3.1 Preparing for Identity Provisioning

There are basic preparations necessary to support any identity provisioning solution.

Perform authorization planning. The project manager must have information that describes the permissions that users are assigned in the application. The permissions are based on roles, attributes, or a combination of both.[4]

Identify native application support for identity provisioning. When selecting solutions, the native level of support for identity provisioning can increase efficiency through automation. For example, the Workday Web Services (WWS) provides a Simple Object Access Protocol (SOAP)-based[5] Web Services Application Programming Interface (API), with corresponding Web Services Description Language (WSDL) and Extensible Markup Language (XML) Schemas. This guides how user provisioning is integrated. This application could use an existing Azure Active Directory user provisioning service that is based on the custom Azure Active Directory (AD) Graph API, or a custom interface using SOAP and SPML could be created. The VA Office of Identity, Credential, and Access Management (OICAM) will confirm if an application is supported without further customization. It is recommended that project teams prioritize solutions that support System for Cross-domain Identity Management (SCIM) 2.0.

Identify the method of trust between systems. Identity provisioning relies on a trust that is created between systems. Before user accounts are provisioned, the changes requested by identity provisioning must be authorized. Transport Layer Security (TLS) mutual authentication, using X.509 certificates, must be used as the primary mechanism for client authentication to the endpoint. The *Non-Person Entity* (NPE) Enterprise Design Pattern provides more

[4] For more information, reference the *IAM Authorization Planning* Enterprise Design Pattern (EDP) at https://www.oit.va.gov/library/recurring/edp/index.cfm.

[5] SOAP is an XML-based messaging protocol that is used for defining higher-level application protocols for increased interoperability in the implementation of web services in computer networks. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission (Source: https://msdn.microsoft.com/en-us/library/ms995800.aspx).

information on system to system authentication.[6] VA OICAM will provide information on supported options for creating a trusted connection to the application.

Identify the workflows for identity lifecycle management. A trigger is an event that starts an identity management workflow. The identity provisioning service must be able to monitor the business triggers to automate the workflow. To do this, identity provisioning must consider all authoritative data sources[7] (ADSs) of user data. For example, a human resources (HR) solution may be the ADS for VA staff, but a procurement system may be the ADS for contractors. To identify common triggers or events, and the approval workflow for all users of the application, the following should be included as part of business flow diagrams:

- New user account provisioning
- Attribute change management
- Role or permissions change management
- Self-service functions, such as access requests, password management, and delegated administration
- Auditing and reporting
- User account deprovisioning

VA OICAM will confirm the options available through the identity provisioning portal.

3.2 Identity Provisioning Protocols

All identity provisioning technical standards should support basic operations, such as add, modify, delete, and list. Not all standards provide the same capabilities, so it is important to understand the limitations of each standard. The use of standard protocols is meant to reduce proprietary provisioning connectors and processes. There are two standards mandated by the enterprise; for identity provisioning, solutions should support either SPML, or System for Cross-Domain Identity Management (SCIM).

Service Provisioning Markup Language (SPML)

SPML remains the default protocol for identity provisioning at VA, but system owners must prepare for evolving technologies/standards. SPML defines an XML and SOAP-based protocol

[6] Refer to the *Non-Person Entity* EDP at https://www.oit.va.gov/library/recurring/edp/.
[7] For more information on ADS, refer to the *Enterprise Data Access* EDP at https://www.oit.va.gov/library/recurring/edp/index.cfm, which includes documentation on the Data Governance Council (DGC), which oversees policy and authoritative data sources. (Also refer to https://vaww.ea.oit.va.gov/enterprise-architecture/data-architecture/, and internally on VA Pulse at https://www.vapulse.net/groups/data-management-council). In addition, the *Data Integration and Interoperability* EDP is currently under development, with projected publication in December 2018.

for creating, managing, and deleting identities. SPML requires a certain amount of manual intervention due to the following:

- SPML lacks a common schema definition for objects.
- SPML is complex. It is extensible, but this requires more customization.
- The specification does not provide a means to discover how resources are presented in the target system.
- The lack of adoption by target systems requires custom integration.

VA IAM has worked to overcome these obstacles by adopting specific functions of SPML and publishing the support for SPML functions and schema. This makes it easier for developers to implement SPML, using the VA Provisioning SPML service.[8]

System for Cross-Domain Identity Management (SCIM)

SCIM is an open standard for identity provisioning to applications that began in the cloud, but it is now also used on premise. SCIM 2.0 is an extensible, Representational State Transfer (REST)-based identity management standard. SCIM is widely supported by cloud service providers (CSPs), such as Azure, and vendors such as CA, GitHub, Oracle, Salesforce, ServiceNow, VMWare, and others. SCIM communicates user identity data between the application and service providers. A benefit of SCIM is that it simplifies and automates the user identity lifecycle management process. The identity provider (IdP) can provide information on identities to the application. When changes are made, such as with create, read, update, and delete (CRUD) permissions, SCIM automatically syncs the changes to the application. The IdP can also read identities from the application to add to its directory. The following are included as SCIM benefits.

- SCIM integrates with Security Assertion Markup Language (SAML) and OpenID Connect (OIDC).
- SCIM is built on REST/JavaScript Object Notation (JSON) formats; it follows the modern API format and is stateless.
- SCIM can provision users automatically to applications across multiple identity domains.
- SCIM supports operations (create, read, replace, delete, update, search, bulk edits), discovery (configurations, resources, schemas), and filtering.
- SCIM can sync custom attributes, or optional user schema, as well as the common attributes.
- SCIM supports automatic deprovisioning across all SCIM-enabled applications when a user is centrally disabled, which can improve security and efficient licensing.

[8] Refer to the IAM Provisioning Playbook at https://vaww.oed.portal.va.gov/sites/vrm/IAM/playbooks/Pages/Prov/Prov.aspx.

4 Application of Practices

The following use case represents the application of the described practices that are related to identity provisioning.

4.1 Integration of a New Software as a Service (SaaS) Solution

4.1.1 Purpose

VA has opted to move to a Software as a Service (SaaS) solution for customer relationship management (CRM) services.

4.1.2 Assumptions

- The SaaS solution complies with the defined standard.
- The SaaS solution natively supports identity provisioning standards.
- VA OICAM supports SCIM 2.0.
- The Authority to Operate (ATO) for the SaaS solution has been completed.

4.1.3 Use Case Description

- VA has procured a SaaS solution for CRM and will need to provision hundreds of existing users. The project team would like to start using the new service within the next two weeks.
- The project team assessed the SaaS solution before it was selected and determined that existing roles could be easily mapped to roles within the SaaS solution that support SCIM 2.0.
- The VA IAM service reviews the SaaS solution and establishes a trust using X.509 certificates and a proxy. Since SCIM 2.0 is supported by both VA and the vendor, no further customization is needed for integration.
- User accounts are provisioned in bulk, and dynamically updated, as users are added to the corresponding roles within the VA directory.

4.2 Key Practices

Table 5 highlights key practices identified in this enterprise design pattern (EDP).

Table 2: Key Practices IAM Identity Provisioning EDP

Category	Area	Description
Identity and Access Management	Identity Provisioning	The design of identity provisioning services must support the VA business goals to increase user productivity, create administrative efficiencies, and support security and compliance.

Category	Area	Description
Identity and Access Management	Identity Provisioning	Project teams should prioritize solutions that support SCIM 2.0.
Identity and Access Management	Identity Provisioning	The primary trust method must be Transport Layer Security (TLS) mutual authentication, using X.509 certificates as a mechanism for client authentication to the endpoint.
Identity and Access Management	Identity Provisioning	The identity provisioning service must be able to monitor the business triggers to automate the workflow.
Identity and Access Management	Identity Provisioning	Solutions should support either SPML or SCIM for identity provisioning.

5 Impacts

If identity provisioning is not properly designed for VA solutions, the following risks are increased:

- Noncompliance with FISMA, Continuous Diagnostics and Mitigation (CDM), other policy, or other audit findings by external agencies with oversight, can contribute to a material weakness, due to improper user account management.
- Manual processes adversely impact the timely delivery of services.

Appendix: 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/FISMASecurityCompliance/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
- 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 must not be used for advertising or product endorsement purposes.