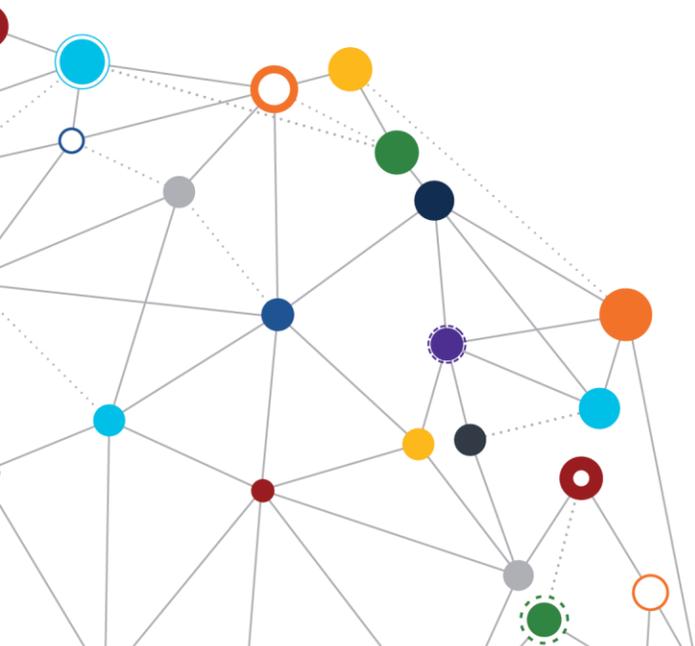


OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

OAuth 2.0 Security Primer

October 2018 | Enterprise Program Management Office



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 OAuth Grant Overview..... 5
 - 3.2 OAuth 2.0 Security Practices..... 6
 - 3.3 Guidance for Selecting an OAuth 2.0 Grant 6
- 4 Application of Practices 7**
 - 4.1 OAuth 2.0 for Mobile Application Making API Call..... 7
 - 4.1.1 Purpose 7
 - 4.1.2 Assumptions..... 7
 - 4.1.3 Use Case Description 8
 - 4.2 Key Practices 9
- 5 Impact..... 12**
- Appendix: References 13**

- Figure 1 - Overview of IAM Progression 4
- Table 1: Change Matrix 2
- Table 2: Guidance for OAuth Grant Selection 7
- Table 3: Key Practices IAM OAuth 2.0 Security Primer EDP 9

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	10/04/18	IAM EDP OAuth 2.0 Segment document approved



1 Context

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) Program that coordinates 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.

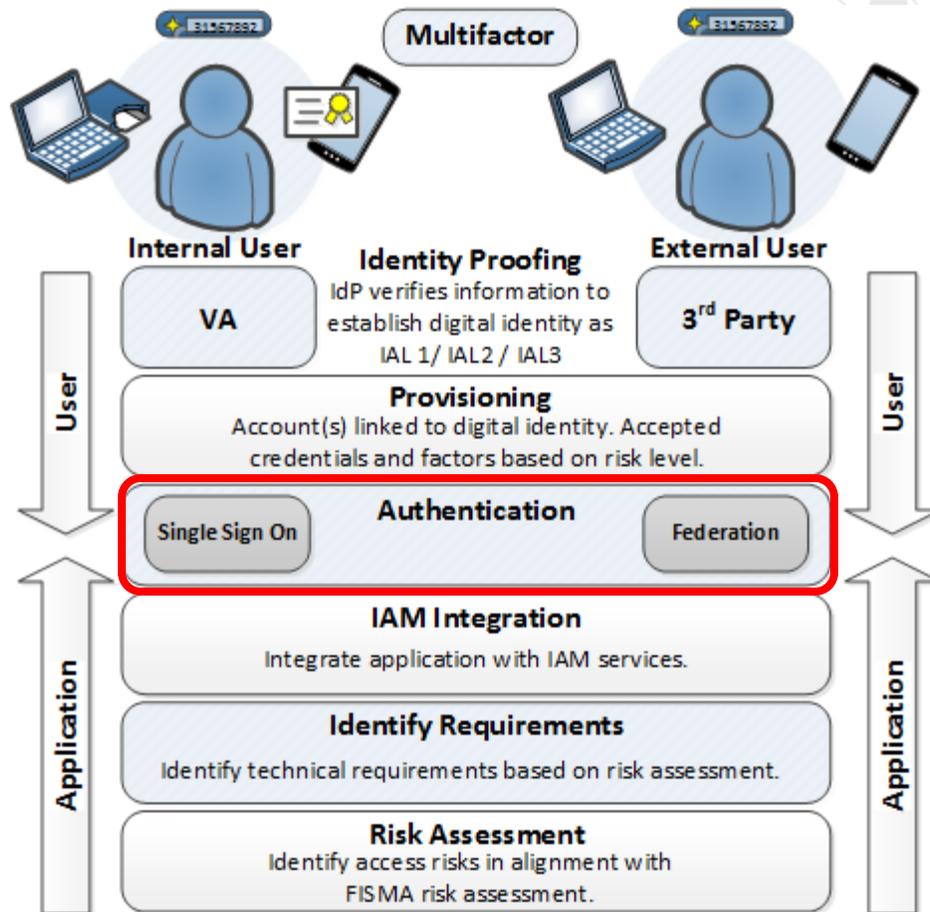
VA has two general populations of users who require access: (1) internal users include employees, contractors, trainees and volunteers; and (2) external users, comprised of Veterans, beneficiaries, and health partners, including employees and contractors from other Government agencies. All require varying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

2 Challenge

The use of the OAuth 2.0 Authorization Framework (OAuth)¹ is expanding at VA, along with the increased use of application programming interfaces (APIs). The improper implementation of OAuth has led to significant unauthorized access risks for services hosted by major commercial organizations.² VA requires enterprise guidance on the design of OAuth to provide consistent security and limit risks. The area addressed in this document is the part of the IAM progression that is highlighted in red in Figure 1.

¹ In this document, OAuth refers to the OAuth 2.0 Authorization Framework, developed in 2012, as the open-standard authorization protocol that describes how unrelated servers and services can safely allow authenticated access to assets, without sharing the initial, related, single logon credential. It is used as a secure, third-party, user-agent, delegated authorization (Source: <https://www.csoonline.com/article/3216404/authentication/what-is-oauth-how-the-open-authorization-framework-works.html>).

² Source: <https://www.csoonline.com/article/3194727/security/google-docs-phishing-attack-undercores-oauth-security-risks.html>.



3

Figure 1 - Overview of IAM Progression

3 Guidance

As developers have migrated from WS-*⁴ for building web services to APIs, OAuth adoption has steadily grown. OAuth is a delegated authorization framework, described under the Internet Engineering Task Force (IETF) Request for Comment (RFC) 6749.⁵ OAuth provides a convenient method for integrating with APIs to provide limited access to resources, without exposing user credentials. The user can select any approved credential service provider (CSP) to authenticate

³ 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>.

⁴ WS-* is a prefix used to indicate specifications associated with web services and there exist many WS* standards including WS-Addressing, WS-Discovery, WS-Federation, WS-Policy, WS-Security, and WS-Trust. For additional information, refer to <https://www.dotnettricks.com/learn/webservice/understanding-ws-star-standards-and-specifications>.

⁵ Reference the IETF at <https://www.ietf.org/rfc/rfc6749.txt>.

and gain access to the desired resource, without exposing the credentials to the resource provider. The CSP only passes a token to the resource provider.

3.1 OAuth Grant Overview

OAuth describes several different methods for obtaining access tokens, referred to as “grants” or “flows,” that are recommended for different use cases:

- **Authorization Code Grant:** The Authorization Code Grant, the most commonly used OAuth grant type, uses an authorization server as an intermediary between the client and resource owner. The authorization server authenticates the resource owner and obtains authorization.
- **Implicit Grant:** The Implicit Code Grant is similar to the Authorization Code Grant, but it directly delivers an access token to the user’s browser. The Implicit Grant flow is used when the client cannot protect a secret, which is often the case for applications that consume a Web API via JavaScript from a browser, such as single page web applications (SPAs).
- **Resource Owner Password Credentials (ROPC) Grant:** The client collects the user credentials and presents them to the resource owner for a token. The ROPC Grant is designed for high trust use cases to eliminate the need for the client to store the resource owner credentials, by exchanging the credentials for an access or refresh token. The ROPC Grant creates several risks: the client impersonates the user, the scope could be modified, and the credentials are exposed. For these reasons, the ROPC Grant must not be used.
- **Client Credentials Grant:** The Client Credentials Grant is used for machine-to-machine authorization, where user permission is not required. The Client Credentials Grant must not be used for this purpose. Please see the *Non-Person Entity* (NPE) Enterprise Design Pattern (EDP) for guidance on device-to-device authentication and authorization.⁶
- **Device Flow for Browserless and Input Constrained Devices:** This is a draft standard⁷ that instructs the user to perform the authorization request on a secondary device, such as a smartphone, to provide authorization for devices, such as Internet of Things (IoT). This grant must not be used since it is still in draft status.
- **Refresh Token Grant:** The Refresh Token Grant provides an optional method to obtain a new access token when the current access token becomes invalid, or expires from using the Authorization Code Grant.

⁶ Reference the *Non-Person Entity* EDP at <https://www.oit.va.gov/library/recurring/edp/index.cfm>.

⁷ Source: <https://datatracker.ietf.org/doc/draft-ietf-oauth-device-flow/>.

3.2 OAuth 2.0 Security Practices

There are two considerations when using OAuth: security and interoperability. RFC 6749 describes the OAuth Framework and RFC 6819 describes the OAuth Threat Model and security considerations. The RFCs provide some insight into potential risks associated with the use of OAuth. Highly publicized weaknesses surrounding the use of OAuth have primarily revolved around weak or improper implementations of the RFC. Using the RFCs with the minimum specifications possible does not provide optimal security. It should also be noted that OAuth must not be used for authentication.

For interoperability, projects must adopt the SMART Application Authorization Guide.⁸ SMART has already been proposed by the Office of the National Coordinator for Health Information Technology (ONC) as part of their draft Trusted Exchange Framework and Common Agreement (TEFCA) for compliance with Health Level 7's (HL7) Fast Healthcare Interoperability Resources (FHIR). Although the profile is built for healthcare sharing, it demonstrates a secure foundation for use of OAuth in many parameters.

SMART defines two profiles: (1) the “confidential application” correlates to the use of the Authorization Code Grant, and (2) the “public application” correlates to the use of the Implicit Grant.⁹ Since SMART does not include all best practices identified in RFC 6819, additional protections are required. The *Key Practices Table*, shown in Table 3, includes SMART and other protections to create best practices across all defined areas. The SMART launch requirements for applications that access Electronic Health Records (EHRs) are not discussed here.¹⁰

3.3 Guidance for Selecting an OAuth 2.0 Grant

The following table provides guidance on when to use each type of OAuth 2.0 Grant.¹¹

⁸ Refer to <https://smarthealthit.org/an-app-platform-for-healthcare/about/>. SMART was originally an acronym for “Substitutable Medical Apps, Reusable Technology,” describing features of the project’s clinical care applications. The Government-funded creation and initial development resulted in standards, open source technology, and app developers that help define a health data layer that builds on the FHIR API. To enable substitutable health apps and third-party application services, SMART applies a set of profiles to express clinical data; and standards for authorization based on the OAuth standard.

⁹ For additional information, reference the *Identity and Access Management (IAM) OAuth 2.0 Implicit Grant Enterprise Design Pattern*, August 2018, at <https://www.oit.va.gov/library/recurring/edp/index.cfm>.

¹⁰ For information on SMART launch requirements, refer to <https://smarthealthit.org/an-app-platform-for-healthcare/about/>.

¹¹ Although SMART allows both the Authorization Code Grant and the Implicit Grant, personally identifiable information (PII) and protected health information (PHI) with a single-page application (SPA) or JavaScript application may not be desired, due to increased security risks created by the technical limitations.

Table 2: Guidance for OAuth Grant Selection

Application	OAuth 2.0 Grant
Web Application with dedicated server-side component	Authorization Code Grant ¹²
Mobile Native Application	Authorization Code Grant ¹³
SPA Application	Implicit Grant ¹⁴
JavaScript Application	Implicit Grant ¹⁵

4 Application of Practices

The following use case relates to the application of the described risk management principles to solution development.

4.1 OAuth 2.0 for Mobile Application Making API Call

4.1.1 Purpose

The Veterans Health Administration (VHA) would like to release a mobile application that uses OAuth to allow Veterans to access their EHRs. The System Owner wants to determine the technical requirements for IAM integration for the API.

4.1.2 Assumptions

- The API is accessing sensitive information, including protected health information (PHI).
- A native mobile application is a possible choice.
- Any external credentials used are approved for use by VA.

¹² For additional information, reference the *Identity and Access Management (IAM) OAuth 2.0 Authorization Code Grant* Enterprise Design Pattern, August 2018, at <https://www.oit.va.gov/library/recurring/edp/index.cfm>.

¹³ Ibid.

¹⁴ For additional information, reference the *Identity and Access Management (IAM) OAuth 2.0 Implicit Grant* Enterprise Design Pattern, August 2018, at <https://www.oit.va.gov/library/recurring/edp/index.cfm>.

¹⁵ Ibid.

4.1.3 Use Case Description

- The system owner begins the intake process for the Veteran-focused Integration Process (VIP)¹⁶ by submitting the business case for a new solution as a VIP Request (VIPR).¹⁷
- The solution is targeting mobile devices and the use of VA API services to access EHRs for Veterans, using their own credentials.
- OAuth 2.0 is identified as the best method to authorize access to VA data.
- A risk assessment is performed due to access to PHI. The system owner decides that the OAuth 2.0 Client Authorization Code Grant with Proof Key for Code Exchange (PKCE)¹⁸ provides the appropriate level of security for the purpose.
- The application owner contacts VA IAM to register their application with the VA-approved authorization server. The OAuth configuration is updated with the provided information.
- Authentication is provided by the approved CSP and authorization is provided by VA IAM authorization services.

¹⁶ Reference the VIP 3.1 Guide, April 2018, at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>.

¹⁷ Reference the VIPR Request Portal at

<https://vaww.vashare.oit.va.gov/sites/dmo/VIPR/SitePages/VIPR%20Home%20Page.aspx>.

¹⁸ PKCE is pronounced "pixy." For additional information, reference *Proof Key for Code Exchange by OAuth Public Clients*, Internet Engineering Task Force (IETF) Request for Comments 6749 at <https://tools.ietf.org/html/rfc7636>.

4.2 Key Practices

The following table highlights key practices identified in this EDP.

Table 3: Key Practices IAM OAuth 2.0 Security Primer EDP

Category	Area	Description
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 User Authentication</p> <ul style="list-style-type: none"> • Only VA-approved CSPs must be used for user authentication. • Native applications must not use a browser embedded within the application to display the authorization request.
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Token Expiration</p> <p>The listed time (in seconds) must be the maximum expiration time for the specified resource type:</p> <ul style="list-style-type: none"> • Access Token: 3600s • Refresh Token: 86400s
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Revocation</p> <ul style="list-style-type: none"> • The authorization server must support revocation of the client id, refresh tokens, and the client secret.
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Resource Binding</p> <ul style="list-style-type: none"> • The “aud” parameter must specify the Uniform Resource Locator (URL) of the resource server. Tokens must be bound to the target resource server. The resource server must validate the target server value.

Category	Area	Description
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Code/Token Thresholds</p> <ul style="list-style-type: none"> A threshold must be defined to block clients that issue more than the threshold of invalid codes or tokens, to prevent denial of service.
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Token Storage</p> <ul style="list-style-type: none"> An application must not store bearer tokens in cookies that are transmitted in the clear. Applications should persist tokens and other sensitive data in application-specific storage locations only, not in system-wide-discoverable locations. Access tokens must not be stored on the authorization server, except as hashes.
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Token Integrity</p> <ul style="list-style-type: none"> Bearer tokens must be digitally signing the token, as specified in RFC 7515. The application must validate the value of the state parameter upon return to the redirect_Uniform Resource Identifier (URI), and must ensure that the state value is securely tied to the user's current session.
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Session Integrity</p> <ul style="list-style-type: none"> Applications must assure that sensitive information is transmitted <i>only</i> to authenticated servers, using the latest Transport Layer Security (TLS) version that is approved in the

Category	Area	Description
		VA Technical Resource Model (TRM). ¹⁹ <ul style="list-style-type: none"> The application must use an unpredictable value for the state parameter, with at least 128 bits of entropy.
Identity and Access Management	Delegated Authorization	OAuth 2.0 Authorization Request <ul style="list-style-type: none"> Applications must include the state with all authorization requests, in addition to mandatory elements. The authorization server's response must include the Hyper Text Transfer Protocol (HTTP) "Cache-Control" response header field, with a value of "no-store," as well as the "Pragma" response header field, with a value of "no-cache."
Identity and Access Management	Delegated Authorization	OAuth 2.0 Scope <ul style="list-style-type: none"> OAuth 2.0 must not be used to grant broad scopes, such as would be granted to an administrator role.
Identity and Access Management	Delegated Authorization	OAuth 2.0 Redirect URI <ul style="list-style-type: none"> The application must register one or more fixed, fully-specified redirect_URIs. The application must not forward the values that are passed back to its redirect URL to any other arbitrary or user-provided URL (a practice known as an "open redirector").

¹⁹ Reference the TRM on the VA internal network at <http://trm.oit.va.gov/>.



Category	Area	Description
		<ul style="list-style-type: none">The application must bind the client_id to the redirect_URI.
Identity and Access Management	Delegated Authorization	OAuth 2.0 Input Validation <ul style="list-style-type: none">All input values must be sanitized to prevent the injection of unintended commands.

5 Impact

If risk management is not used to define technical requirements for IAM components of VA solutions, inadequate technical protections for sensitive data may contribute to unauthorized access or data breach.

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/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>
- OAuth 2.0 Framework: <https://tools.ietf.org/html/rfc6749#section-1.2>
- OAuth 2.0 Threat Model: <https://tools.ietf.org/html/rfc6819#page-16>
- SMART Application Authorization Guide: <http://docs.smarthealthit.org/authorization/>
- 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.