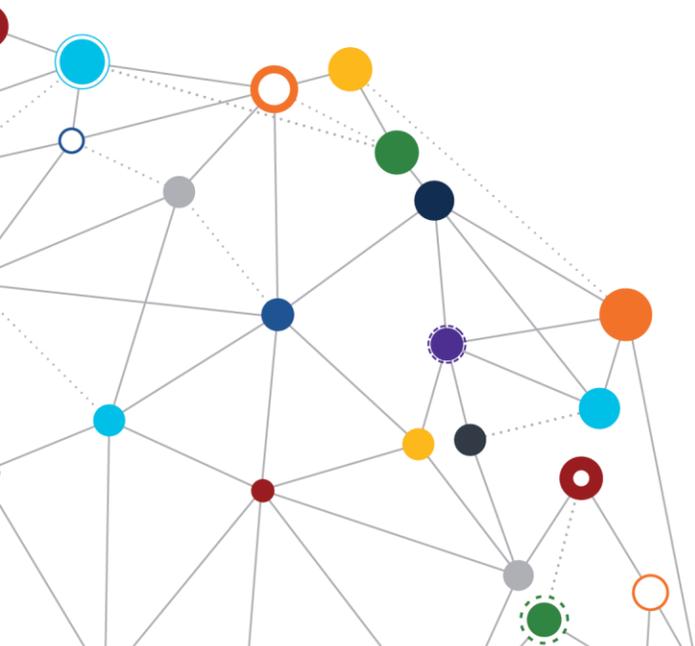


OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

OAuth 2.0 Implicit Grant

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 Implicit Code Grant 5
- 4 Application of Practices 6**
 - 4.1 OAuth 2.0 for Mobile Application Making API Call..... 6
 - 4.1.1 Purpose 6
 - 4.1.2 Assumptions..... 6
 - 4.1.3 Use Case Description 7
 - 4.2 Key Practices 8
- 5 Impact..... 8**
- Appendix: References 9**

- Figure 1 - Overview of IAM Progression 4
- Figure 2 - Implicit Grant Overview 5

- Table 1: Change Matrix 2
- Table 3: Key Practices IAM OAuth 2.0 EDP 8

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>.

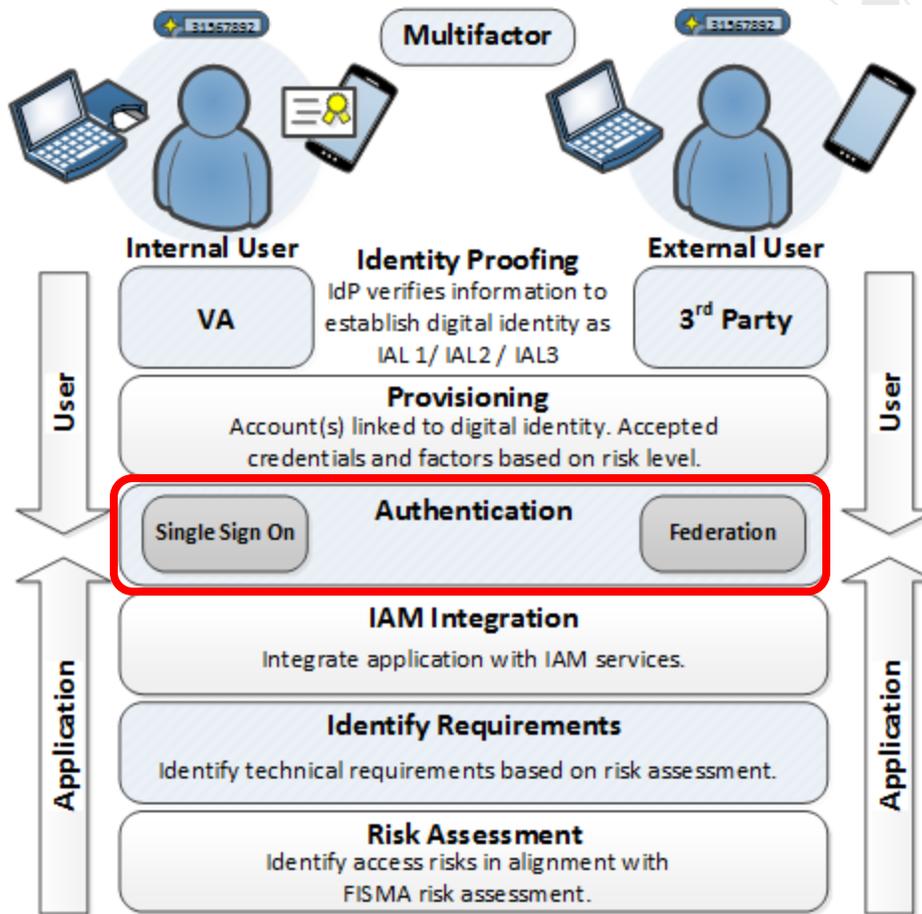


Figure 1 - Overview of IAM Progression³

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.

OAuth describes several different methods of obtaining access tokens, referred to as “grants” or “flows.” The Implicit Code Grant directly delivers an access token to the user’s browser.

3.1 Implicit Code Grant

The Implicit Grant Flow is used when the client cannot protect a secret, such as with single-page applications (SPAs) that consume a Web API via JavaScript from a browser. There are some drawbacks, including additional security attack vectors. The access token is now exposed to the user agent, the client is not authenticated, and refresh tokens are not supported. The Implicit Grant is described in Figure 3.

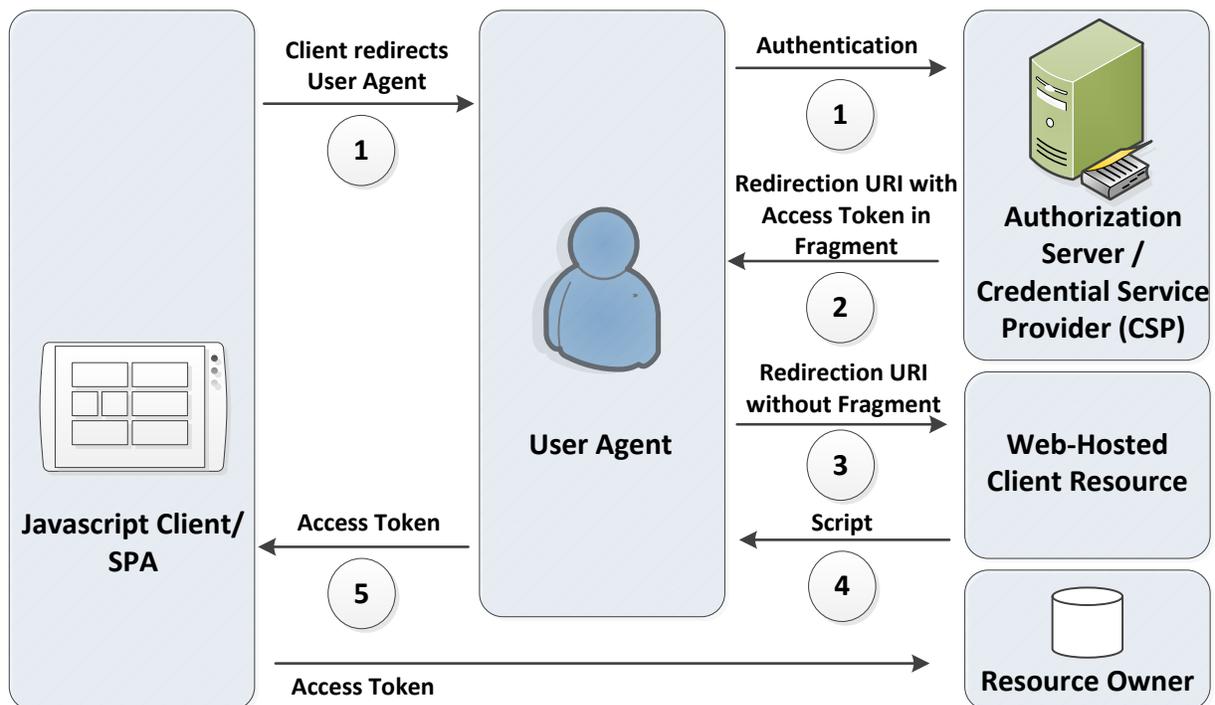


Figure 2 - Implicit Grant Overview⁶

⁶ Figure 2 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 Internet Engineering Task Force (IETF) Request for Comments 6749 at <https://tools.ietf.org/html/rfc6749>.

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 redirect Uniform Resource Identifier (URI), which is registered using the client id/secret. The authorization server will send the user-agent to the URI. The user is required to authenticate to the authorization server. The authorization server may authenticate the user directly or by using a service (both require VA approval). Upon being presented with an authenticated user, the authorization service must ensure that requested scopes are authorized by the resource owner by presenting a list of requested scopes and the option to approve or deny the request. The scope(s) are defined by the API or web application. If the user approves, the authorization server will include the requested scope(s) when the access token is generated (the source of data for step 5).
2. The authorization server redirects the user-agent back to the client using the redirection URI that was provided earlier. The redirection URI includes the access token in the URI fragment.
3. The user-agent makes a request to the web-hosted client resource using the redirect URI. The user-agent retains the fragment information locally.
4. The web-hosted client resource returns a web page that can access the full redirection URI, including the fragment retained by the user-agent, and extracts the access token and other parameters contained in the fragment. The user-agent executes the script locally to extract the token.
5. The user-agent passes the access token to the client, who presents it to the resource owner. The resource owner determines which resources are accessed.

4 Application of Practices

The following use case relates to the application of the described risk management principles to the 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 electronic health records (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 that are used are approved for use by VA.

4.1.3 Use Case Description

- The system owner begins the intake process for the Veteran-focused Integration Process (VIP)⁷ by submitting the business case for a new solution as a VIP Request (VIPR).⁸
- The solution is targeting mobile devices and 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 the VA data.
- A risk assessment is performed due to access to PHI. The system owner decides that the OAuth 2.0 Client Implicit Code Grant, with Proof Key for Code Exchange (PKCE),⁹ 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 by VA IAM authorization services.

⁷ Source: The Veteran-focused Integration Process (VIP) Guide 3.1, April 2018, at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>.

⁸ Reference the VIPR Request Portal at <https://vaww.vashare.oit.va.gov/sites/dmo/VIPR/SitePages/VIPR%20Home%20Page.aspx>.

⁹ 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 Enterprise Design Pattern (EDP).

Table 2: Key Practices IAM OAuth 2.0 EDP

Category	Area	Description
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Client Authentication</p> <p>Client authentication must not be used with the Implicit Grant.</p>
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Grant Types</p> <p>The Implicit Grant must only be used with applications that cannot protect a secret.</p>
Identity and Access Management	Delegated Authorization	<p>OAuth 2.0 Client Secret</p> <p>A client secret must not be used with Implicit Grant.</p>

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.