

# Evolution, not Revolution

## How MCP is Reshaping OAuth

Aaron Parecki • April 2026 • MCP Dev Summit

### The Nuts and Bolts of OAuth 2.0

Covering OAuth 2.0, OpenID, PKCE, deprecated OAuth, JWT, API Gateway, and more. No programming knowledge needed.

Created by Aaron Parecki | Updated Dec 2023

Enroll Now

This course includes:

- 3 hours, 32 minutes on-demand video
- 4 Quizzes
- Full lifetime access
- Access on mobile, desktop and TV
- Certificate of Completion

### Advanced OAuth Security

Learn the high-security OAuth extensions described in FAPI, PAV, JAR, JARM, DPoP, Mutual TLS, and HTTP Signatures.

Created by Aaron Parecki | Updated 10/2023

What you'll learn:

- How to integrate OAuth 2.0 into a web application for higher security.
- Learn the purpose of JAR, JARM, TLS, DPoP, and HTTP Signatures, and their relationship to OAuth 2.0.
- How to integrate the FAPI specification, including the PAV, Security Profile, and PEP, Message Signing.
- How to integrate JAR, JARM, TLS, DPoP, and HTTP Signatures into every major OAuth 2.0 implementation.

This course includes:

- 15 hours on-demand video
- 1 Coding exercise
- Access on mobile and TV
- Audited certificate in pending state
- Certificate of completion

Top companies offer this course to their employees

Subscribe to Udemy's top courses

Try Personal Plan for free



# okta

## OAuth 2.0 Simplified

A guide to building OAuth 2.0 servers

okta

Aaron Parecki

### Model Context Protocol

Version 2023-11-25 (Draft)

Documentation | Overview | Specification | Registry | SFPs | Community

#### Base Protocol

## Authorization

Copy page

### 1. Introduction

#### 1.1 Purpose and Scope

The Model Context Protocol provides authorization capabilities at the transport level, enabling MCP clients to make requests to one kind MCP servers on behalf of resource owners. This specification defines the authorization flow for HTTP-based transports.

#### 1.2 Protocol Requirements

Authorization is **OPTIONAL** for MCP implementations. When required:

- Implementations using an HTTP-based transport **SHOULD** conform to this specification.
- Implementations using an STDIO transport **SHOULD NOT** follow this specification, and instead retrieve credentials from the environment.
- Implementations using alternative transports **MUST** follow established security best practices for their protocol.

# I E T F



### draft-ietf-oauth-v2-1-09

Internet-Draft: draft-ietf-oauth-v2-1-09  
Published: 30 July 2023  
Intended Status: Standards Track  
Expires: 11 January 2024

D. Hardt  
Hello  
A. Parecki  
ota  
T. Lodderstedt  
yes rse

#### The OAuth 2.1 Authorization Framework

**Abstract**

The OAuth 2.1 authorization framework enables an application to obtain limited access to a protected resource, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and an authorization service, or by allowing the application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 2.0 Authorization Framework described in RFC 6749 and the OAuth Token Usage in RFC 6750.

**Discussion Venues**

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the OAuth Working Group mailing list ([oauth@ietf.org](mailto:oauth@ietf.org)), which is archived at <https://mailarchive.ietf.org/arch/browse/oauth/>.

Source for this draft and an issue tracker can be found at <https://github.com/oauthwg/oauth-v2-1>.

**Status of This Memo**

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

### draft-ietf-oauth-client-id-metadata-01

Aaron Parecki, Ota, G. Smith

#### OAuth Client ID Metadata Document

**Abstract**

This specification defines a mechanism through which an OAuth client can identify itself to authorization servers, without prior dynamic client registration or other existing registration. This is through the usage of a URI, as a client\_id to an OAuth flow, where the URI refers to a document containing the necessary client metadata, enabling the authorization server to fetch the metadata about the client as needed.

**About This Document**

This note is to be removed before publishing as an RFC.

The latest version of this draft can be found at <https://datatracker.ietf.org/doc/draft-ietf-oauth-client-id-metadata/>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-oauth-client-id-metadata/>.

Discussion of this document takes place on the Web Authorization Protocol Working Group mailing list ([oauth@ietf.org](mailto:oauth@ietf.org)), which is archived at <https://mailarchive.ietf.org/arch/browse/oauth/>. Subscribe at <https://www.ietf.org/mail/subscribe/oauth/>.

Source for this draft and an issue tracker can be found at <https://github.com/oauthwg/oauth-client-id-metadata>.

**Status of This Memo**

Document type: Active Internet Draft ([Search ID](#))

Select version: 01 02 03 04 05 06 07 08 09

Compare versions: draft-ietf-oauth-v2-1-08 draft-ietf-oauth-v2-1-09

Authors: [Rick Hancock](#), [Aaron Parecki](#), [Tanner Loderstedt](#)

Replaces: [draft-ietf-oauth-v2-1](#)

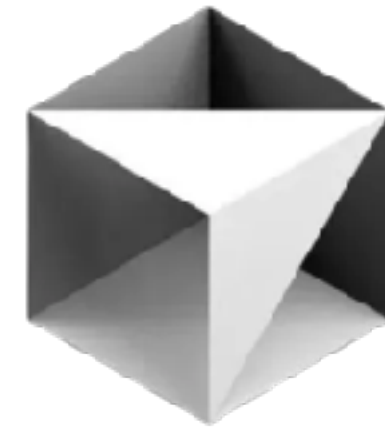
Other formats: [HTML](#) [PDF](#) [XML](#)

Raise your hand if you're building...

an MCP server



an MCP client



an OAuth server



Updated by: [8252](#)

PROPOSED STANDARD

[Errata Exist](#)

Internet Engineering Task Force (IETF)

D. Hardt, Ed.

Request for Comments: 6749

Microsoft

Obsoletes: [5849](#)

October 2012

Category: Standards Track

ISSN: 2070-1721

### The OAuth 2.0 Authorization Framework

#### Abstract

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 1.0 protocol described in [RFC 5849](#).

#### Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in [Section 2 of RFC 5740](#).

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc6749>.

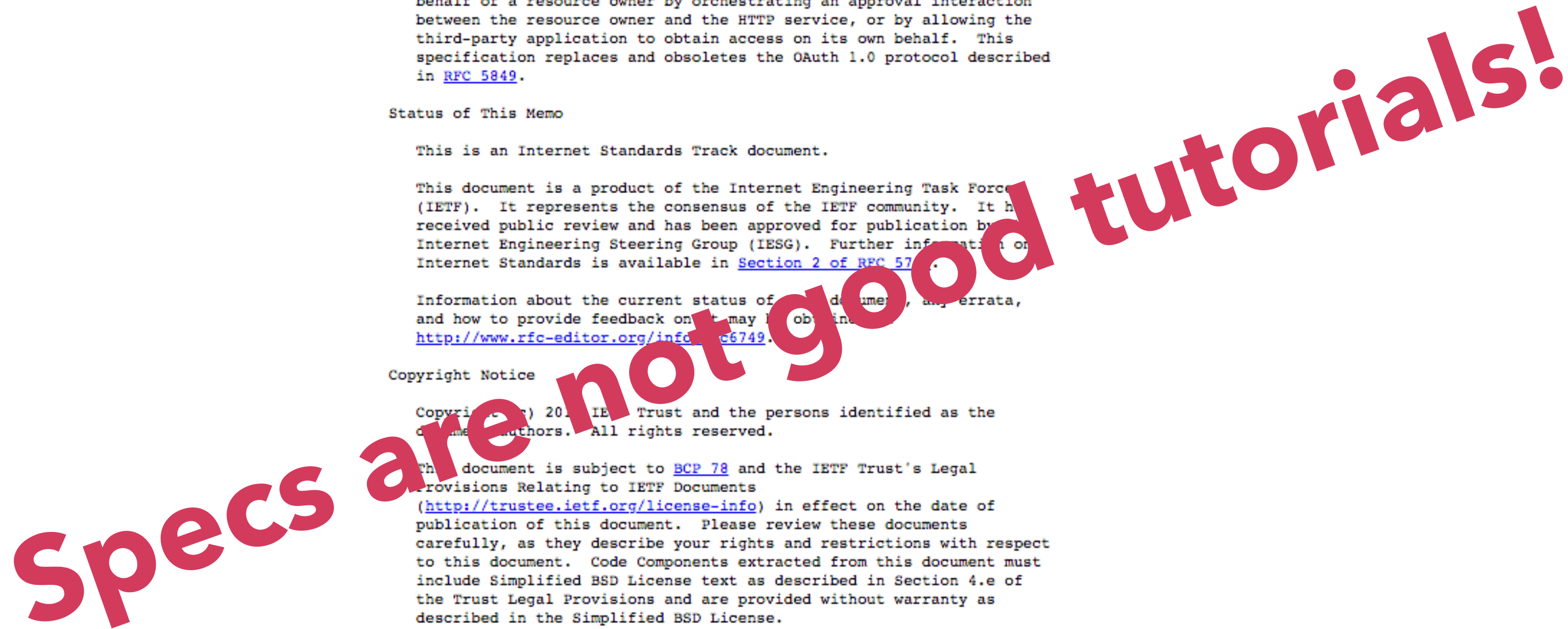
#### Copyright Notice

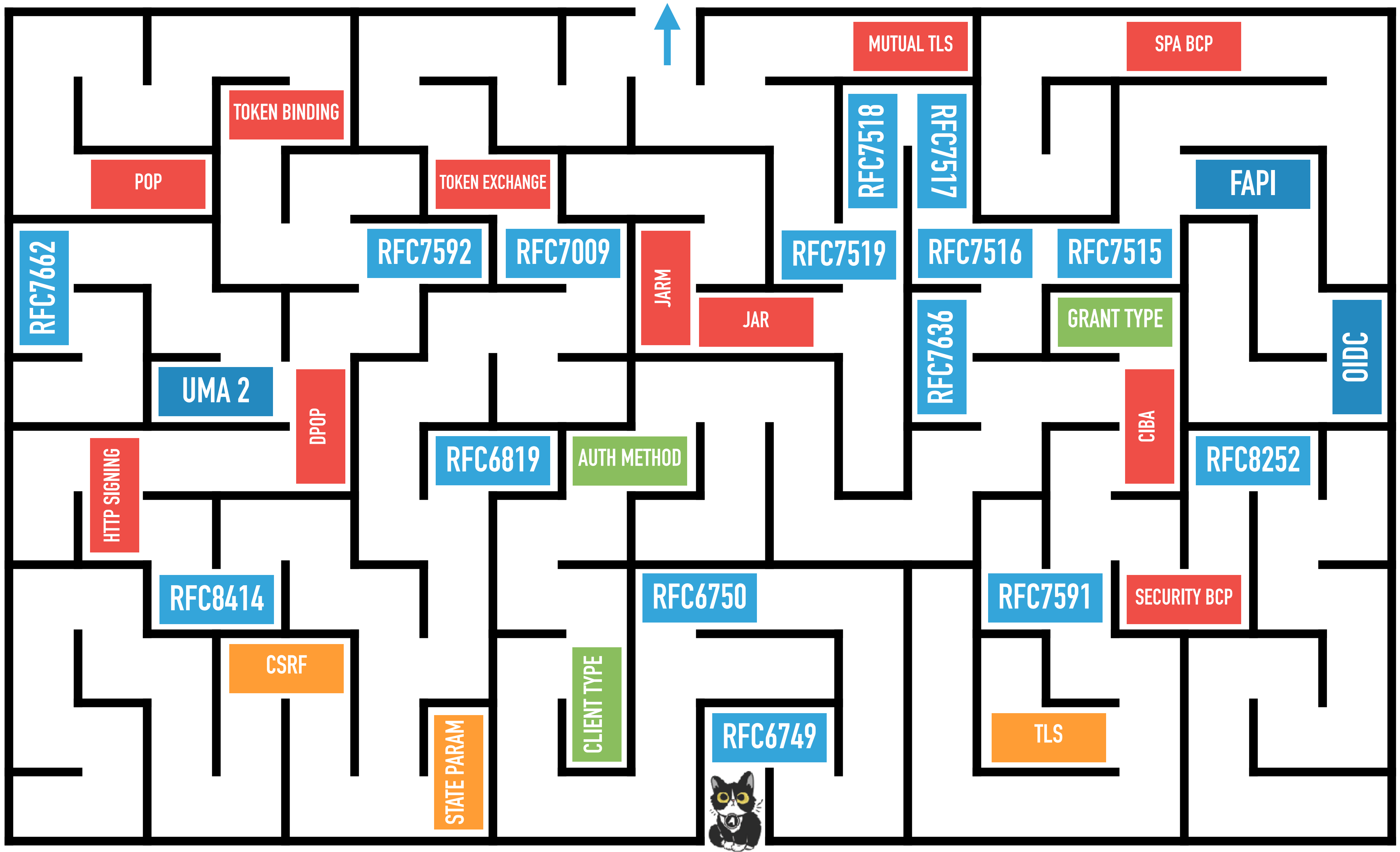
Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

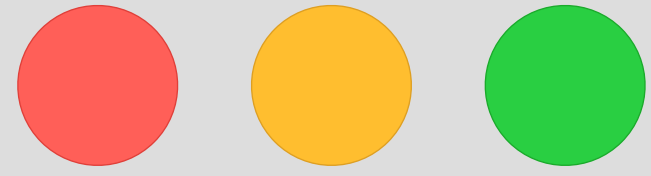
This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

#### Table of Contents

- [1. Introduction](#) .....4
- [1.1. Roles](#) .....6
- [1.2. Protocol Flow](#) .....7
- [1.3. Authorization Grant](#) .....8
  - [1.3.1. Authorization Code](#) .....8
  - [1.3.2. Implicit](#) .....8
  - [1.3.3. Resource Owner Password Credentials](#) .....9
  - [1.3.4. Client Credentials](#) .....9
- [1.4. Access Token](#) .....10
- [1.5. Refresh Token](#) .....10
- [1.6. TLS Version](#) .....12
- [1.7. HTTP Redirections](#) .....12







 **Secure** | <https://yelp.com/>

 Sign in with Facebook

 Sign in with Google

 Sign in with LinkedIn

 Sign in with Twitter

# The Password Anti-Pattern

## Are your friends already on Yelp?

Many of your friends may already be here, now you can find out. Just log in and we'll display all your contacts, and you can select which ones to invite! And don't worry, we don't keep your email password or your friends' addresses. We loathe spam, too.

Your Email Service



 Hotmail



 MAIL



 Mail





Your Email Address

*(e.g. bob@gmail.com)*

Your Gmail Password

*(The password you use to log into your Gmail email)*

[Skip this step](#)

[Check Contacts](#)


# The Password Anti-Pattern

**Step 1**  
Find Friends

**Step 2**  
Profile Information

**Step 3**  
Profile Picture


**Are your friends already on Facebook?**  
Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.

 **Gmail**


Your Email:

Email Password:


[Find Friends](#)

 Facebook will not store your password.


---

 **Yahoo!** [Find Friends](#)

---

 **Windows Live Hotmail** [Find Friends](#)

---

 **Other Email Service** [Find Friends](#)

# The Password Anti-Pattern

- How do you revoke this app's access?
- Do you trust the app to not store your password?
- Do you trust the app to access only the things it says it needs?
- Do you trust the app to not do things like change your password or delete your account?



Google Contacts



how can I let an app

**access my data**

without giving it my password?



**Authorization Server**



**Access Token**



**Resource (API)**





Google Contacts

last.fm

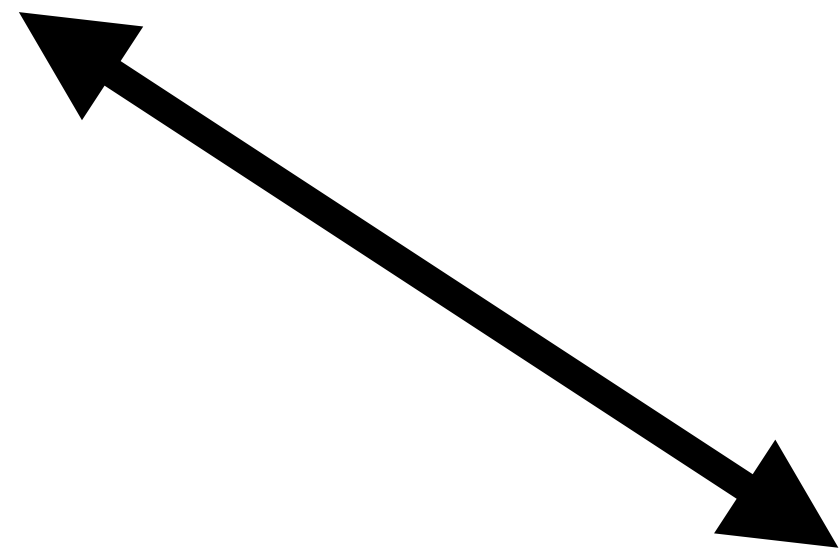
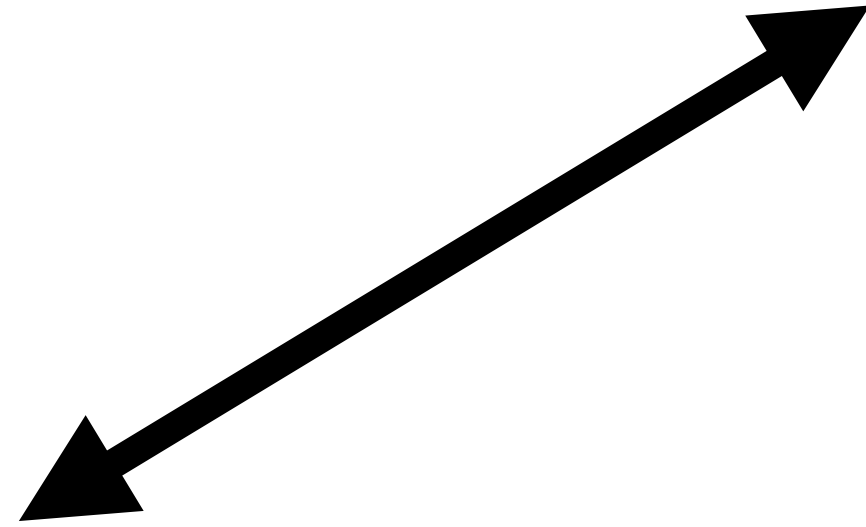
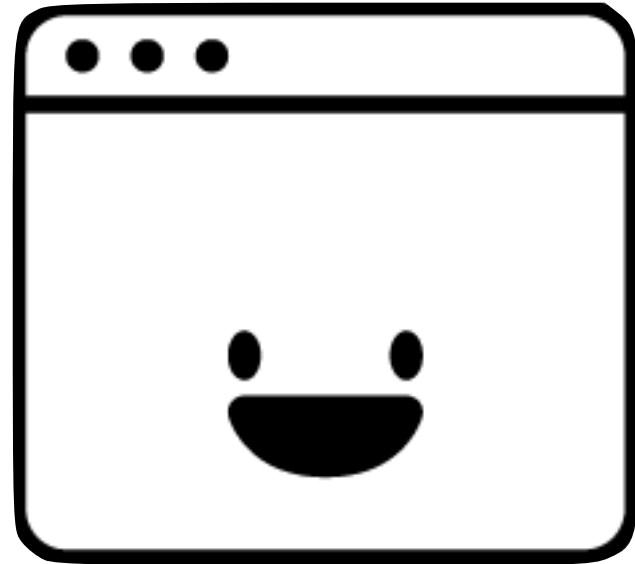
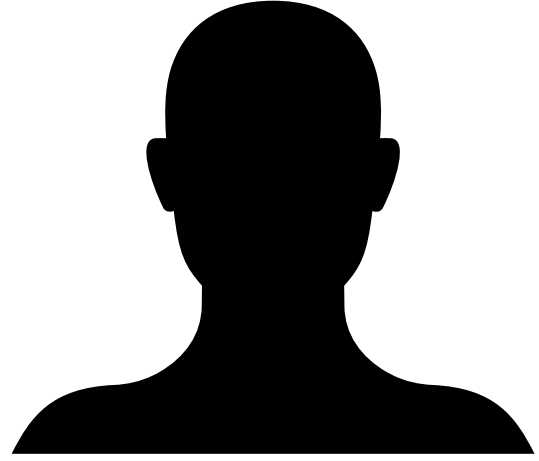


Spotify®

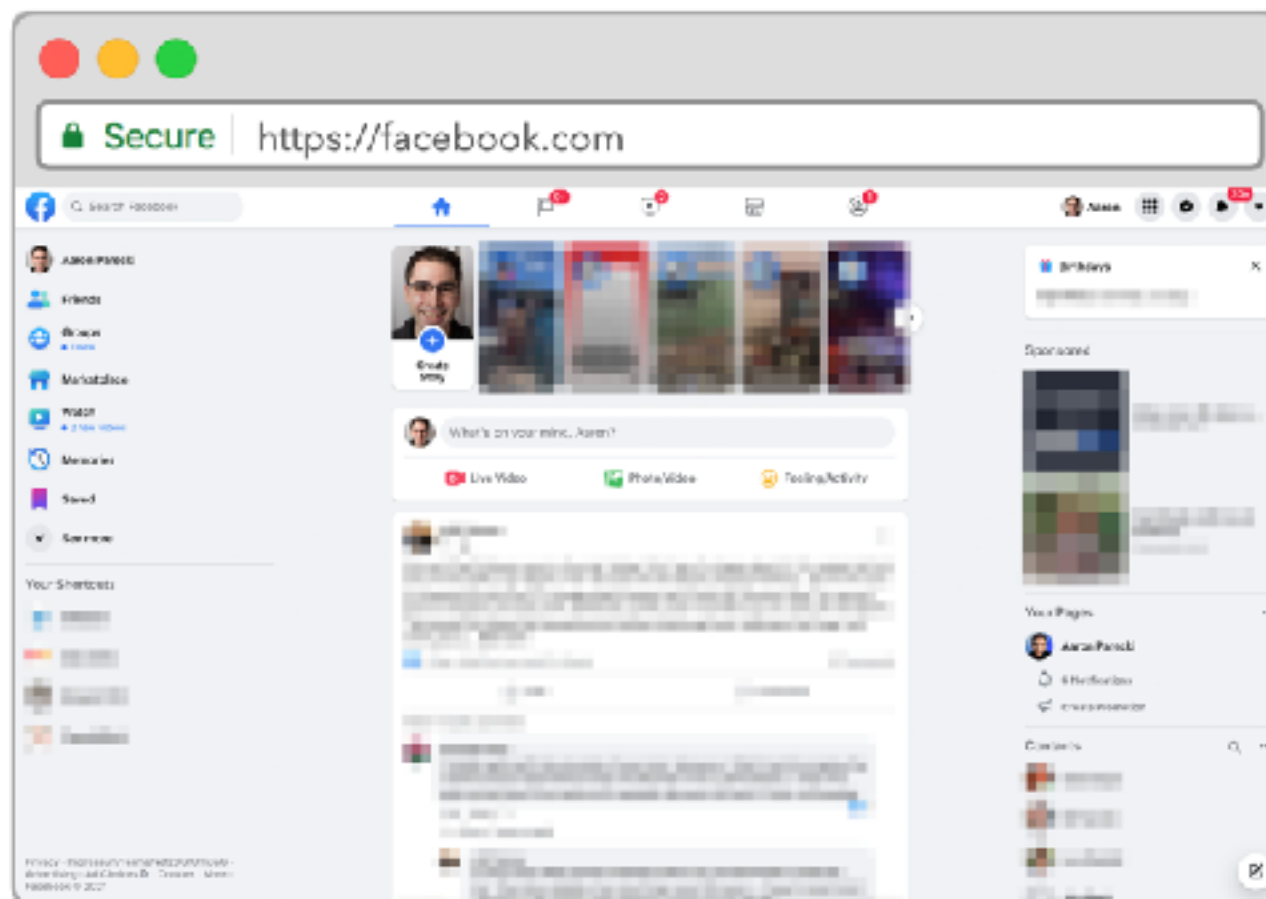
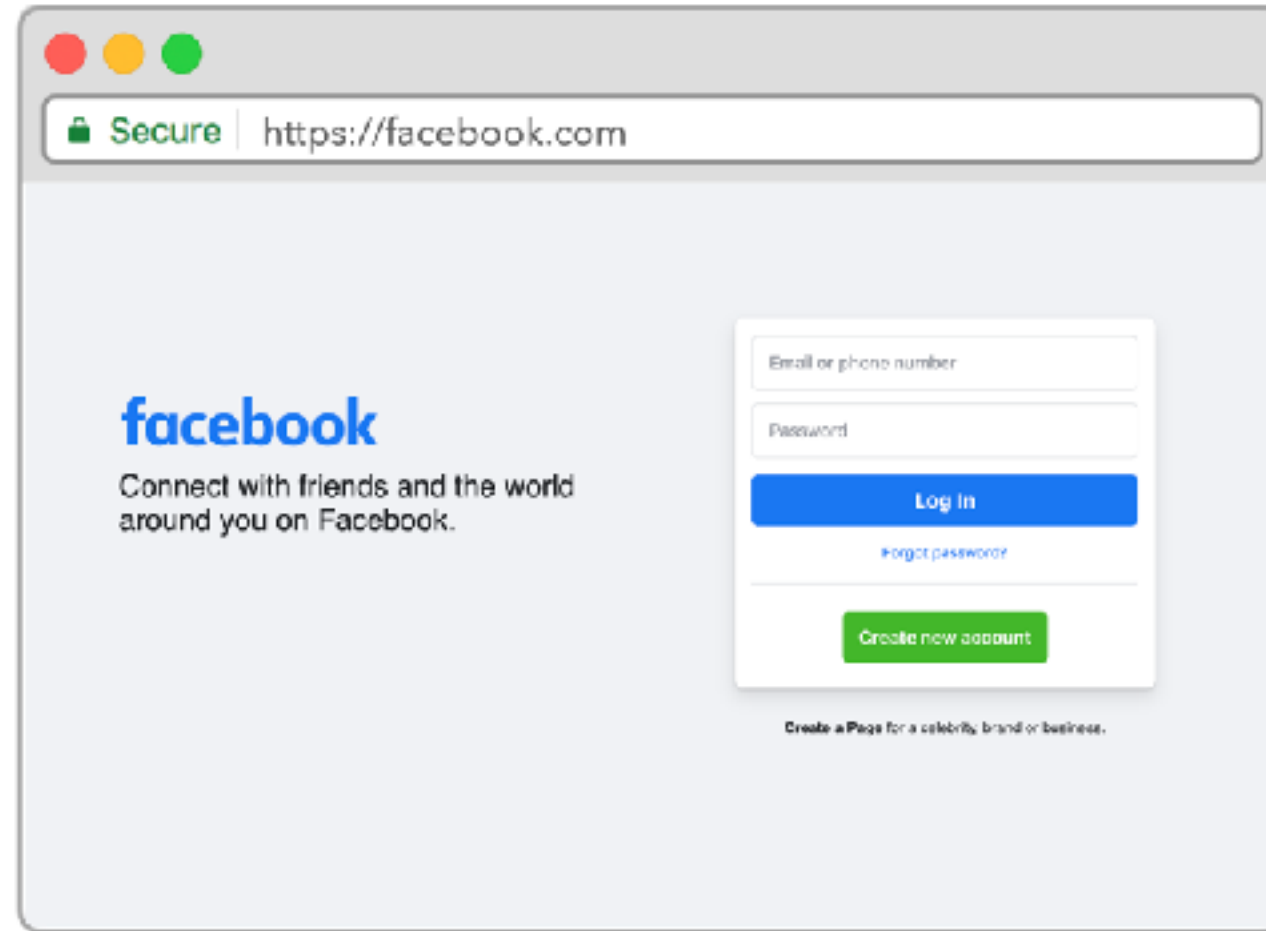


buffer

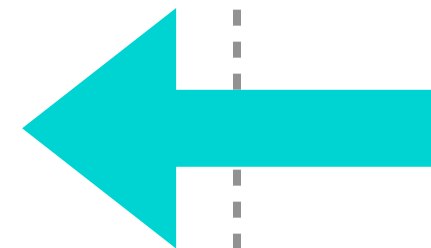
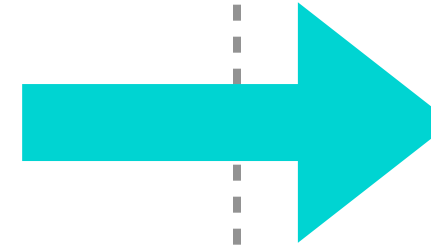
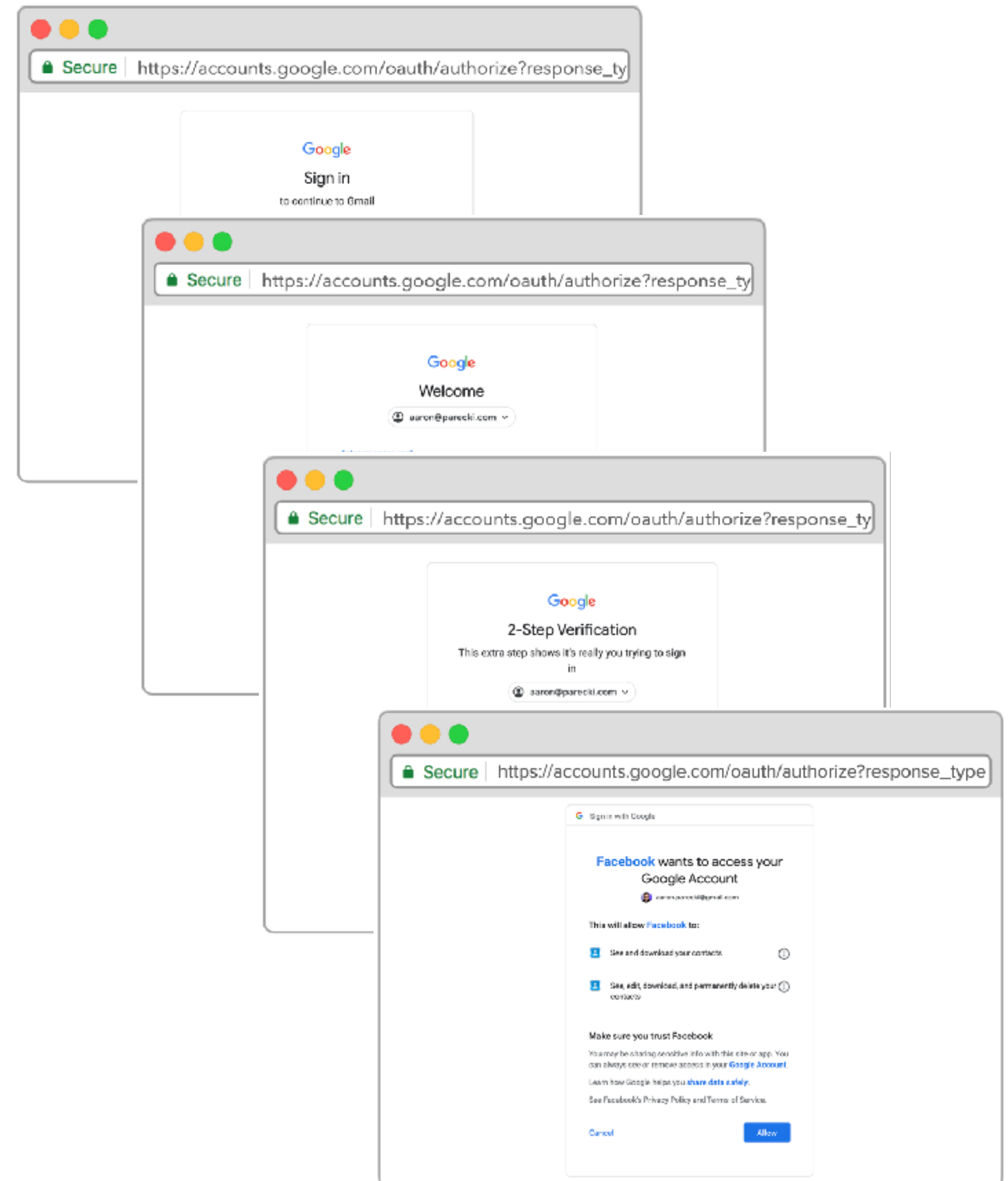




# Application







# OAuth Server



## Facebook wants to access your Google Account

 aaron.parecki@gmail.com

This will allow **Facebook** to:

-  See and download your contacts 
-  See, edit, download, and permanently delete your contacts 

### Make sure you trust Facebook

You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

See Facebook's Privacy Policy and Terms of Service.

[Cancel](#)

[Allow](#)

## Authorize Example App to access your account?

Authorize app

Cancel

### This application will be able to:

- See Tweets from your timeline (including protected Tweets) as well as your Lists and collections.
- See your Twitter profile information and account settings.
- See accounts you follow, mute, and block.

Learn more about third-party app permissions in the [Help Center](#).



Example App

By Aaron Parecki

example-app.com

Free Version Control with unlimited private and public repositories.



## Authorize OAuth 2 Example App



**OAuth 2 Example App** by [aaronpk](#)  
wants to access your aaronpk account



**Personal user data**  
Full access




**Repositories**  
Public only



### Organization access

 **indieweb** ✓

 **microformats** ✓

 **oauth2** ✓

 **okta** ✓

 **w3c** ✓

**Authorize aaronpk**

Authorizing will redirect to  
<https://example-app.com.dev>



## Register a new OAuth app

---

**Application name \***

Something users will recognize and trust.

**Homepage URL \***

The full URL to your application homepage.

**Application description**

This is displayed to all users of your application.

**Authorization callback URL \***

Your application's callback URL. Read our [OAuth documentation](#) for more information.

**Enable Device Flow**

Allow this OAuth App to authorize users via the Device Flow.

Read the [Device Flow documentation](#) for more information.

---

**Register application**

[Cancel](#)

General

Optional features

Advanced

# OAuth 2 Example App



**aaronpk** owns this application.

Transfer ownership

You can list your application in the [GitHub Marketplace](#) so that other users can discover it.

List this application in the Marketplace

1 user




Revoke all user tokens

## Client ID

0d74d0134cb9a1102e5d

## Client secrets

Generate a new client secret

 Client secret	*****afa1b7ff Added on Jul 15, 2025 by aaronpk Last used within the last 9 months	Delete
 Client secret	*****b36bfe44  No recent activity	Delete

## Application logo

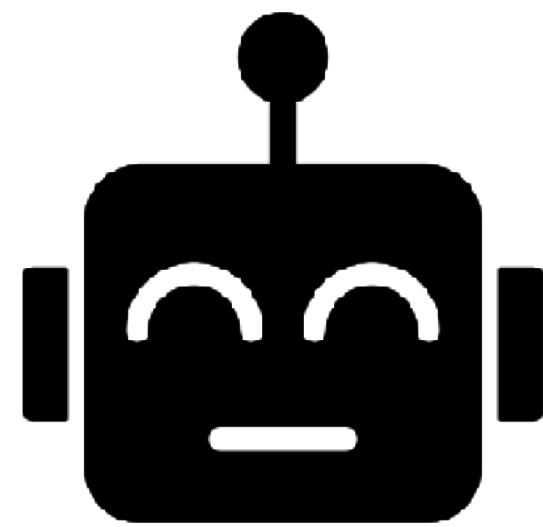


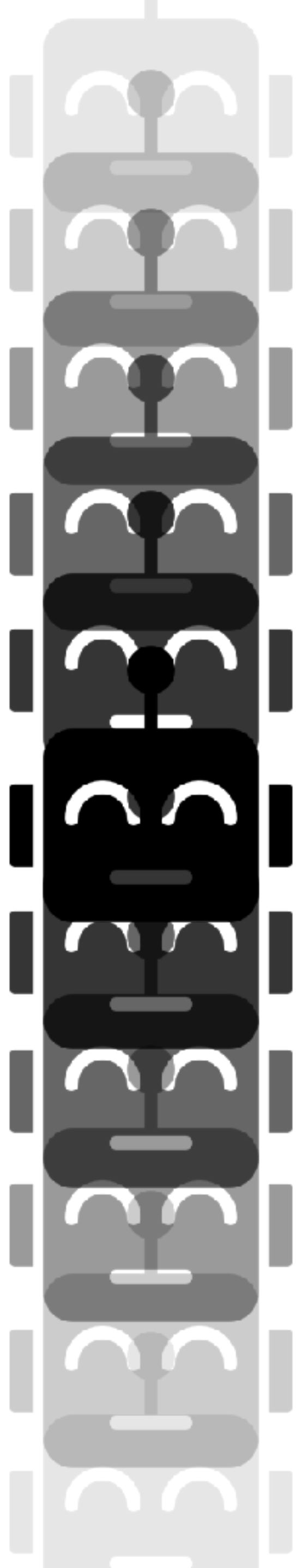
Upload new logo

You can also drag and drop a picture from your computer.



# Enter the AI Agent







WORDPRESS



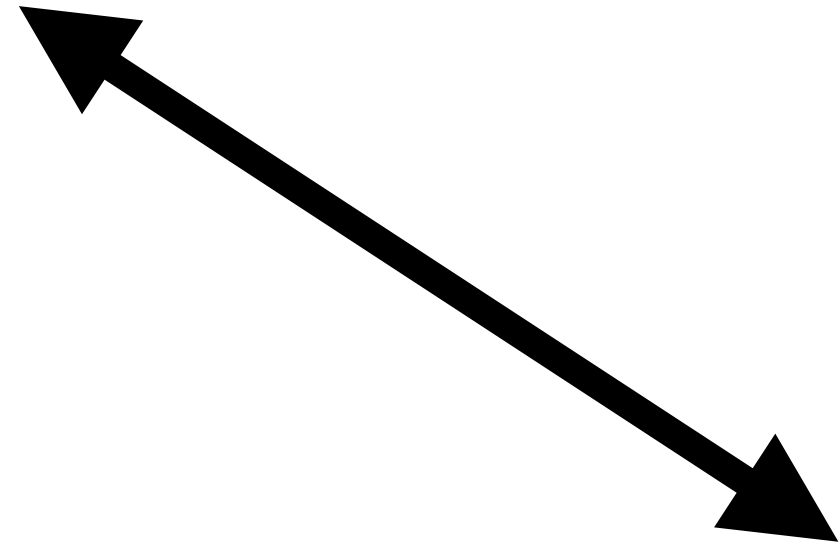
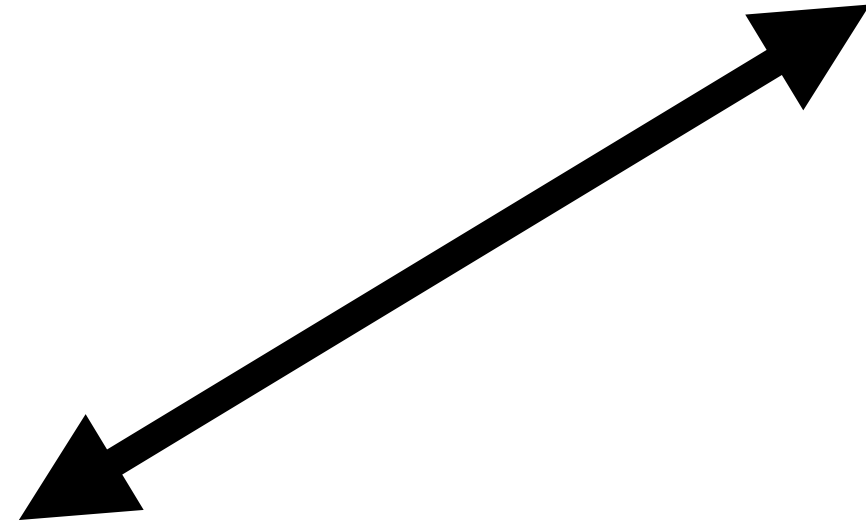
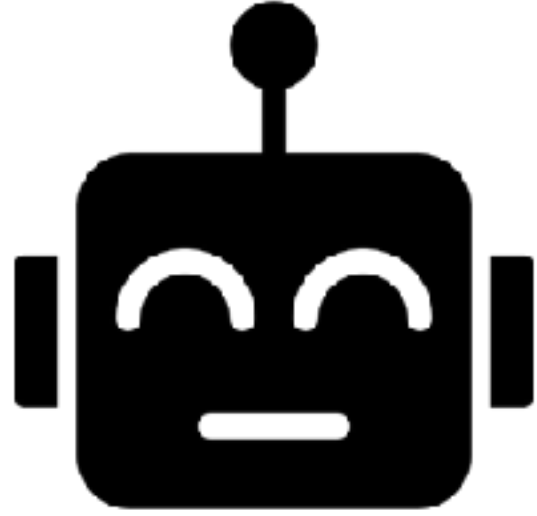
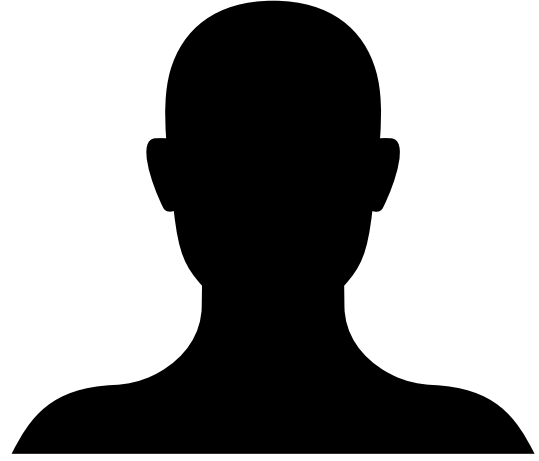
Bluesky



mastodon



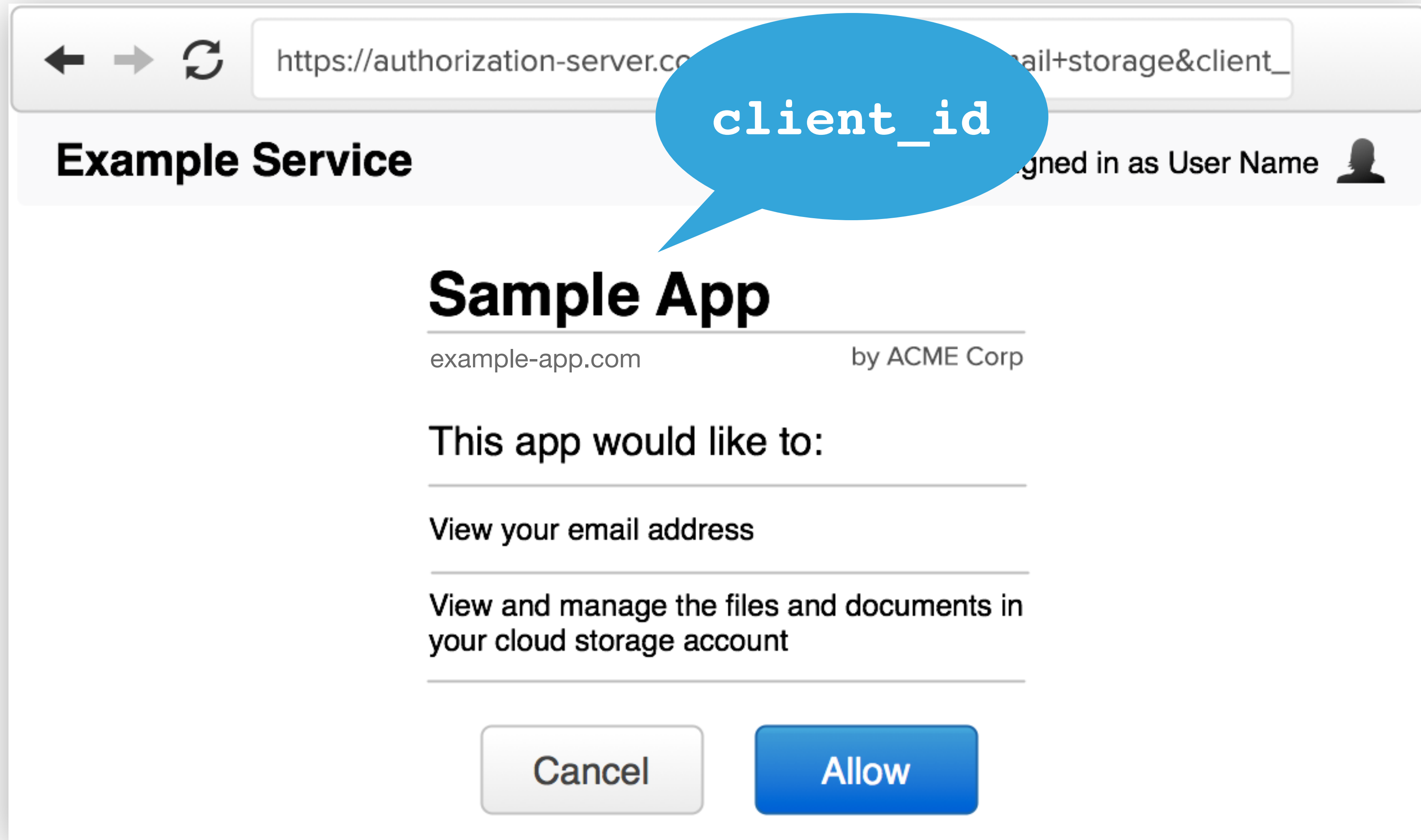
SMTP  
IMAP



- 1. Client Identification**
- 2. Dynamic Discovery**
- 3. Click-Through Fatigue**


# **CLIENT IDENTIFICATION**

# Authorization Interface



The image shows a browser window displaying an authorization interface. The address bar contains the URL `https://authorization-server.com/authorize?scope=email+storage&client_id=...`. A blue speech bubble highlights the `client_id` parameter in the URL. The page header shows "Example Service" and "Signed in as User Name" with a user icon. The main content area displays "Sample App" by ACME Corp, with the domain `example-app.com`. Below this, it lists permissions: "View your email address" and "View and manage the files and documents in your cloud storage account". At the bottom, there are "Cancel" and "Allow" buttons.

← → ↻ `https://authorization-server.com/authorize?scope=email+storage&client_id=...`

**Example Service** Signed in as User Name 

## Sample App

`example-app.com` by ACME Corp

This app would like to:

- View your email address
- View and manage the files and documents in your cloud storage account

General

Optional features

Advanced

# OAuth 2 Example App



**aaronpk** owns this application.

Transfer ownership

You can list your application in the [GitHub Marketplace](#) so that other users can discover it.

List this application in the Marketplace

1 user




Revoke all user tokens

## Client ID

0d74d0134cb9a1102e5d

## Client secrets

Generate a new client secret

 Client secret	*****afa1b7ff Added on Jul 15, 2025 by aaronpk Last used within the last 9 months	Delete
 Client secret	*****b36bfe44  No recent activity	Delete

## Application logo



Upload new logo

You can also drag and drop a picture from your computer.



```
POST /oauth/register HTTP/1.1
Host: auth.example.com
Content-Type: application/json
```

```
{
  "client_name": "Claude",
  "logo_uri": "https://claude.ai/logo.png",
  "redirect_uris": ["https://auth.example.com/redirect"]
  ...
}
```

```
HTTP/1.1 201 Created
Content-Type: application/json
```

```
{
  "client_id": "ad2669221ba94de0ee0",
  "client_secret": "6a58a307937e98c459be3bfe8e19af3a",
  ...
}
```



# PROBLEMS WITH DYNAMIC CLIENT REGISTRATION

## FOR AUTHORIZATION SERVERS

- **Unbounded database growth**
- **No authority of the client information**
- **No correlation between instances of client software**
- **Public DCR endpoint requires protections like rate limiting**

## FOR CLIENTS

- **Managing client credentials in addition to access token/refresh token**
- **No way to verify if a client ID is still valid**
- **Unclear lifecycle - No guidance on when to re-register**
- **Clients risk sending the user to a dead end, or register a new client on each login**

# CLIENT ID METADATA DOCUMENT (CIMD)

"BRING YOUR OWN CLIENT ID"

Client publishes their metadata at a URL

The URL is used as the `client_id` in the authorization request

```
...&client_id=https://example.com/client.json&scope=...
```

<https://datatracker.ietf.org/doc/draft-ietf-oauth-client-id-metadata-document/>

# CLIENT ID METADATA DOCUMENT (CIMD)

## SIMPLE EXAMPLE

```
{  
  "client_id": "https://example.com/client.json",  
  "client_name": "Example Client",  
  "client_uri": "https://example.com",  
  "logo_uri": "https://example.com/logo.png",  
  "redirect_uris": [  
    "https://example.com/redirect"  
  ]  
}
```

The URL is used in an Authorization request

`/authorize?client_id=https://example.com/client.json&scope=...`

# CLIENT ID METADATA DOCUMENT (CIMD)

- Client hosts their metadata at a URL
- Metadata can contain `jwtks_uri` for clients to authenticate
- Authorization server can allow any client, or can allow specific clients
- Domain name acts as authority, e.g. "*I trust claude.ai clients*"

Learn More!

Demistifying Client ID Metadata Documents in MCP - Den Delimarsky, Anthropic

📅 Friday April 3, 2026 11:30am - 11:55am EDT

📍 Empire Complex (7th Floor)

# OAuth Client ID Metadata Document

## draft-ietf-oauth-client-id-metadata-document-01

Status

IESG evaluation record

[IESG writeups](#)

[Email expansions](#)

[History](#)

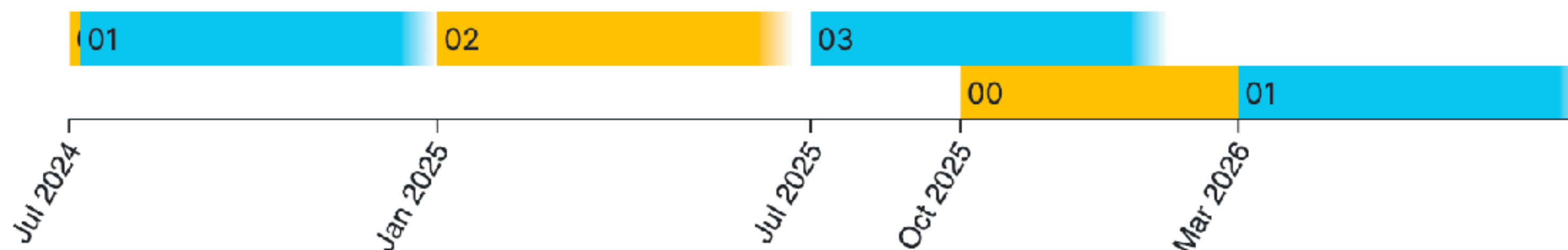
### Versions:

00

01

draft-parecki-oauth-client-id-metadata-document

draft-ietf-oauth-client-id-metadata-document



**Document**

**Type**

Active Internet-Draft ([oauth WG](#))

**Authors**

[Aaron Parecki](#) ✉, [Emelia Smith](#) ✉

**Last updated**

2026-03-01

**Replaces**

[draft-parecki-oauth-client-id-metadata-document](#)

**RFC stream**

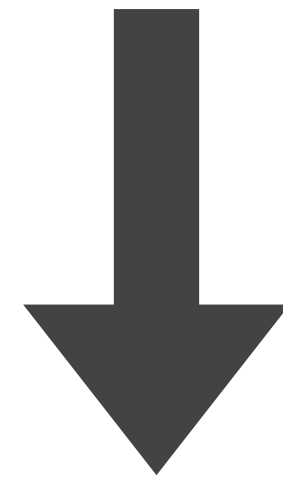
Internet Engineering Task Force (IETF)

# **DYNAMIC DISCOVERY**

<https://github.com/login/oauth/authorize>

<https://api.github.com/orgs>

<https://example.com/.well-known/oauth-authorization-server>



RFC8414  
Authorization Server Metadata

<https://example.com/oauth/authorize>

<https://example.com/oauth/token>

## Add custom connector BETA

Connect Claude to your data and tools. [Learn more about connectors](#) or get started with [pre-built ones](#).

✓ Advanced settings

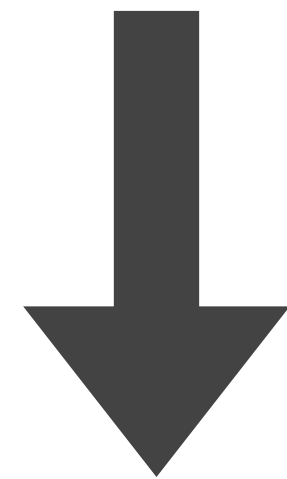
Only use connectors from developers you trust. Anthropic does not control which tools developers make available and cannot verify that they will work as intended or that they won't change.

Building an MCP server? [Report issues and subscribe to updates here](#)

Cancel

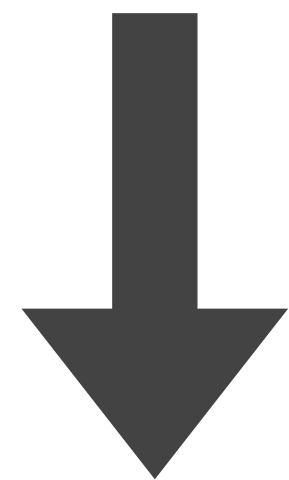
Add

<https://example.com/mcp>



RFC9728  
Protected Resource Metadata

<https://example.com/.well-known/oauth-authorization-server>



RFC8414  
Authorization Server Metadata

<https://example.com/oauth/authorize>

<https://example.com/oauth/token>

# OAuth 2.0 Protected Resource Metadata RFC 9728

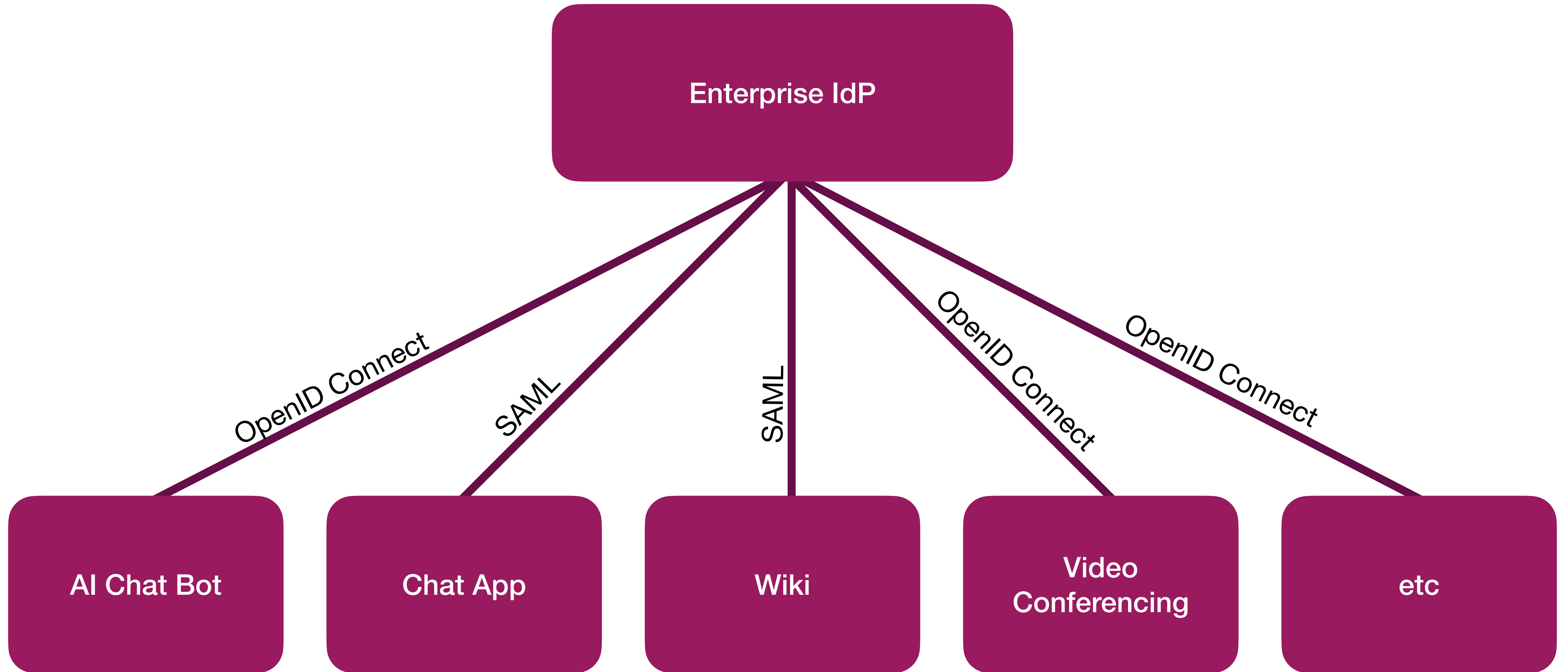
Status Email expansions History



<b>Document</b>	<b>Type</b>	RFC - Proposed Standard (April 2025) Was <a href="#">draft-ietf-oauth-resource-metadata</a> (oauth WG)
	<b>Authors</b>	<a href="#">Michael B. Jones</a> ✉, <a href="#">Phil Hunt</a> ✉, <a href="#">Aaron Parecki</a> ✉
	<b>Last updated</b>	2025-04-23
	<b>RFC stream</b>	Internet Engineering Task Force (IETF)

# **CLICK-THROUGH FATIGUE**

# Enterprise Single Sign-On



Search menu

Use style >

Extended thinking

---

Web search

Drive search Connect

Gmail search Connect

Calendar search BETA

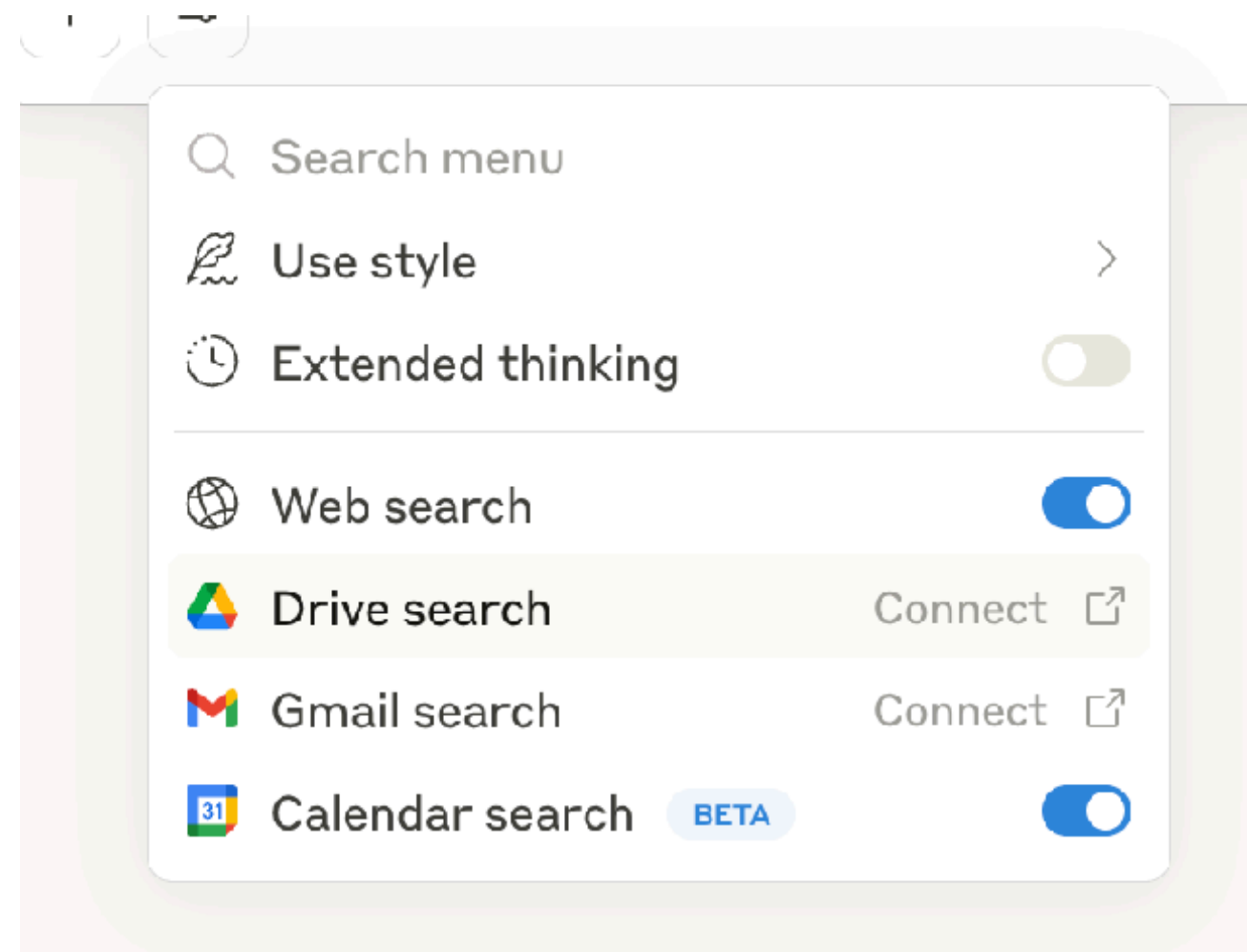
Dropbox Dash

### Add apps to find your content in one place

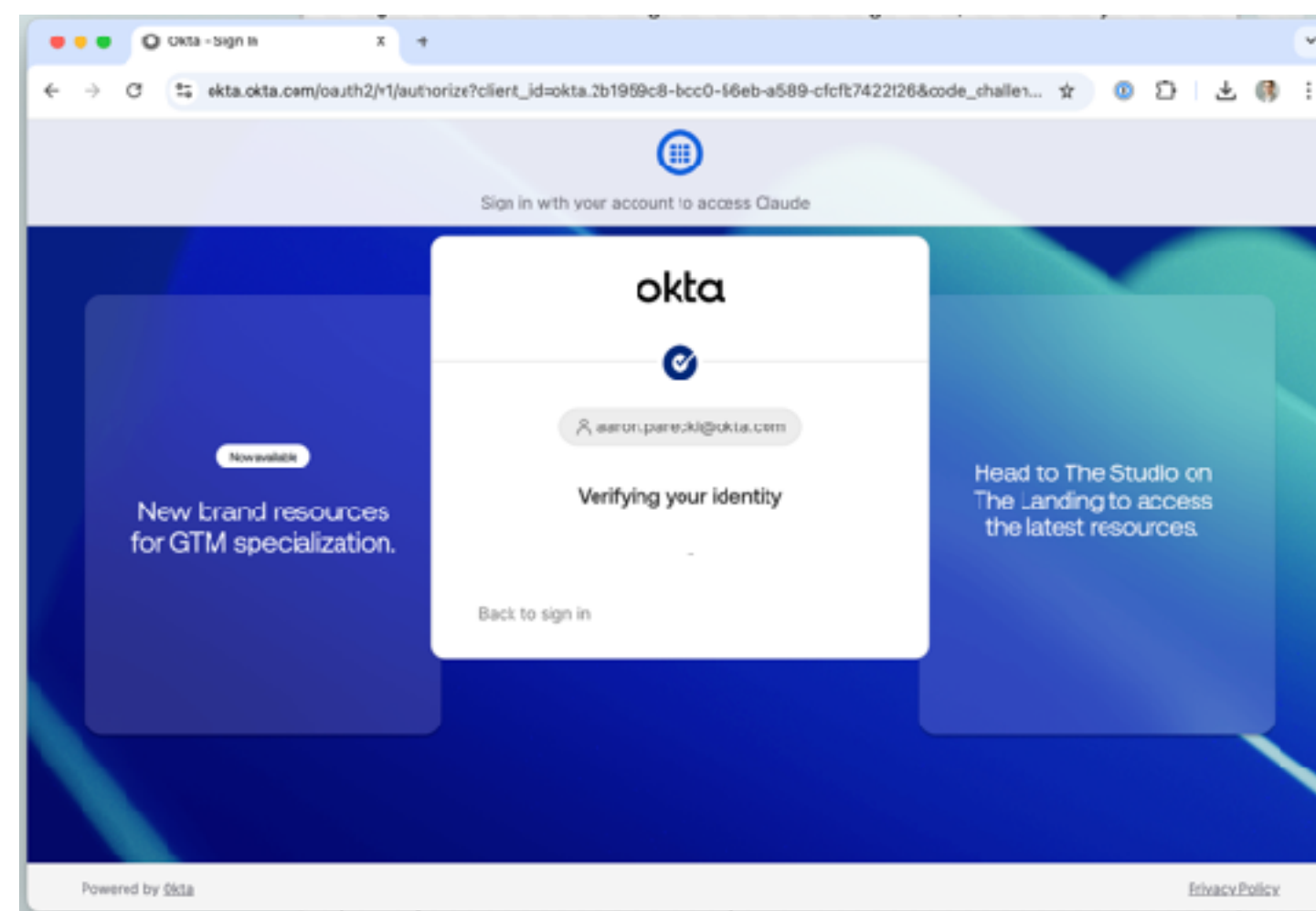
Save time with Dash by searching your content in one place instead of 10.  
Learn more about our [privacy measures](#) and [AI](#).

<b>Dropbox</b> Connected by admin <input checked="" type="checkbox"/>	<b>Confluence</b> Connected by admin <input checked="" type="checkbox"/>
<b>Gmail</b> <input type="checkbox"/>	<b>Microsoft OneDrive</b> <input type="checkbox"/>
<b>Google Calendar</b> <input type="checkbox"/>	<b>Google Drive</b> <input type="checkbox"/>
<b>Microsoft OneDrive</b> <input type="checkbox"/>	<b>Microsoft Outlook</b> <input type="checkbox"/>

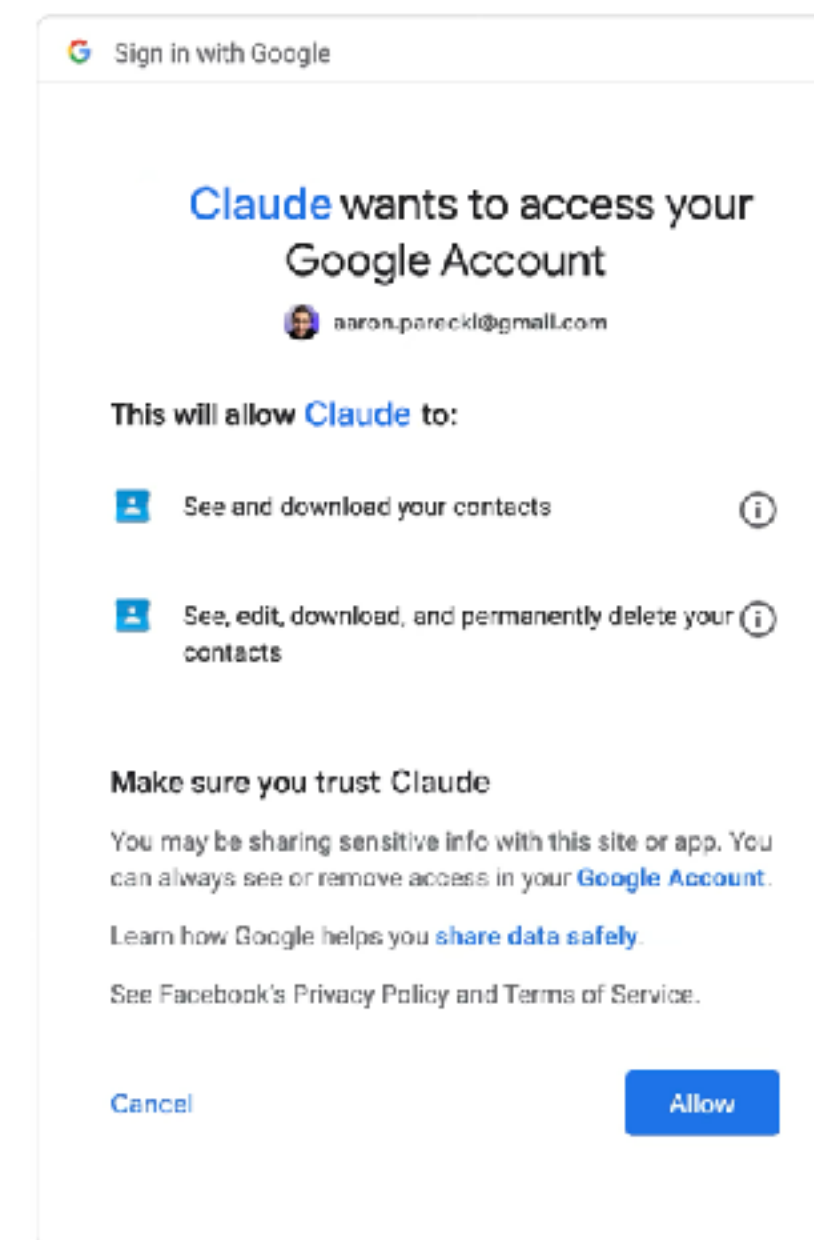
[Continue](#)



1. Connect Button



2. Login to Google through IdP



3. Google Consent Prompt



**Google**  
AISHA, CONNECT YOUR GOOGLE ACCOUNT

M G D S

APPROVE APPROVE

**CONNECT YOUR SLACK TO NOTION**

Allow Allow

**GITHUB ACCESS REQUESTED**

- Permissions with Gloudpt
- GitHub access
- Permissions with dianget

Permission Detail

**NEW**

AISHA, APPROVE TIKTCK TO USE YOUR PHOTO LIBRARY

AGREE AGREE

**Aisha, connect your Google Account.**

Permissions: Access Gmail, manage drive, tried contacts.

Approve Approve

**NEW**

**Connect Aisha to Jira**

- Project & Alaka dea
- Anthony Tambes luto
- Anthania Trafe

Approve Approve

**Aisha, logn to Spotify with Facebook.**

Share your music and friends like.

Allow! Play

**NEW**

**Aisha's Portfolio needs data from Dropbox.**

Giant permissions?

Allow!

Approve Approve

**Aisha, geet that sete con account**

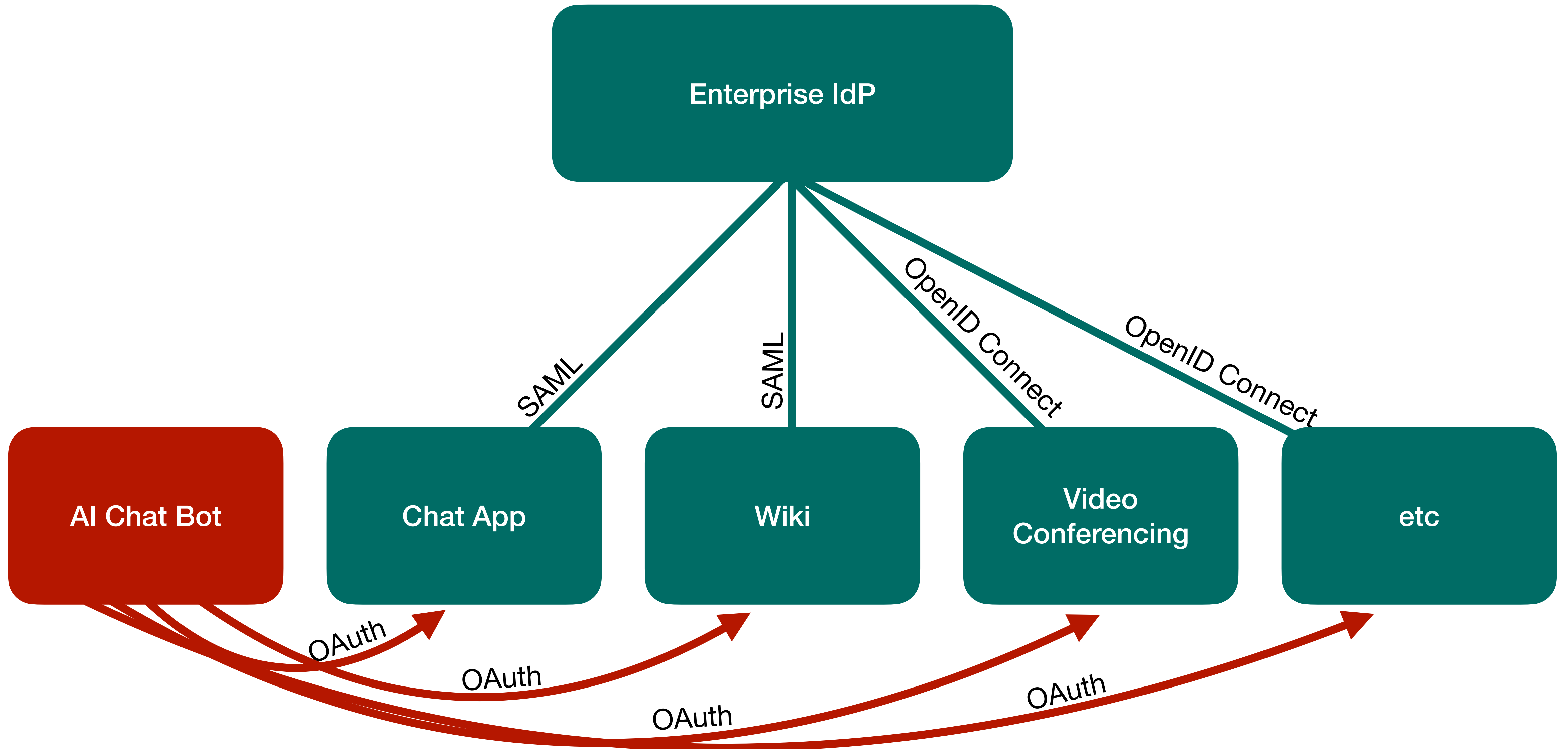
Approve Approve

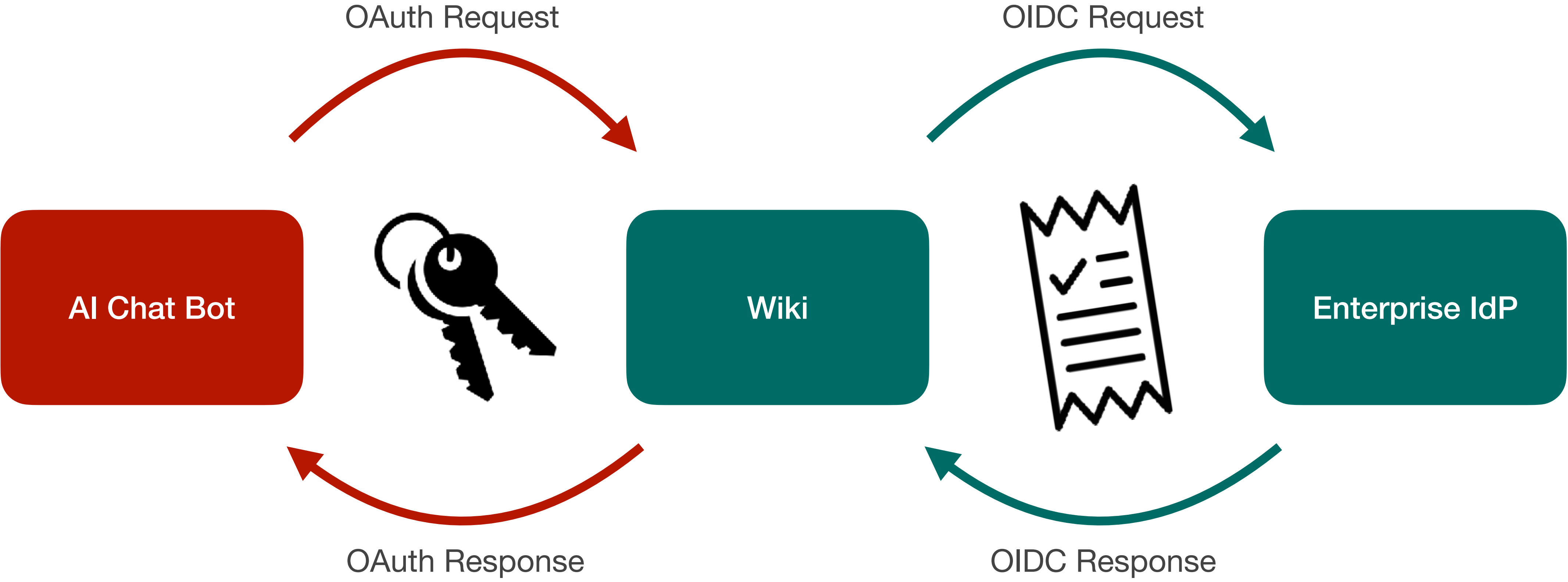
**Aisha, great Tuffio needs data a Google Account.**

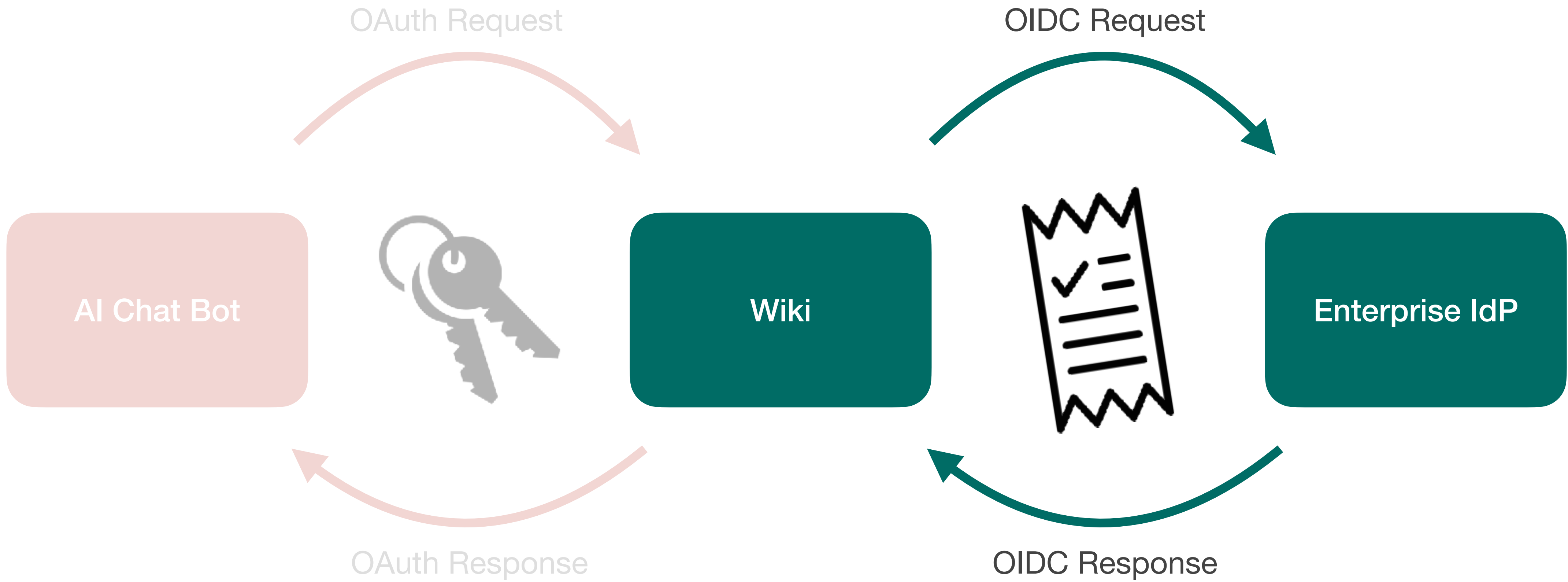
Allow!

Approve Approve

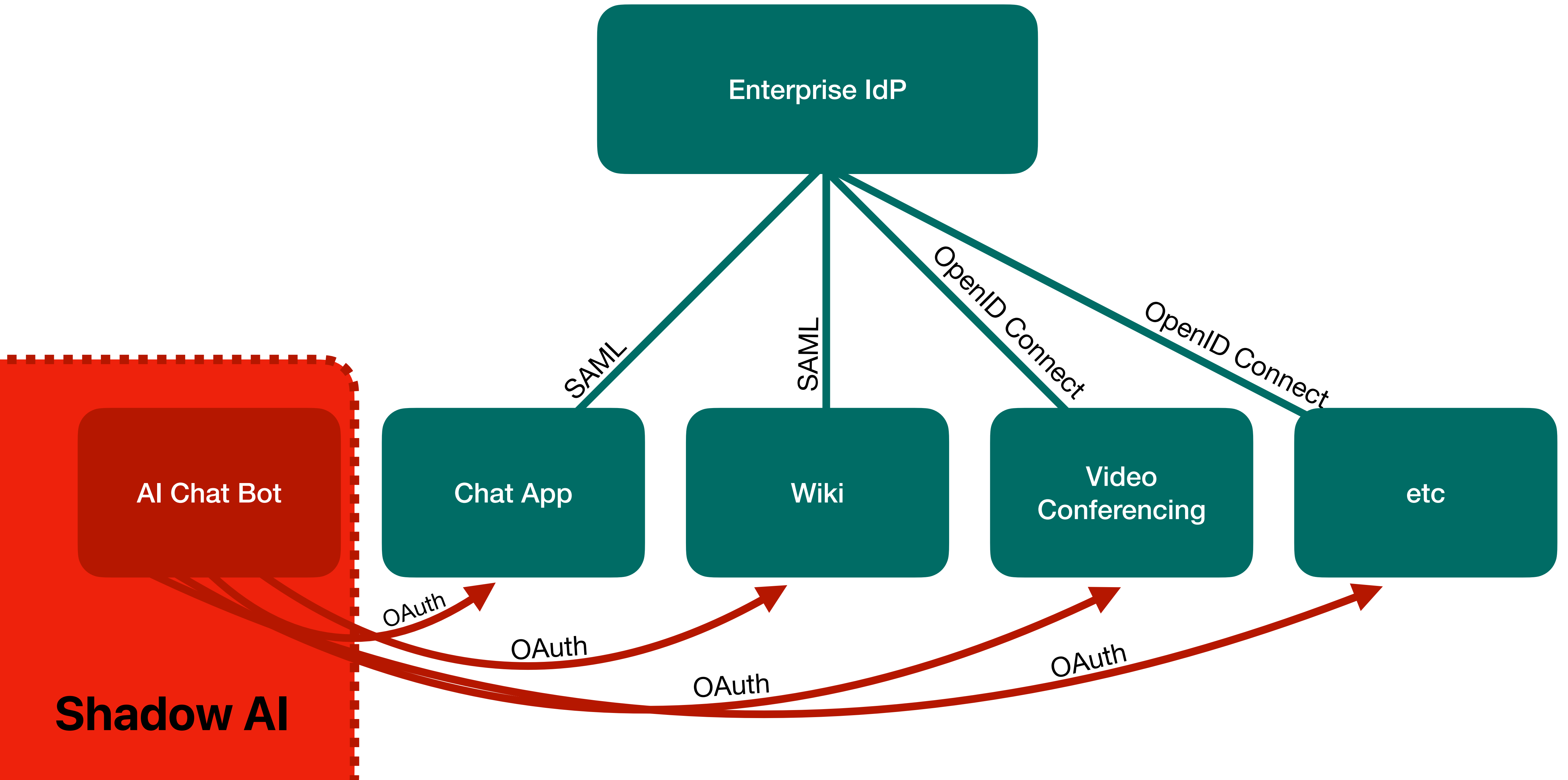
# Enterprise API Access Today







# Enterprise API Access Today



**No control or  
visibility by the  
enterprise  
IT admin**

**Terrible UX  
for Employees**

# Identity Assertion JWT Authorization Grant

## draft-ietf-oauth-identity-assertion-authz-grant-01

Status

[IESG evaluation record](#)

[IESG writeups](#)

[Email expansions](#)

[History](#)

### Versions:

[00](#) [01](#)

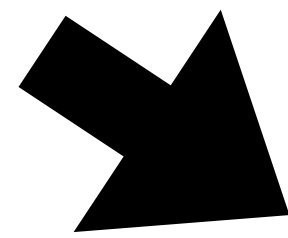
draft-parecki-oauth-identity-assertion-authz-grant  
draft-ietf-oauth-identity-assertion-authz-grant



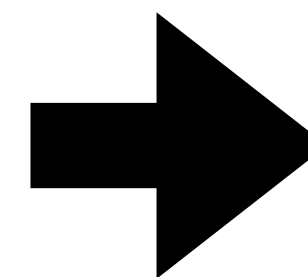
<b>Document</b>	<b>Type</b>	Active Internet-Draft ( <a href="#">oauth WG</a> )
	<b>Authors</b>	<a href="#">Aaron Parecki</a> , <a href="#">Karl McGuinness</a> , <a href="#">Brian Campbell</a>
	<b>Last updated</b>	2025-10-19
	<b>Replaces</b>	<a href="#">draft-parecki-oauth-identity-assertion-authz-grant</a>
	<b>RFC stream</b>	Internet Engineering Task Force (IETF)



**RFC 8693**  
**OAuth Token Exchange**

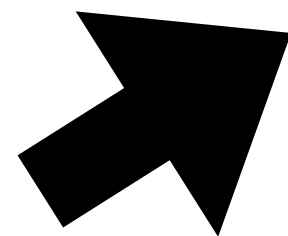


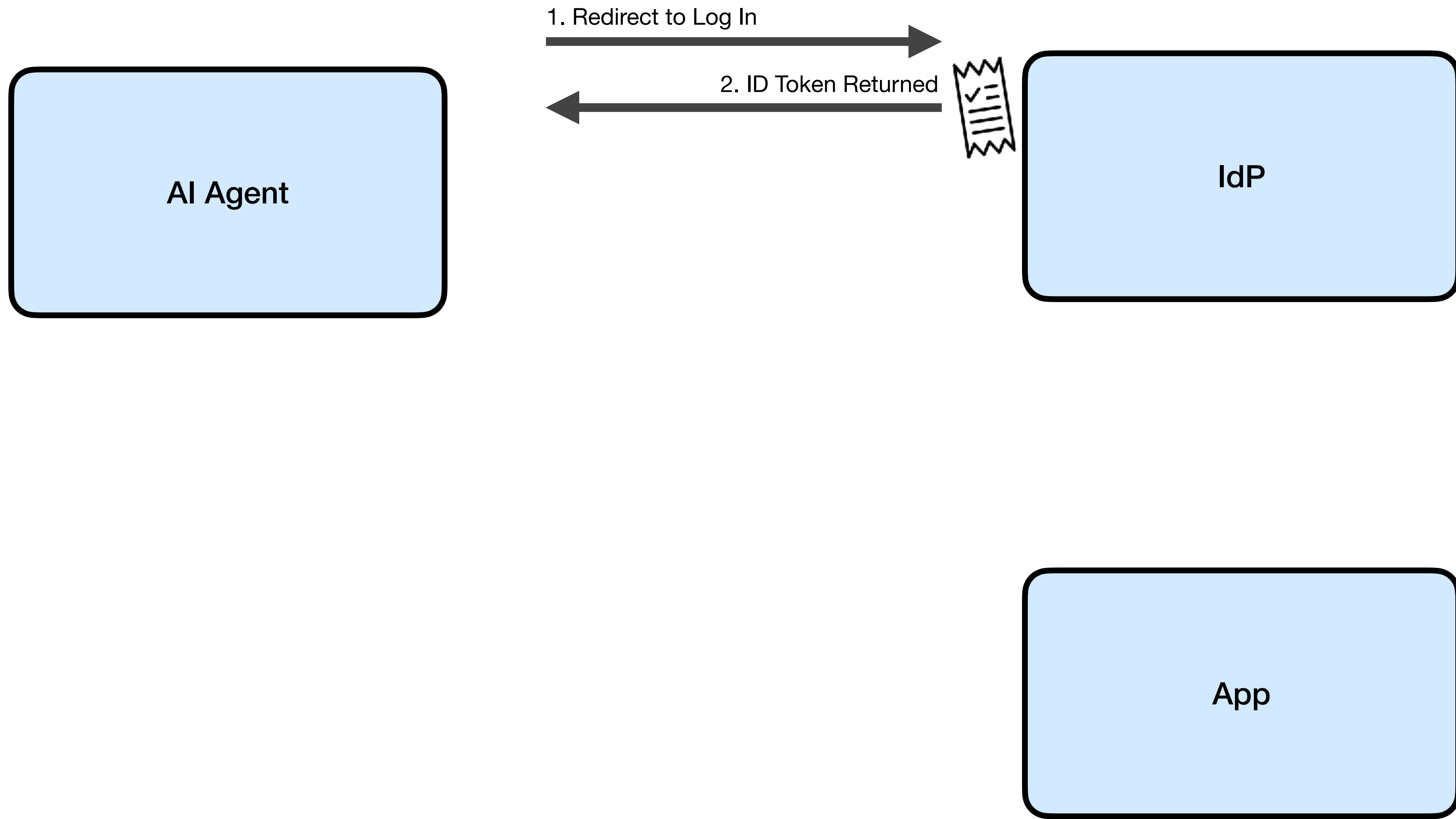
**(Working Group Draft)**  
**OAuth Identity and Authorization**  
**Chaining Across Domains**

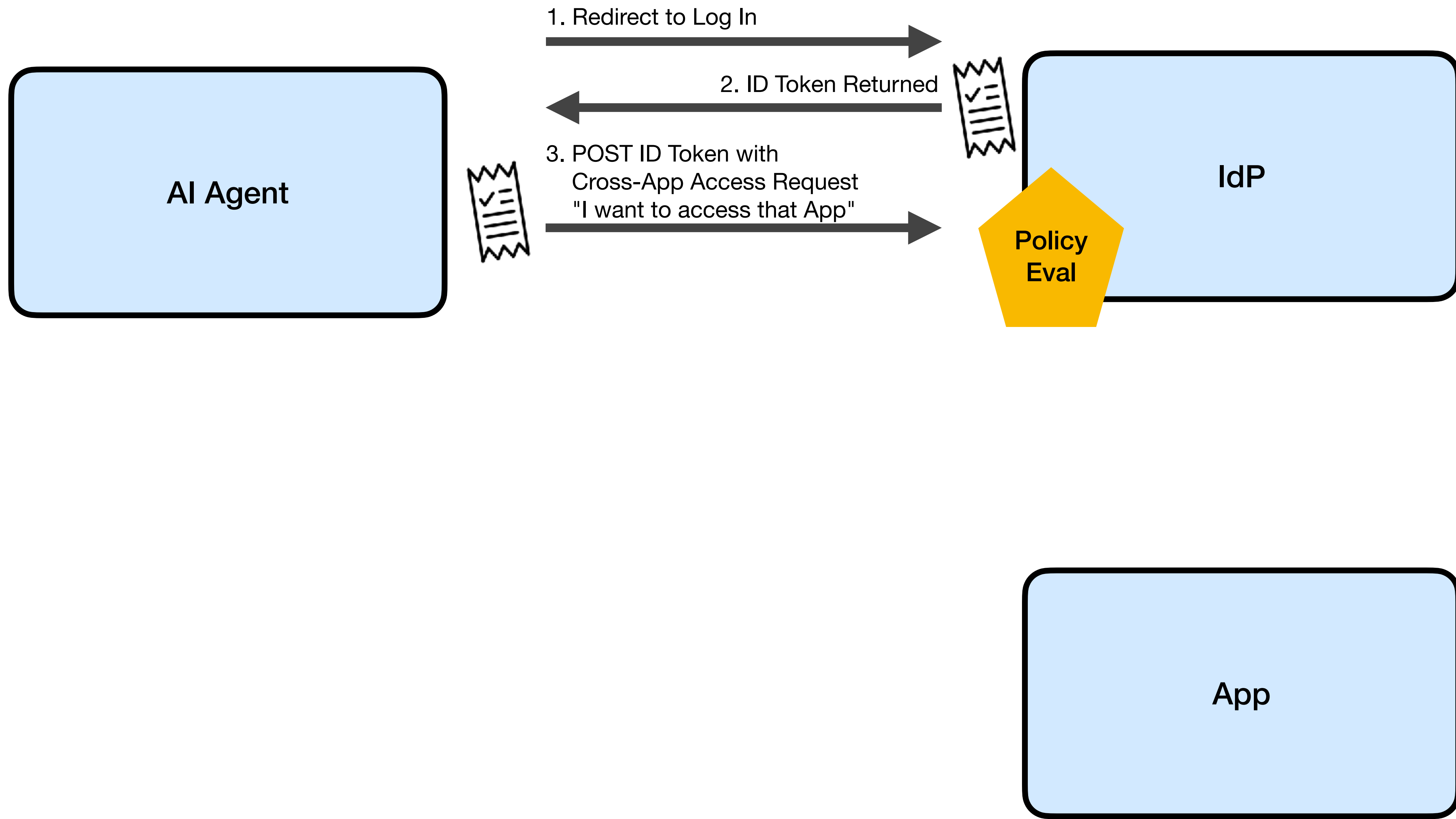


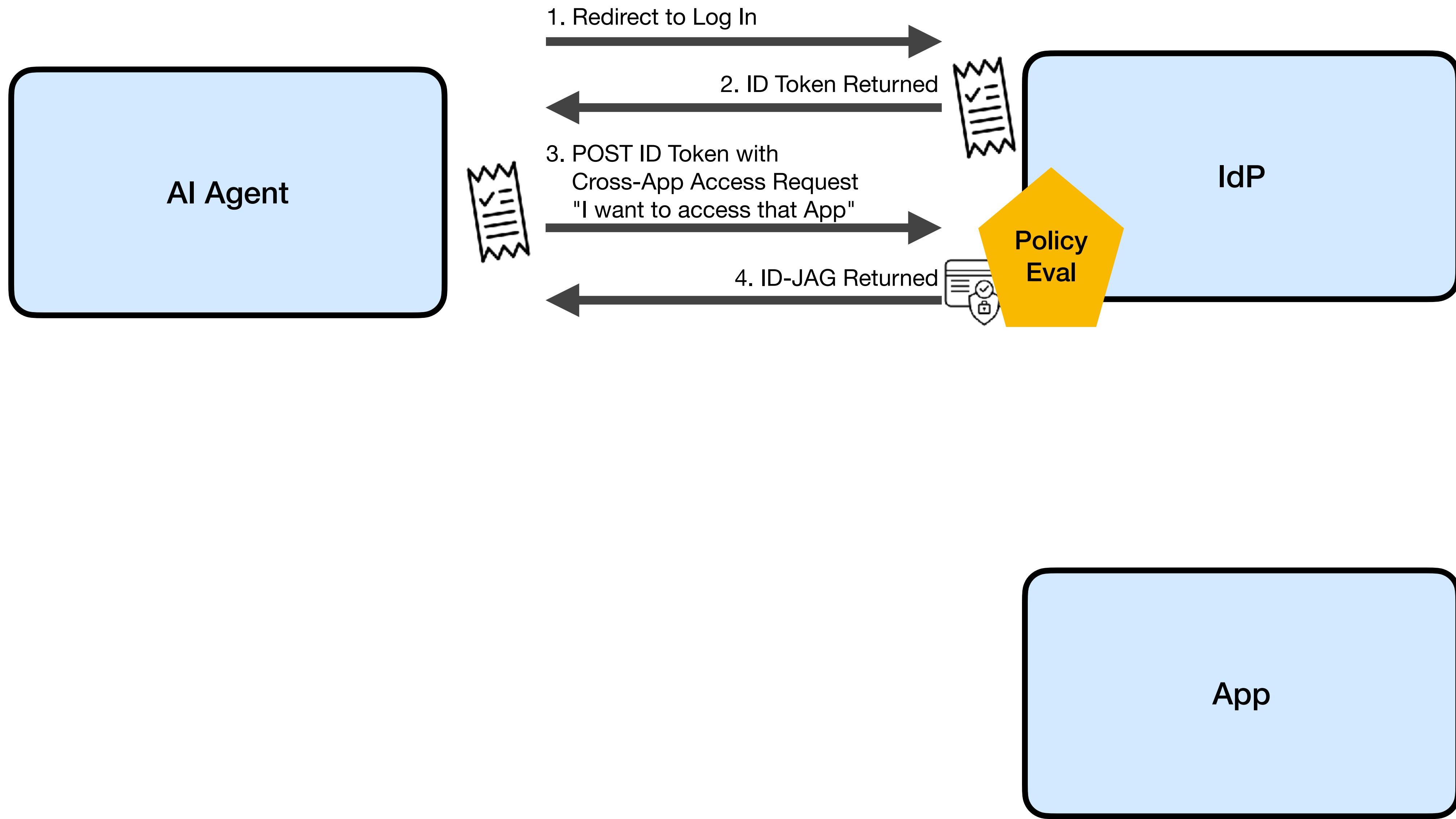
**Cross-App Access**  
**(Working Group Draft)**  
**Identity Assertion**  
**JWT Authorization Grant**

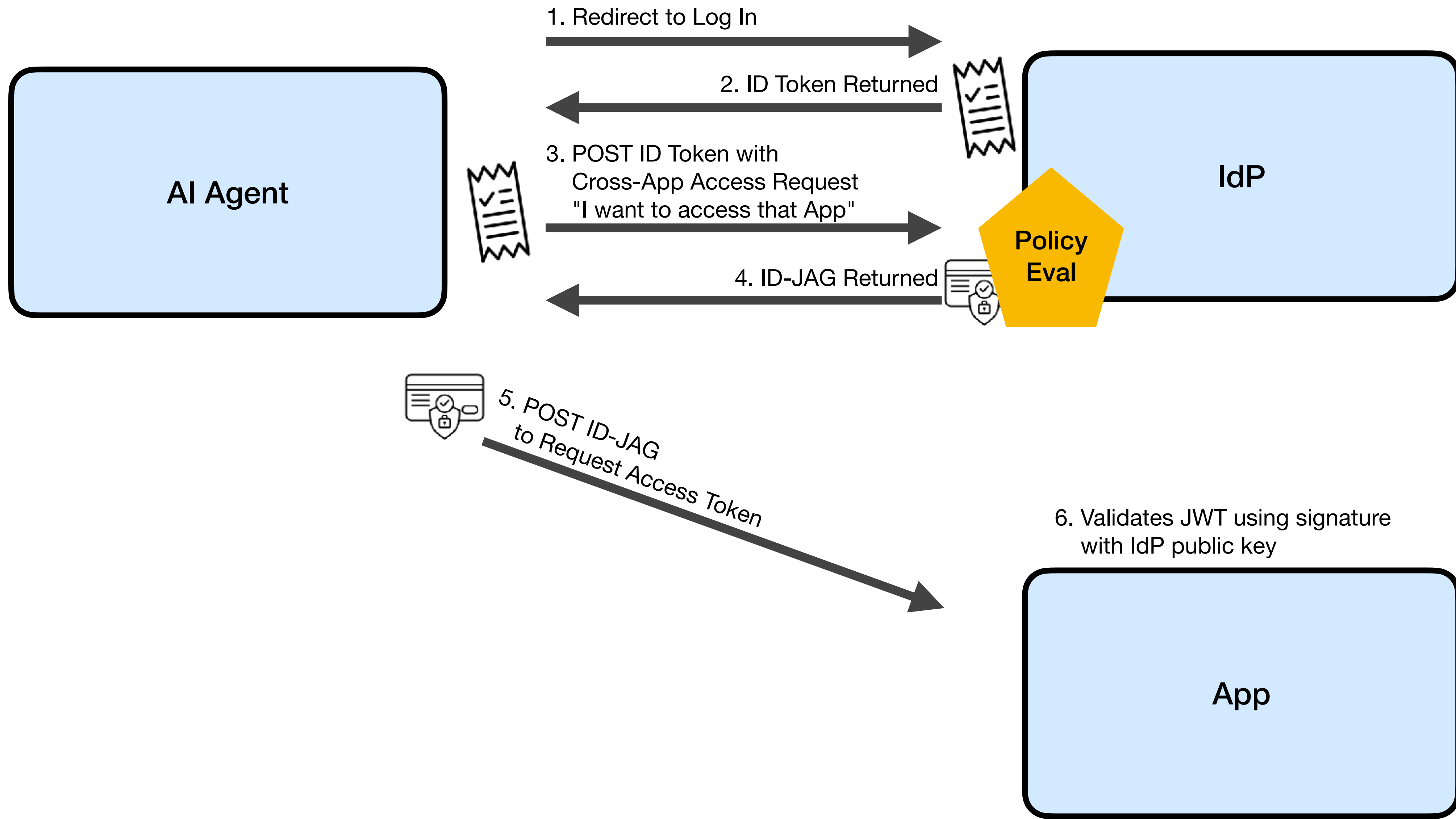
**RFC 7523**  
**JWT Profile for OAuth**  
**Authorization Grants**

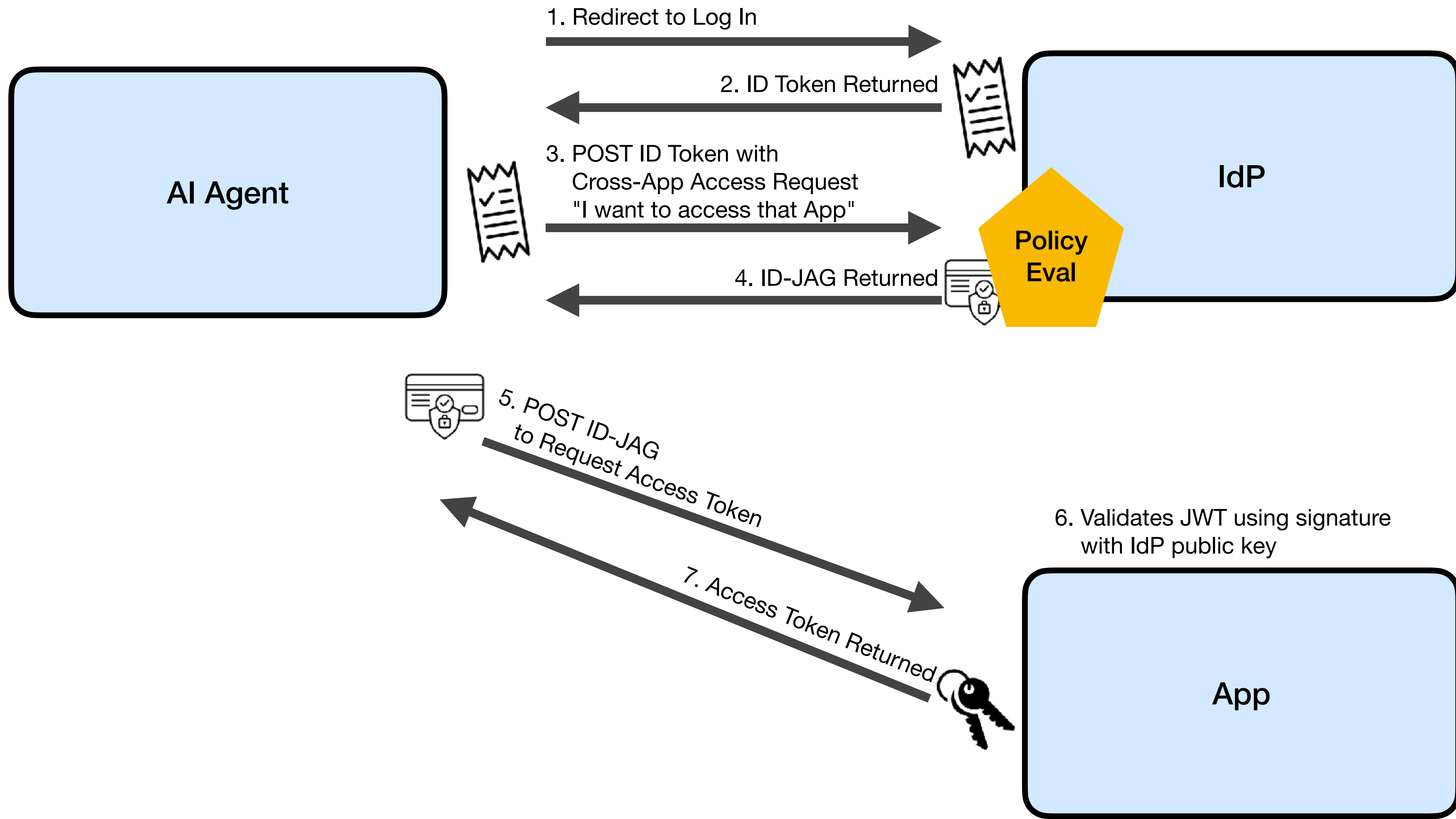




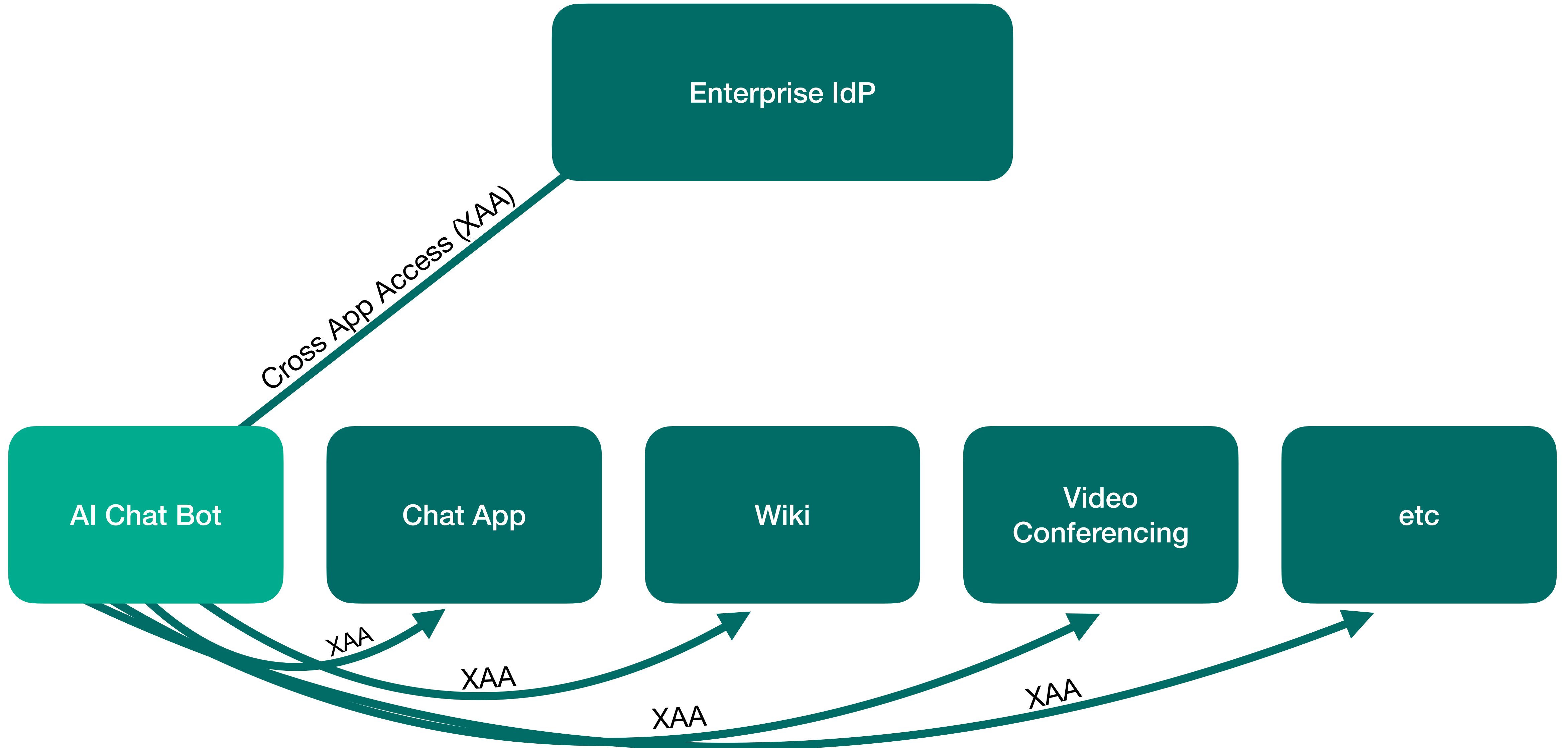









# Cross App Access



Live Demo!

**Putting the Single Back in Single Sign-On: Cross-App Access for MCP -  
Paul Carleton, Anthropic & Max Gerber, Twilio**

 Friday April 3, 2026 2:25pm - 2:50pm EDT

 Empire Complex (7th Floor)

# Evolution, not revolution



RFC6749

RFC6750

draft-ietf-oauth-v2-1

RFC8414

RFC9728

draft-ietf-oauth-client-id-metadata-document

draft-ietf-oauth-identity-assertion-authz-grant

[aaronpk.com](http://aaronpk.com)

[oauth.wtf](http://oauth.wtf)

[oauth.net](http://oauth.net)