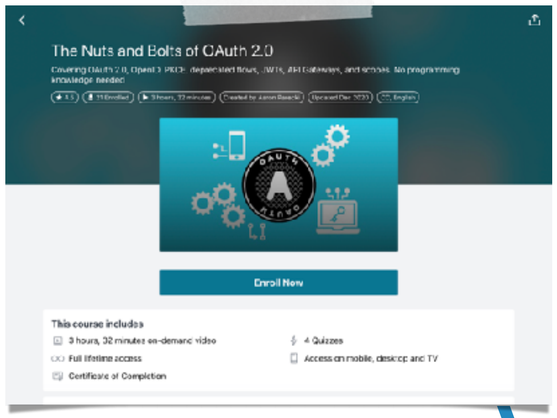
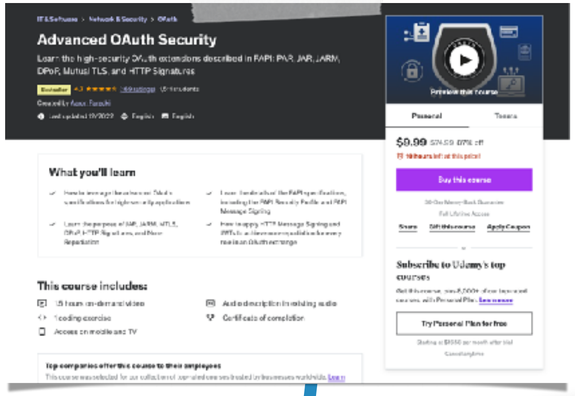
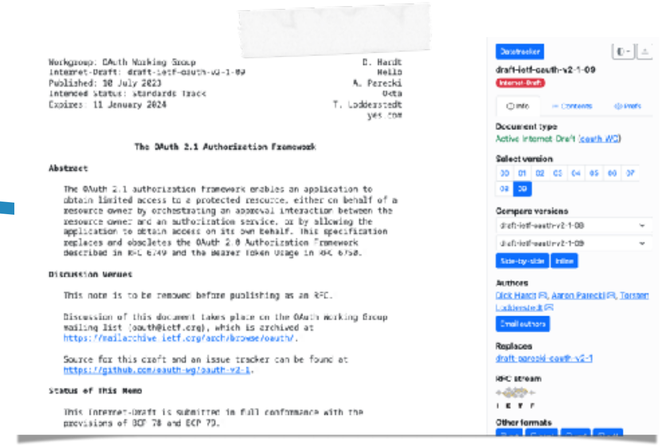
Evolution, not Revolution

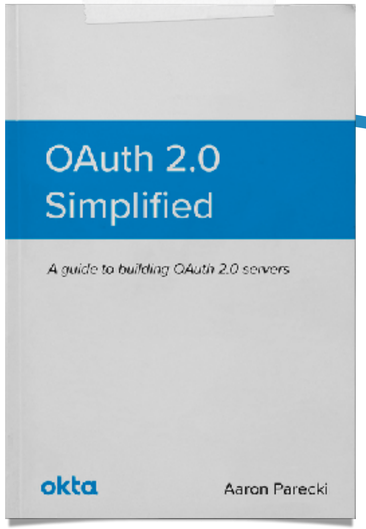
How MCP is Reshaping OAuth

Aaron Parecki • April 2026 • MCP Dev Summit


The Nuts and Bolts of OAuth 2.0
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
What you'll learn
This course includes:
Buy this course
Try Personal Plan for free

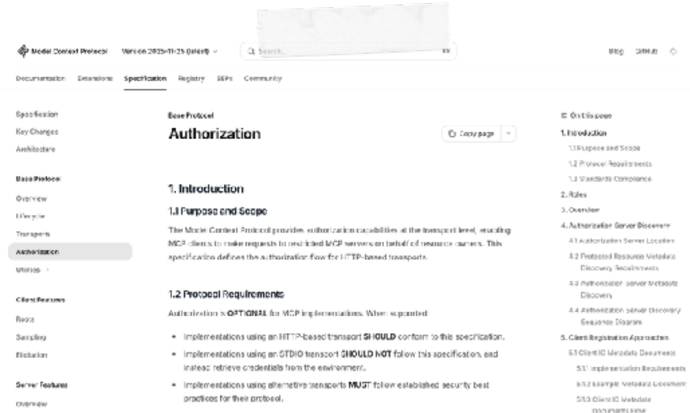

Workgroup: OAuth Working Group
Internet-Draft: draft-ietf-oauth-v2-1-09
Published: 30 July 2023
Intended status: Standards Track
Expires: 11 January 2024
The OAuth 2.1 Authorization Framework
Abstract
Discussion Venues
Status of This Memo
draft-ietf-oauth-v2-1-09
Document type
Select version
Compare versions
Authors
Replaces
IRTF stream
Other formats


OAuth 2.0
Simplified
A guide to building OAuth 2.0 servers
okta
Aaron Parecki

okta

I E T F®


Workgroup: Web Authorization Protocol
Internet-Draft:
draft-ietf-oauth-client-id-metadata-document-01
Published: 2 March 2026
Intended Status: Standards Track
Expires: 3 September 2026
OAuth Client ID Metadata Document
Abstract
About This Document
Status of This Memo
draft-ietf-oauth-client-id-metadata-document-01
Document type
Select version
Compare versions
Authors
Replaces
IRTF stream
Intended RFC status
Other formats
Additional resources


Model Context Protocol
Authorization
1. Introduction
1.1 Purpose and Scope
1.2 Protocol Requirements

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 5741.

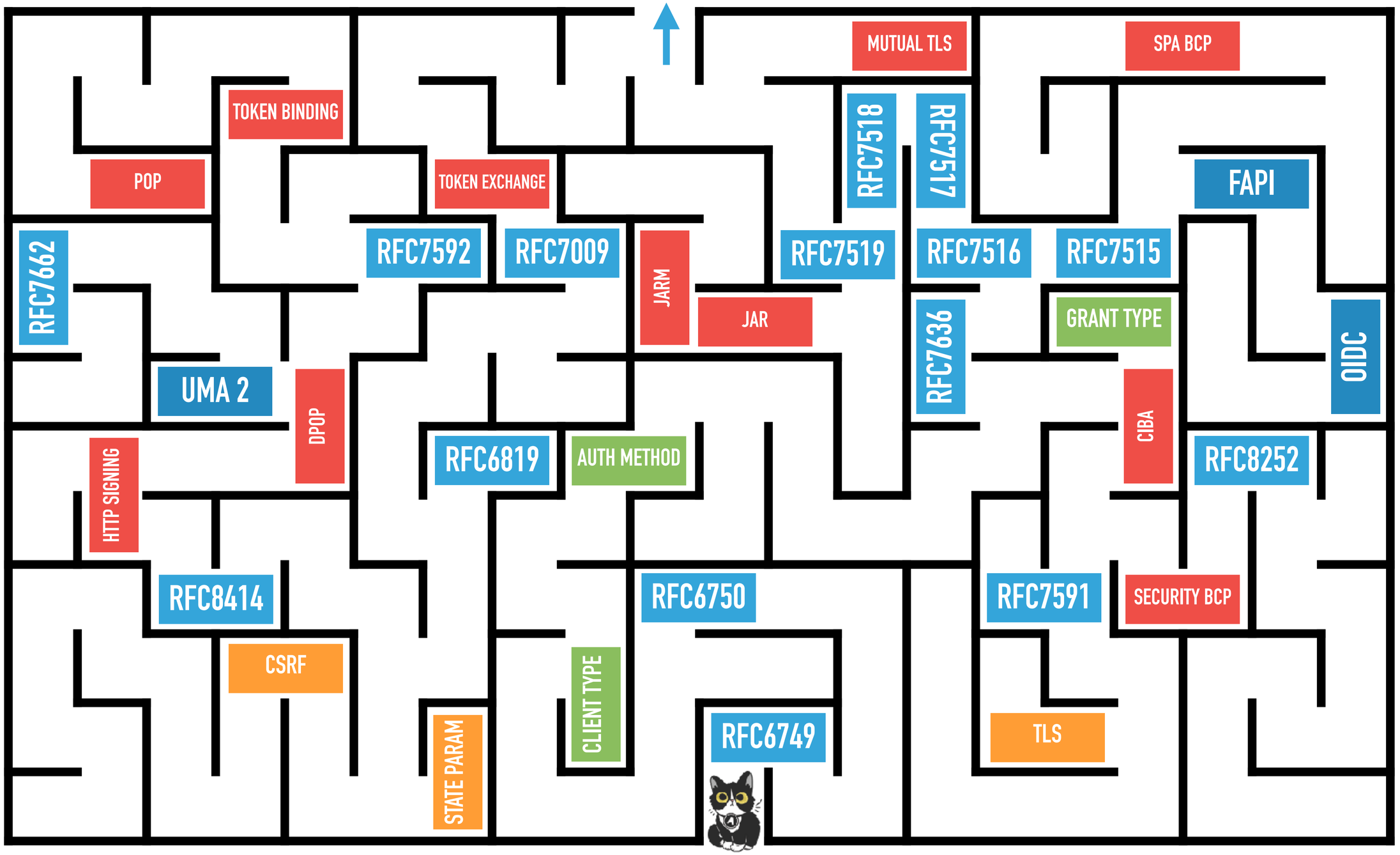
Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6749.

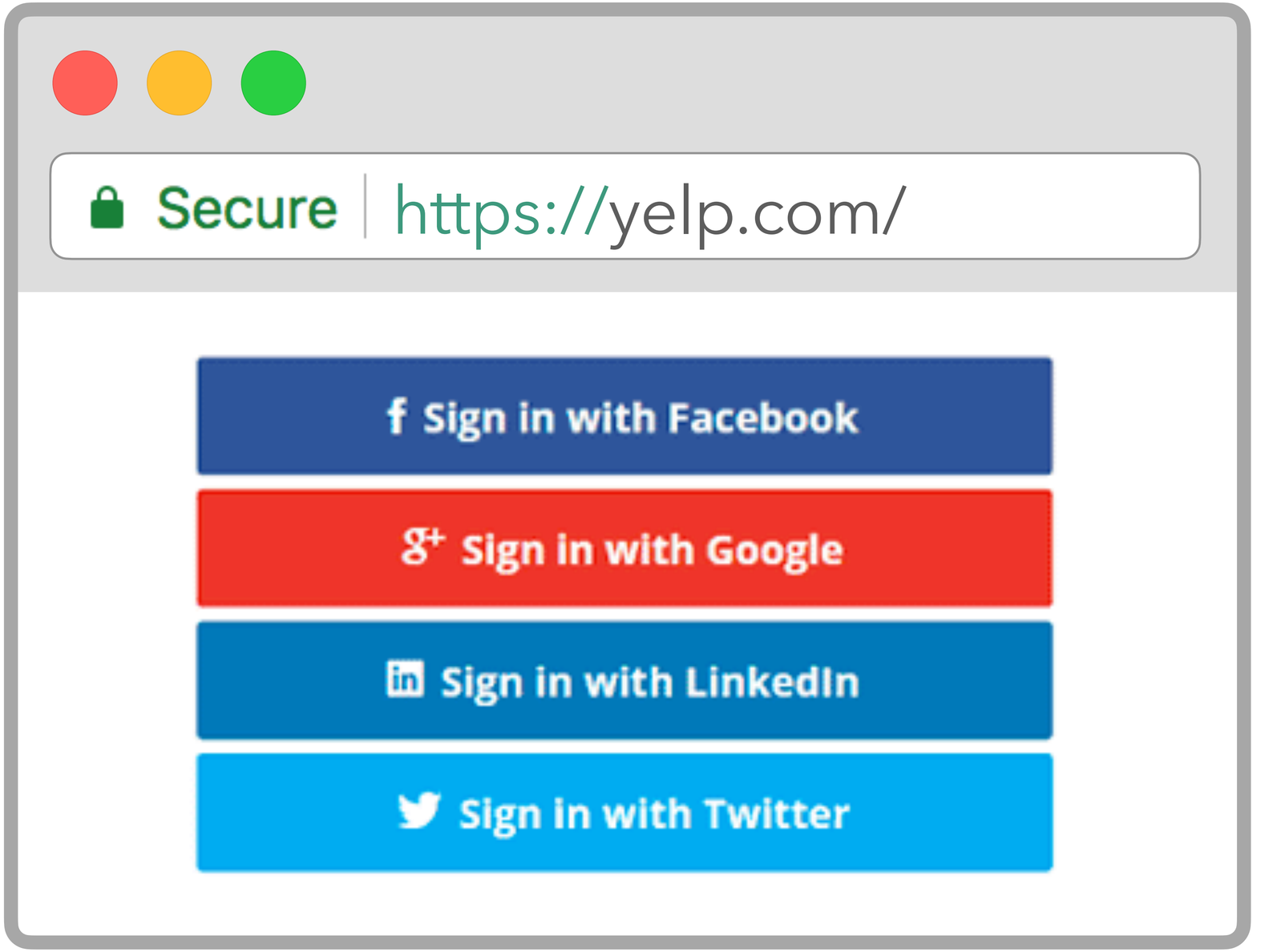
Copyright Notice

Table of Contents

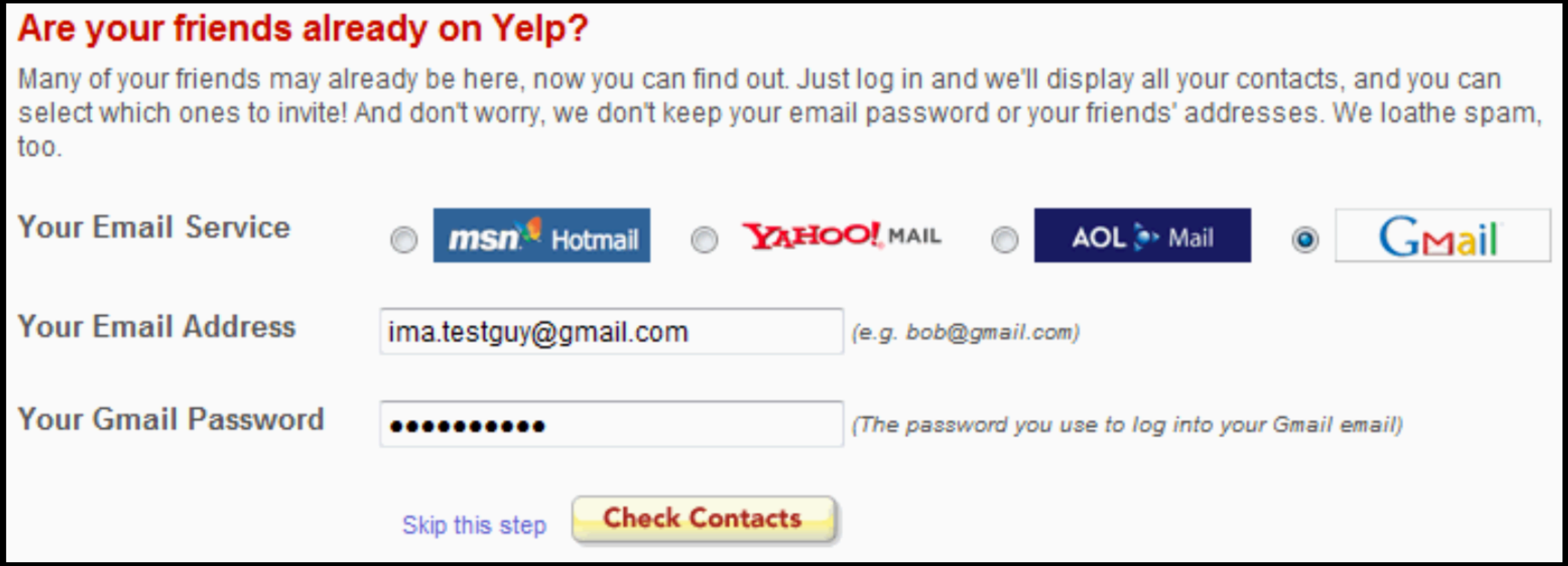
1. Introduction 4
1.1. Roles 6
1.2. Protocol Flow 7
1.3. Authorization Grant 8
1.3.1. Authorization Code 8
1.3.2. Implicit 8
1.3.3. Resource Owner Password Credentials 9
1.3.4. Client Credentials 9
1.4. Access Token 10
1.5. Refresh Token 10
1.6. TLS Version 12
1.7. HTTP Redirections 12

Specs are not good tutorials!

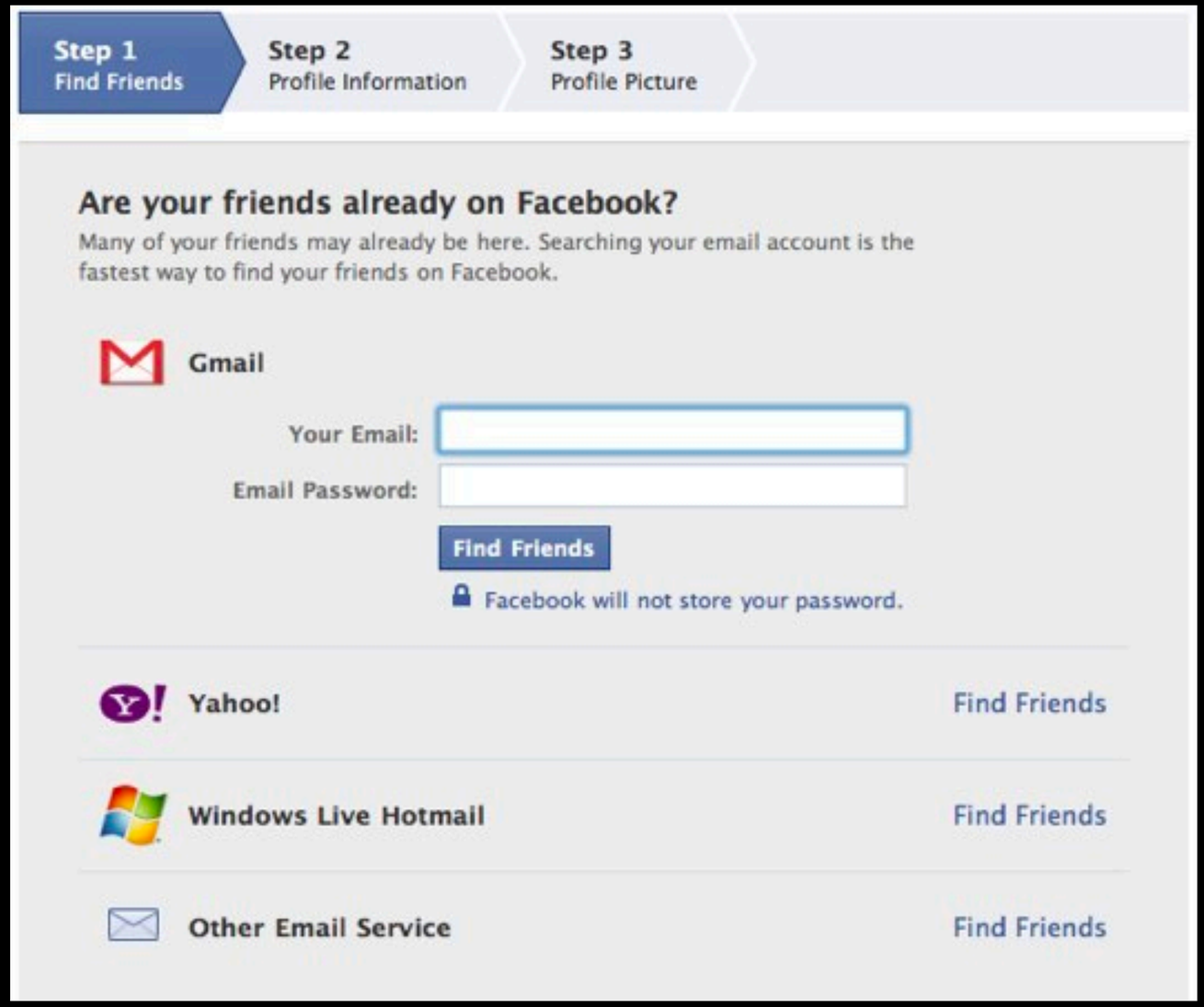

MUTUAL TLS
SPA BCP
TOKEN BINDING
RFC7518
RFC7517
POP
TOKEN EXCHANGE
FAPI
RFC7662
RFC7592
RFC7009
JARM
RFC7519
RFC7516
RFC7515
JAR
RFC7636
GRANT TYPE
OIDC
UMA 2
DPOP
CIBA
HTTP SIGNING
RFC6819
AUTH METHOD
RFC8252
RFC8414
RFC6750
RFC7591
SECURITY BCP
CSRF
CLIENT TYPE
RFC6749
TLS
STATE PARAM


Secure
https://yelp.com/
Sign in with Facebook
Sign in with Google
Sign in with LinkedIn
Sign in with Twitter

The Password Anti-Pattern



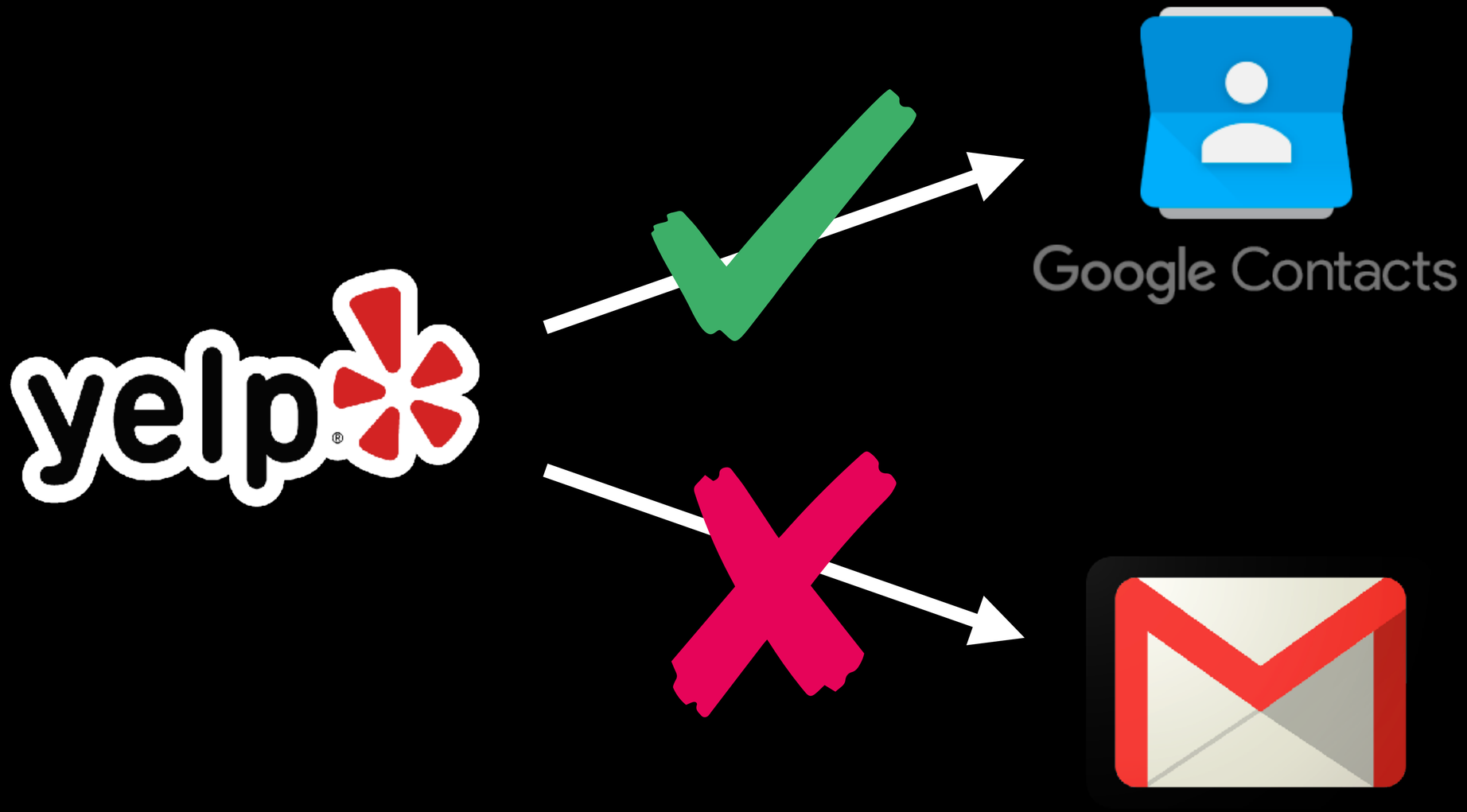
The Password Anti-Pattern



facebook.com ~2010

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?


yelp
Google Contacts

how can I let an app

access my data

without giving it my password?

Authorization Server

Access Token

Resource (API)

https://unsplash.com/photos/GJY1eAw6tn8

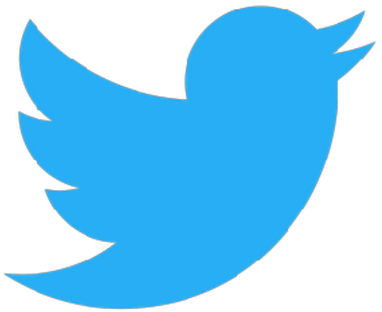

yelp

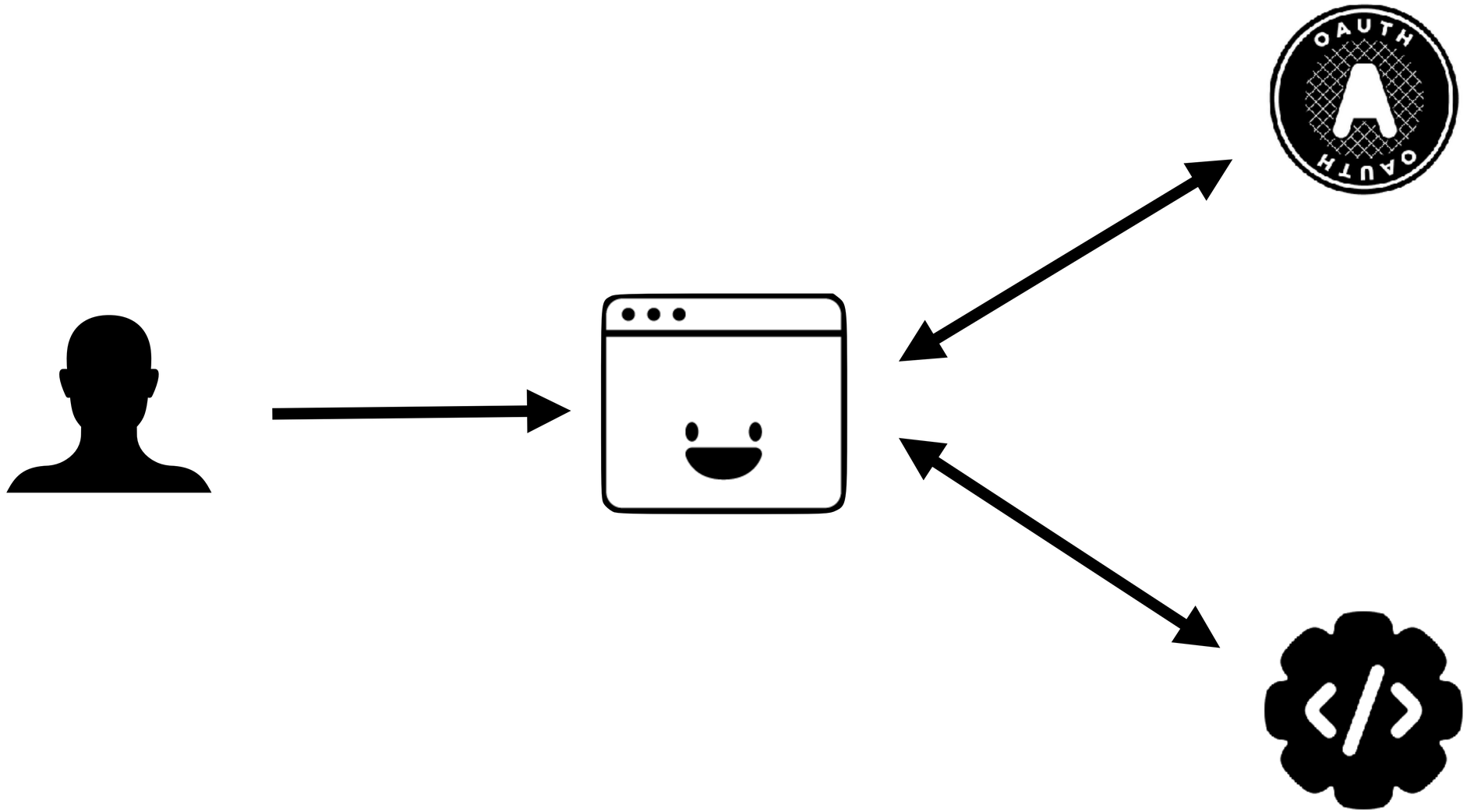

Google Contacts


last.fm

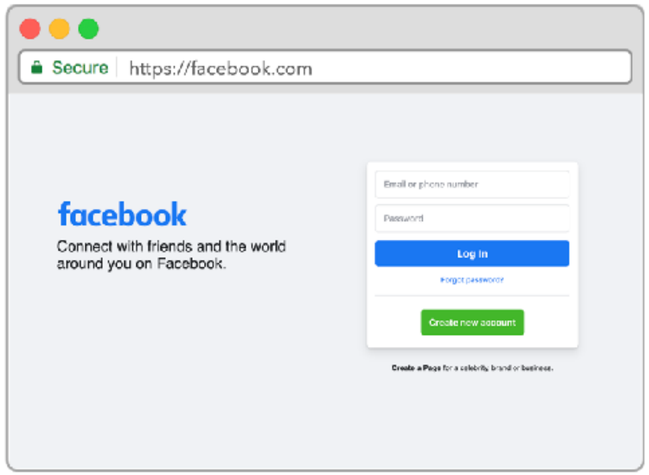

Spotify®

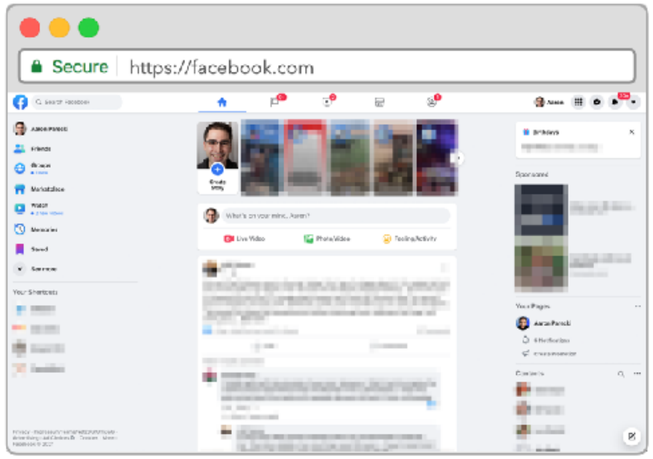

buffer



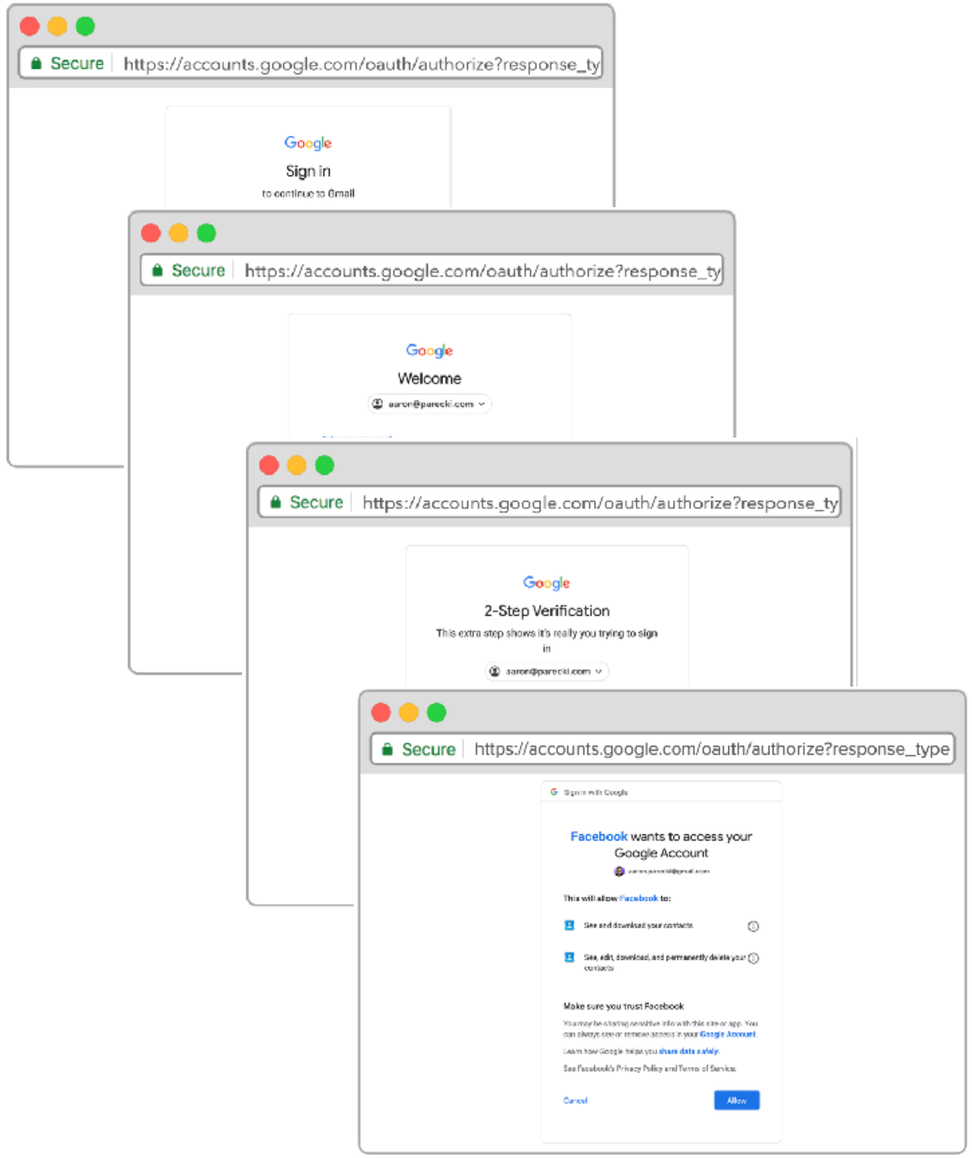

OAUTH
OAUTH

Application





OAuth Server



Sign in with Google

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

Example App

By Aaron Parecki

example-app.com

Free Version Control with unlimited private and public repositories.

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.

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

Application description is optional

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

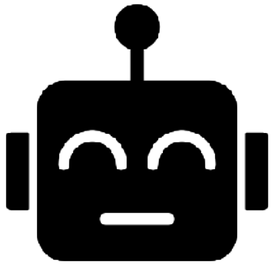
Application logo

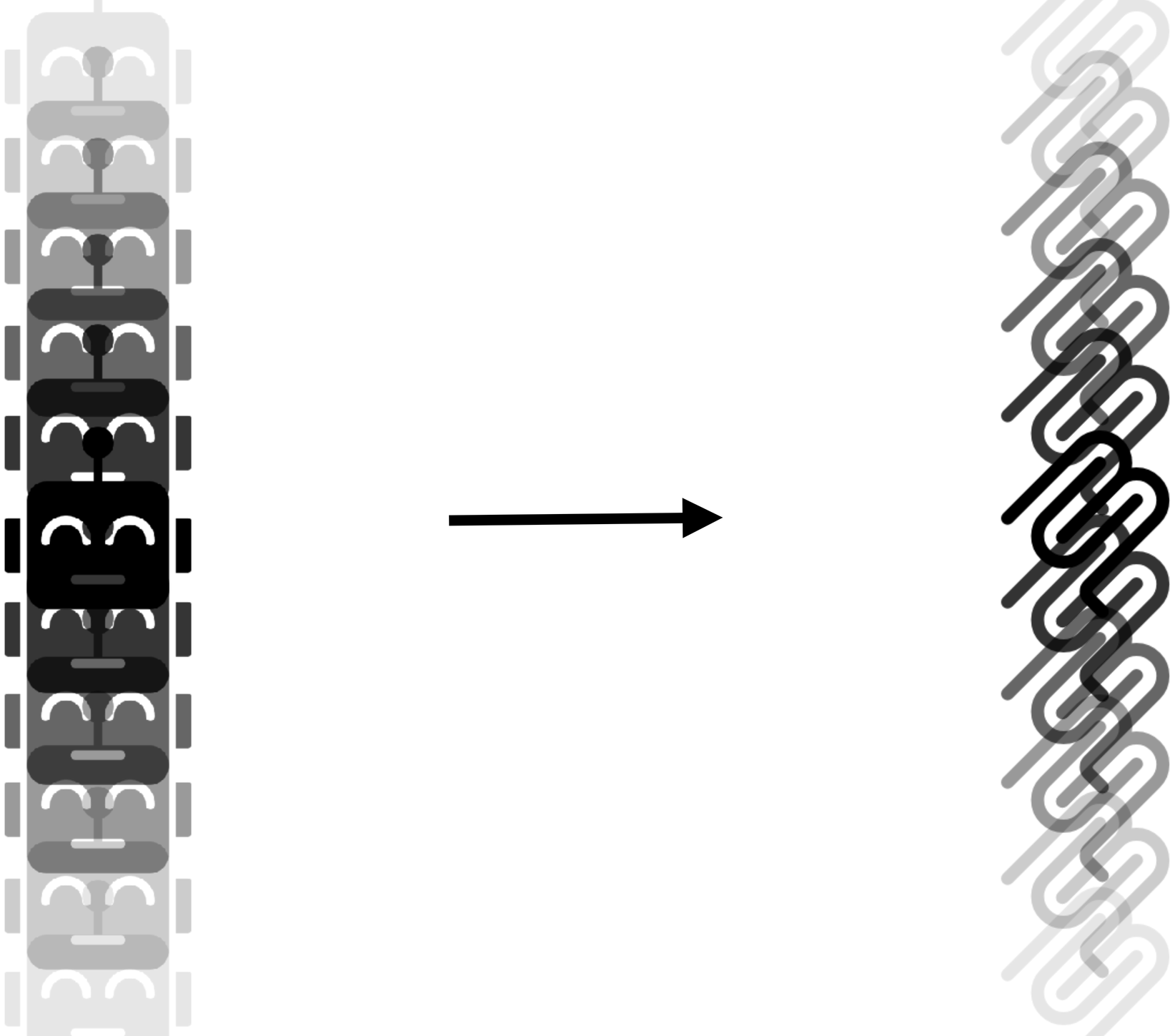
Upload new logo

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

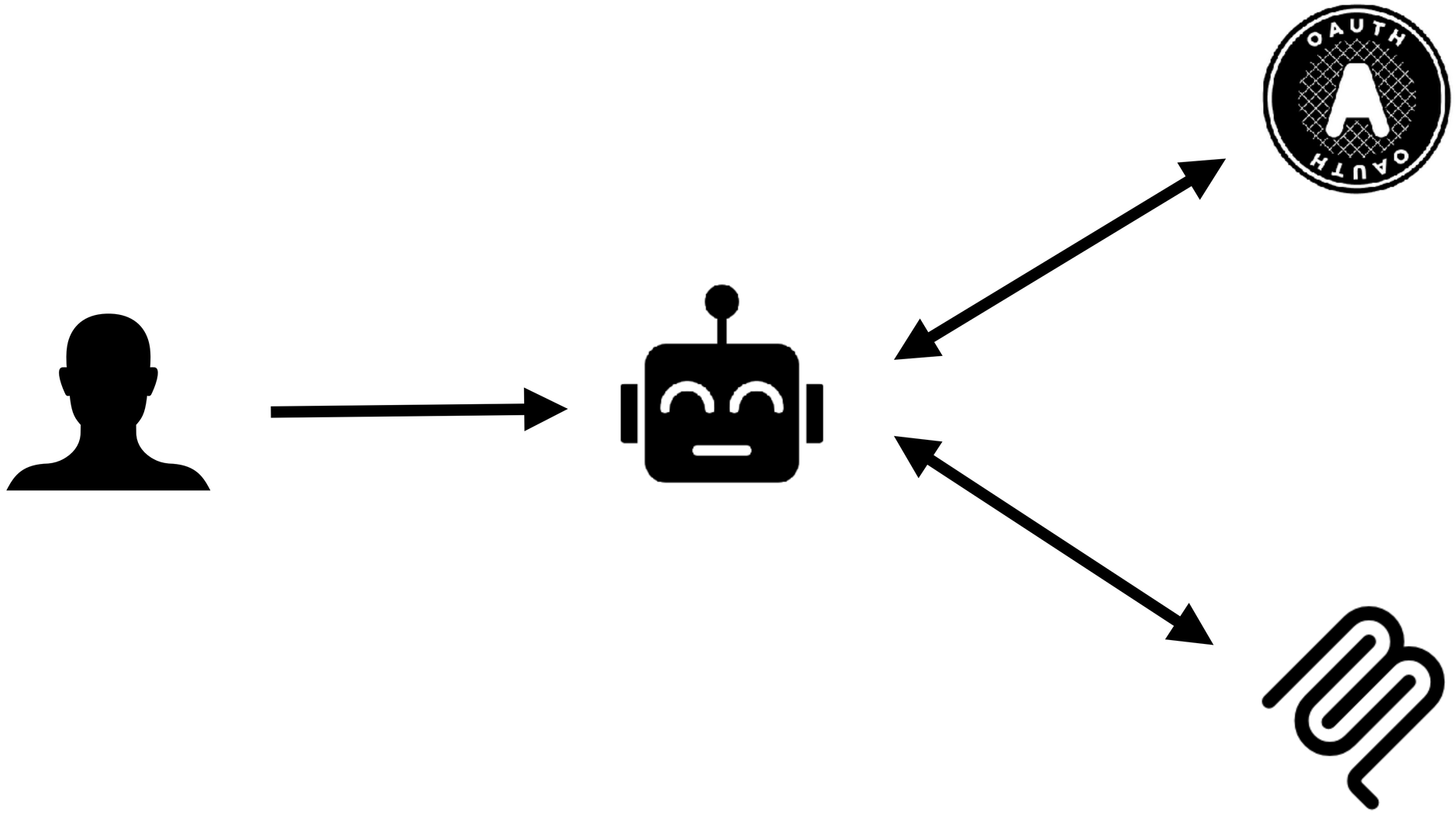

You Tube
Uber
AUTH
TRAIN
SWG
BF
WTL
AUTH
PORS
Uber
Uber
FIT
HEALTH
MEDS
STRAVA
SLEP
JS
JS
aws
RSS
MOVIES
NEWS
CODE
MRE
SITHUB
SITHUB NOME
HUE
aws
AWS
GOP
TER
DEV
APP
FEAT
HUST
SDF
AUTH
AUTH
CODE
SITHUB
AWASS HUSE
HUE
AWSZ HUST
AWASS MOUS
HUST
SDF
AUTH
AUTH

Enter the AI Agent





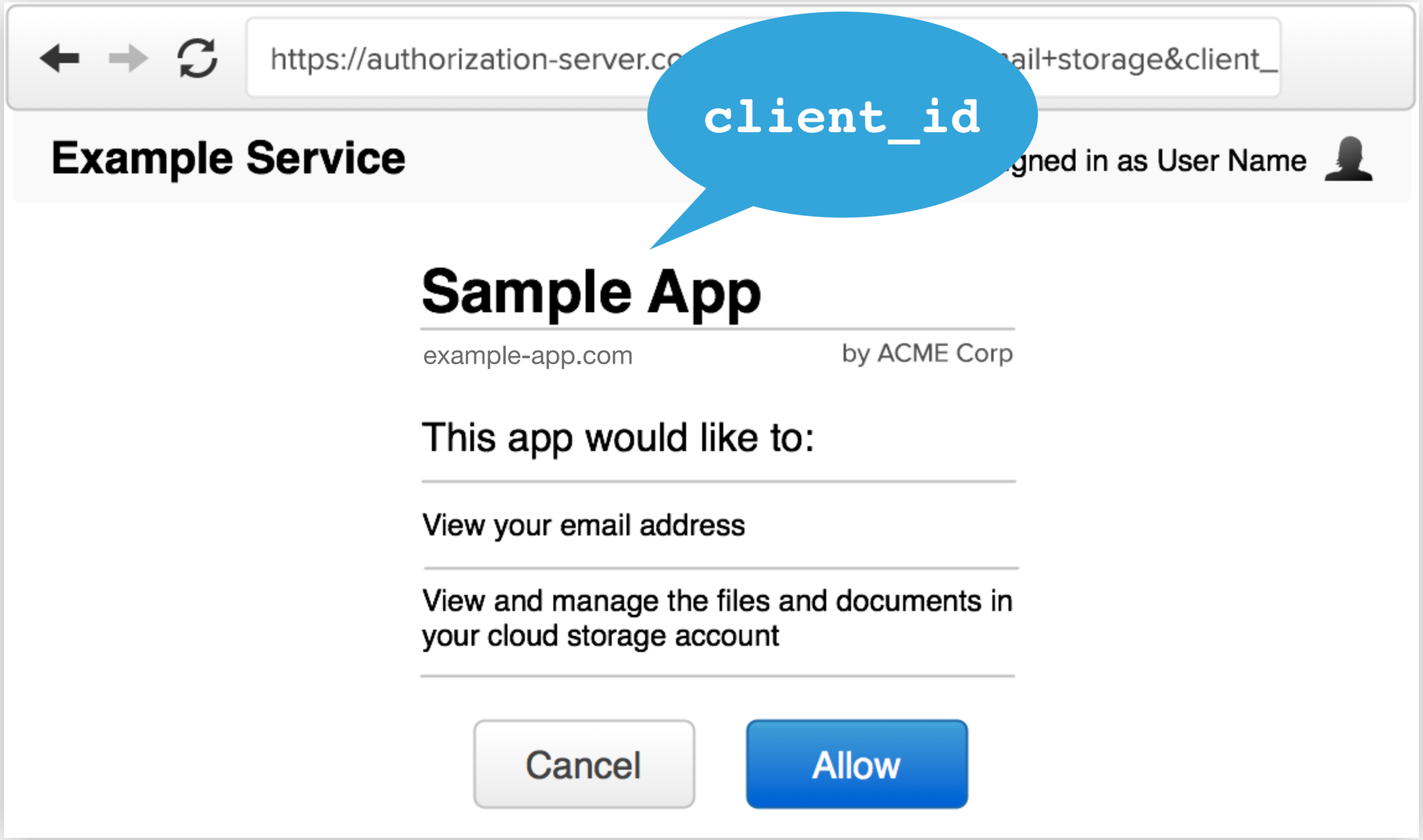

WordPr
Bluesky
mastodo
SMTP
IMAP


OAUTH
OAUTH

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

CLIENT IDENTIFICATION

Authorization Interface



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.


NEW

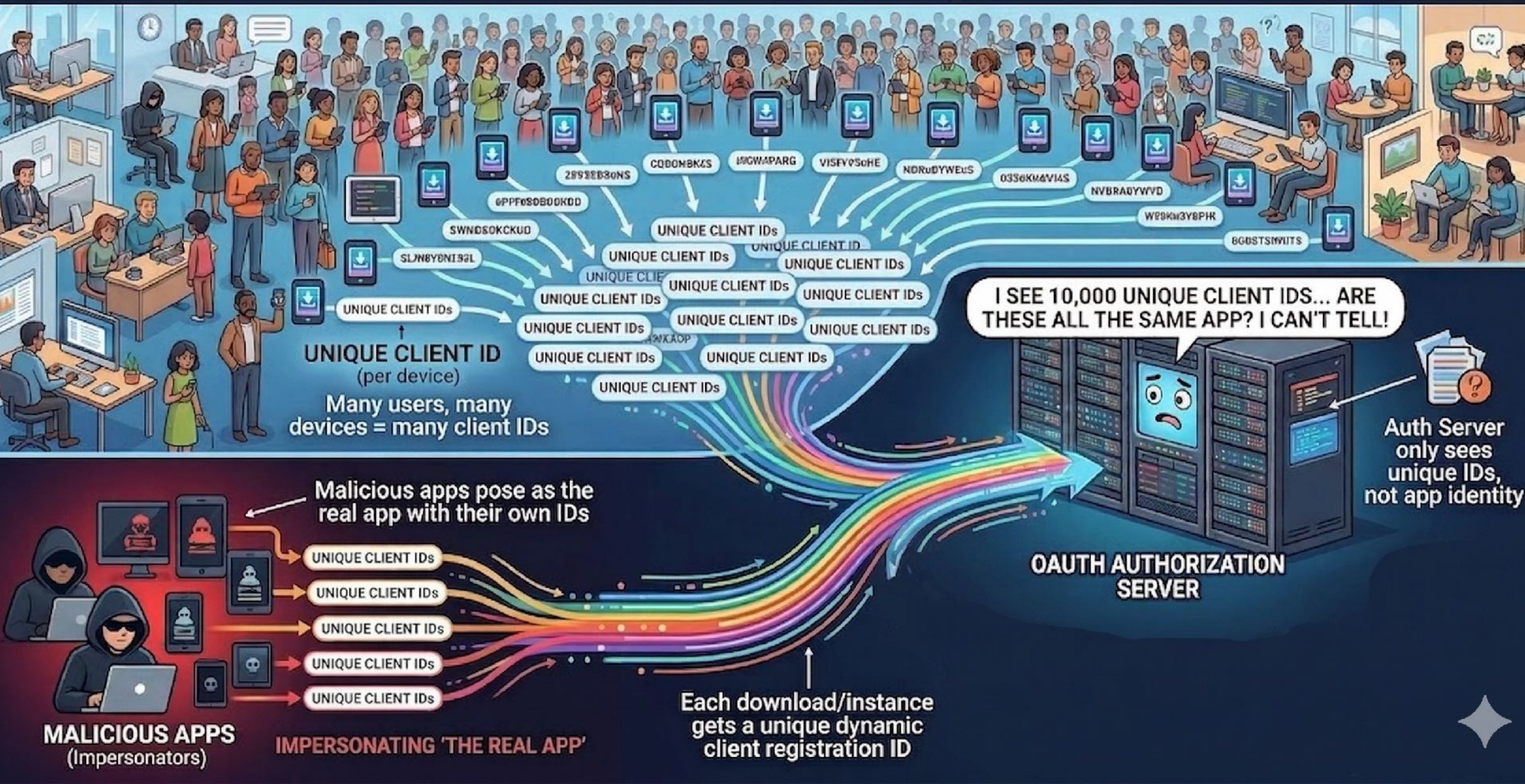
```
POST /oauth/register HTTP/1.1
Host: auth.example.com
Content-Type: application/json

{
  "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",
  ...
}
```

THE CHALLENGE: Dynamic Client IDs and App Impersonation in OAuth



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"
  ]
}
```

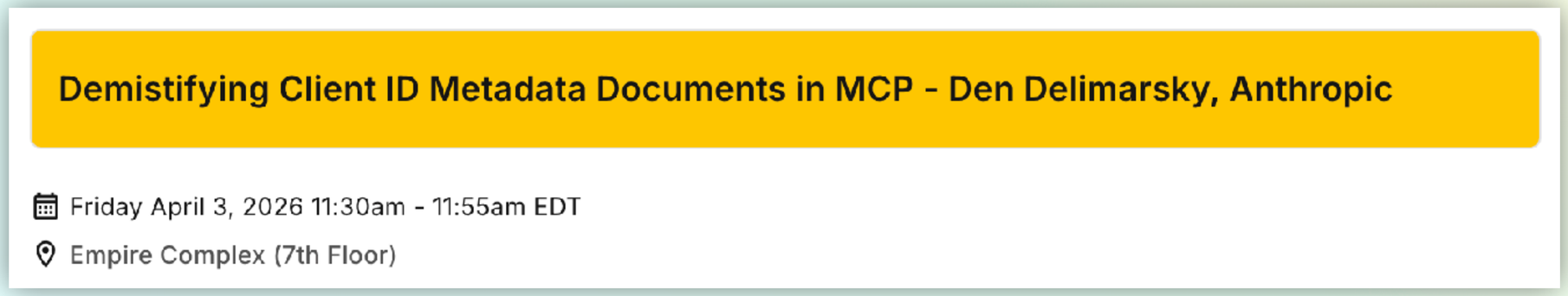
The URL is used in an Authorization request

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

CLIENT ID METADATA DOCUMENT (CIMD)

- Client hosts their metadata at a URL
- Metadata can contain `jwks_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!



Datatracker Groups Documents Meetings Other aaron Document search

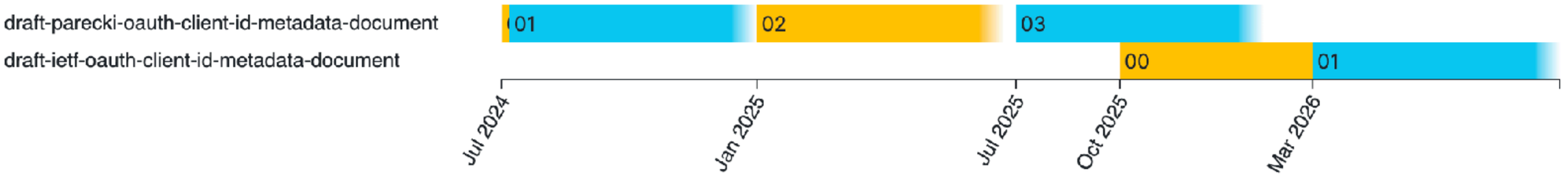
OAuth Client ID Metadata Document

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

Status | IESG evaluation record | IESG writeups | Email expansions | History

Versions:

00 01



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)

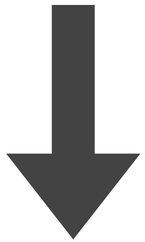
https://datatracker.ietf.org/doc/draft-ietf-oauth-client-id-metadata-document/

DYNAMIC DISCOVERY

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

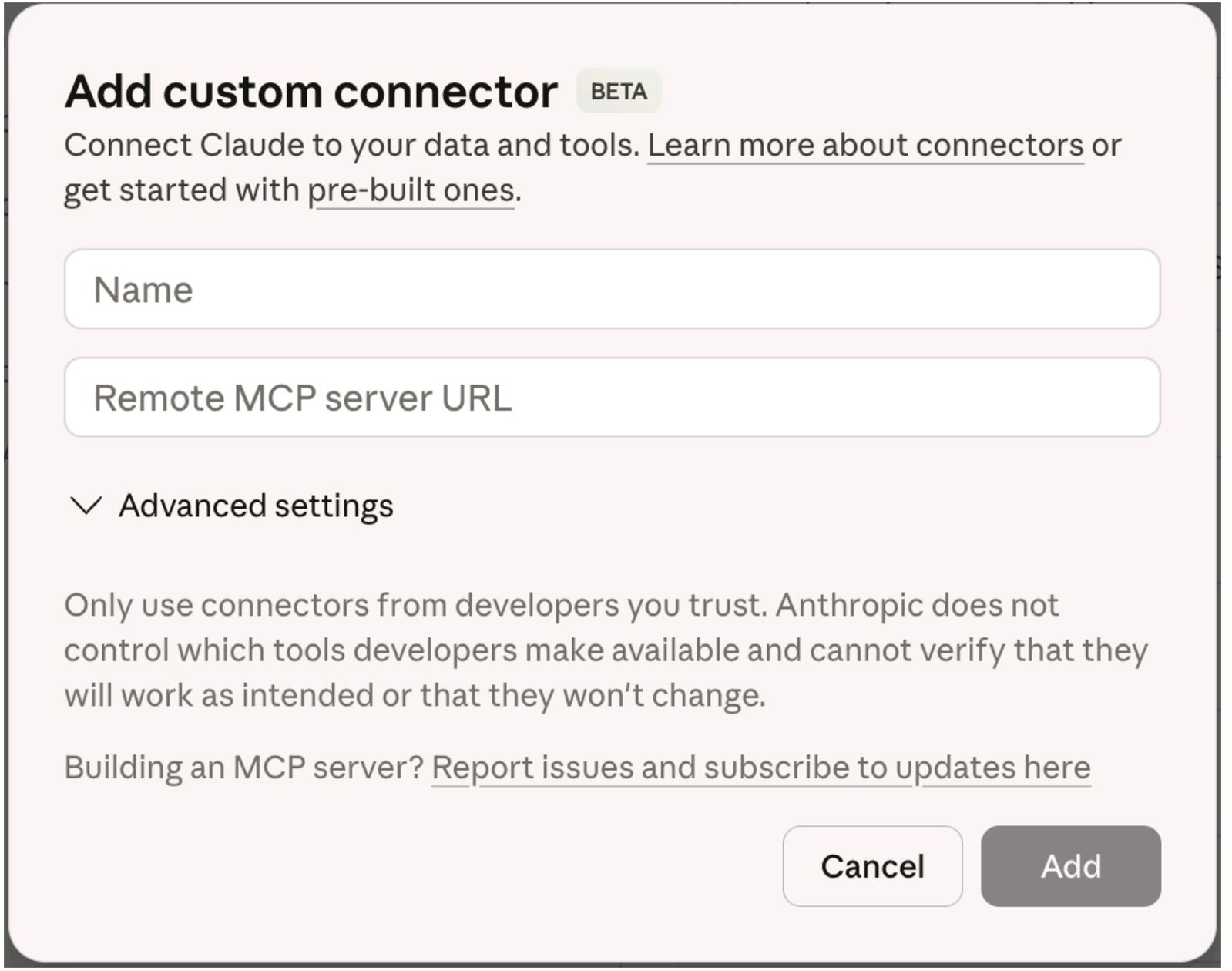
https://api.github.com/orgs

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

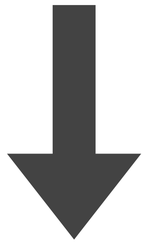


RFC8414
Authorization Server Metadata

https://example.com/oauth/authorize
https://example.com/oauth/token

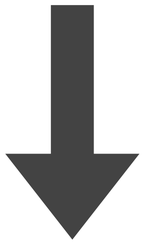

Add custom connector
BETA
Connect Claude to your data and tools. Learn more about connectors or get started with pre-built ones.
Name
Remote MCP server URL
Advanced settings
Only use connectors from developers you trust. Anthropic does not control which tools developers make available and cannot verify 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

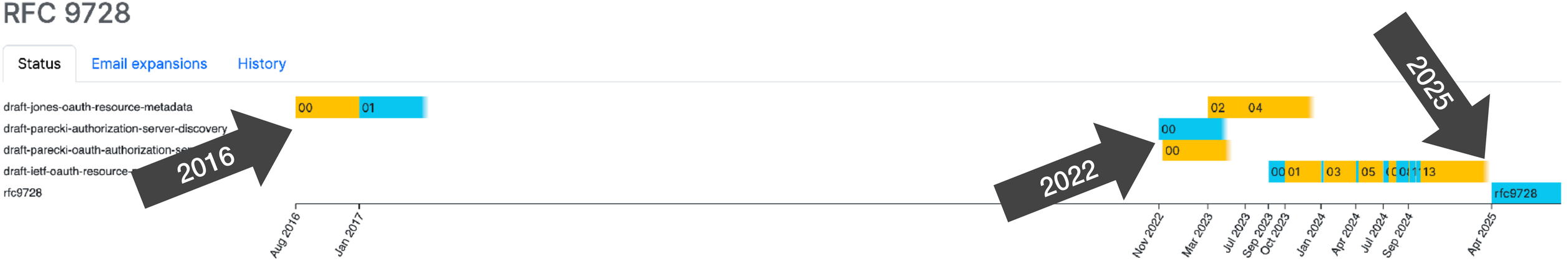
https://example.com/oauth/authorize
https://example.com/oauth/token

Datatracker Groups Documents Meetings Other aaron Report a bug Document search

OAuth 2.0 Protected Resource Metadata

RFC 9728

Status Email expansions History

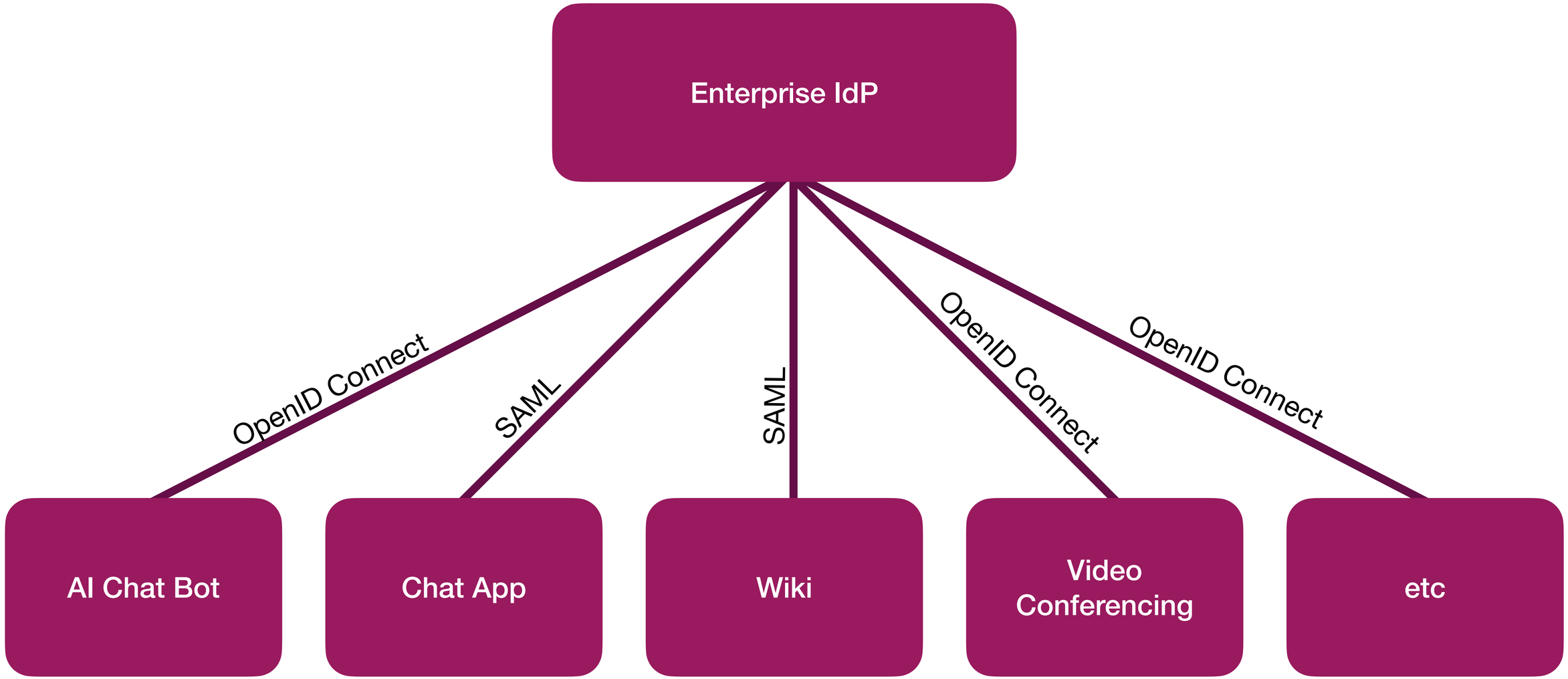


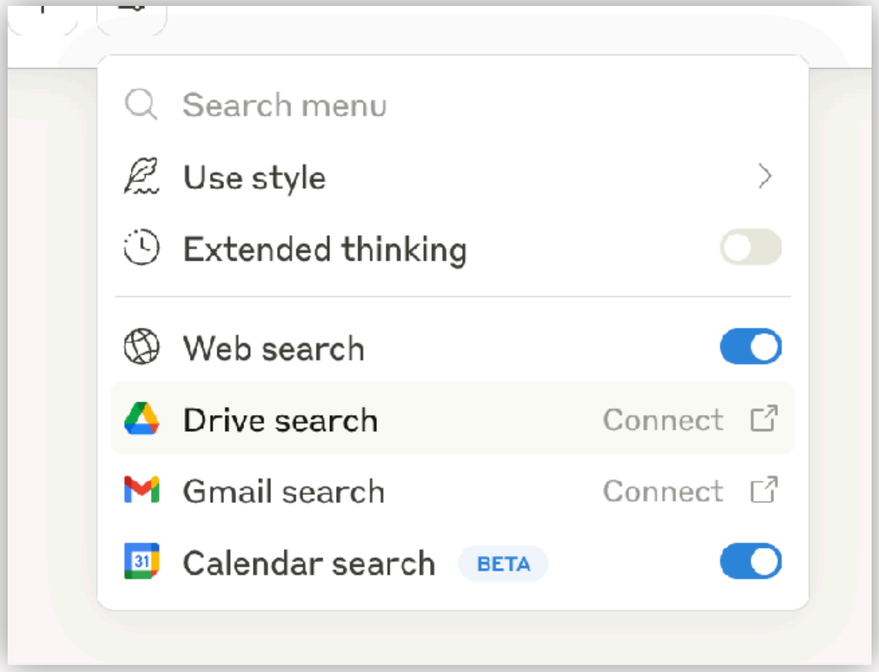
Document	**Type**	RFC - Proposed Standard (April 2025) Was draft-ietf-oauth-resource-metadata (oauth WG)
	Authors	Michael B. Jones ✉, Phil Hunt ✉, Aaron Parecki ✉
	Last updated	2025-04-23
	RFC stream	Internet Engineering Task Force (IETF)

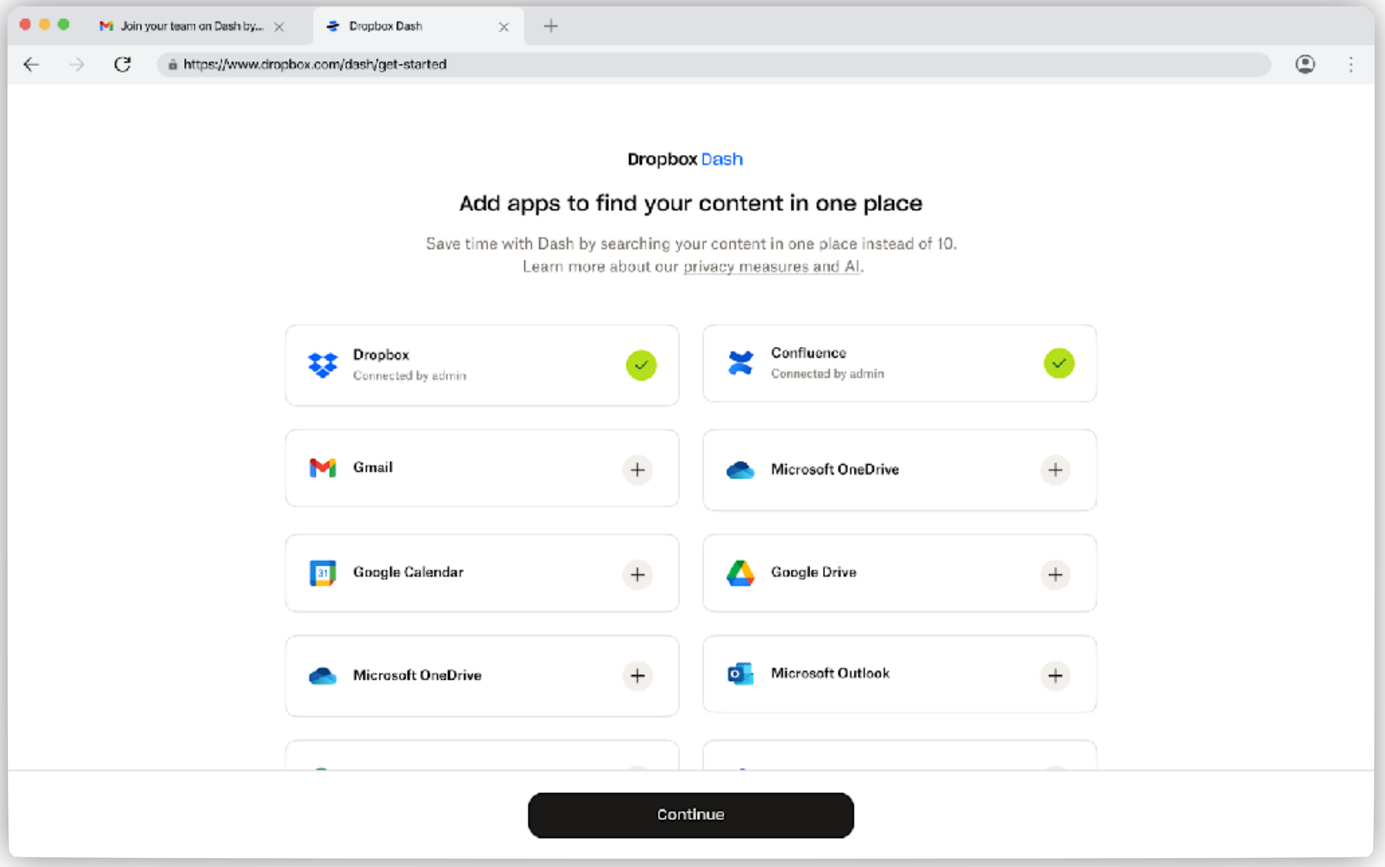
https://datatracker.ietf.org/doc/rfc9728/

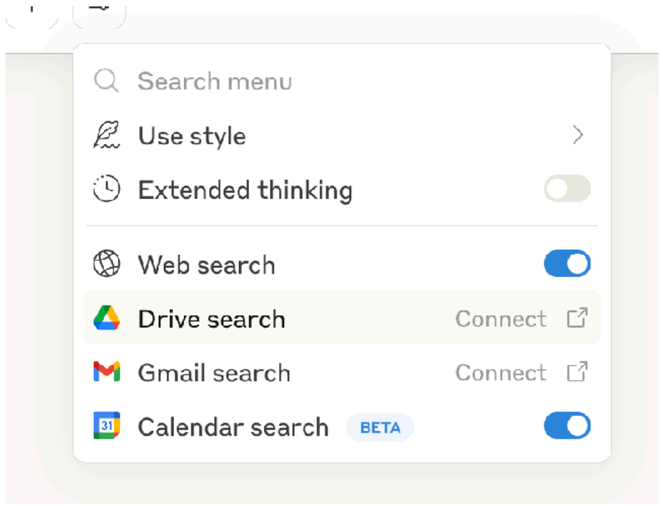
CLICK-THROUGH FATIGUE

Enterprise Single Sign-On

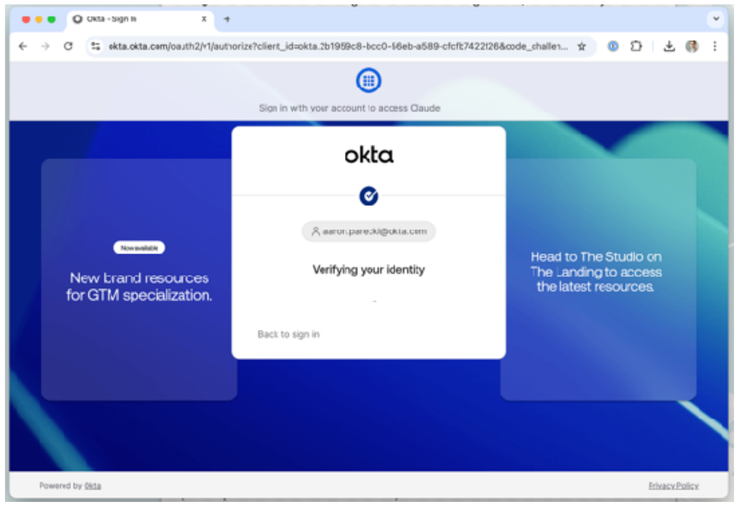



Search menu
Use style
Extended thinking
Web search
Drive search
Connect
Gmail search
Connect
Calendar search
BETA

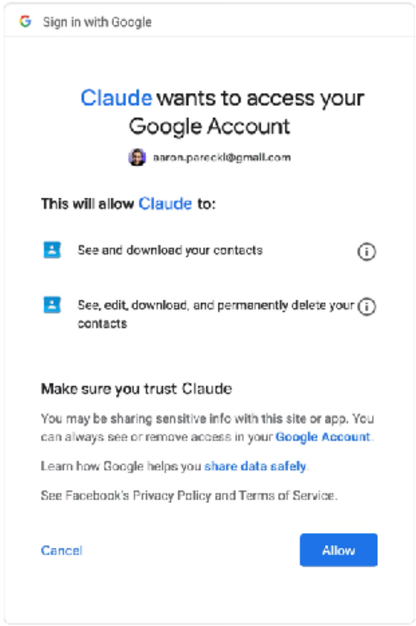

Join your team on Dash by...
Dropbox Dash
https://www.dropbox.com/dash/get-started
Dropbox Dash
Add apps to find your content in one place
Save time with Dash by searching your content in one place instead of 10.
Learn more about our privacy measures and AI.
Dropbox
Connected by admin
Confluence
Connected by admin
Gmail
Microsoft OneDrive
Google Calendar
Google Drive
Microsoft OneDrive
Microsoft Outlook
Continue



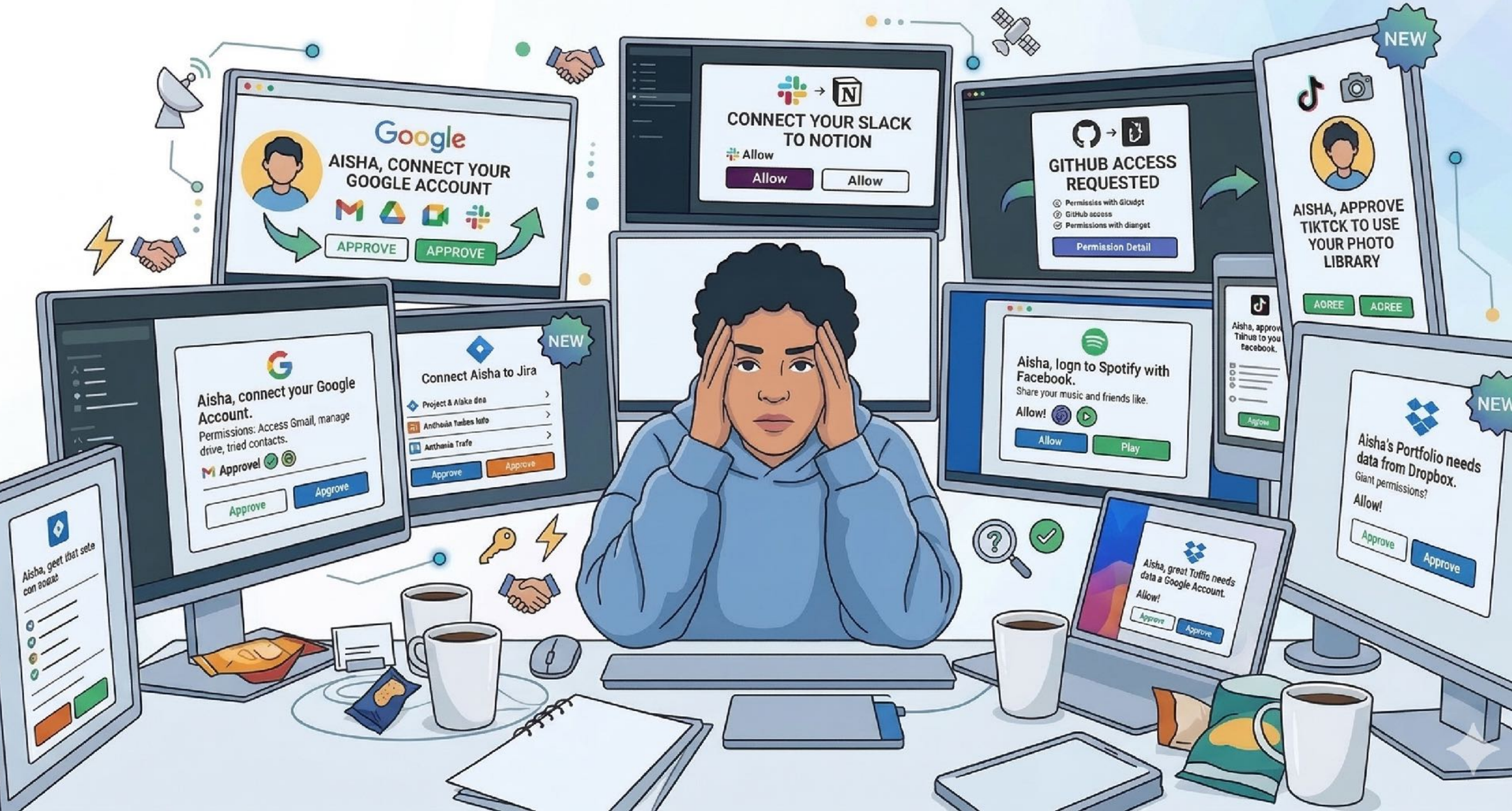
1. Connect Button



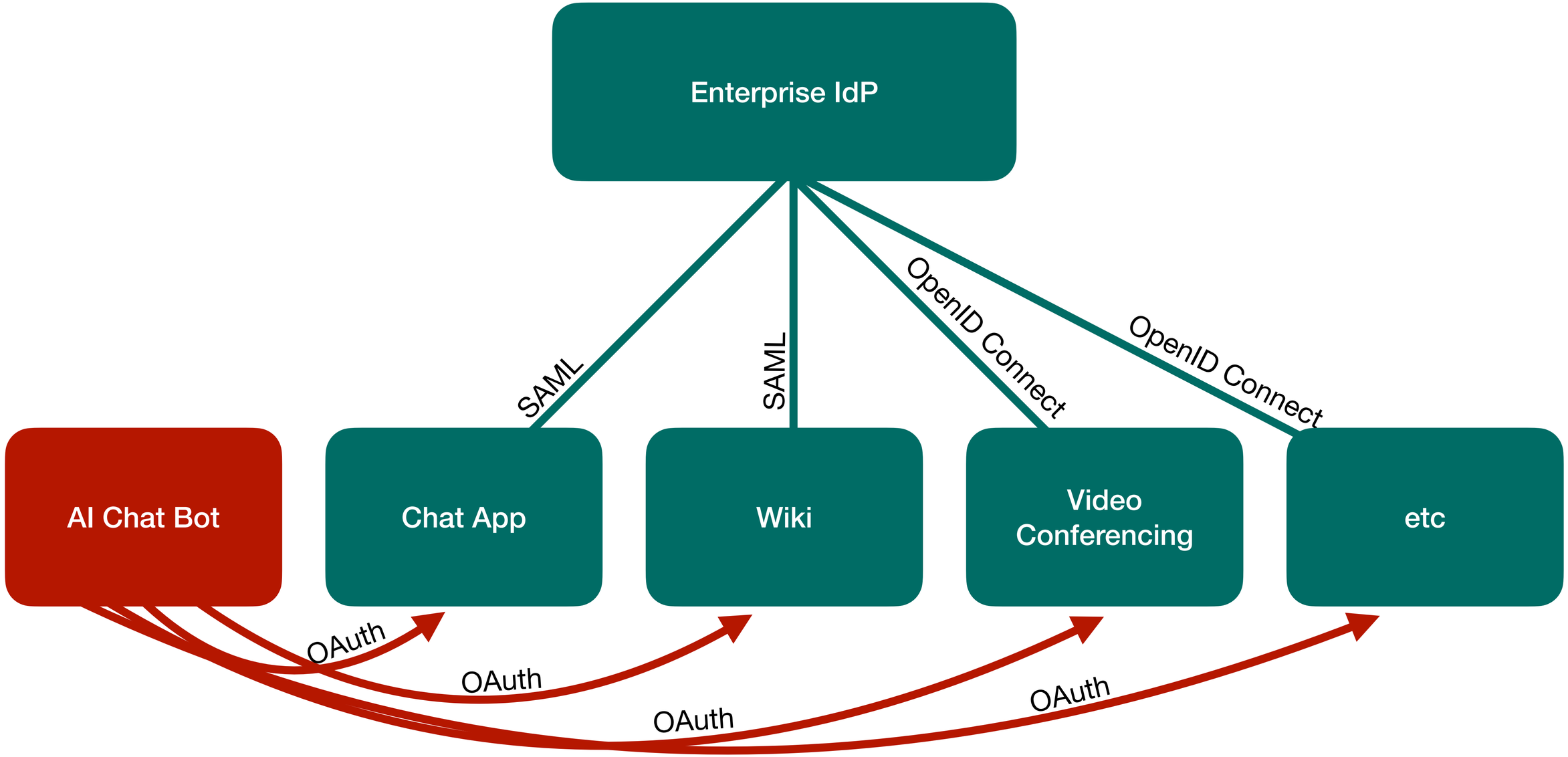
2. Login to Google through IdP

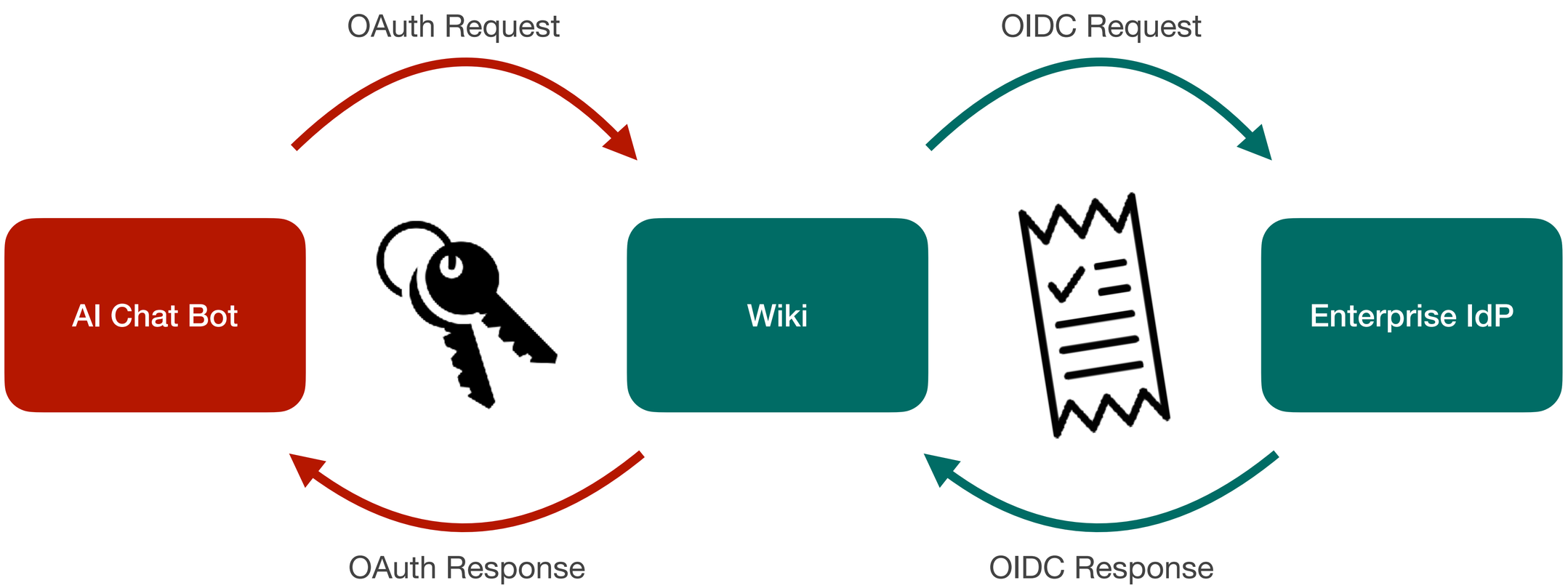


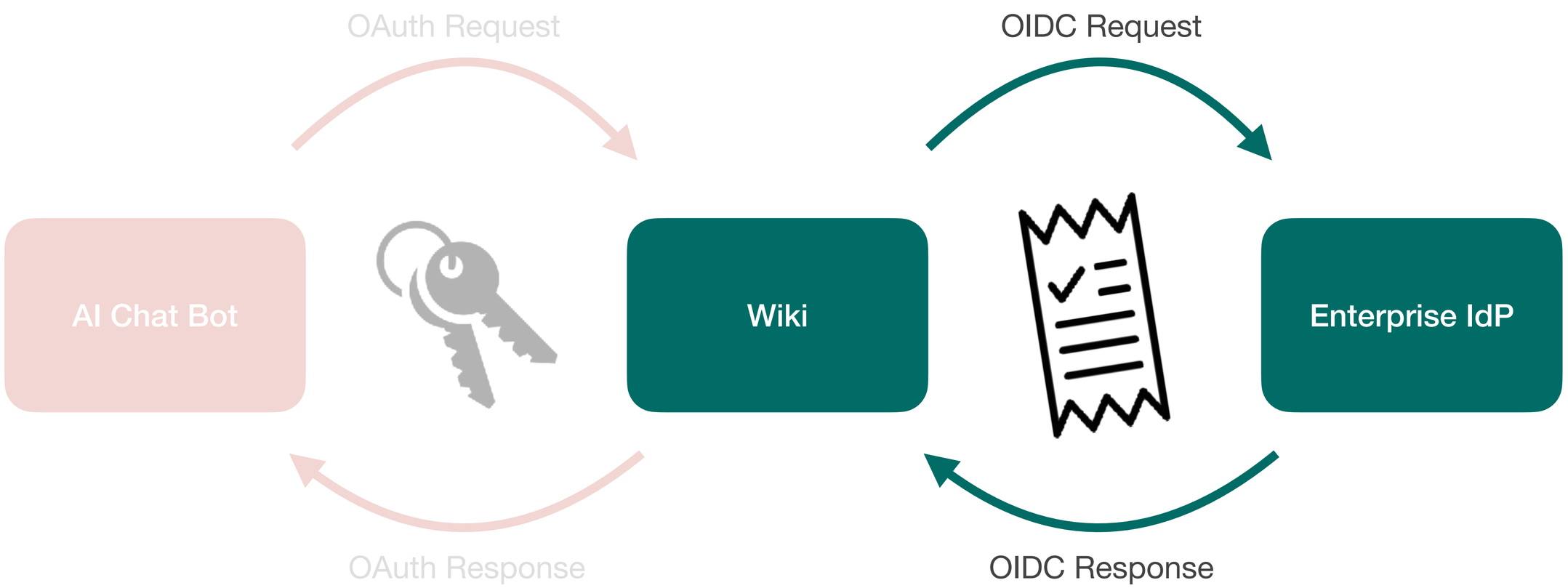
3. Google Consent Prompt


Google
AISHA, CONNECT YOUR GOOGLE ACCOUNT
APPROVE
APPROVE
CONNECT YOUR SLACK TO NOTION
Allow
Allow
Allow
GITHUB ACCESS REQUESTED
Permission Detail
NEW
AISHA, APPROVE TIKTCK TO USE YOUR PHOTO LIBRARY
AOREE
AOREE
Aisha, connect your Google Account.
Permissions: Access Gmail, manage drive, tried contacts.
Approve
Apgrove
Connect Aisha to Jira
Approve
Approve
NEW
Aisha, logn to Spotify with Facebook.
Share your music and friends like.
Allow!
Allow
Play
Aisha's Portfolio needs data from Dropbox.
Giant permissions?
Allow!
Approve
Approve
NEW
Aisha, great Toffie needs data a Google Account.
Allow!
Approve
Approve

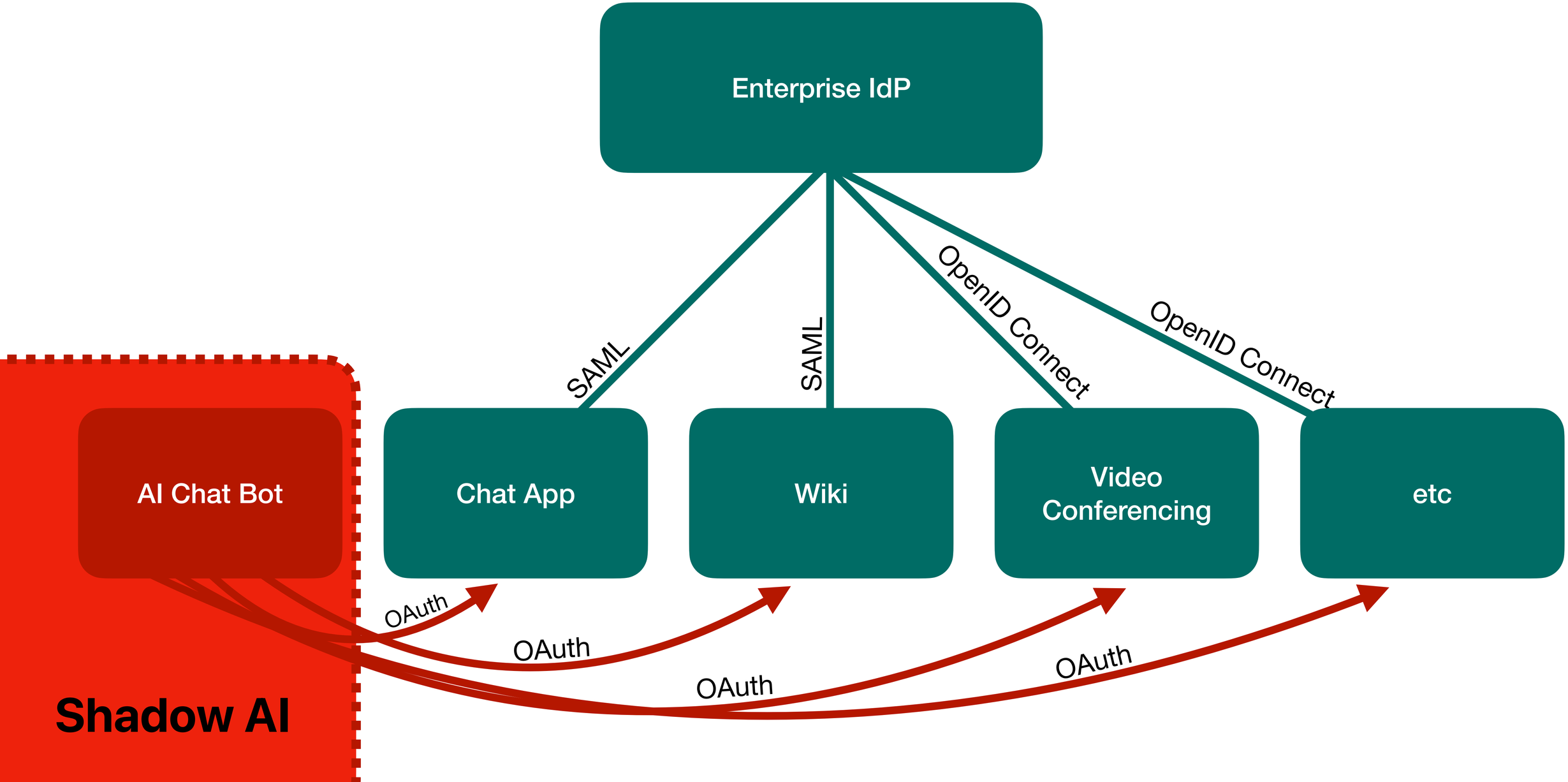
Enterprise API Access Today




OAuth Request
OIDC Request
AI Chat Bot
Wiki
Enterprise IdP
OAuth Response
OIDC Response


OAuth Request
OIDC Request
AI Chat Bot
Wiki
Enterprise IdP
OAuth Response
OIDC Response

Enterprise API Access Today



No control or visibility by the enterprise IT admin

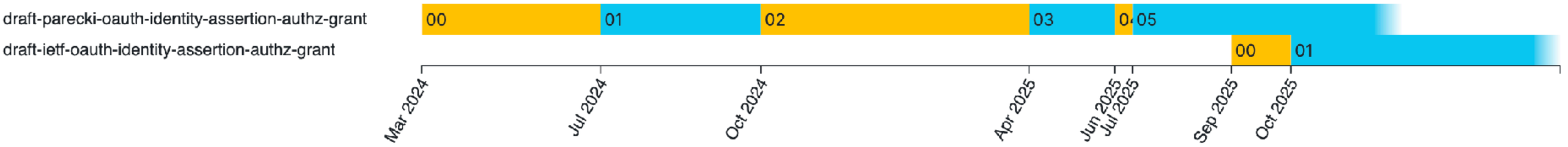
Terrible UX for Employees

Identity Assertion JWT Authorization Grant

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

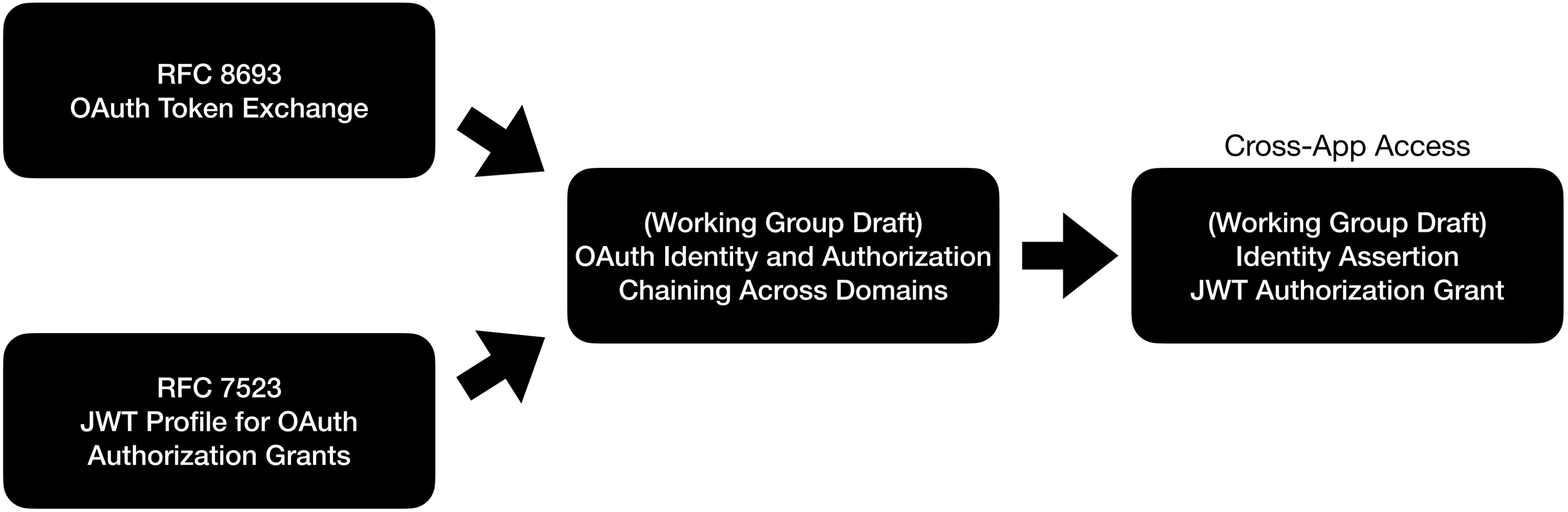
Versions:

00 01

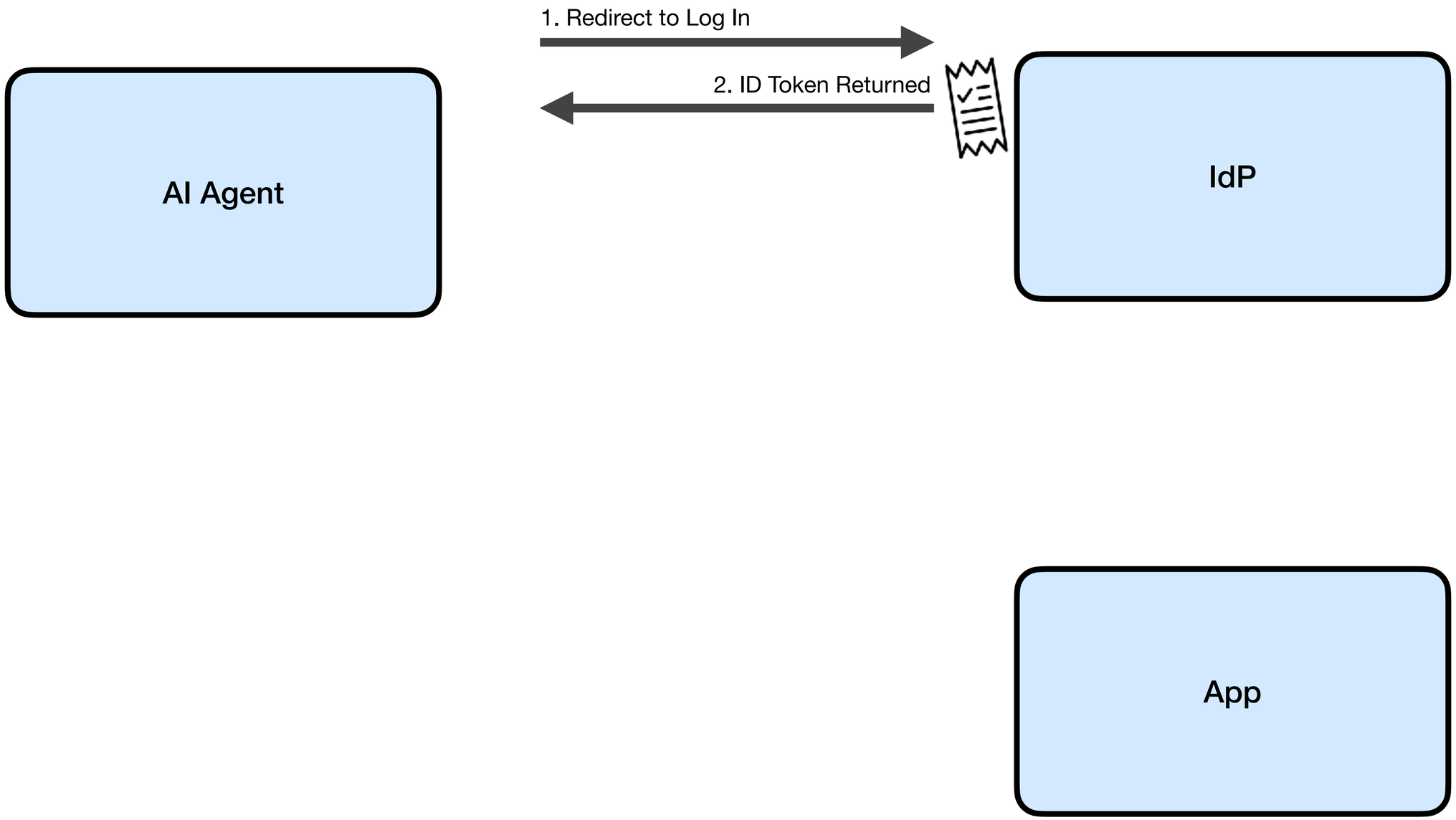


Document	**Type**	Active Internet-Draft (oauth WG)
	Authors	Aaron Parecki ✉, Karl McGuinness ✉, Brian Campbell ✉
	Last updated	2025-10-19
	Replaces	draft-parecki-oauth-identity-assertion-authz-grant
	RFC stream	Internet Engineering Task Force (IETF)

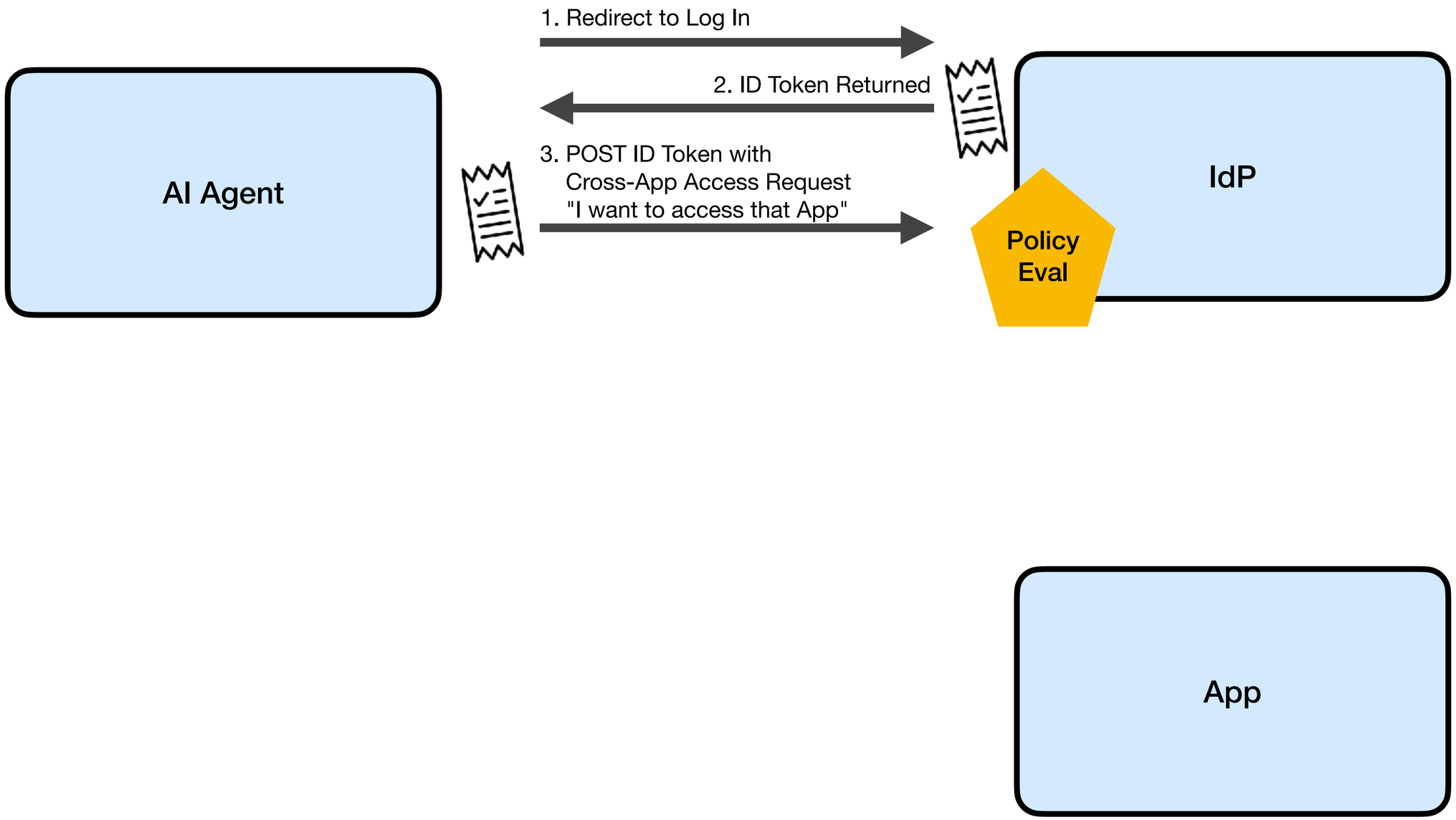
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/



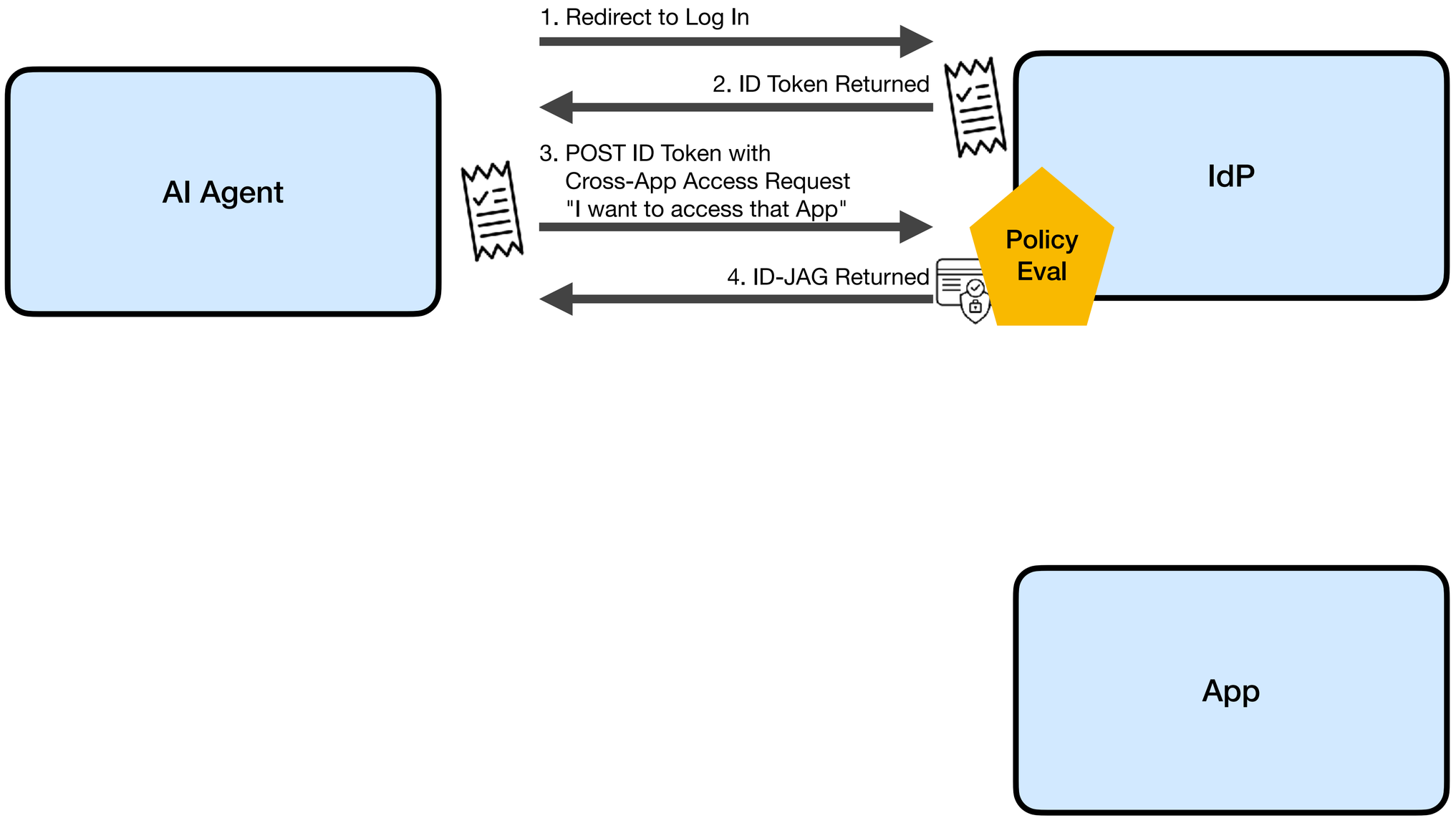
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/



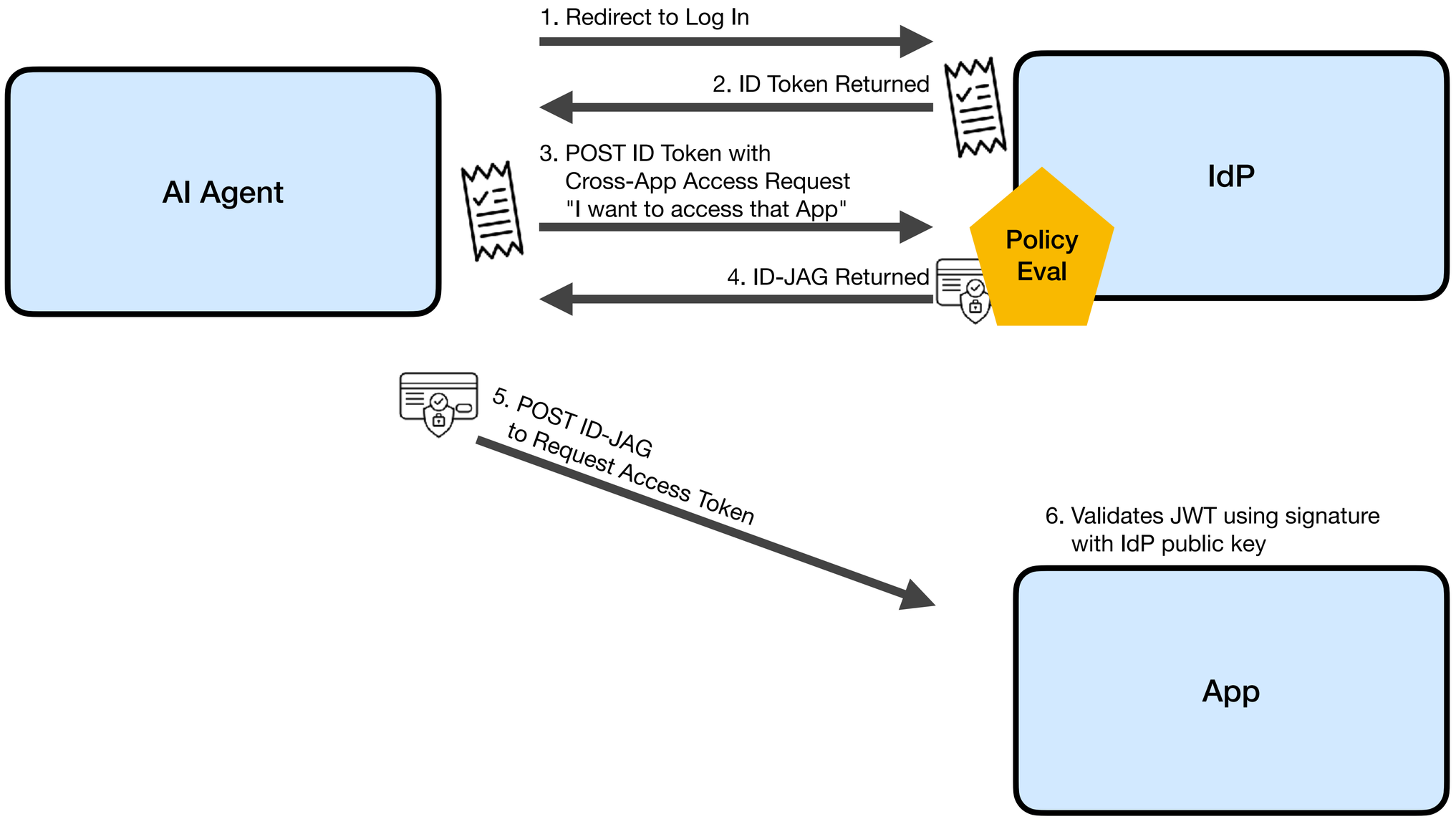
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/



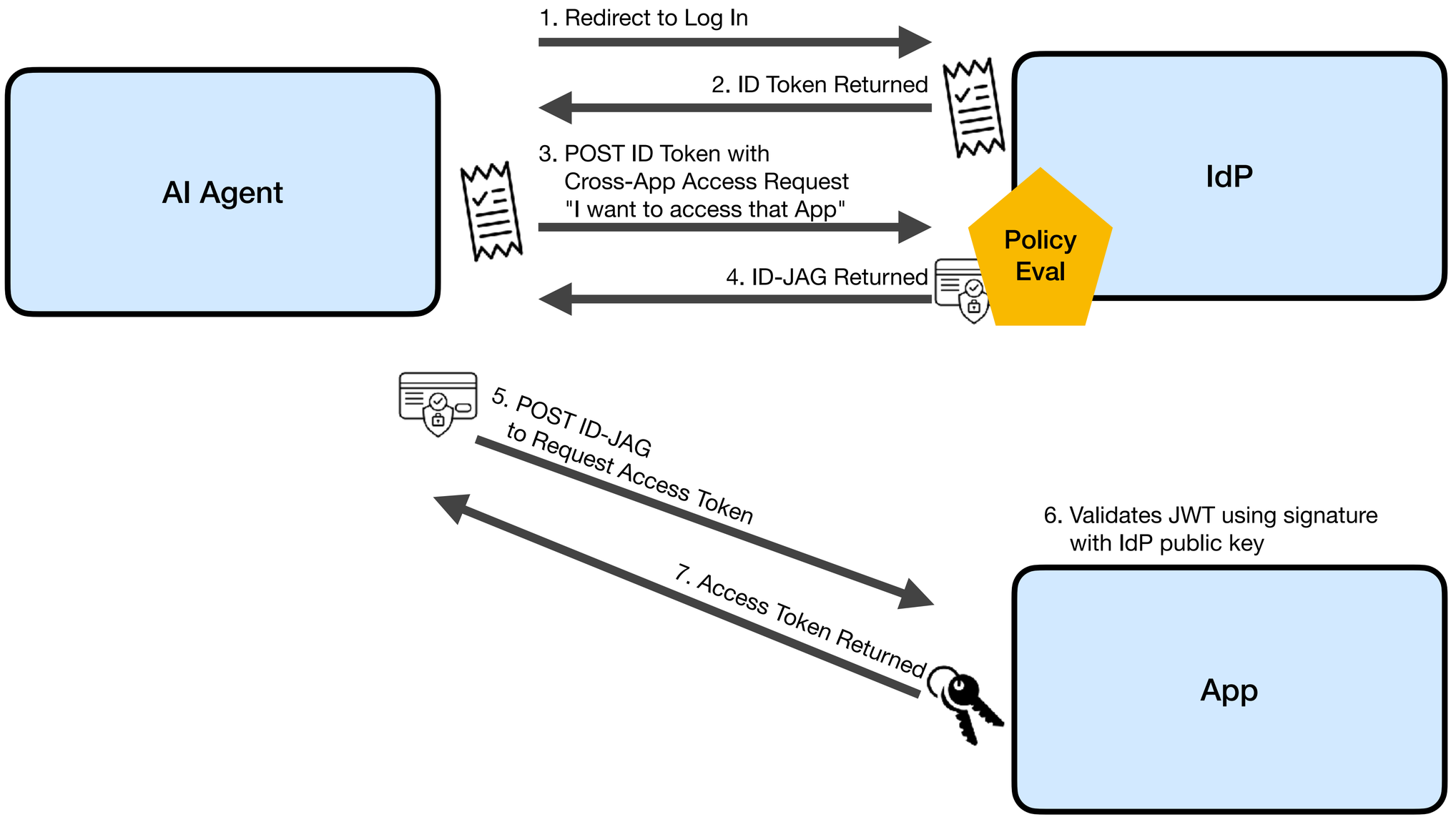
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/



https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/

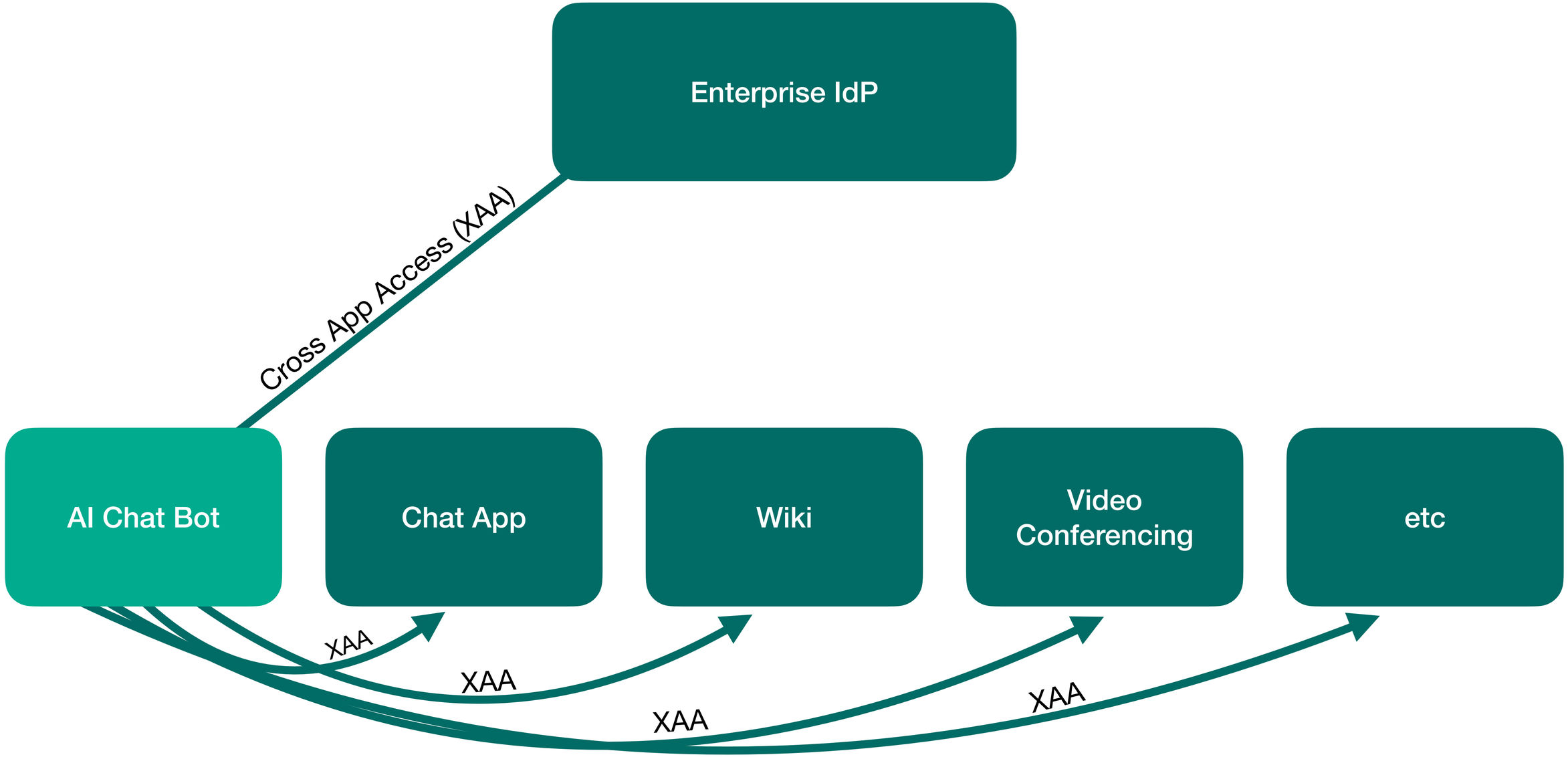


https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/



https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/

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

oauth.wtf

oauth.net