Governing the "Shadow AI" Mesh with Open Standards

Aaron Parecki
Director of Identity Standards
Okta

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.

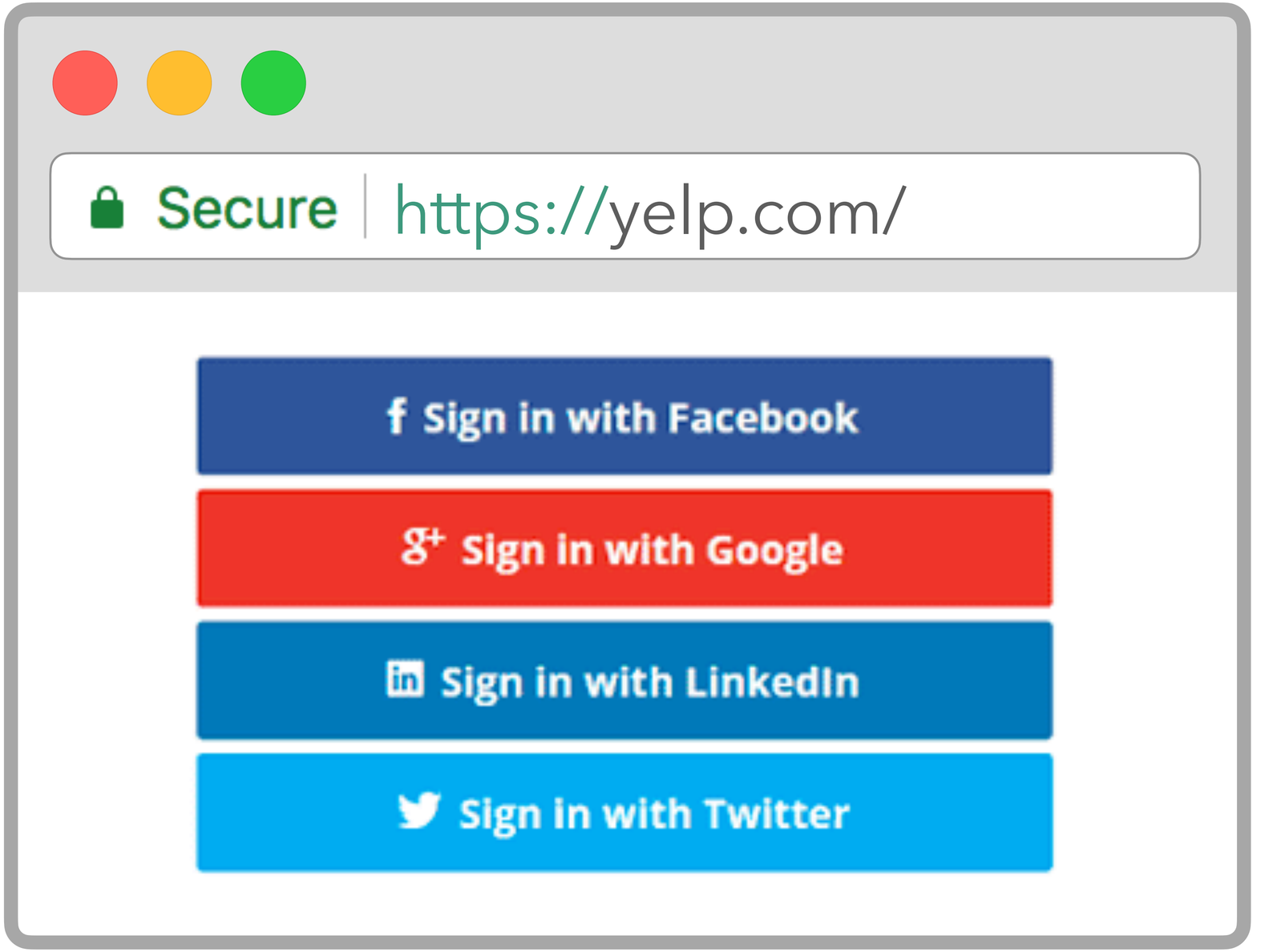
This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in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

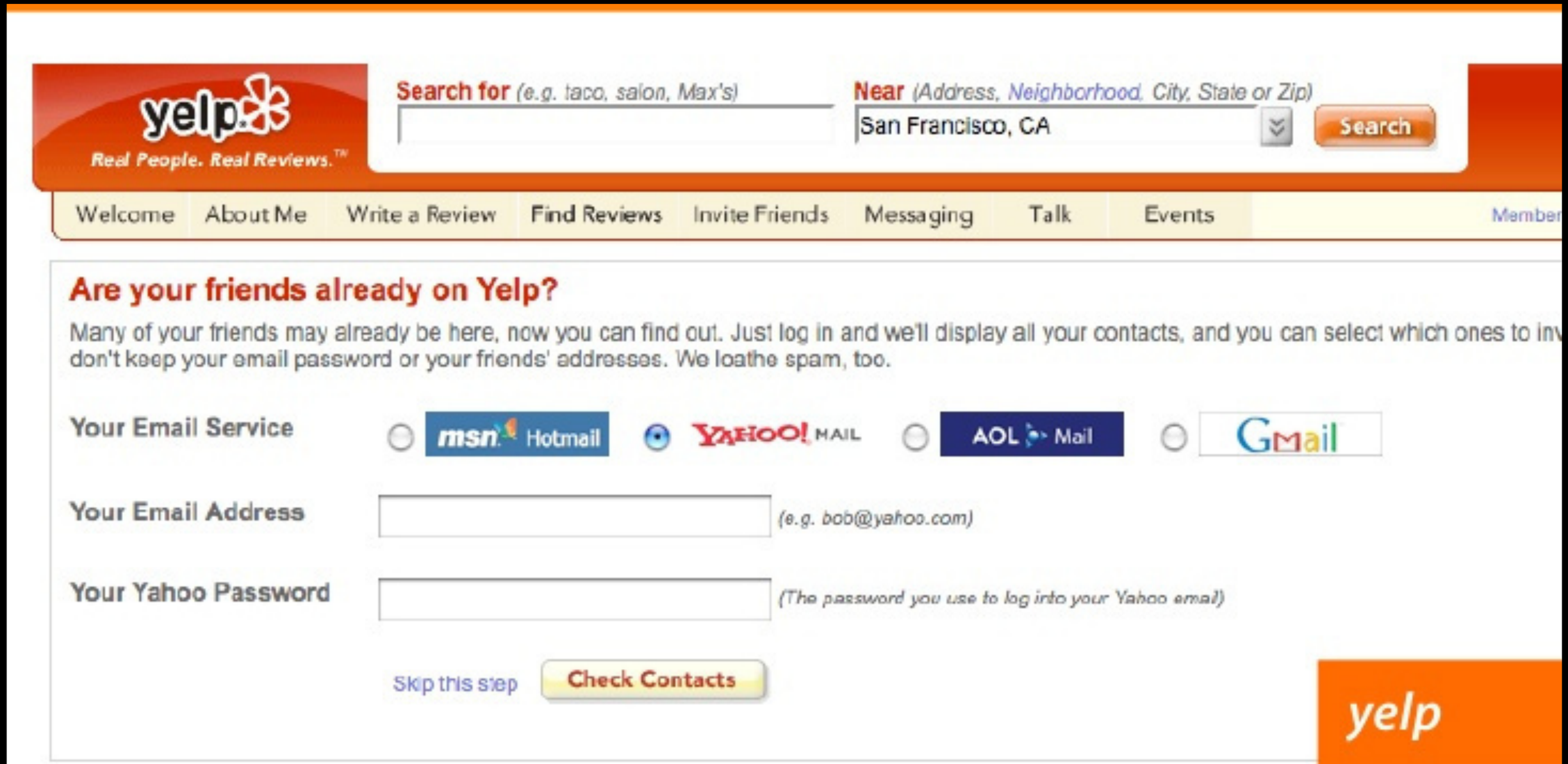
Copyright Notice

Table of Contents

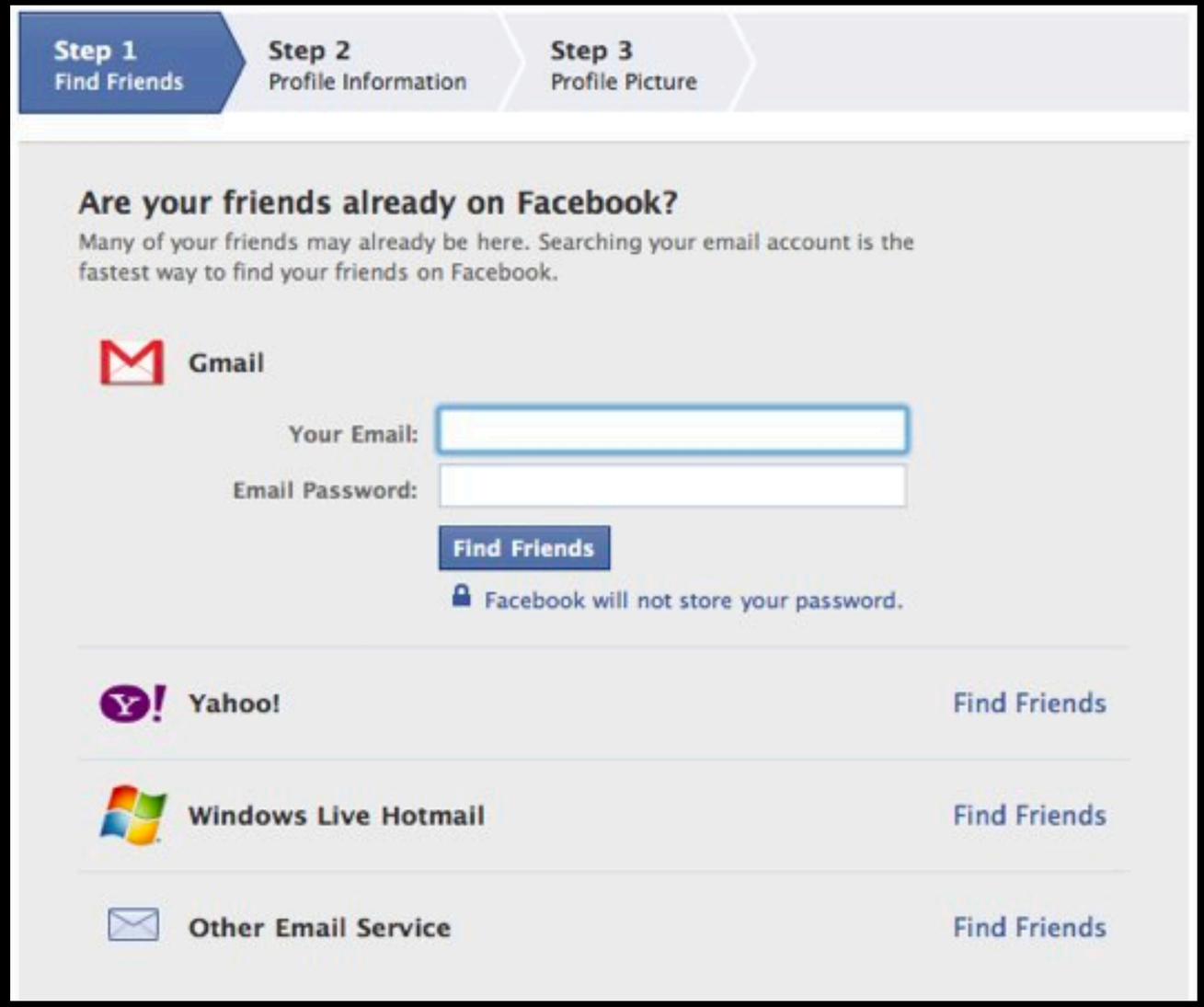
Specs are not good tutorials!


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

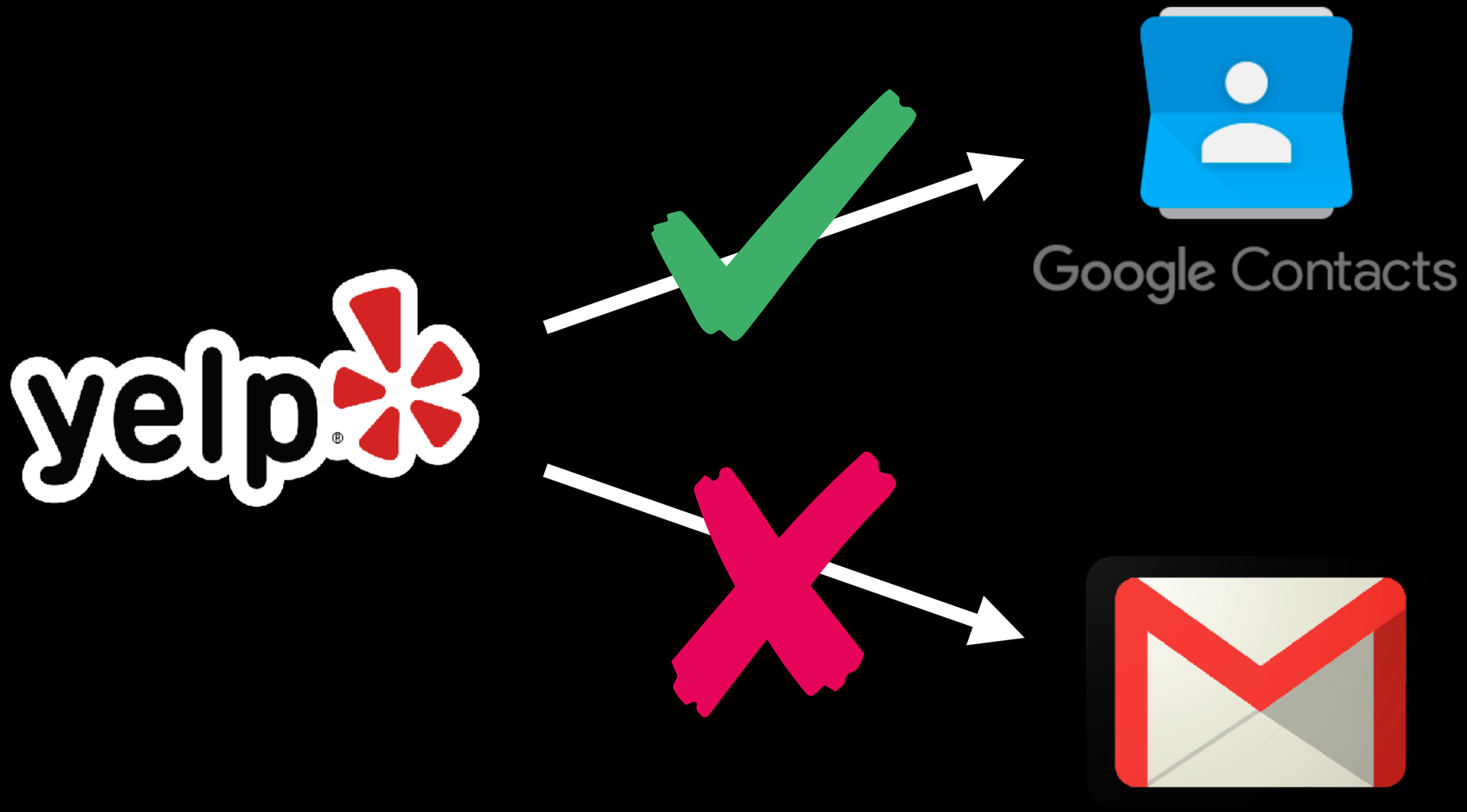
The Password Anti-Pattern



The Password Anti-Pattern



facebook.com ~2010


yelp
Google Contacts

how can I let an app

access my data

without giving it my password?

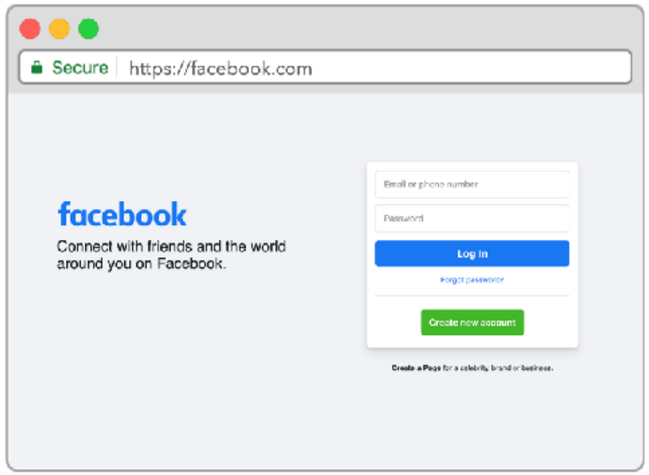
Authorization Server

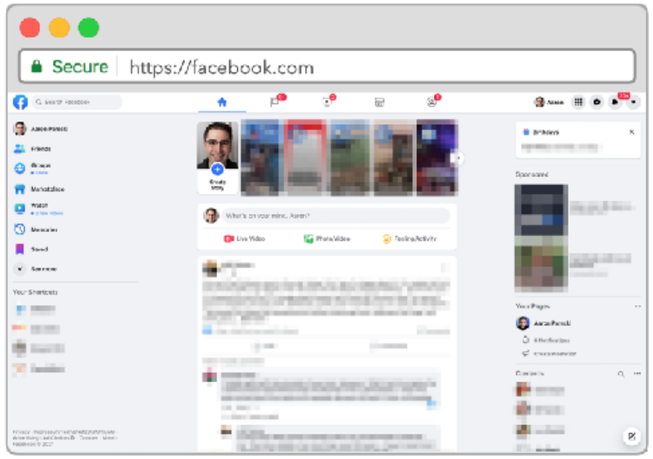
Access Token

Resource (API)

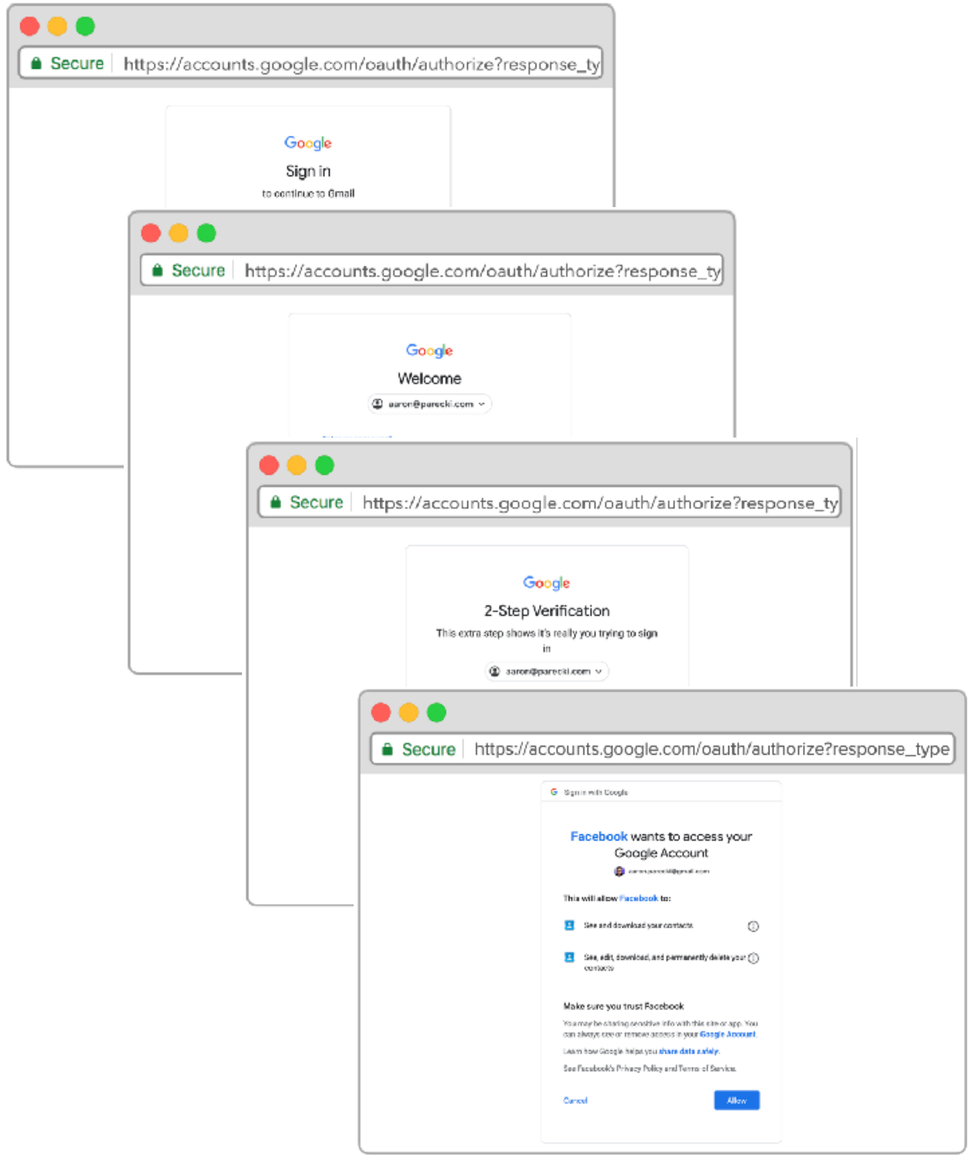
https://unsplash.com/photos/GJY1eAw6tn8

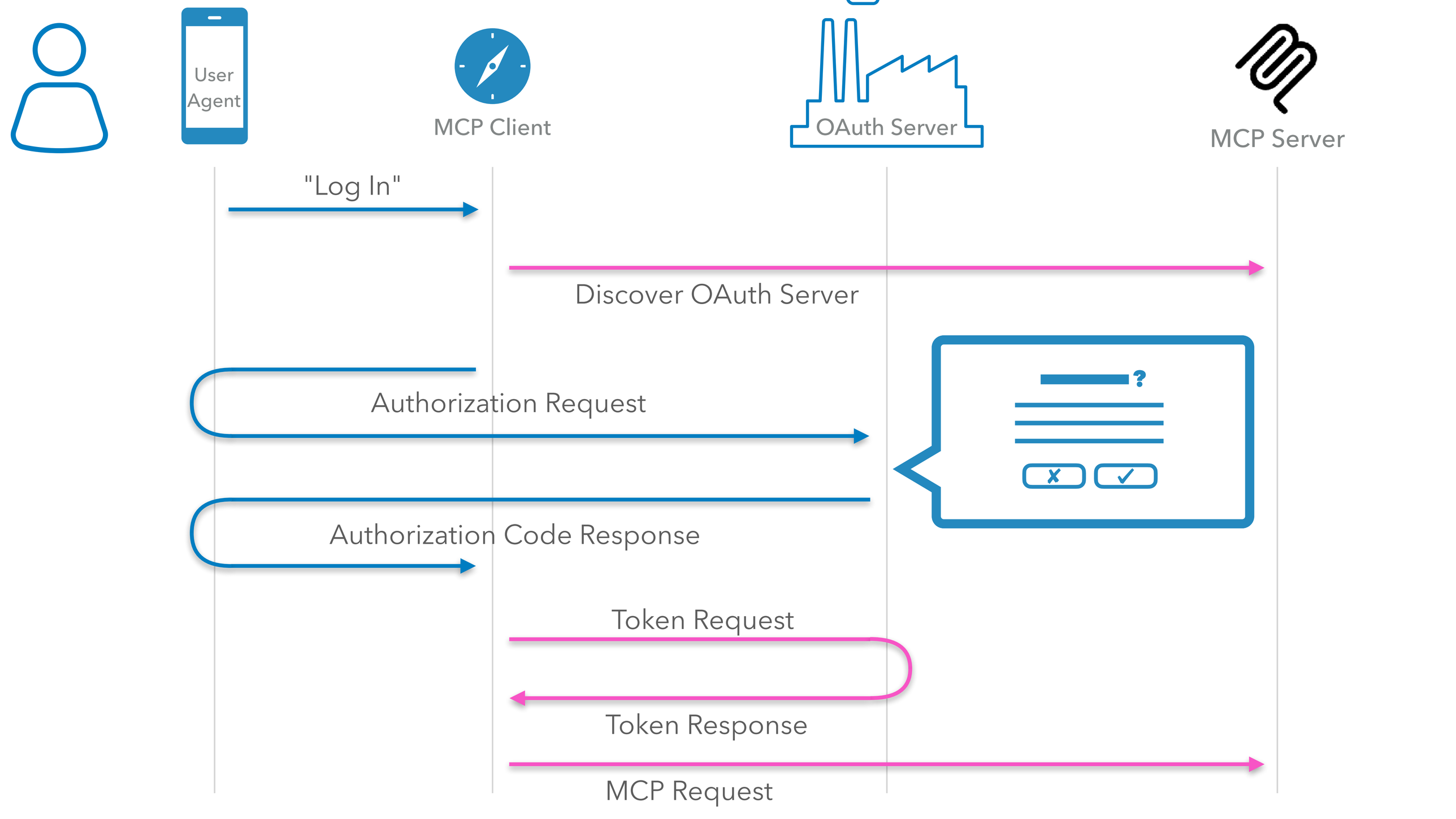
Application





OAuth Server




User Agent
MCP Client
OAuth Server
MCP Server
"Log In"
Discover OAuth Server
Authorization Request
Authorization Code Response
Token Request
Token Response
MCP Request

Gives the application a way to make API requests

Accessing APIs

Tells the application about the user authenticating

Identification

Gives the application a way to make API requests

Access Token

Tells the application about the user authenticating

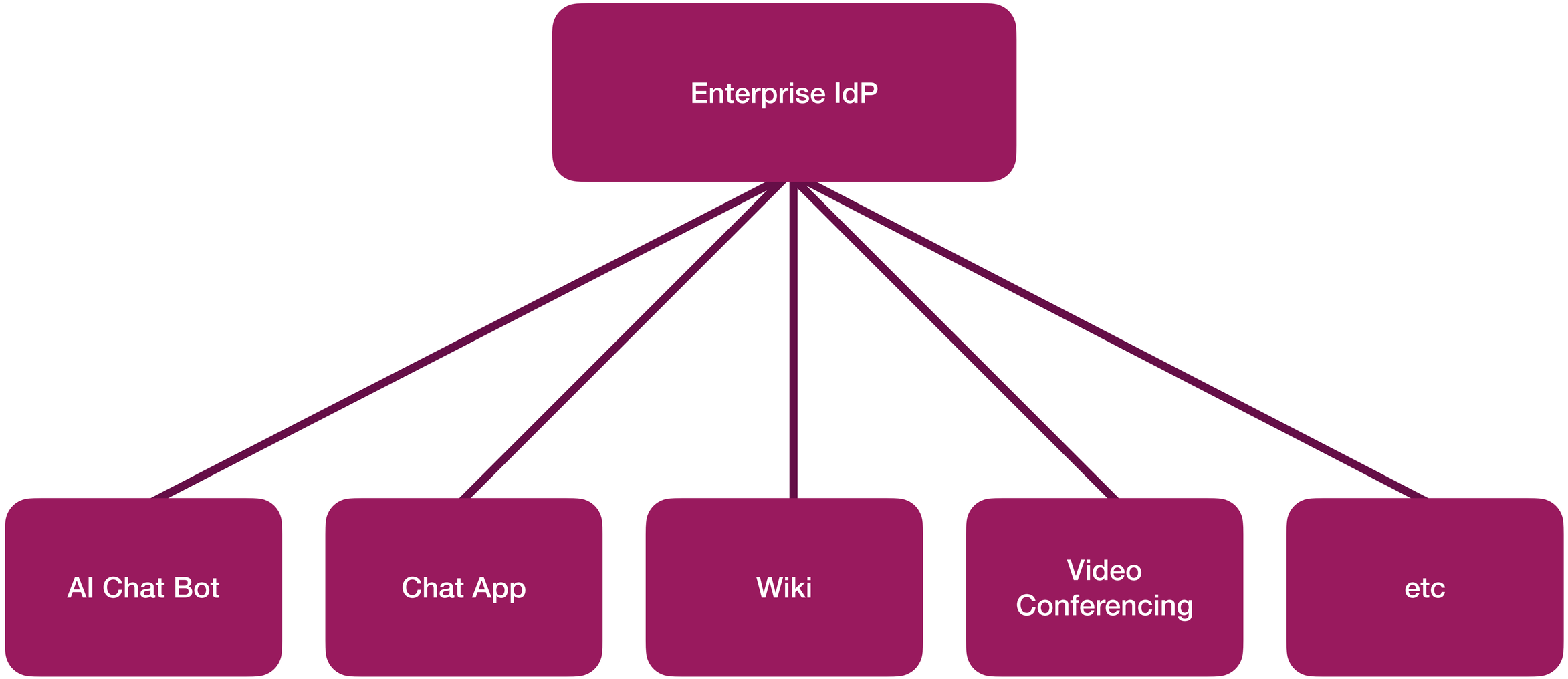
ID Token

Access Token

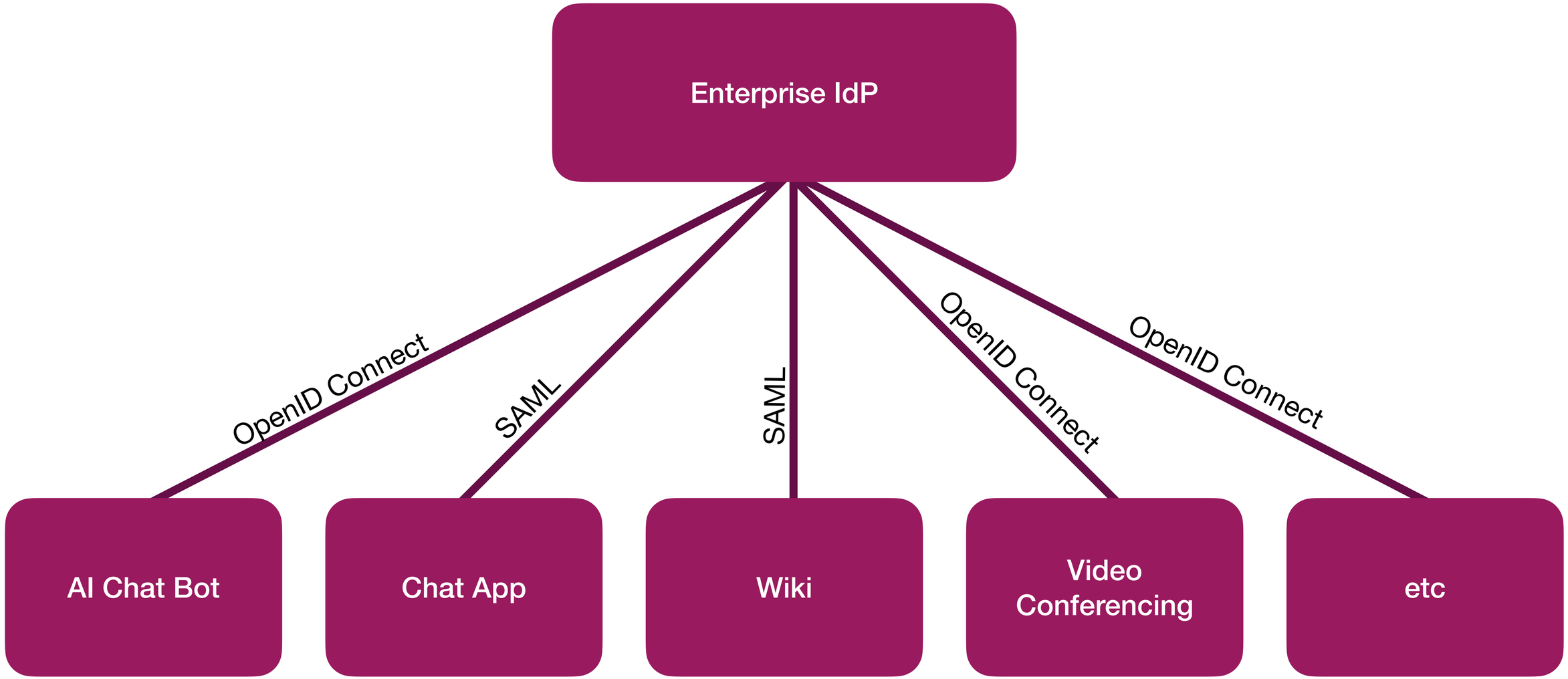
ID Token


Enterprise IdP

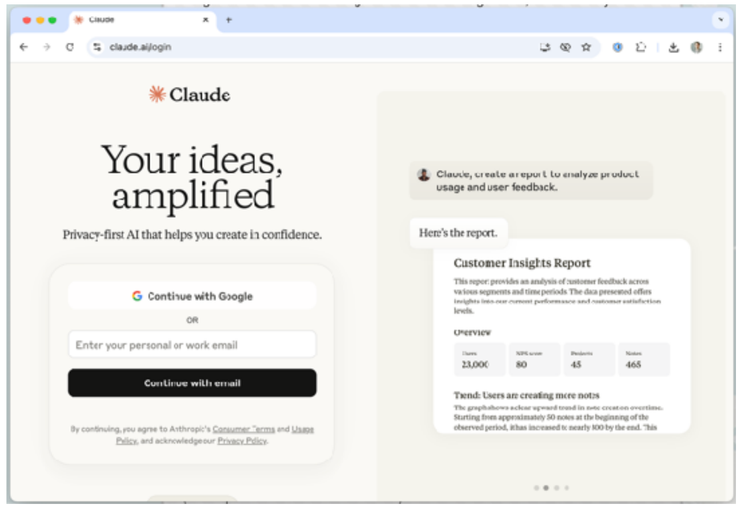
Enterprise Single Sign-On



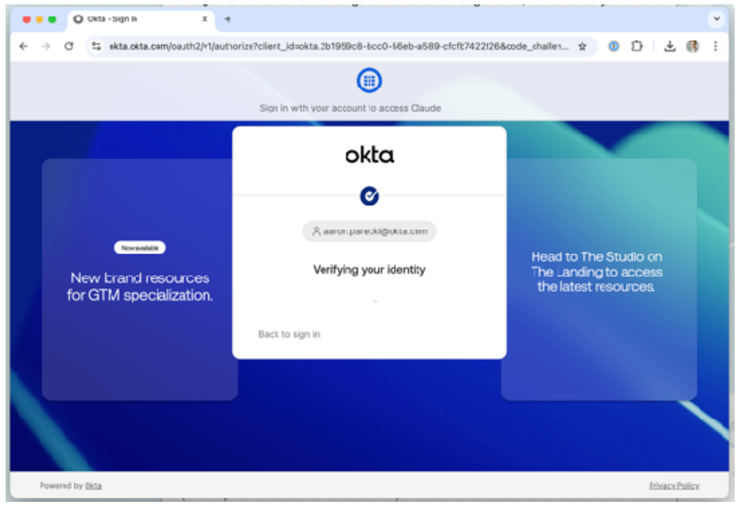
Enterprise Single Sign-On



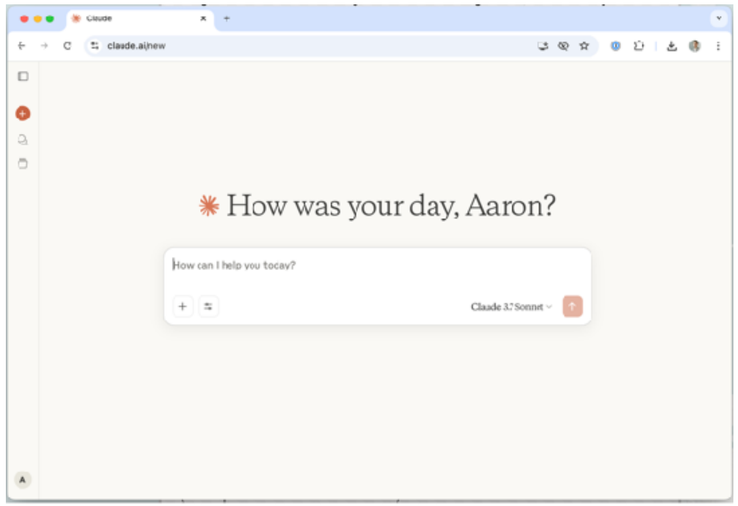
Logging in to an app with SSO



1. Login Screen

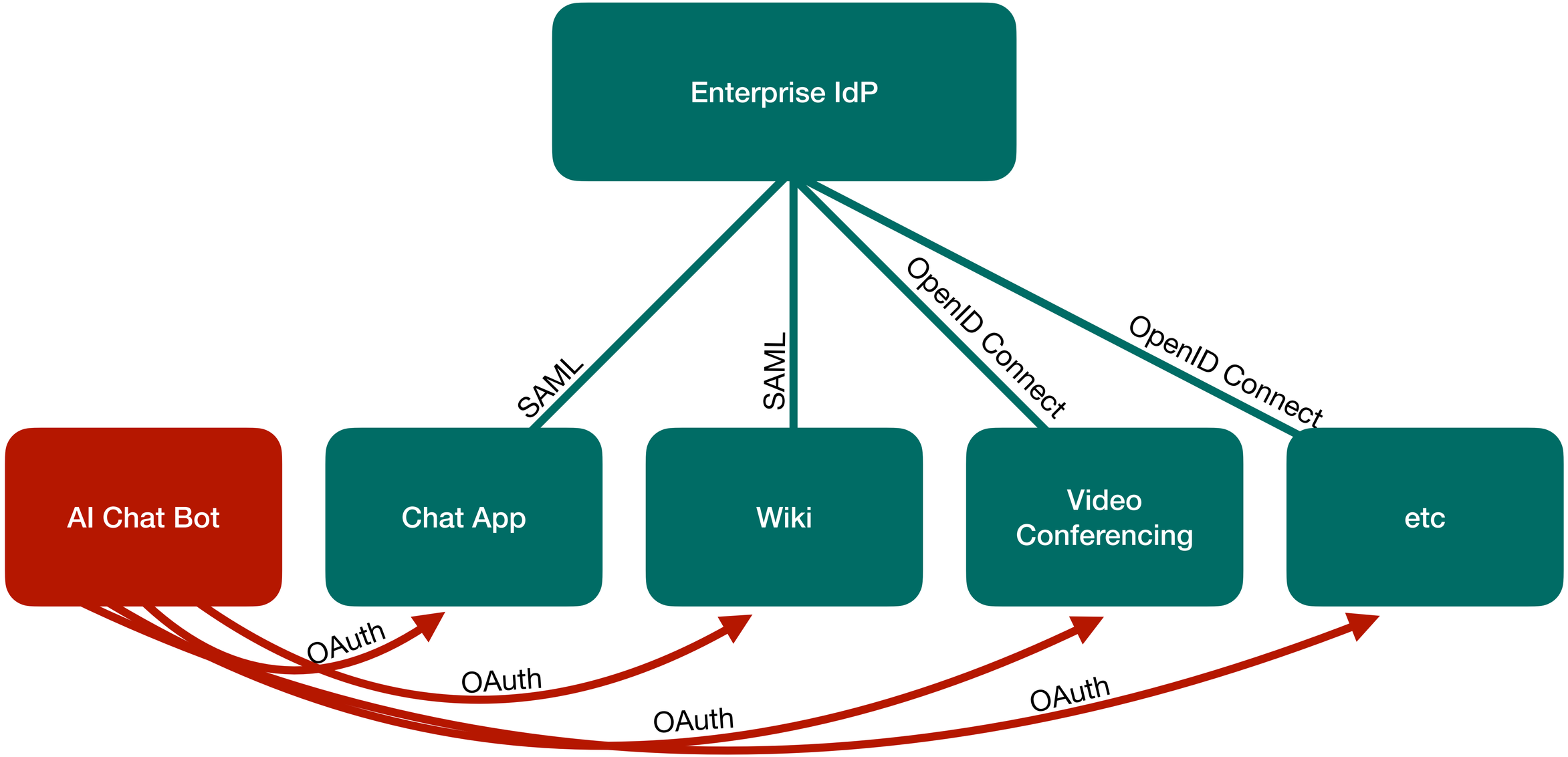


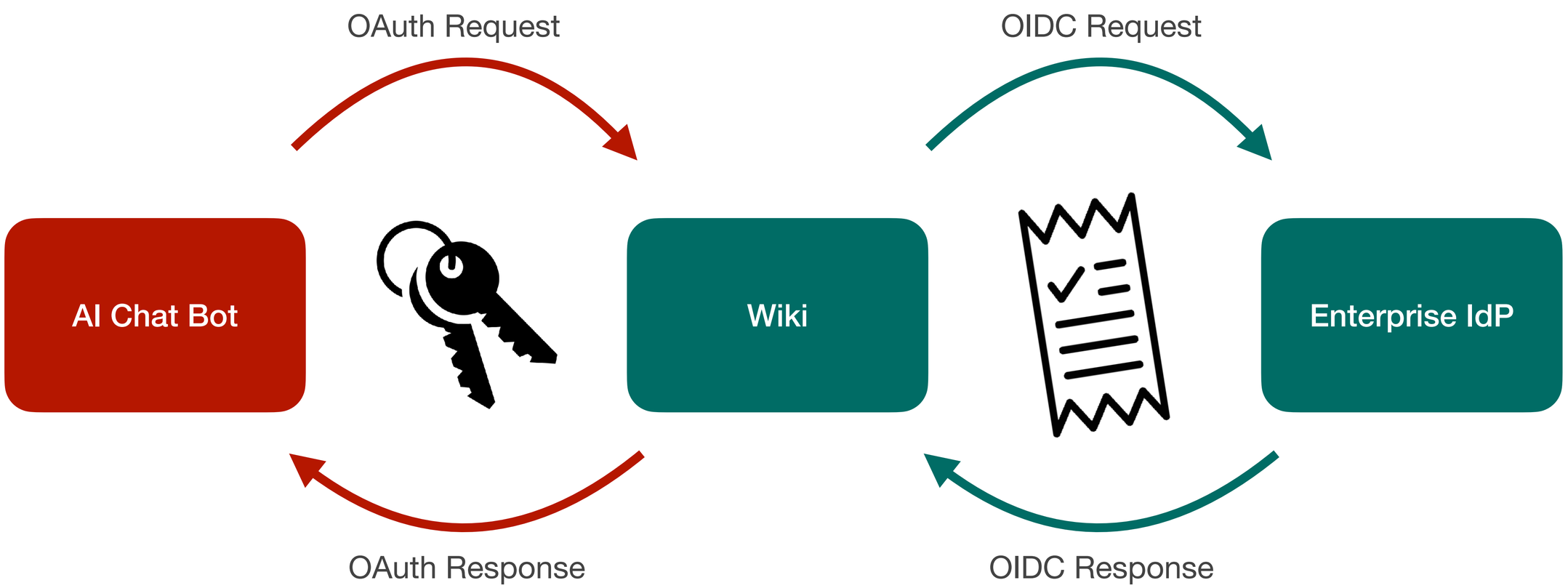
2. Redirect to IdP

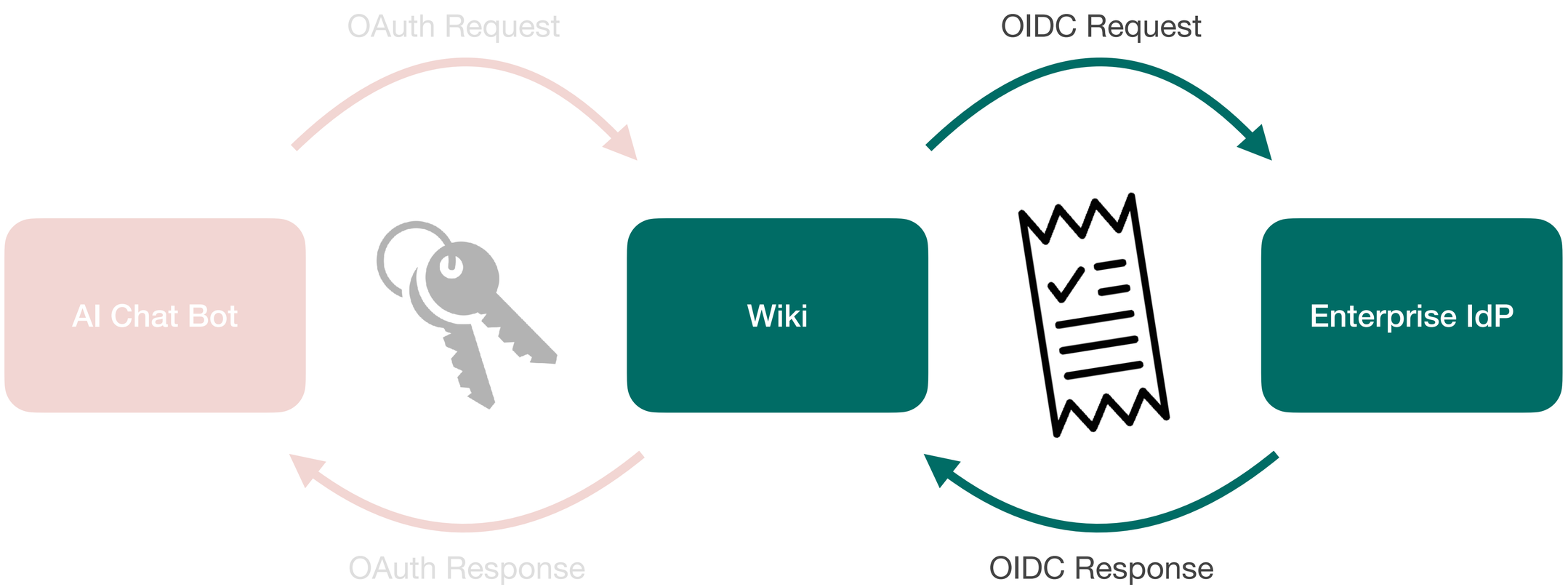


3. Logged In

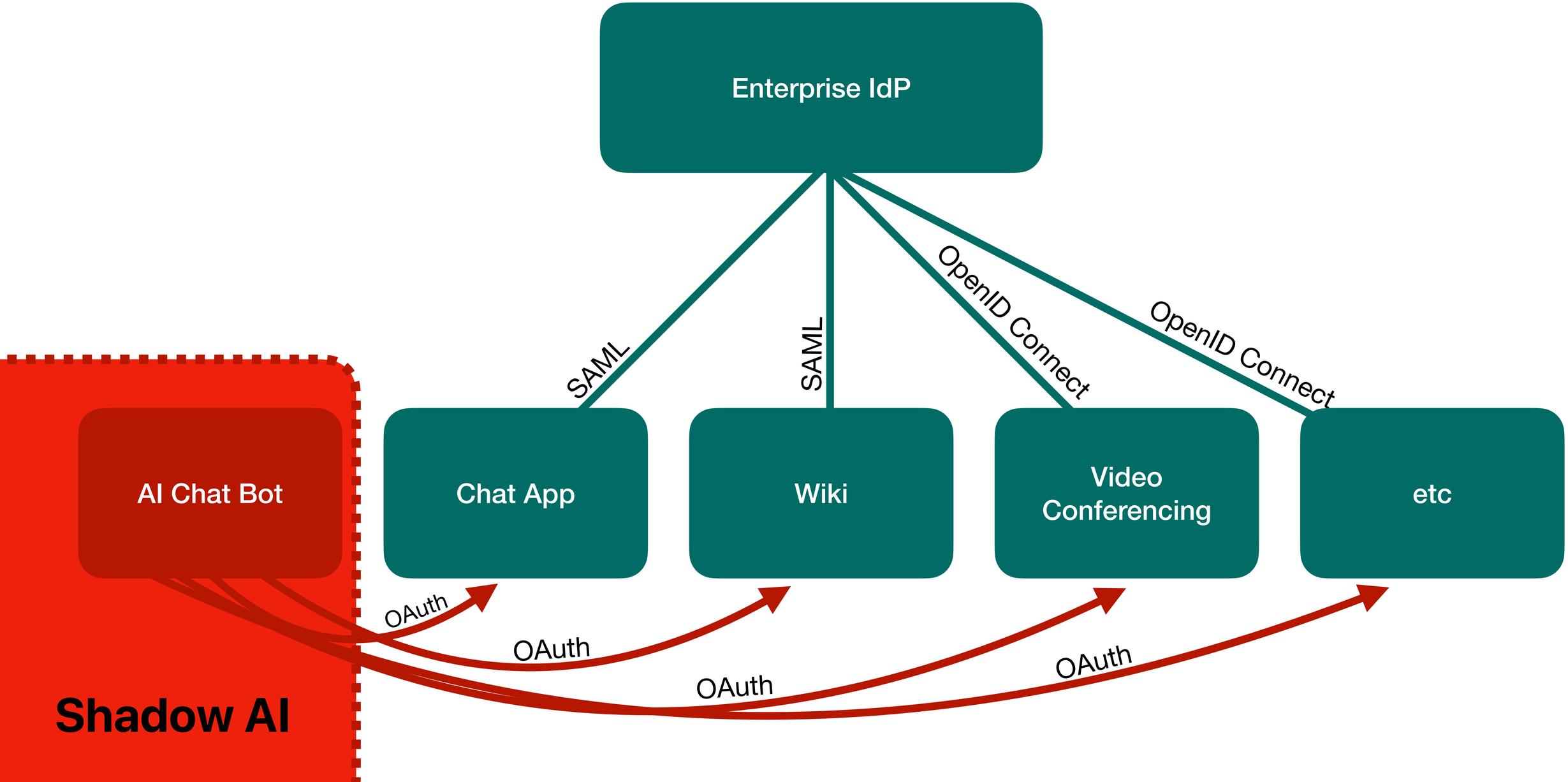
Enterprise API Access Today




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

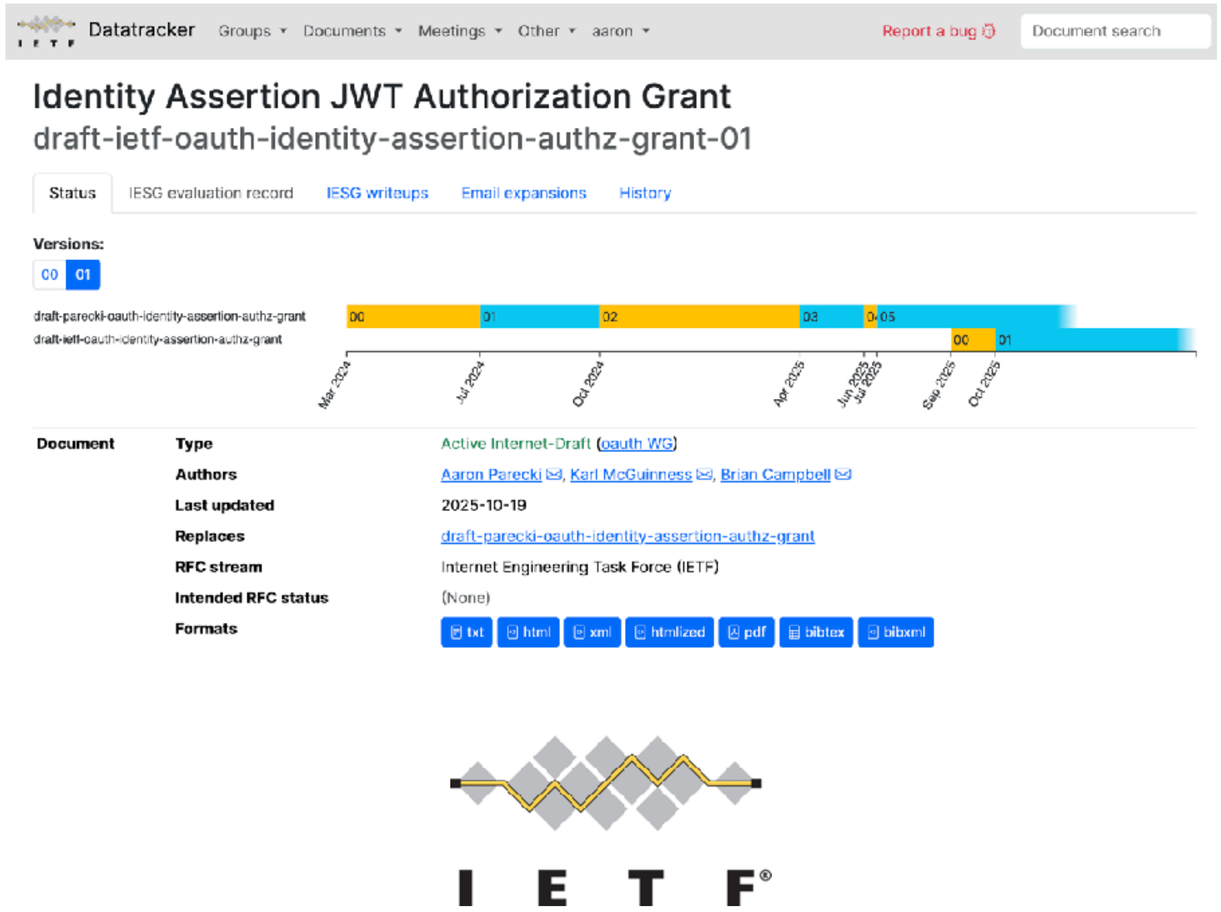


No control or visibility by the enterprise IT admin

Terrible UX for Employees

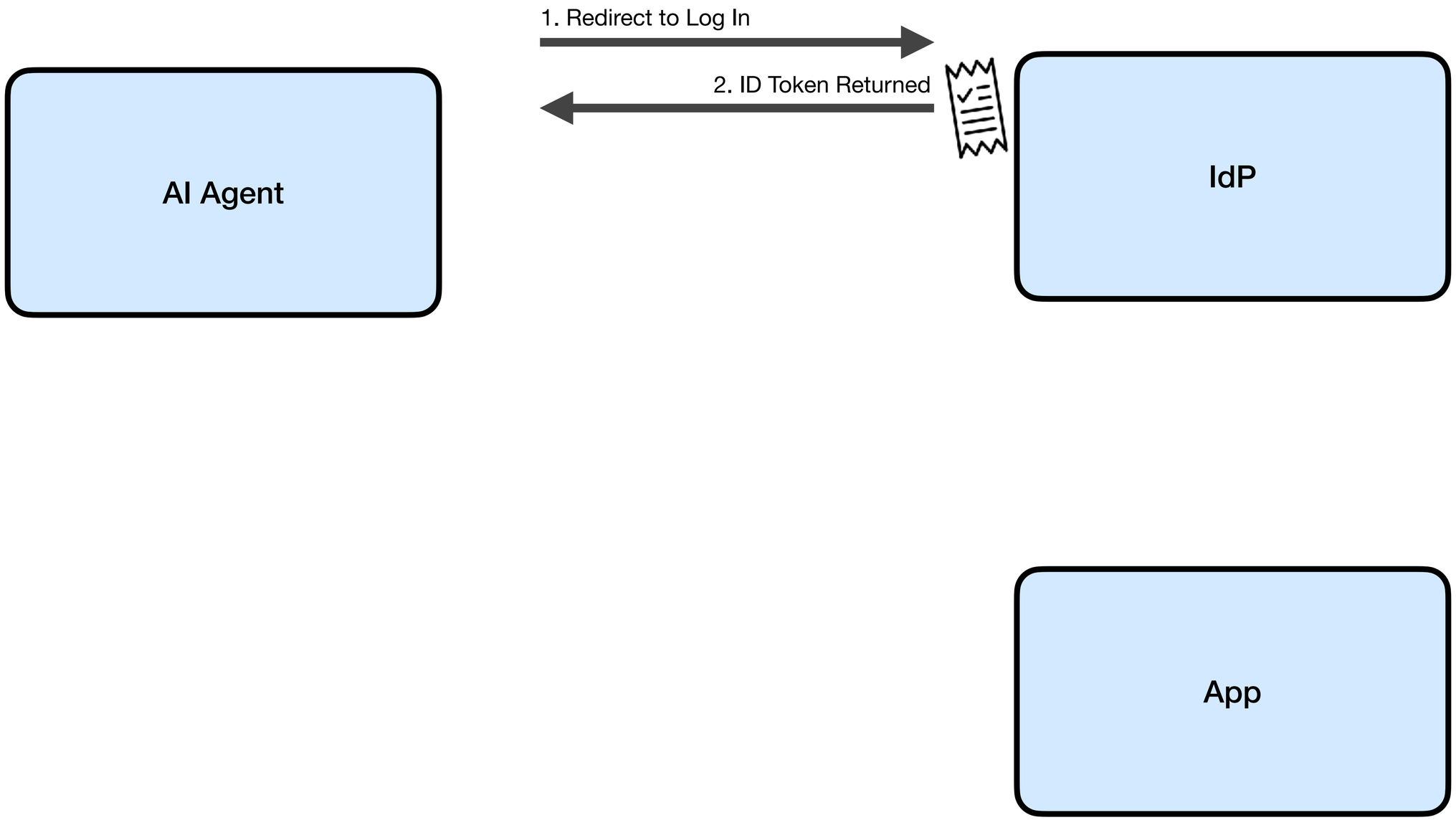
Cross App Access

aka Identity Assertion JWT Authorization Grant

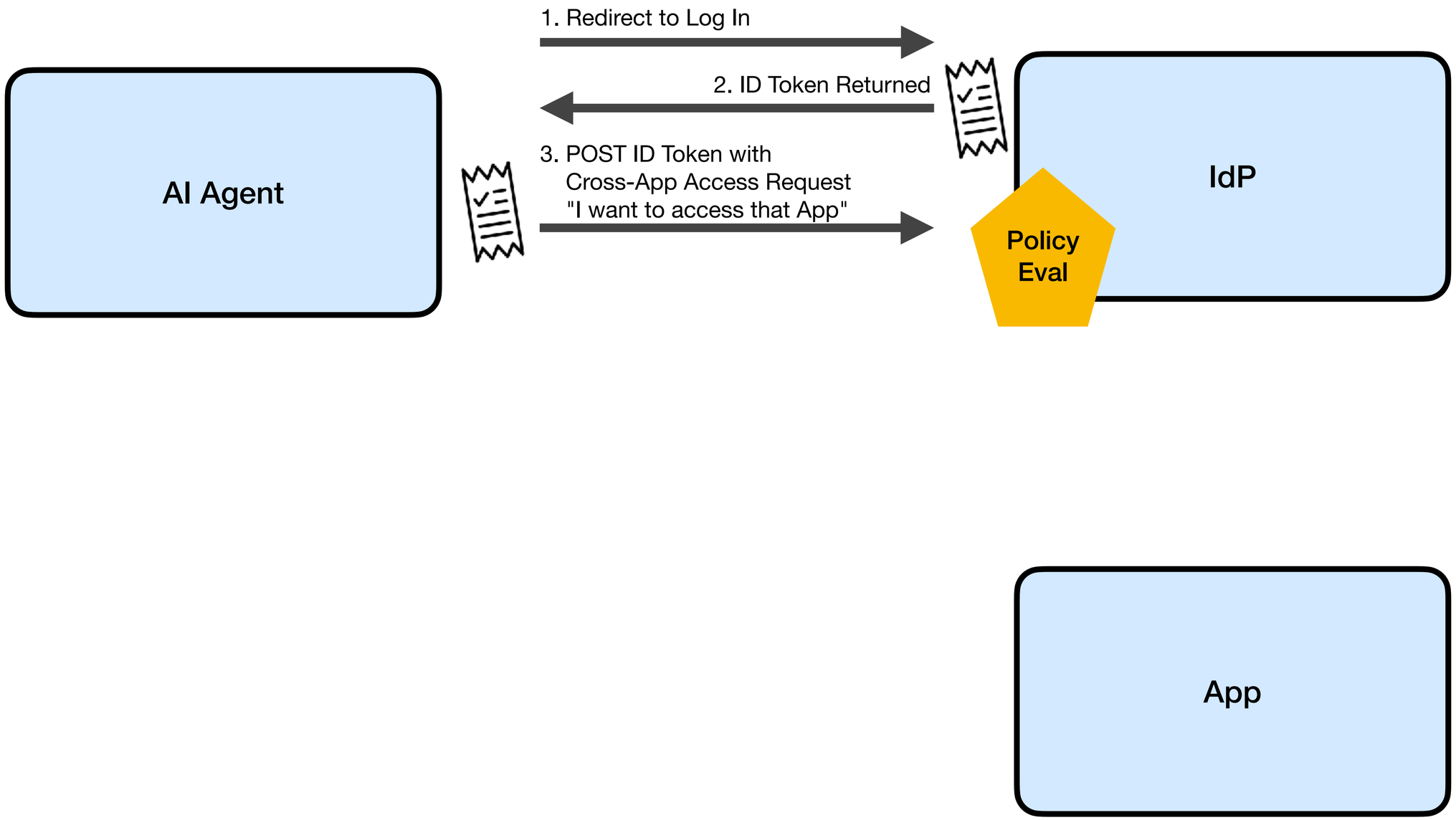


- Developed in the open
- First draft published March 2024
- Based on existing RFCs and work from many authors

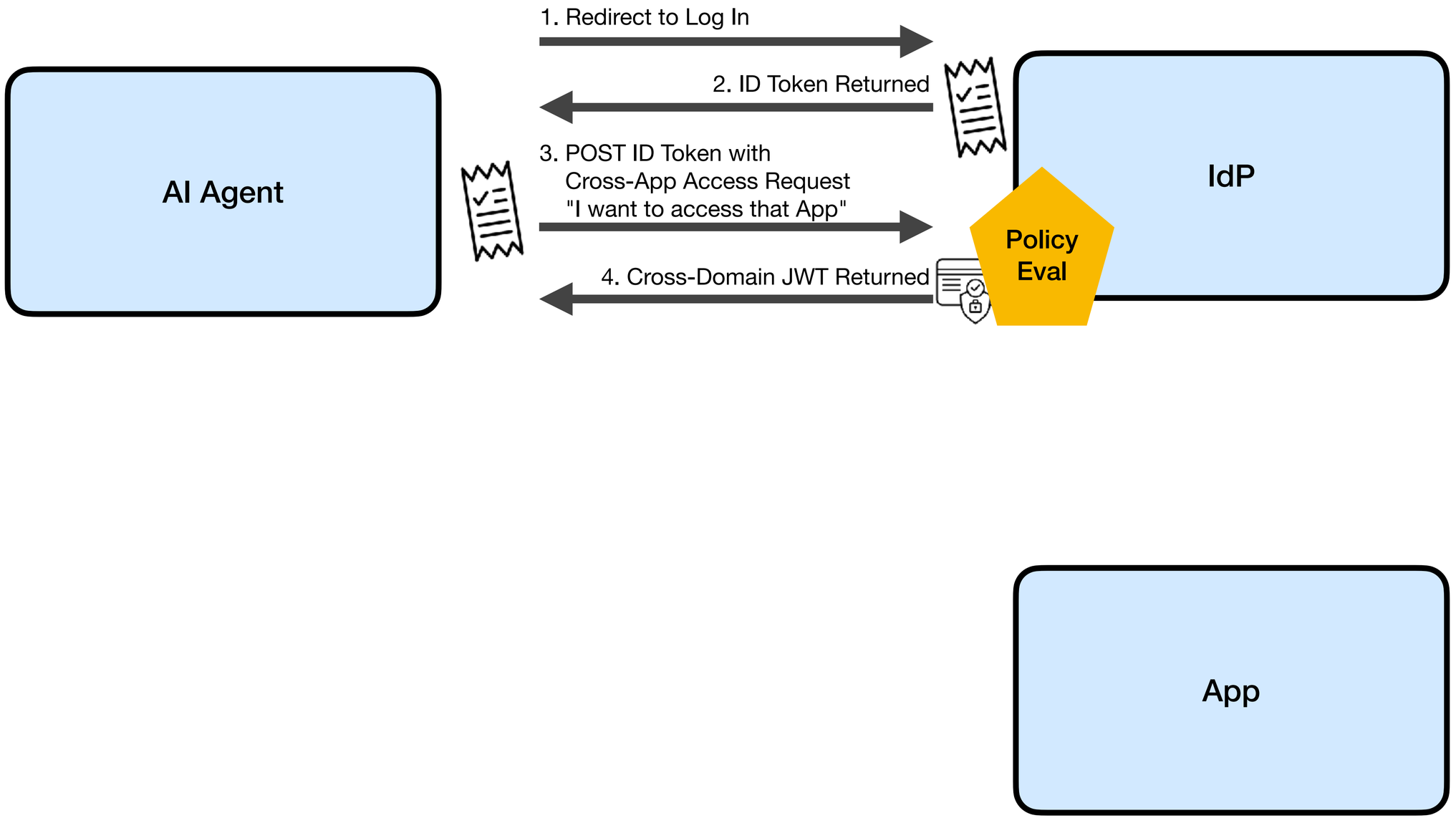
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/



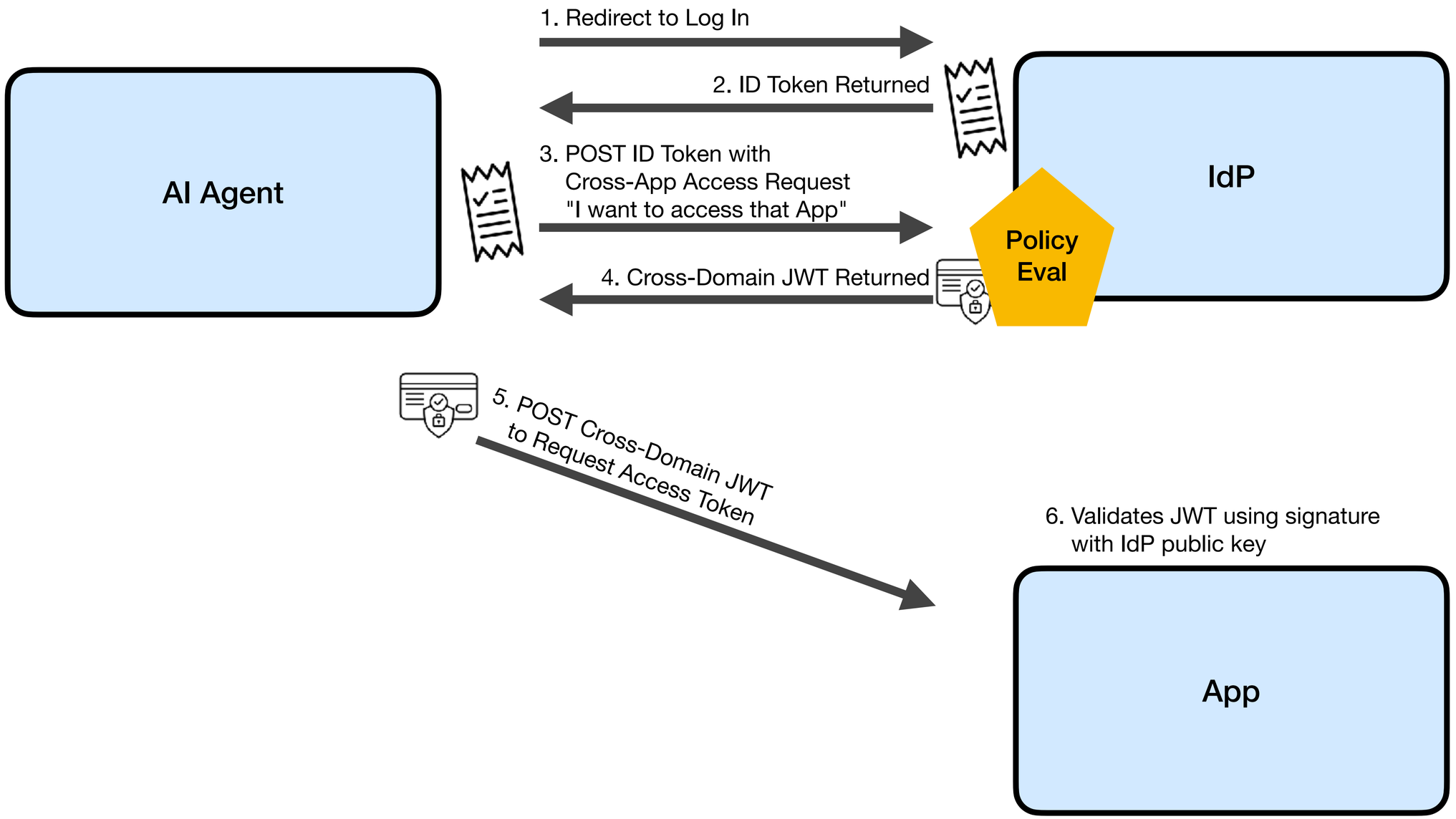
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/



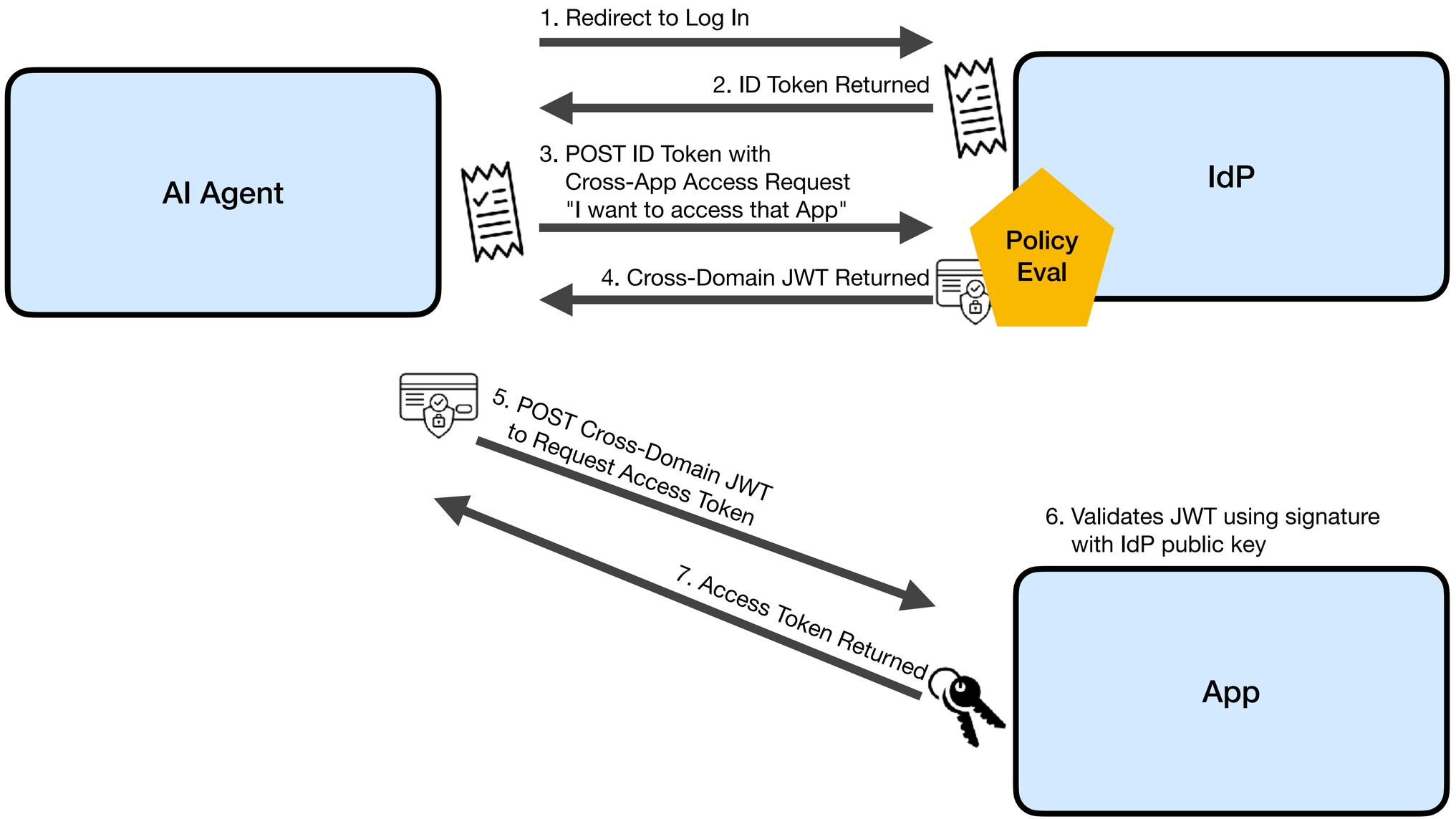
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/



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

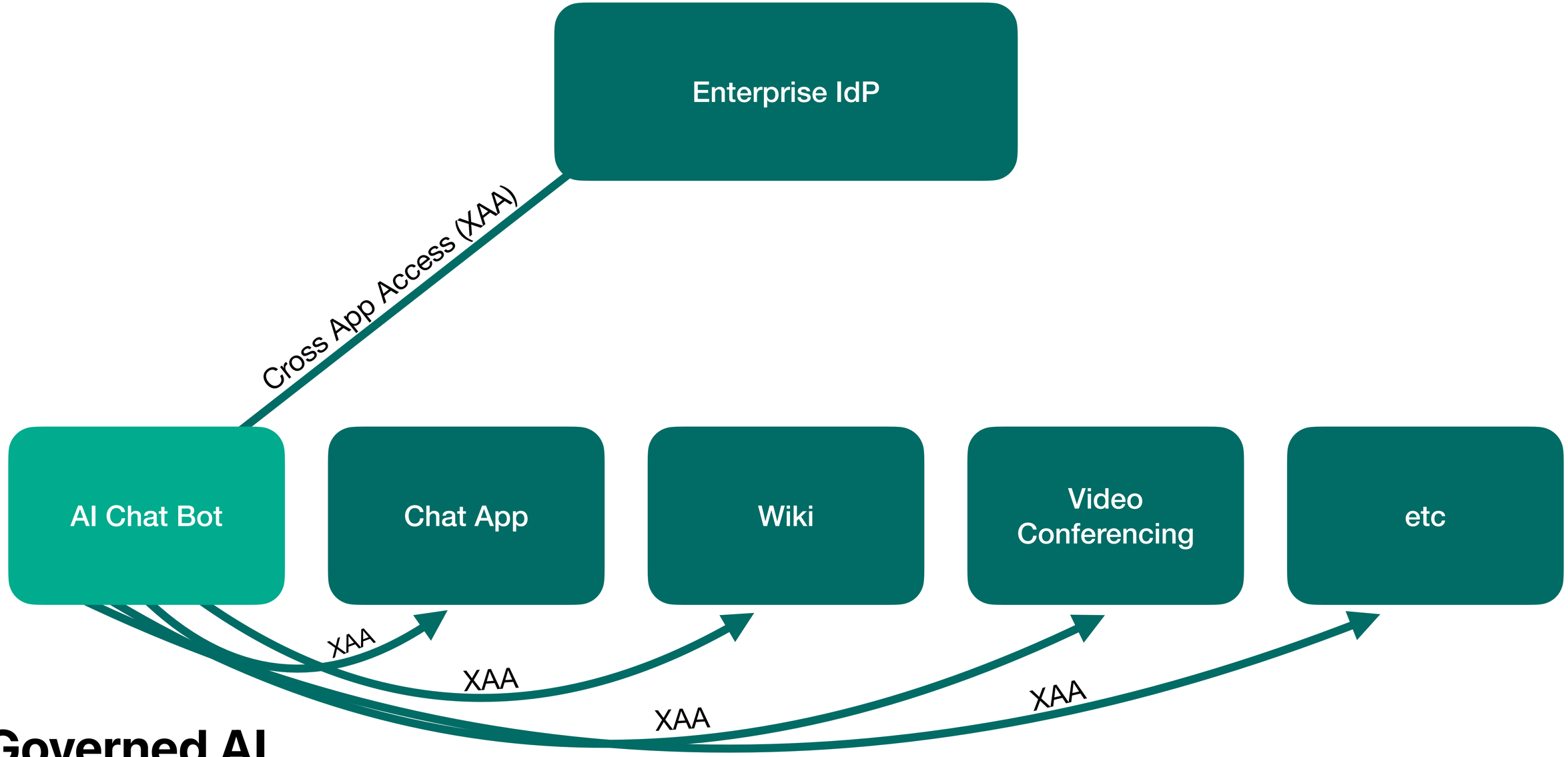


https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/

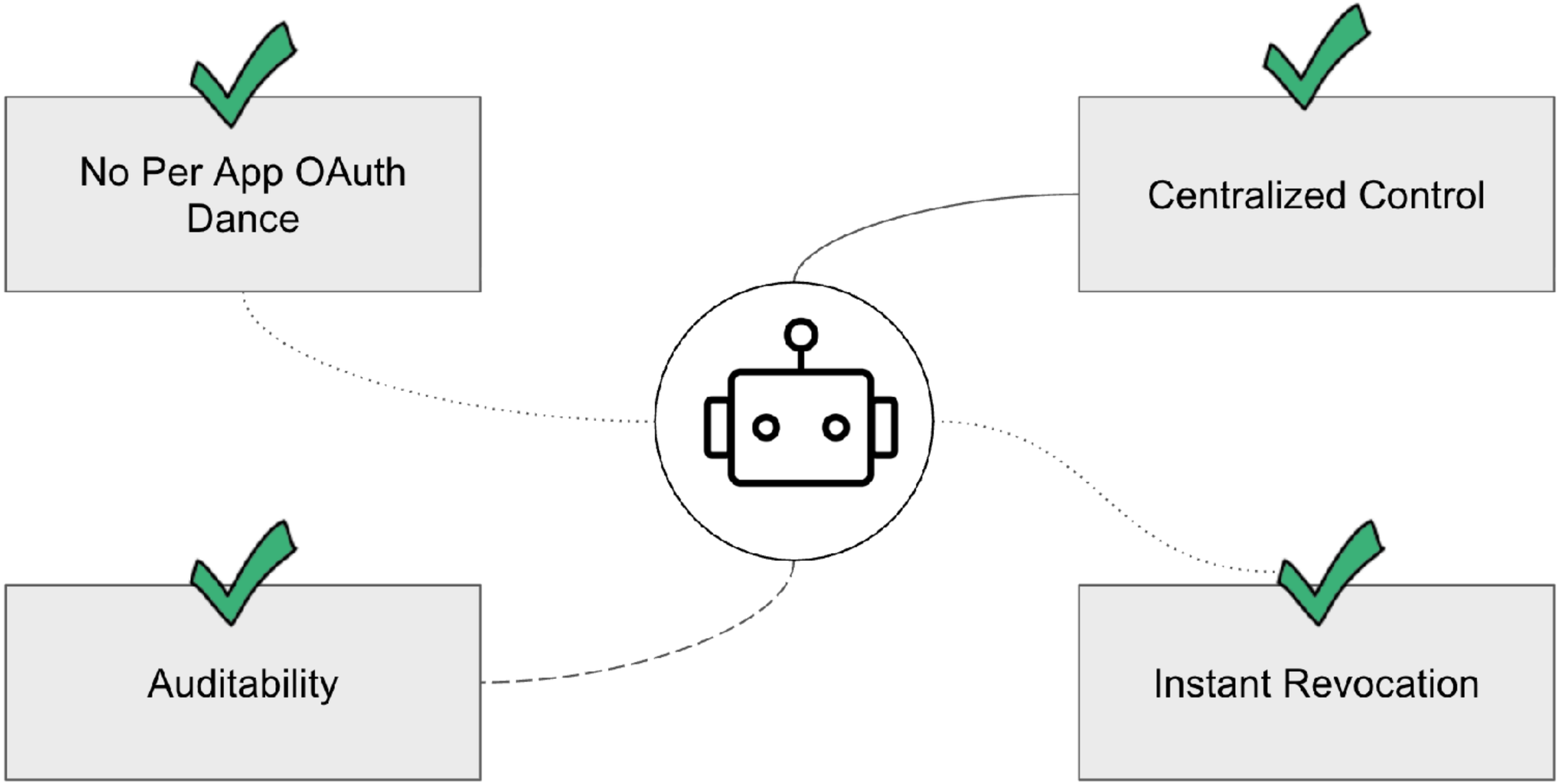


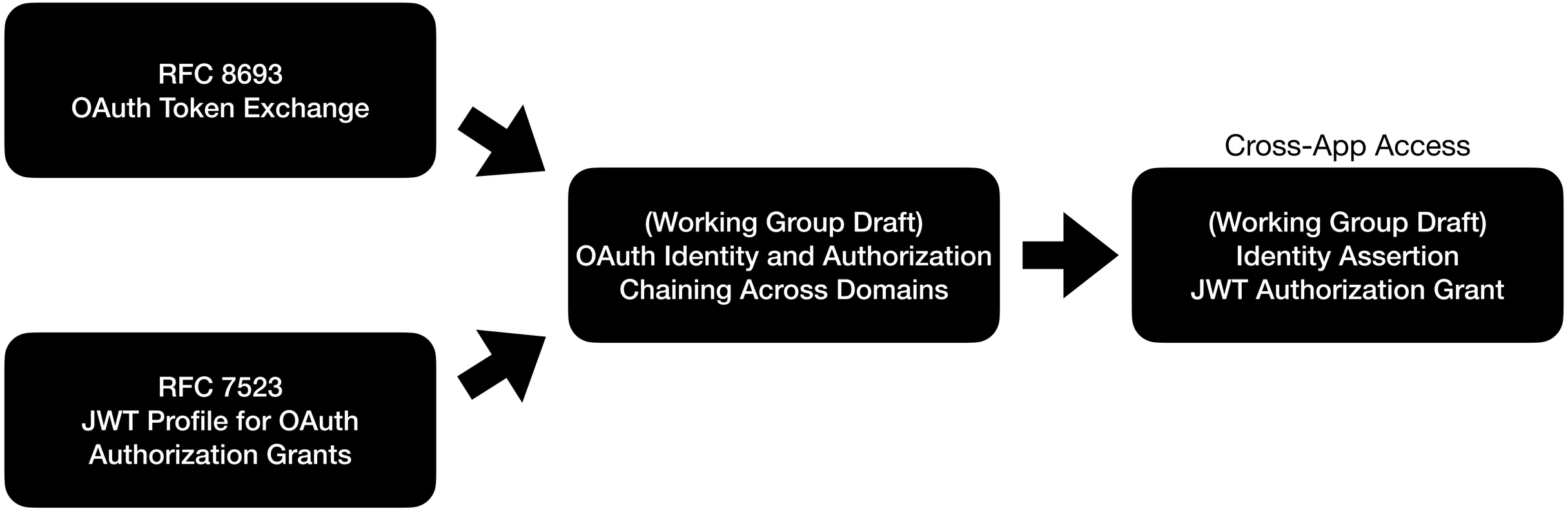
https://datatracker.ietf.org/doc/draft-ietf-oauth-identity-assertion-authz-grant/

Cross App Access



Governed AI


No Per App OAuth Dance
Centralized Control
Auditability
Instant Revocation



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

Cross App Access (XAA)

The open sandbox for testing enterprise cross-application access flows

Test secure agent-to-app and app-to-app authorization on behalf of users using the OAuth Identity Assertion Authorization Grant (ID-JAG).

Try the XAA Flow →

What is Cross App Access (XAA) ?

Cross App Access (XAA) describes the use case where an application requires access to a third-party application, such as when your company's chat application displays the latest code update from a separate source code management tool. Using the OAuth extension "Identity Assertion Authorization Grant," the enterprise identity provider manages the connection between two applications, replacing the user's manual approval step with a seamless token exchange behind the scenes.

Explore the Roles

Requesting App

applications that request access to protected resources u

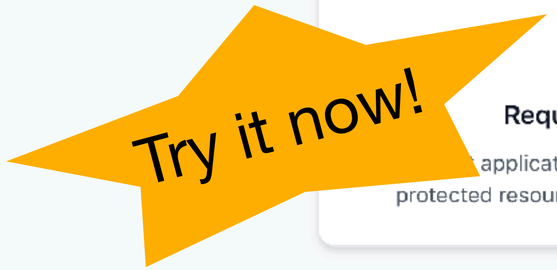
Resource App

Configure and test resource servers that validate

Identity Provider

Manage users and authenticate identities

vider



https://xaa.dev