Identity 101

How username/password got so complicated

Bobby Johnson
Developer Evangelist

Auth0

auth0.com

The Game Plan

1. Introduction

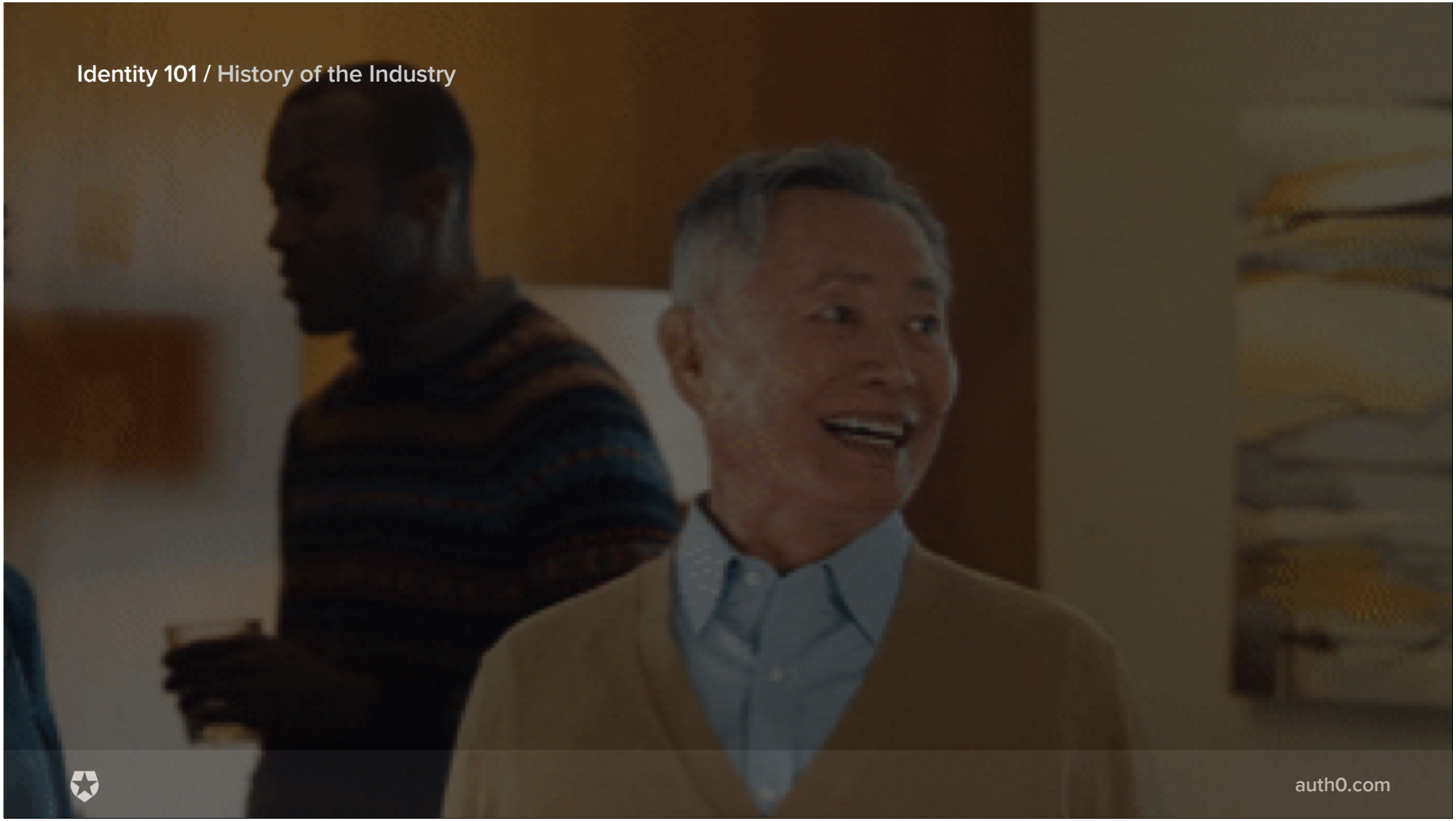
a. The Problem

b. The Role of Open Standards

2. History of the Industry

a. Business/Enterprise Use Cases

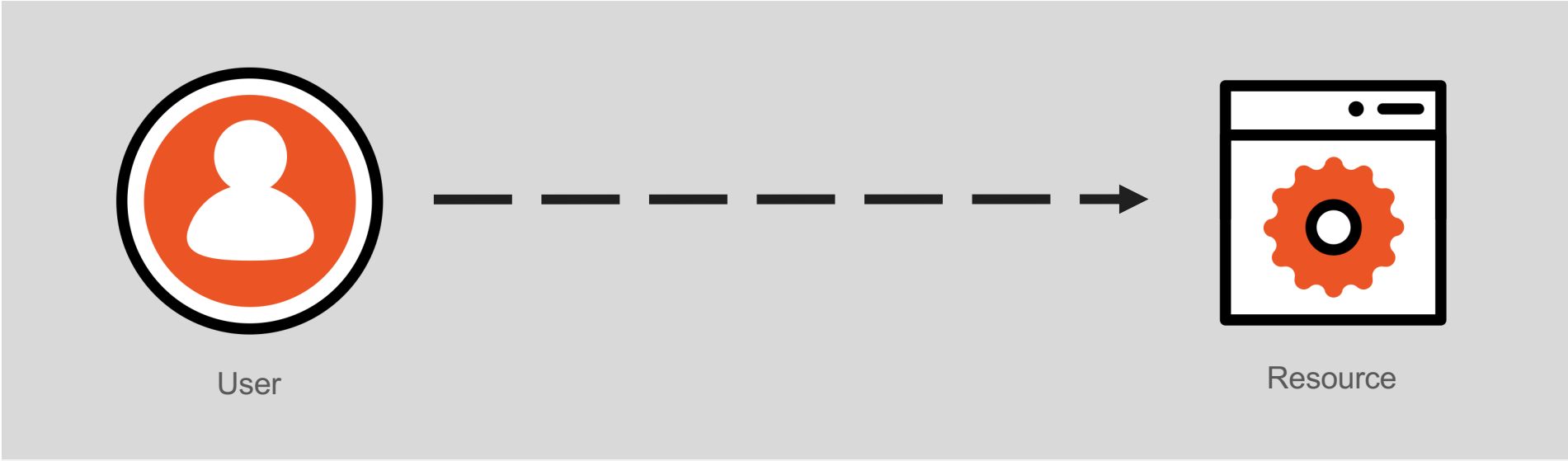
b. Consumer Internet Use Cases


Identity 101 / History of the Industry
auth0.com

The Problem

The Problem

The problem is deceivingly simple; you have a user who wants to access a resource. If you look at this picture, it looks easy, right?



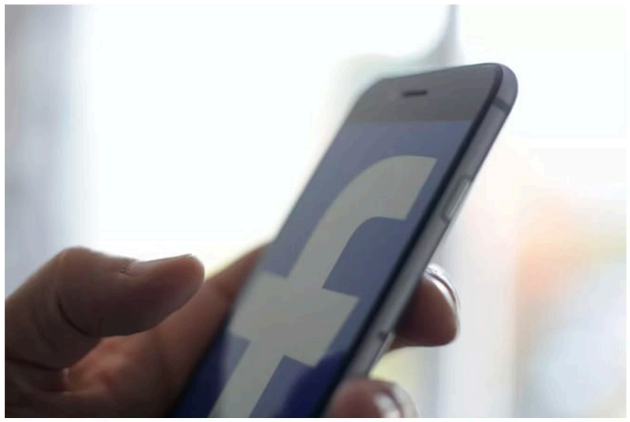
Identity 101

The Problem

Facebook fined $11.4M in Italy over data misuse

After a year of woe, the social network's data-related troubles aren't yet over.

BY KATIE COLLINS | DECEMBER 7, 2018 5:36 AM PST



Facebook just got hit with another fine.

NurPhoto

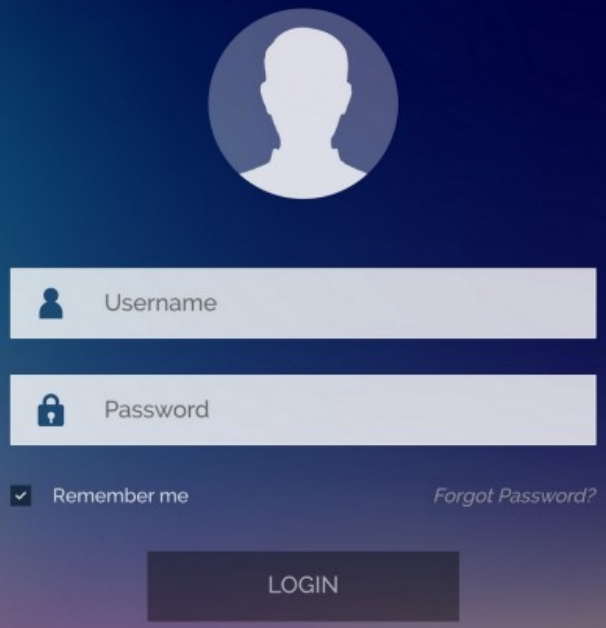
Italy's Competition Authority on Friday slapped Facebook with two fines that total 10 million euros ($11.4M) for using people's data for commercial purposes in ways that break the country's laws.

Identity 101

The Problem

Identity 101

The Problem



Identity 101

The Problem

Identity 101

The Role of Open Standards


Identity 101 / The Role of Open Standards
auth0.com


Identity 101 / The Role of Open Standards
auth0.com

Identity 101

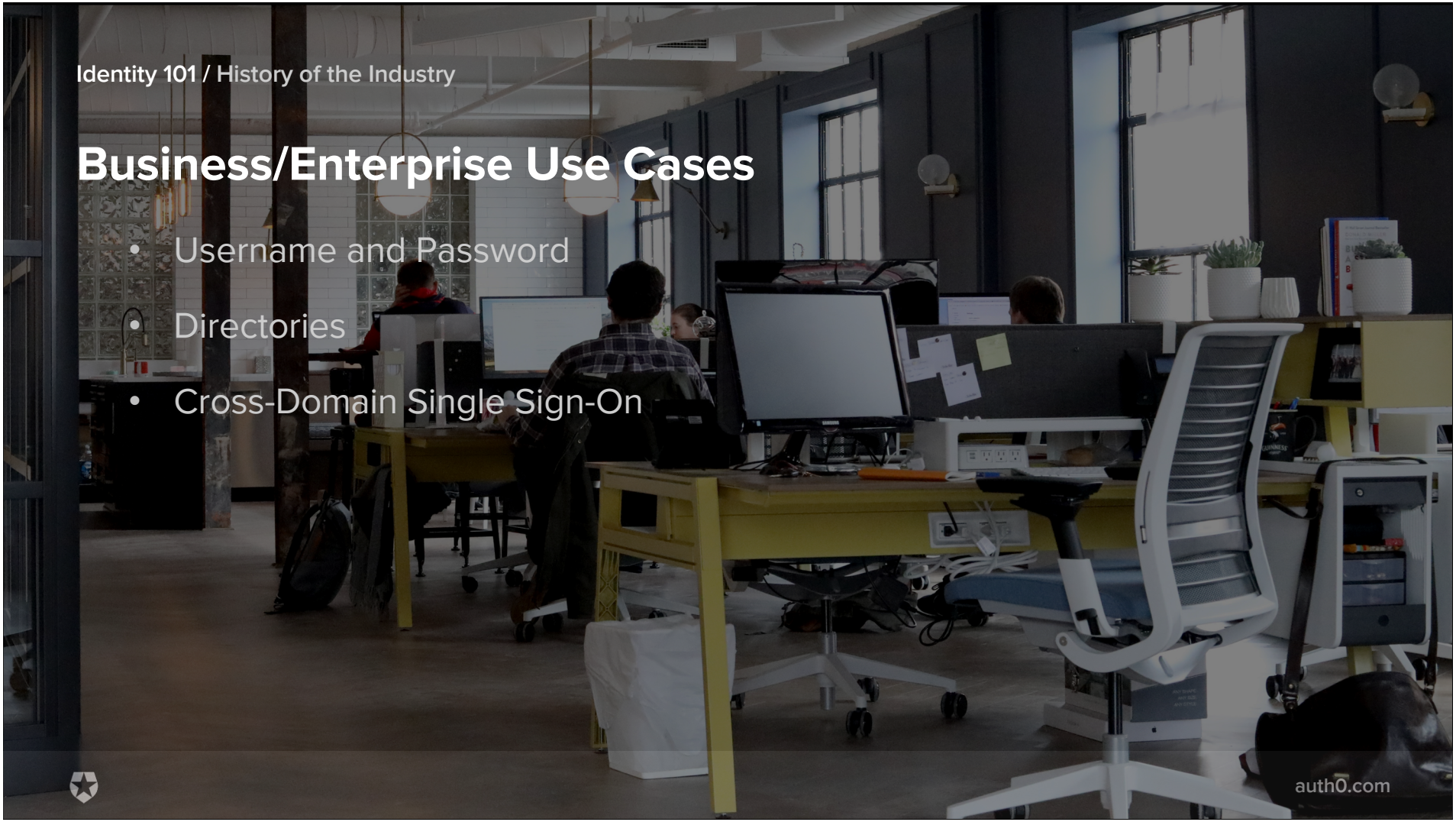
The Role of Open Standards

- SAML
- OAuth2
- OpenID Connect

History of the Industry

2. Consumer Internet

- Username and Password
- Delegated Authorization
- Cross-Domain Single Sign-On


Identity 101 / History of the Industry
Business/Enterprise Use Cases
• Username and Password
• Directories
• Cross-Domain Single Sign-On
auth0.com

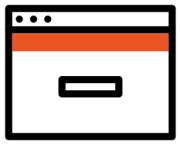
Username and Password

Concepts:

- Digital Identity
- Raw Credentials

Username and Password

User



Browser

Web App

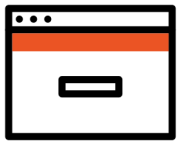
Attributes

Concepts:

- Digital Identity
- Raw Credentials

Username and Password

User



Browser

Web App

Concepts:

- Digital Identity
- Raw Credentials

Username and Password

Concepts:

- Digital Identity
- Raw Credentials

Username and Password

Concepts:

- Digital Identity
- Raw Credentials

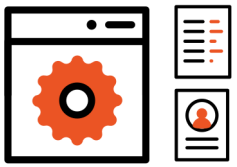
Username and Password

Concepts:

- Digital Identity
- Raw Credentials

Directories

User Browser

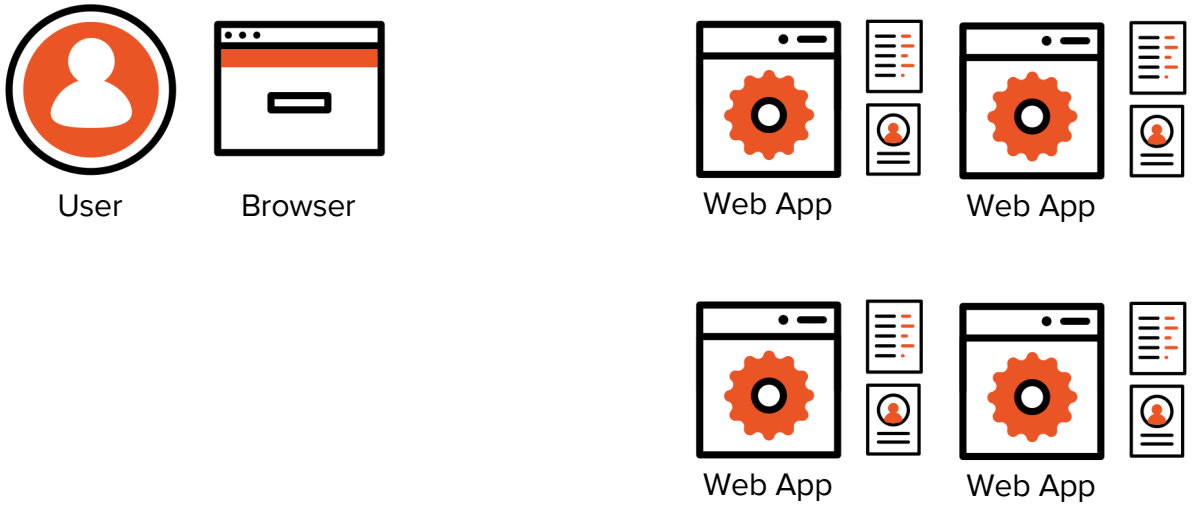


Web App

Concepts:

- Directory
- Boundaries/Perimeter
- Kerberos

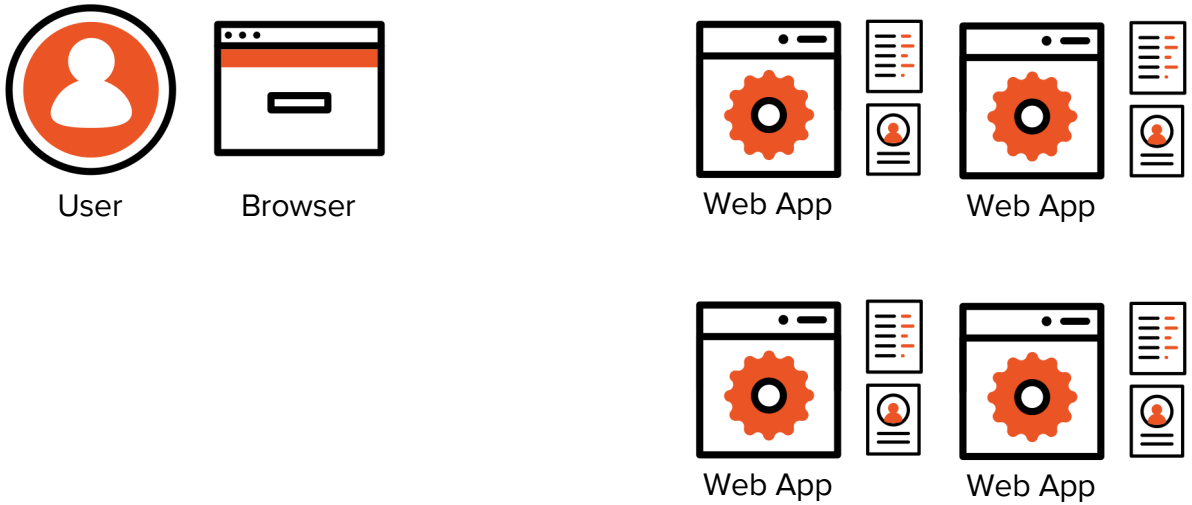
Directories



Concepts:

- Directory
- Boundaries/Perimeter
- Kerberos

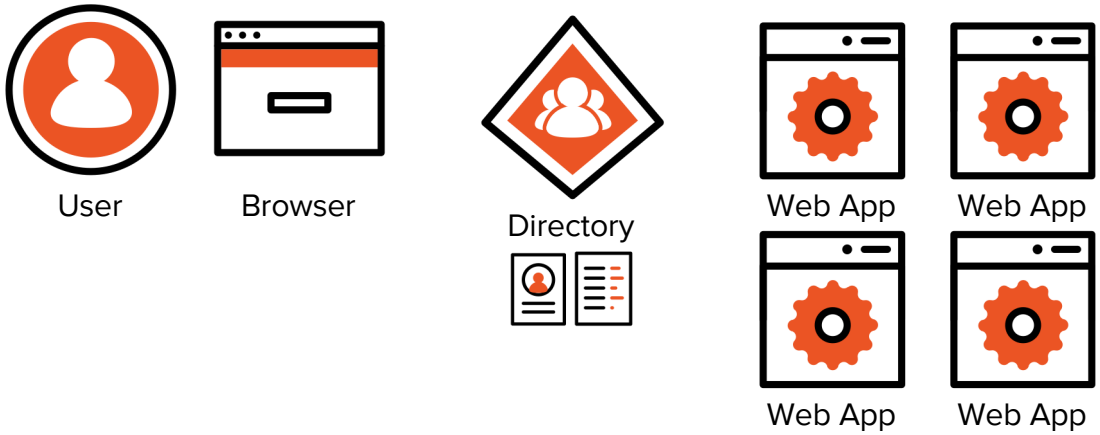
Directories



Concepts:

- Directory
- Boundaries/Perimeter
- Kerberos

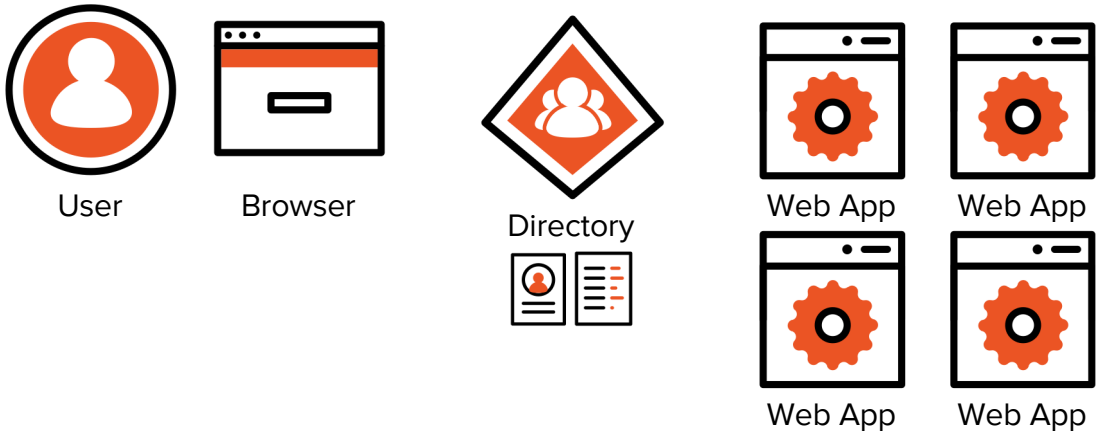
Directories



Concepts:

- Directory
- Boundaries/Perimeter
- Kerberos

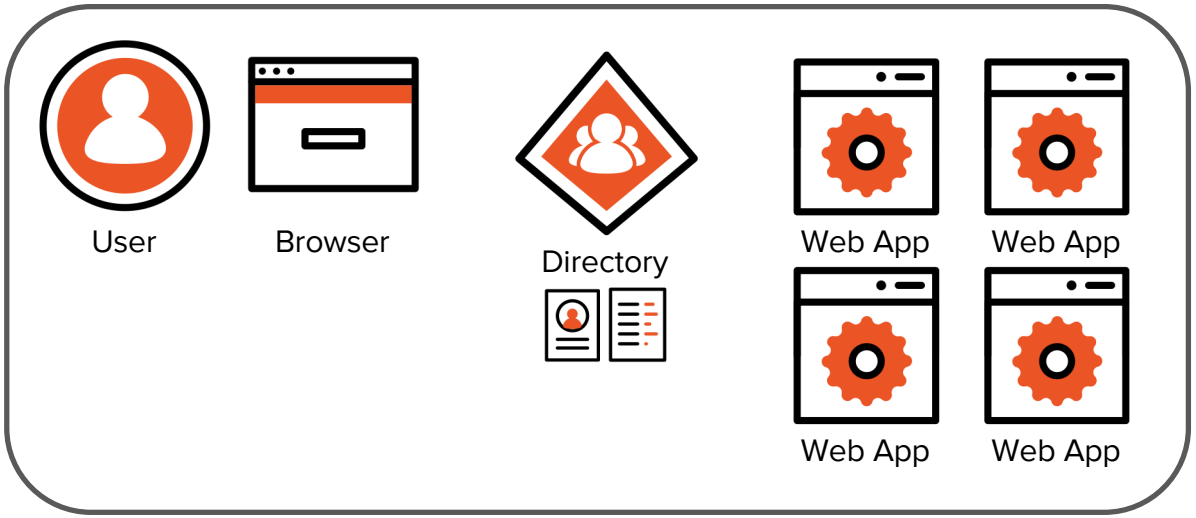
Directories



Concepts:

- Directory
- Boundaries/Perimeter
- Kerberos

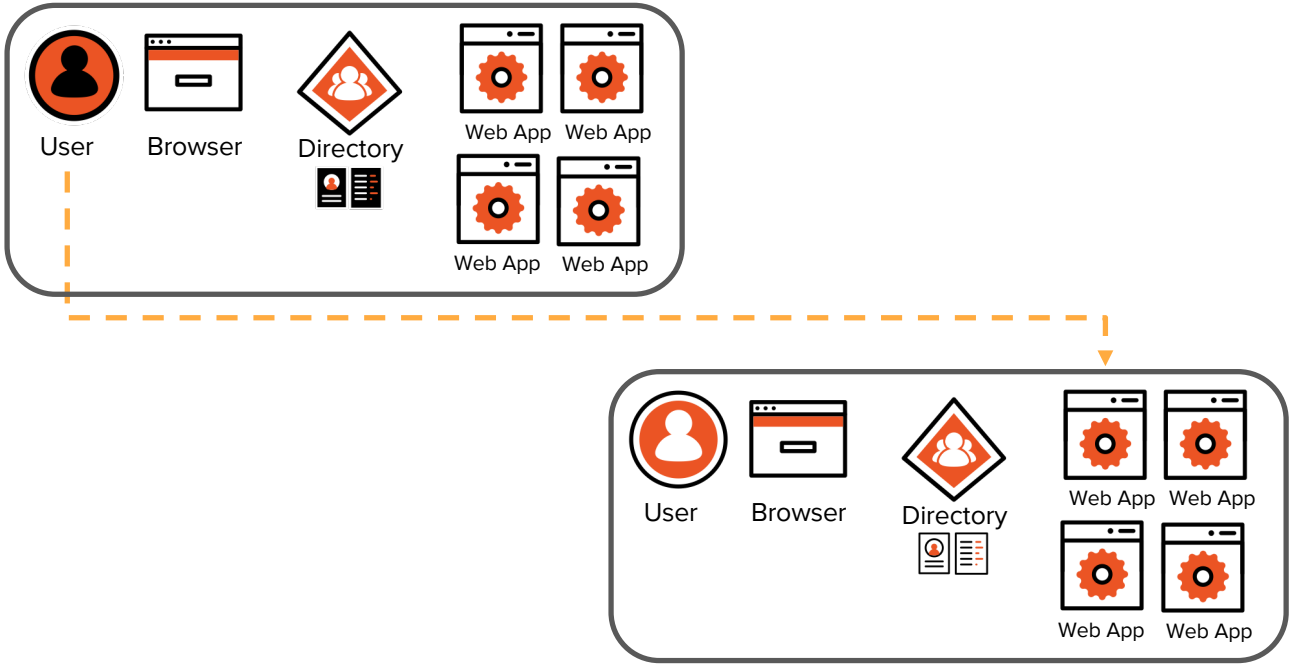
Cross-Domain Single Sign-On



Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

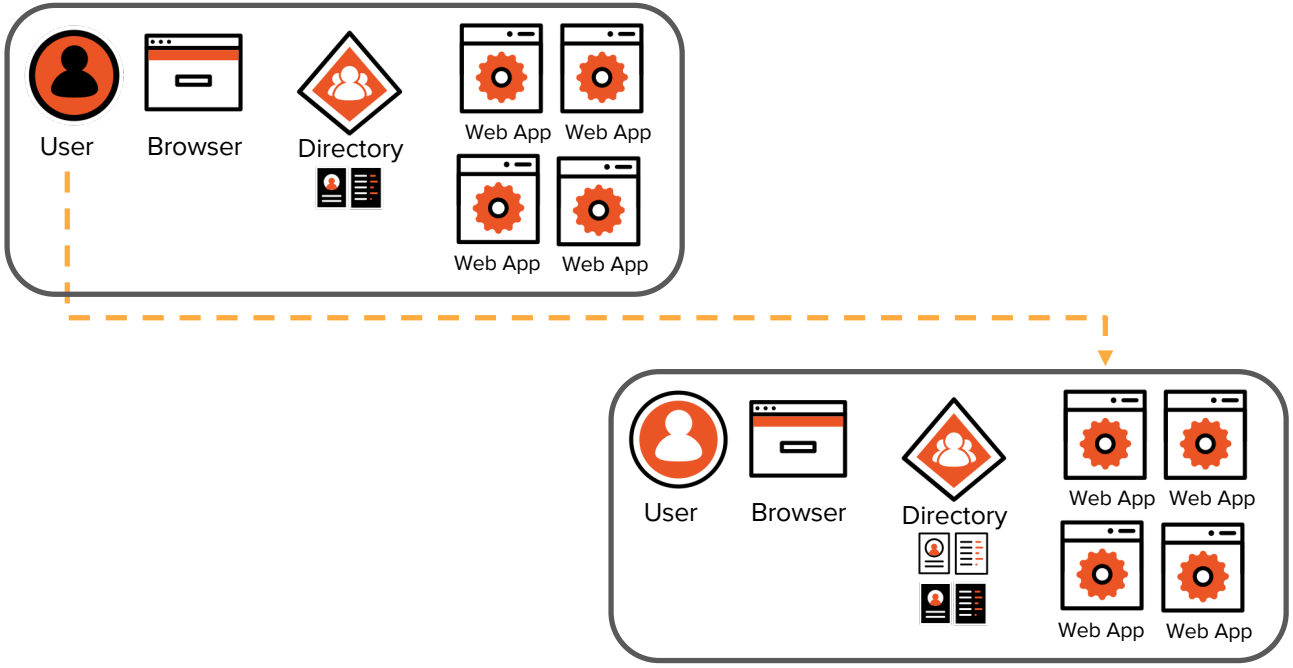
Cross-Domain Single Sign-On



Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

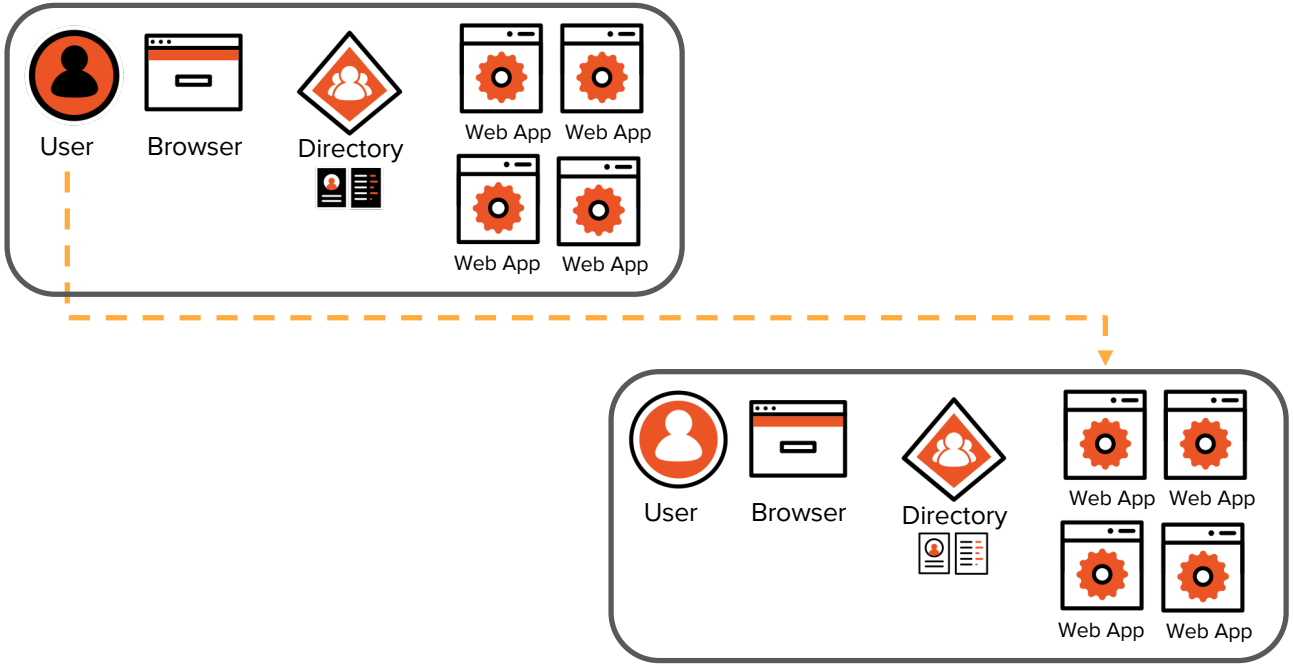
Cross-Domain Single Sign-On



Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

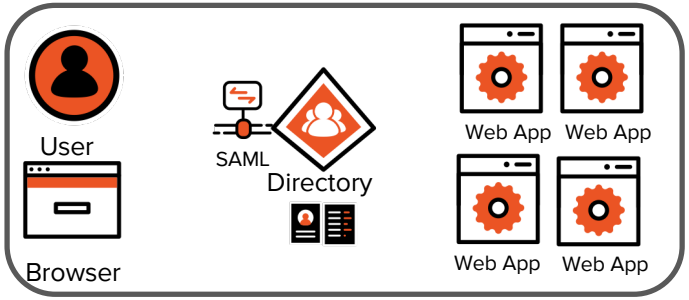
Cross-Domain Single Sign-On

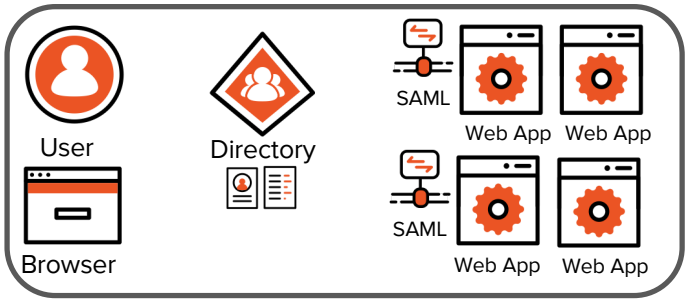


Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

Cross-Domain Single Sign-On

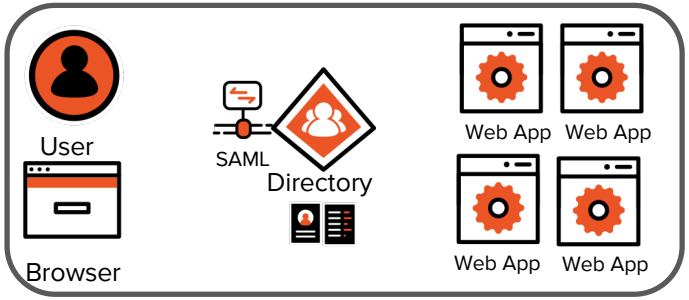


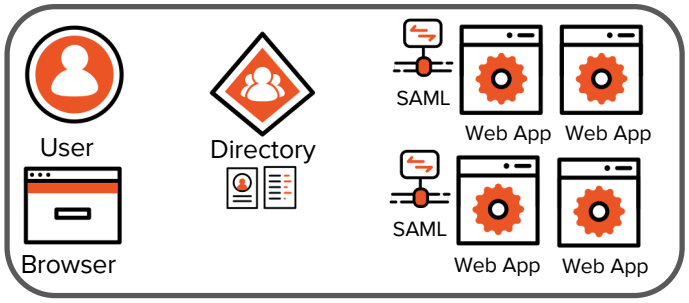


Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

Cross-Domain Single Sign-On



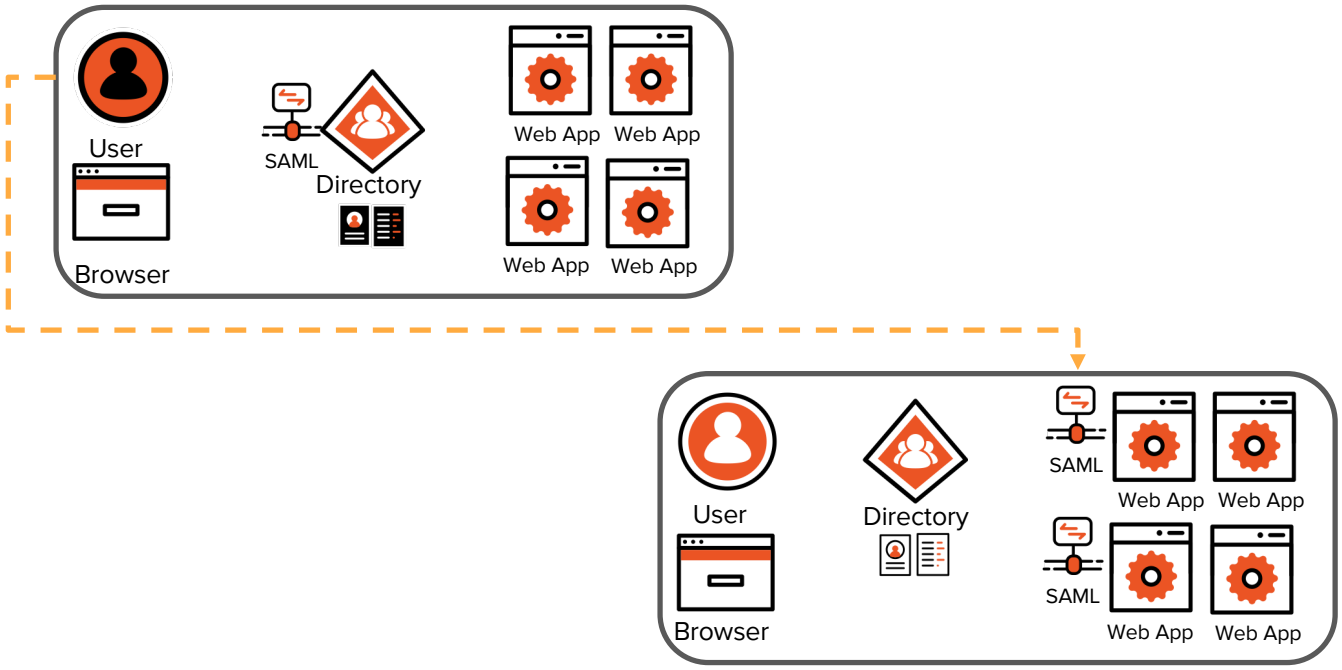


Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

"I am an application and I trust that this source of identity information is telling me the truth."

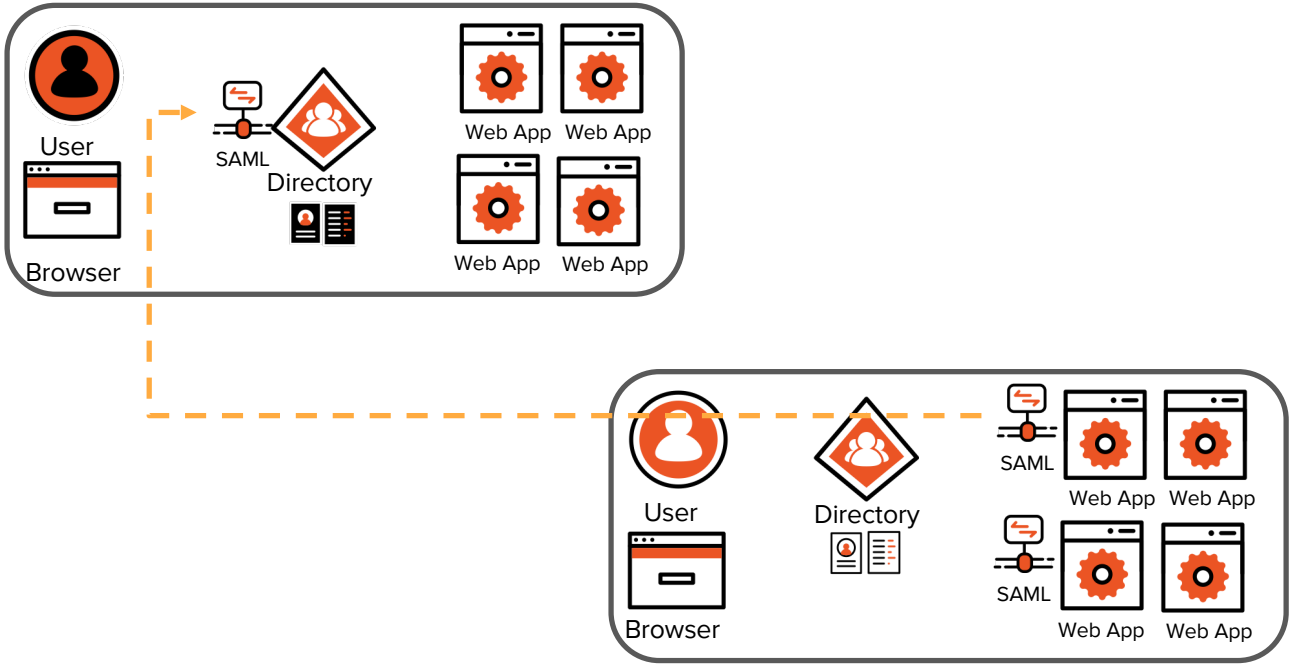
Cross-Domain Single Sign-On



Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

Cross-Domain Single Sign-On

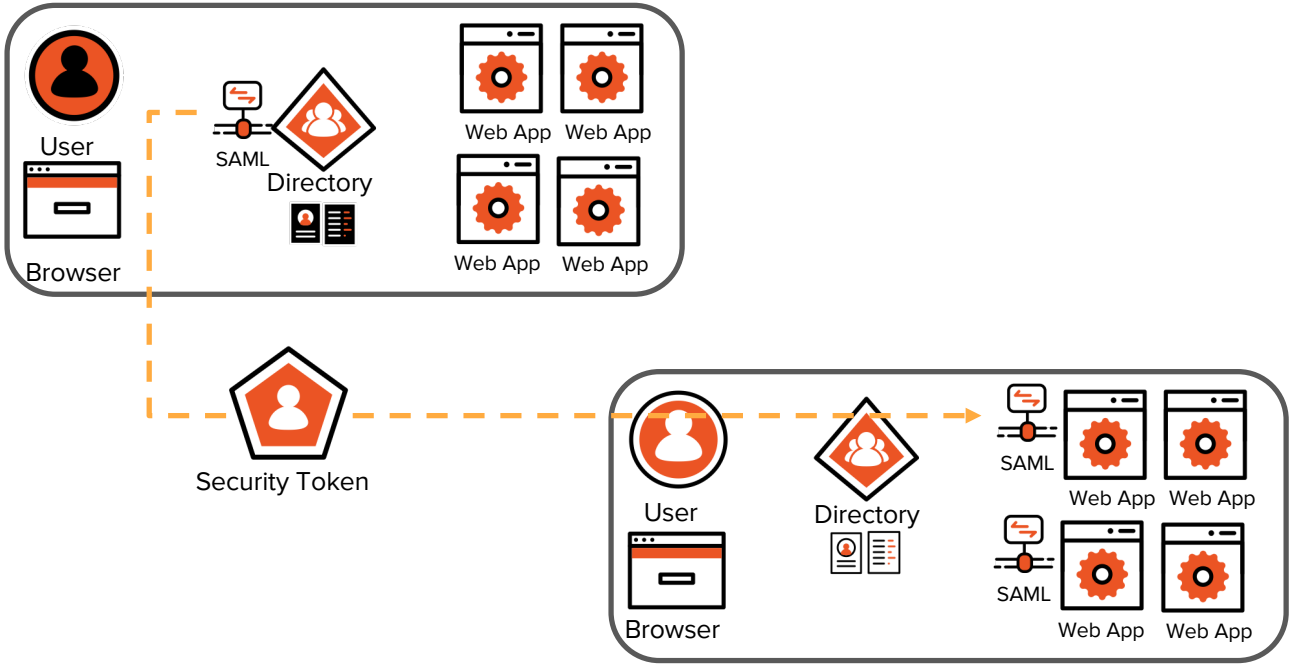


Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

Cross-Domain Single Sign-On

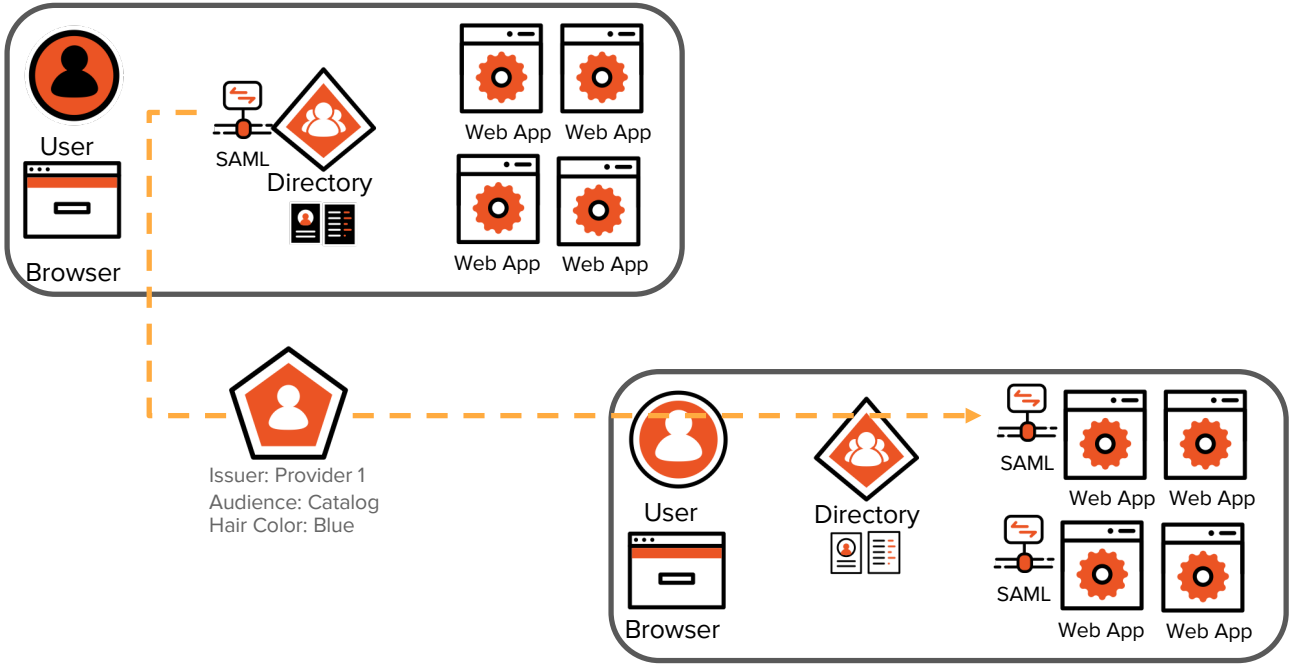
Issuer: Provider 1
Audience: Catalog
Hair Color: Blue



Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

Cross-Domain Single Sign-On



Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

Identity 101

Security Tokens

Issuer: Provider 1
Audience: Catalog
Hair Color: Blue

Identity 101

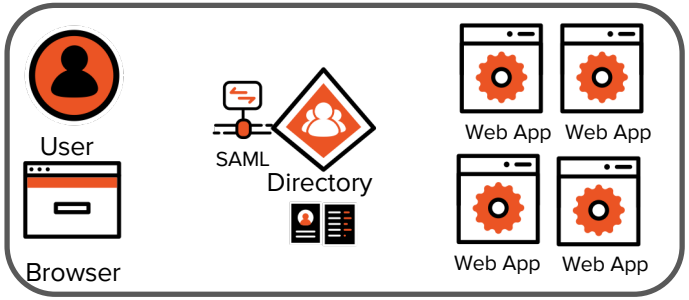
Security Tokens

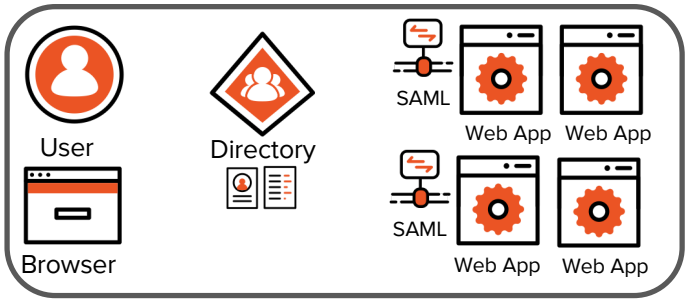
Issuer: Provider 1
Audience: Catalog
Hair Color: Blue

Security Tokens

Issuer: Provider 1
Audience: Catalog
Hair Color: Blue

Cross-Domain Single Sign-On





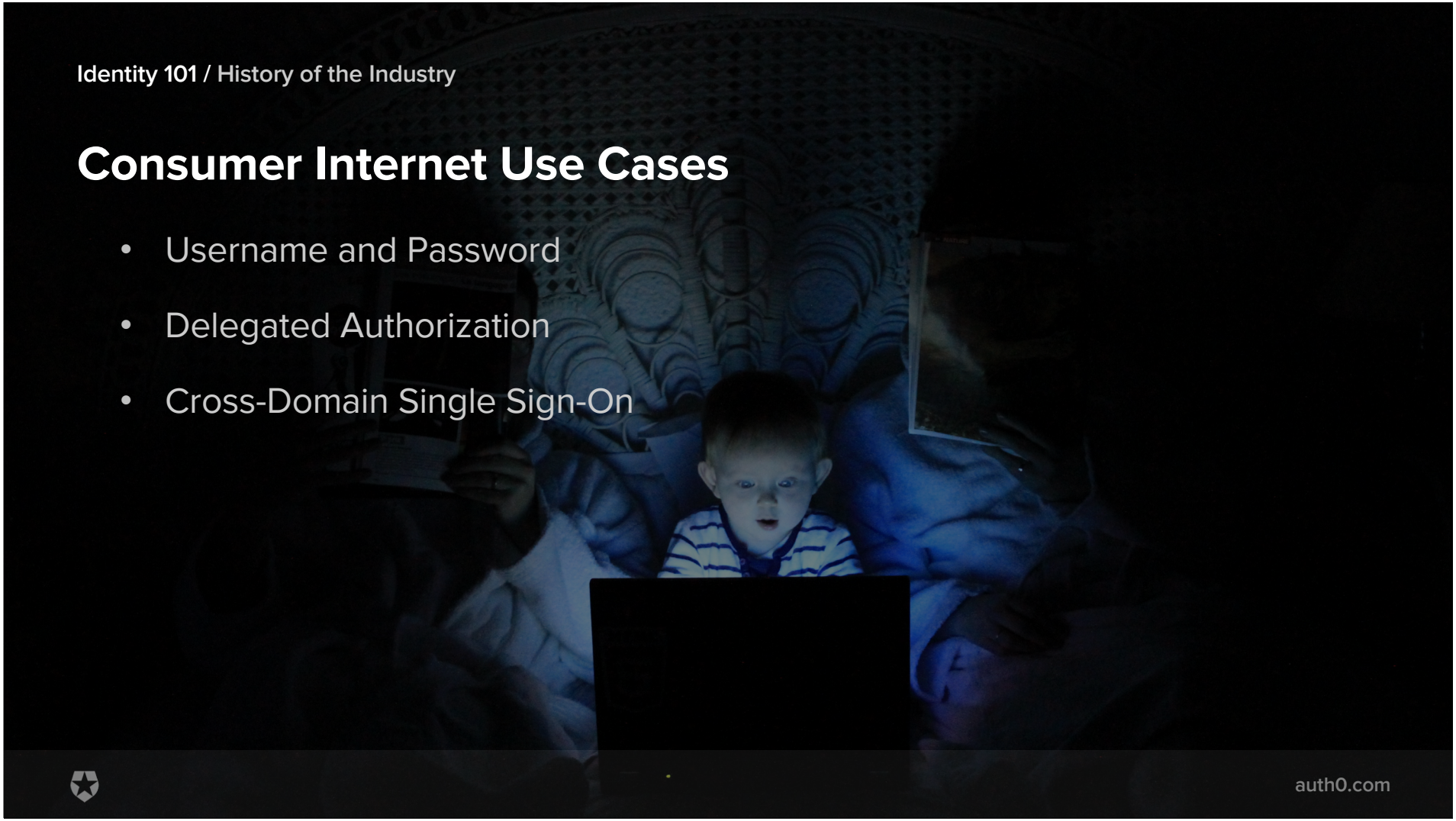
Concepts:

- SAML
- Trust
- Claims
- Session Cookies
- Shadow Accounts

Cross-Domain Single Sign-On

Consumer Internet Use Cases

- Username and Password
- Delegated Authorization
- Cross-Domain Single Sign-On



Username and Password

Username and Password

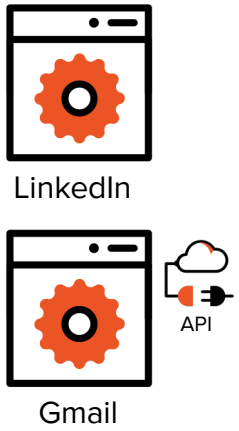
Username and Password

Username and Password

"In general, people should never give credentials to any place other than the origin of those credentials."

Vittorio Bertocci, Principal Architect Auth0

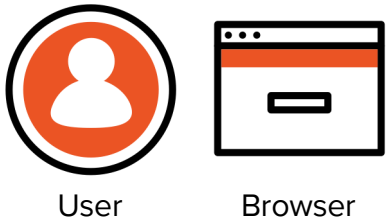
Delegated Authorization

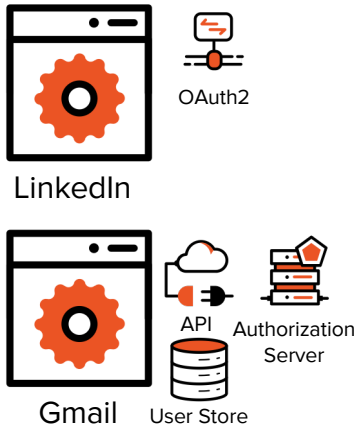


Concepts:

- OAuth2
- Authorization Server
- Clients
- Delegation
- Scopes
- Access Token
- Refresh Token

Delegated Authorization





Concepts:

- OAuth2
- Authorization Server
- Clients
- Delegation
- Scopes
- Access Token
- Refresh Token

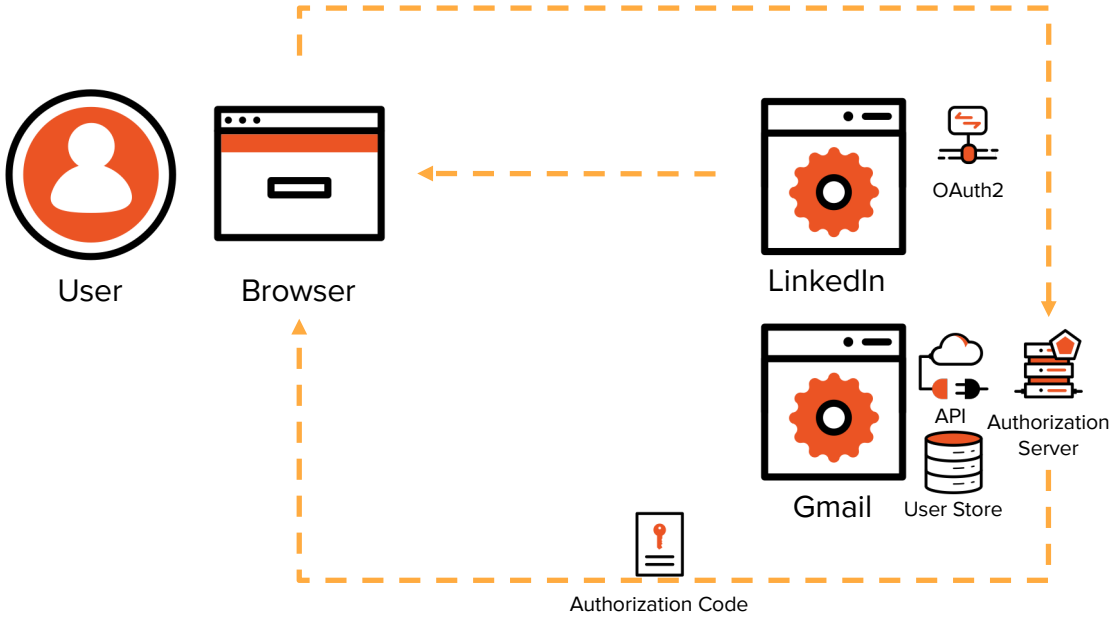
"Dear Gmail, I am LinkedIn. You know me because I am registered with you, I am a known client. Here I have a user. I would like you to grant access to their contacts and the ability to send emails on behalf of this user."

LinkedIn, Popular Website

"Dear user, Here is LinkedIn. They would like to access your contacts and to send emails on your behalf. Are you OK with that?"

Gmail, 800 Pound Gorilla

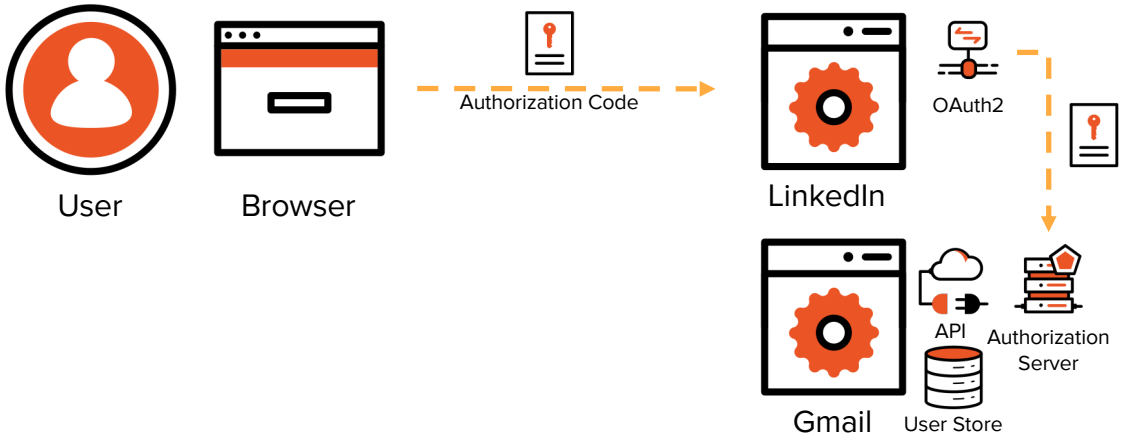
Delegated Authorization



Concepts:

- OAuth2
- Authorization Server
- Clients
- Delegation
- Scopes
- Access Token
- Refresh Token

Delegated Authorization



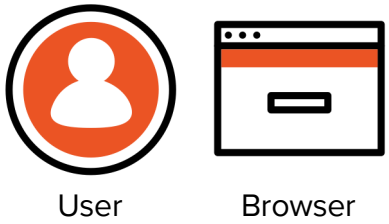
Concepts:

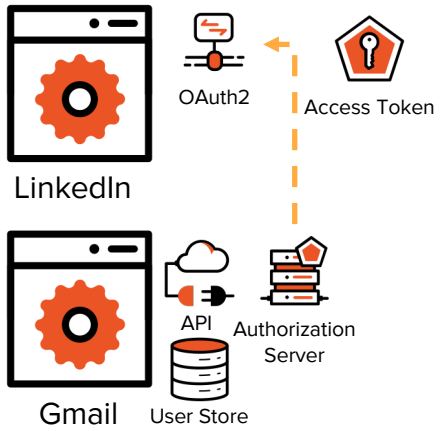
- OAuth2
- Authorization Server
- Clients
- Delegation
- Scopes
- Access Token
- Refresh Token

"Dear Gmail, I am LinkedIn; here is proof. I have a code that proves this user gave consent for me to access your APIs on their behalf."

LinkedIn, Popular Website

Delegated Authorization

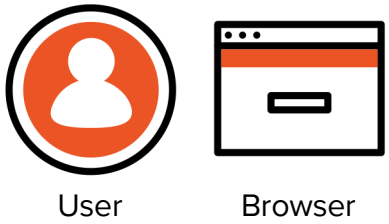


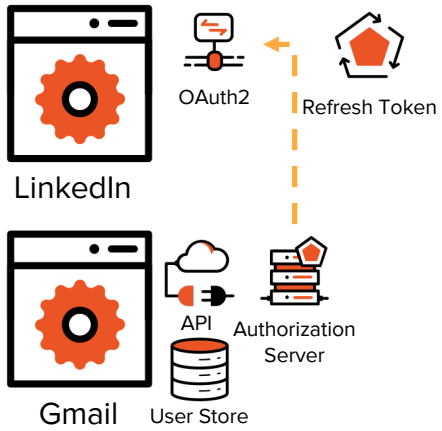


Concepts:

- OAuth2
- Authorization Server
- Clients
- Delegation
- Scopes
- Access Token
- Refresh Token

Delegated Authorization

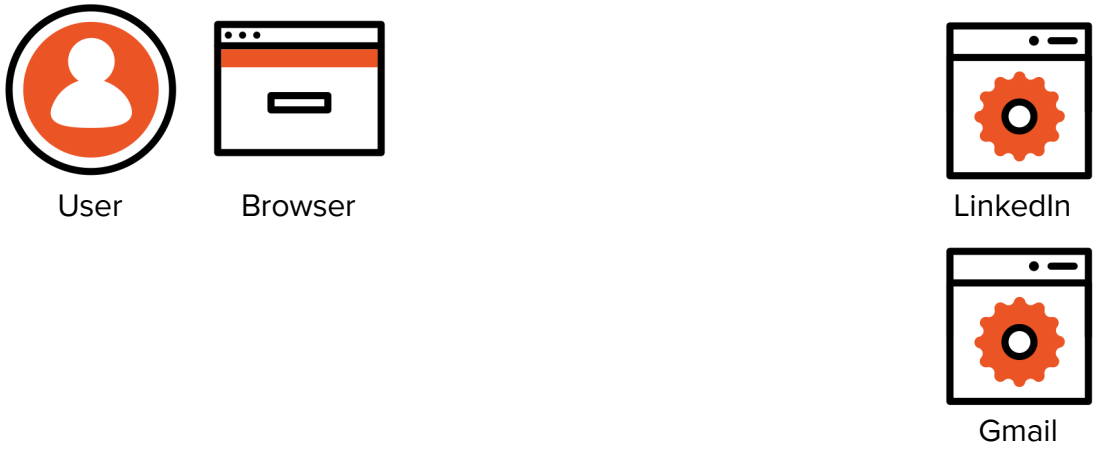




Concepts:

- OAuth2
- Authorization Server
- Clients
- Delegation
- Scopes
- Access Token
- Refresh Token

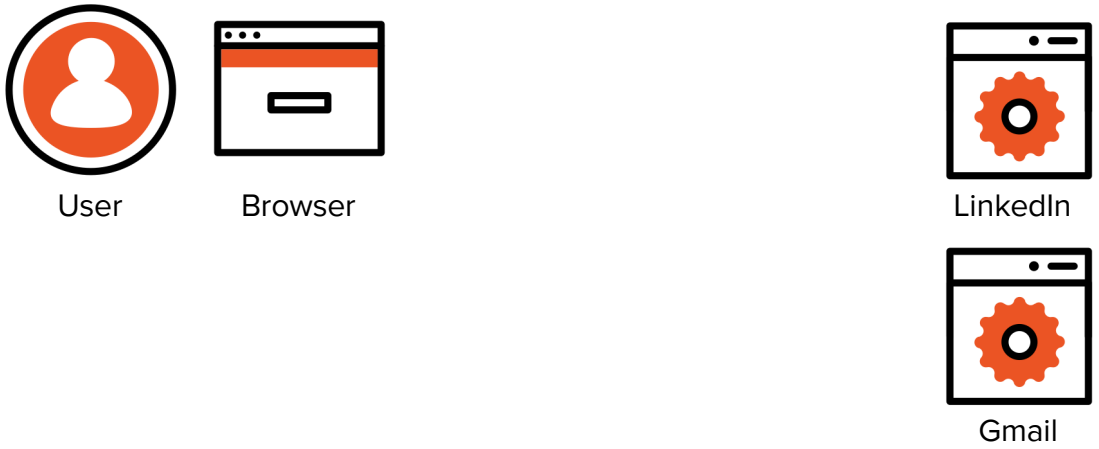
Cross-Domain Single Sign-On



Concepts:

- OpenID Connect
- ID Token
- JWT
- User Info Endpoint

Cross-Domain Single Sign-On



Concepts:

- OpenID Connect
- ID Token
- JWT
- User Info Endpoint

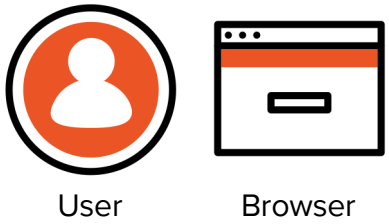
Confused Deputy

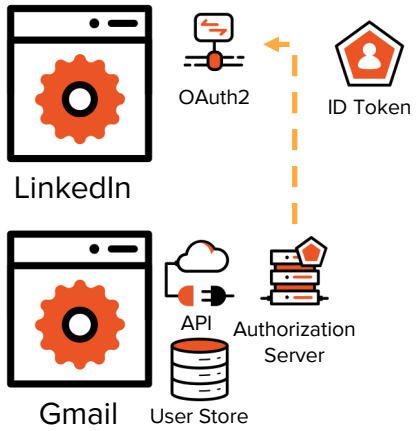
Remember with OAuth the access token is opaque. The token issued by Gmail has no meaning to LinkedIn.

Incomplete Spec

The OAuth access token is opaque to LinkedIn. The only way to use it is to send it back to Gmail.

Cross-Domain Single Sign-On





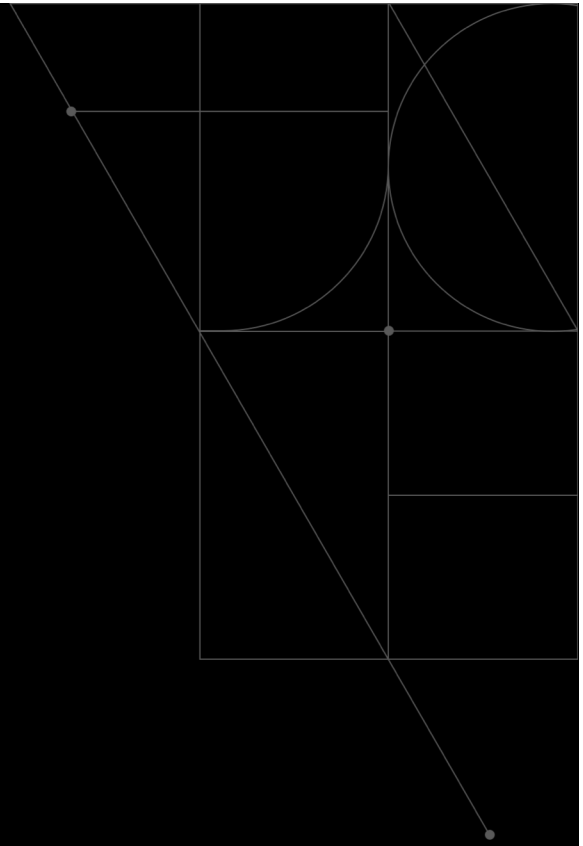
Concepts:

- OpenID Connect
- ID Token
- JWT
- User Info Endpoint

Wrapping Up

This was just a taste of the world of identity and how the industry evolved over the years.

Thanks!



auth0.com

Resources

Typography (Proxima Nova)

Headline 1

Headline 2

Subtitle

Paragraph

Disclaimer

LINK

Color Palette

ELEMENTS #EB5424	ELEMENTS #0D96C6	
TEXT #333333	TEXT #666666	TEXT #CCCCCC
BG #000000	BG #333333	BG #FFFFFF