Authentication & Authorization Options

Julio Rafael Pochet Edmead

CSD 370 – Secure Software Development

Module 1: Assignment 1.2 – Authentication and Authorization

This assignment compares three popular authentication methods to help Mesusa Corporation choose the right access management strategy.

**Overview**

Mesusa Corp wants to step up its security game. They’re looking into three ways to manage who gets access to what: SSO, OAuth, and OpenID Connect. This breakdown explains what each does, how to implement them, and their pros and cons.

**SSO (Single Sign-On)**

SSO lets users sign in once to access many apps. It simplifies login experiences—one password, one login, and you’re good across platforms like Gmail, Slack, or Dropbox.

How to Set Up SSO:

Use an identity provider (like Okta or Azure AD)

Connect apps to the identity provider

Configure SAML or OAuth protocols

Set access rules

**SSO: The Good & The Not-So-Good**

✔ Easy login for users  
✔ Fewer passwords = less reset hassle  
✔ Better control over access  
✘ If SSO goes down, users can’t access anything  
✘ Takes effort to set up securely

**OAuth (Open Authorization)**

OAuth lets one app get permission to use info from another—without sharing passwords. Think: using your Google account to sign into Spotify.

How to Set Up OAuth:

Register your app with the provider (Google, Facebook, etc.)

Get client ID and secret

Handle redirect and token exchange

Use scopes to limit what info is shared

**OAuth: Strengths & Weaknesses**

✔ No need to store user passwords  
✔ Safer user experience  
✔ Widely supported  
✘ Can be complex for devs  
✘ Needs secure token storage

**OpenID Connect**

OpenID Connect builds on OAuth but adds login features. It confirms who the user is and gives some profile info. It’s like OAuth with ID verification.

How to Set Up OpenID Connect:

Use an OpenID provider (Google, Microsoft, etc.)

Set up OAuth 2.0 first

Request ID token with authentication

Verify token and use claims

**OpenID Connect: Upsides & Downsides**

✔ Combines OAuth + user ID  
✔ Simplifies login flow  
✔ Supports mobile and web  
✘ Setup can be confusing  
✘ Still evolving in some areas

**Recommendation for Mesusa**

For Mesusa, OpenID Connect might be the best fit—it provides authentication and access control together. If the goal is just access management between apps, OAuth is enough. SSO works well for simplifying user login across internal enterprise tools.

**References**

NIST. (2023). Digital Identity Guidelines. https://pages.nist.gov/800-63-3/

OAuth.net. (n.d.). OAuth 2.0. https://oauth.net/2/

OpenID Foundation. (n.d.). OpenID Connect. https://openid.net/connect/

Microsoft Docs. https://learn.microsoft.com/

Okta Developer Docs. https://developer.okta.com/docs/