

# SSO – OAUTH – OPENID

A comparison of the  
three technologies

Jason Luttrell  
CSD 370-T301 Secure Software Development  
Module 1.2

---

# UNDERSTANDING SSO, OAUTH, OPENID



## Single Sign-On (SSO)

SSO allows users to log in to multiple applications with a single set of credentials. This simplifies user experience.

## OAuth

OAuth is a protocol that allows secure authorization of resources without sharing credentials. It is widely used for web applications.

## OpenID

OpenID is an authentication protocol that allows users to be verified by third-party services. It enhances security and convenience.

---



---

## KEY DEFINITIONS

### **SSO**


Single Sign-On (SSO) is a session and user authentication service that permits a user to use one set of login credentials to access multiple applications.

### **OAuth**

OAuth is an open standard for access delegation, commonly used as a way to grant websites or applications limited access to a user's information without exposing passwords.

### **OpenID**

OpenID is an authentication protocol that allows users to verify their identity on different websites without having to create multiple accounts.



Username

Password

☒ Remember me [Forgot Password?](#)

[LOGIN](#)

---

# SINGLE SIGN-ON (SSO)

## **Simplifies User Experience**

SSO simplifies the user experience by allowing users to access multiple applications with one login, reducing password fatigue.

## **Improves Security**

SSO improves security by decreasing the number of passwords users need to manage, reducing the number of attack vectors.

The more passwords a user has to manage the more likely poor password practices will creep in to the security culture

---



---

# OAuth EXPLAINED

## **Access Delegation Standard**

OAuth is a standard for delegating access, granting limited access to user information without exposing passwords.

## **Token Issuance**

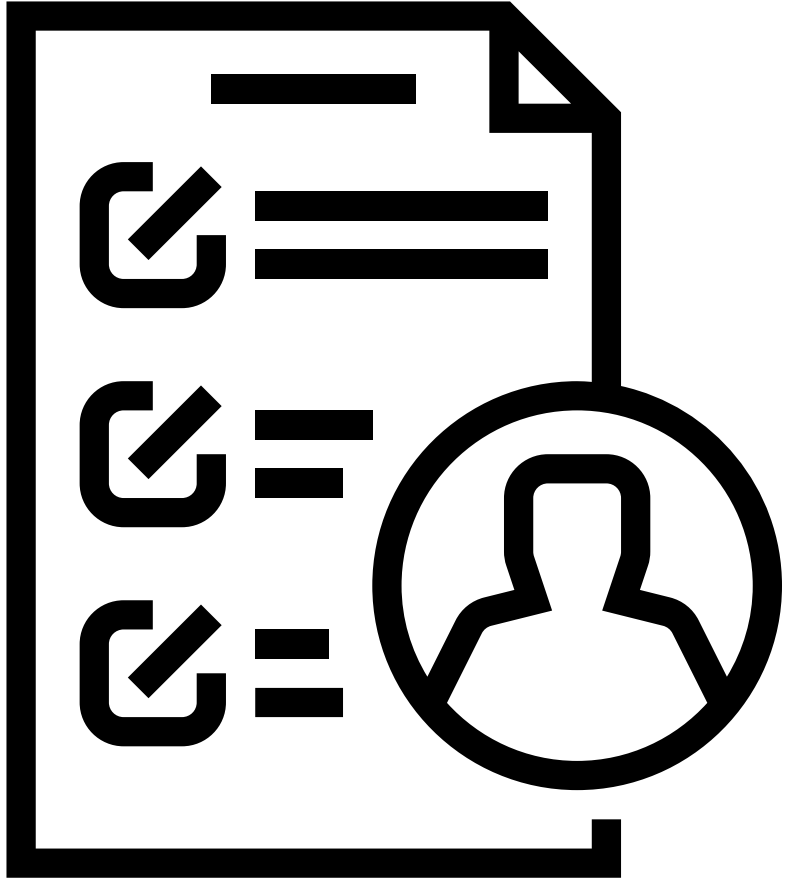
OAuth works by issuing tokens to third-party applications with user consent via an authorization server.

## **User Consent**

The authorization server issues tokens to third-party applications only with the user's consent, ensuring secure access.

## **Examples Include**

- Giving Spotify permission to access your Alexa account
- Using Facebook or Google to log into a webpage



---

# OAuth IS AUTHORIZATION

- OAuth is not an API authentication service. Rather it more about authorization or checking to see what permissions or privileges a user has for accessing resources.
  - For a simple simile, consider the following: authentication is showing your ID to get into an airport while authorization is what allows you to access some areas and not others.
  - The process of authentication is handled by the application or site serving as the identity provider (like OpenID).
  - As an authorization standard, OAuth doesn't manage authentication directly. But it can give already-authenticated users access to appropriate resources.
-



---

# WHAT IS OPENID?

## **Single Login Credentials**

OpenID allows users to log in to multiple websites using a single set of login credentials.

## **OpenID Provider**

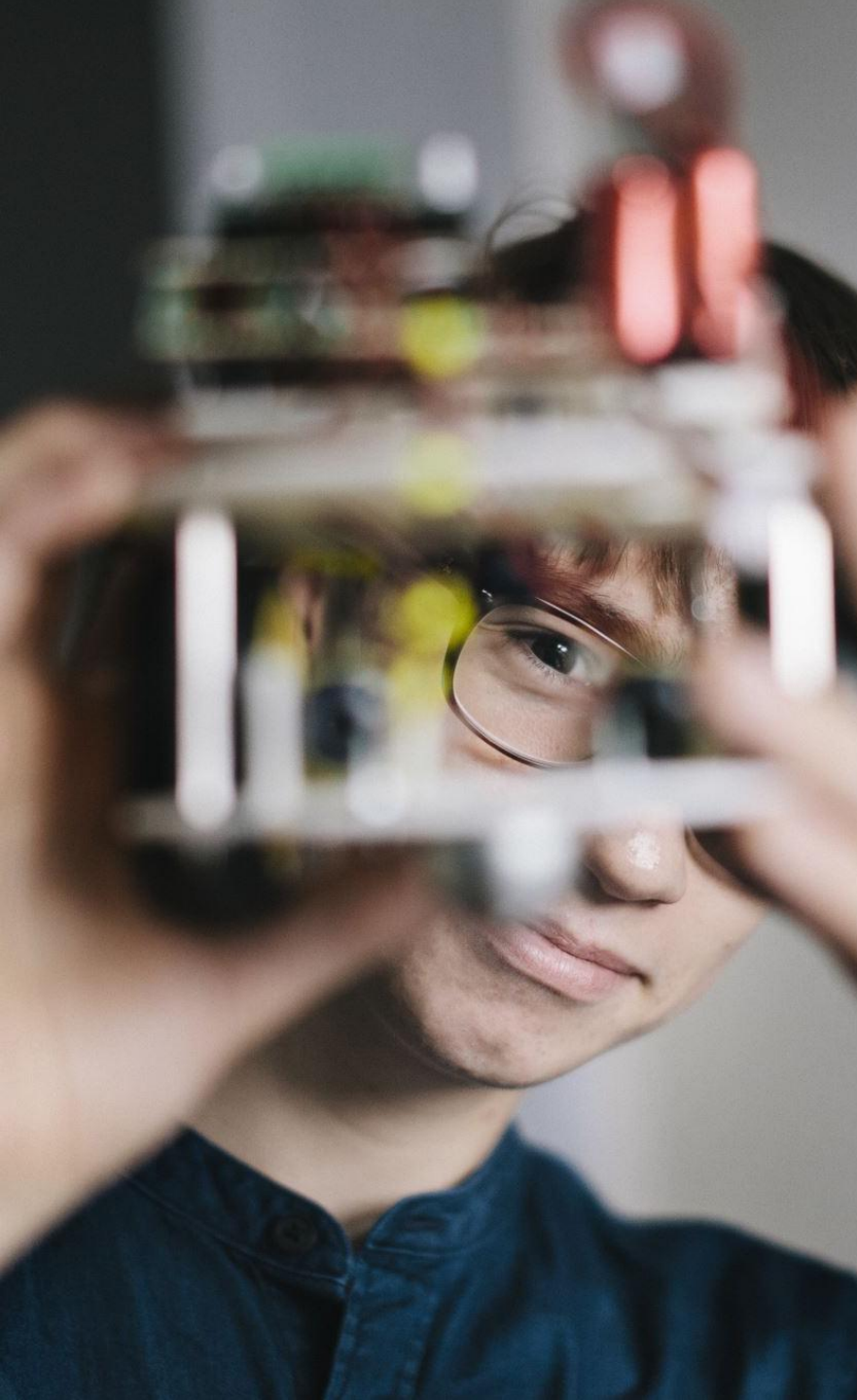
Users authenticate to an OpenID provider, which then allows access to OpenID-enabled websites.

## **Seamless Login Experience**

OpenID provides a seamless login experience across multiple websites by using a single authentication process.

---



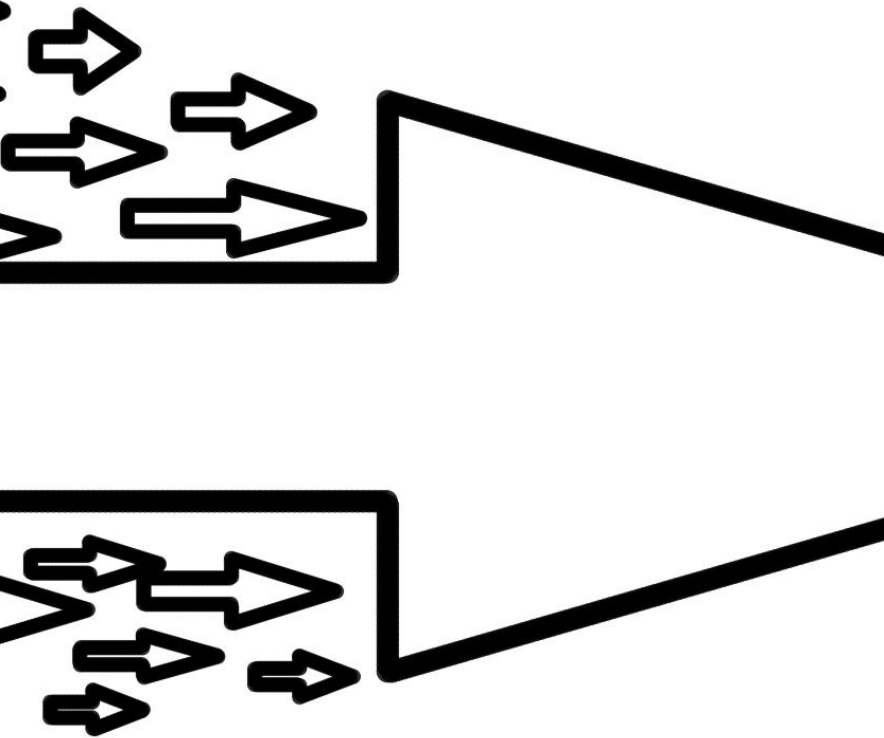


---

# IMPLEMENTING SSO, OAUTH, AND OPENID

- Begin with a clear understanding of user requirements.
- Select a reliable SSO provider that fits organizational needs.
- Integrate OAuth by implementing an authorization server.
- Choose an OpenID provider that aligns with security standards.
- Thoroughly test the integrations to ensure seamless user experience.



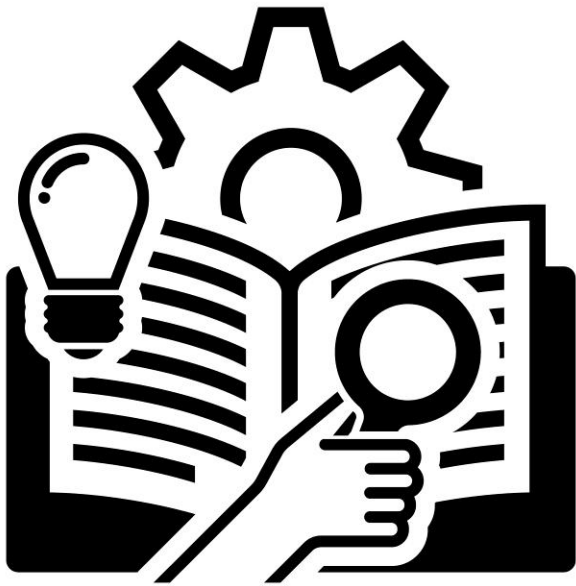


---

## SUMMARY

The combination of OpenID and OAuth to enable your Enterprise SSO is a robust solution that can enhance user efficiency and satisfaction while providing the security needs that Mesusa Corp. requires.

---



---

## REFERENCES

Conklin, W. A., & Shoemaker, D. P. (n.d.). *CSSLP secure software lifecycle professional all-in-one exam guide* (3rd ed.). Retrieved from <https://platform.virdocs.com/read/2096595/2/#/4/4>

Frontegg. (n.d.). *OIDC authentication guide*. Retrieved June 2, 2025, from <https://frontegg.com/guides/oidc-authentication>

Kong. (n.d.). *What is OAuth?* Kong. Retrieved June 2, 2025, from <https://konghq.com/blog/learning-center/what-is-oauth>

---