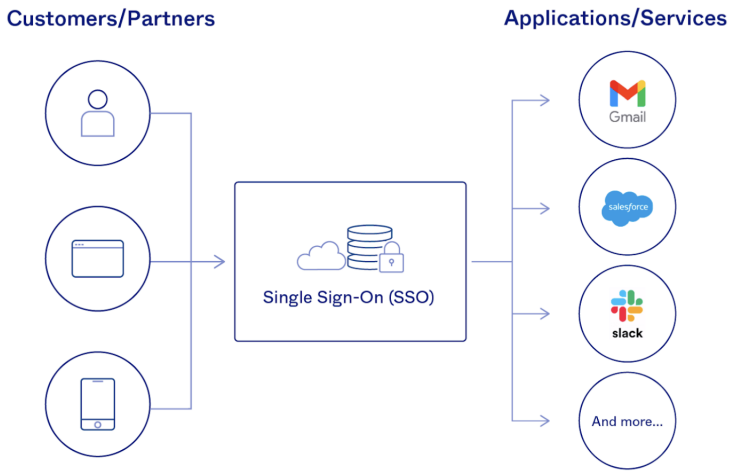
Single Sign-On (SSO)

Overview

SSO is built on the concept of federated identity, which is the sharing of identity attributes across trusted but autonomous systems. When a user is trusted by one system, they are automatically granted access to all others that have established a trusted relationship with it. This provides the basis for modern SSO solutions, which are enabled through protocols like OpenID Connect and SAML 2.0.

When a user signs in to a service with their SSO login, an authentication token is created and stored either in their browser or in the SSO solution's servers. Any app or website the user subsequently accesses will check with the SSO service, which then sends the user's token to confirm their identity and provide them with access.



Types of SSO

- **Security Access Markup Language** (**SAML):** SAML is an open standard that encodes text into machine language and enables the exchange of identification information. It has become one of the core standards for SSO and is used to help application providers ensure their authentication requests are appropriate. SAML 2.0 is specifically optimized for use in web applications, which enables information to be transmitted through a web browser

- **Open Authorization (OAuth):** OAuth is an open-standard authorization protocol that transfers identification information between apps and encrypts it into machine code. This enables users to grant an application access to their data in another application without them having to manually validate their identity—which is particularly helpful for native apps.

- **OpenID Connect (OIDC):** OIDC sits on top of OAuth 2.0 to add information about the user and enable the SSO process. It allows one login session to be used across multiple applications. For example, it enables a user to log in to a service using their Facebook or Google account rather than entering user credentials.

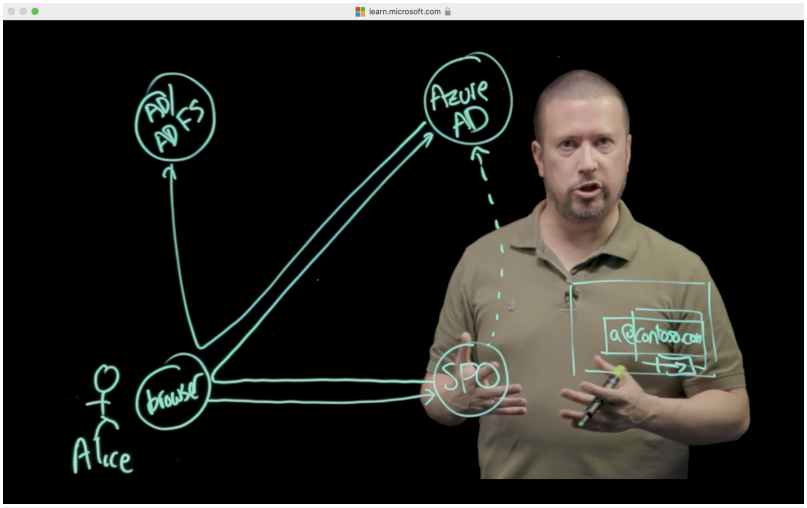
- **Kerberos:** Kerberos is a protocol that enables mutual authentication, whereby both the user and server verify the other's identity on insecure network connections. It uses a ticket-granting service that issues tokens to authenticate users and software applications like email clients or wiki servers.

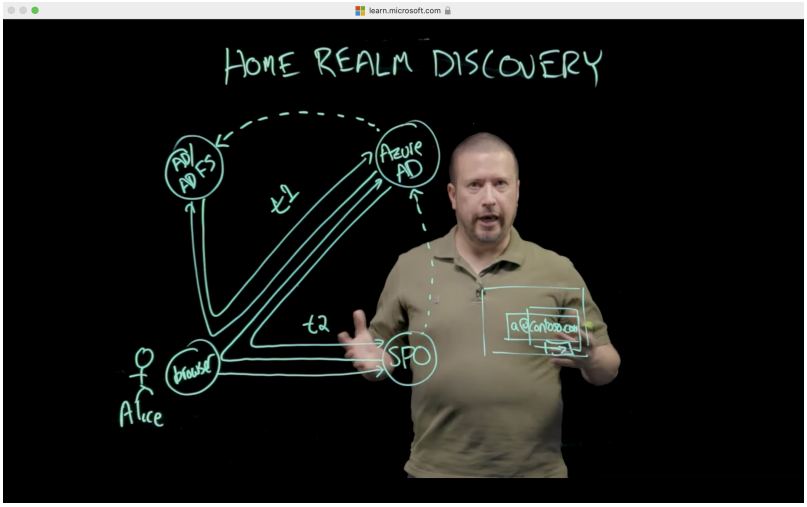
- **Smart card authentication:** Beyond traditional SSO, there is also hardware that can facilitate the same process, such as physical smart card devices that users plug into their computer. Software on the computer interacts with cryptographic keys on the smart card to authenticate the user. While the smart cards are highly secure and require a PIN to be operated, they have to be physically carried by the user—running the risk of being lost—and they can be expensive to operate.

Federation

When you set up SSO to work between multiple identity providers, it's called federation. An SSO implementation based on federation protocols improves security, reliability, end-user experiences, and implementation.

With federated single sign-on, Azure AD authenticates the user to the application by using their Azure AD account. This method is supported for SAML 2.0, WS-Federation, or OpenID Connect applications. Federated SSO is the richest mode of SSO. Use federated SSO with Azure AD when an application supports it, instead of password-based SSO and Active Directory Federation Services (AD FS).





References

Reference	URL
What Is Single Sign-On (SSO)?	https://www.okta.com/blog/2021/02/single-sign-on-sso/
What is single sign-on in Azure Active Directory?	https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on
Authentication fundamentals: Federation | Azure Active Directory	https://www.youtube.com/watch?v=CjarTgjKcX8&t=378s