SSO

Single Sign On

- Single Sign On (SSO) is a type of authentication in which a user logs in to one system and is automatically granted access to other services.

- Single Sign On is typically found in enterprise environments where employees access numerous apps and services on a daily basis.
  - Rather than having an employee create a separate set of credentials for each app, they simply login once and can access any app the IT administrator has given them access to.

Example of SSO

- You have most likely come across Single Sign On before, even if you didn't know it at the time.

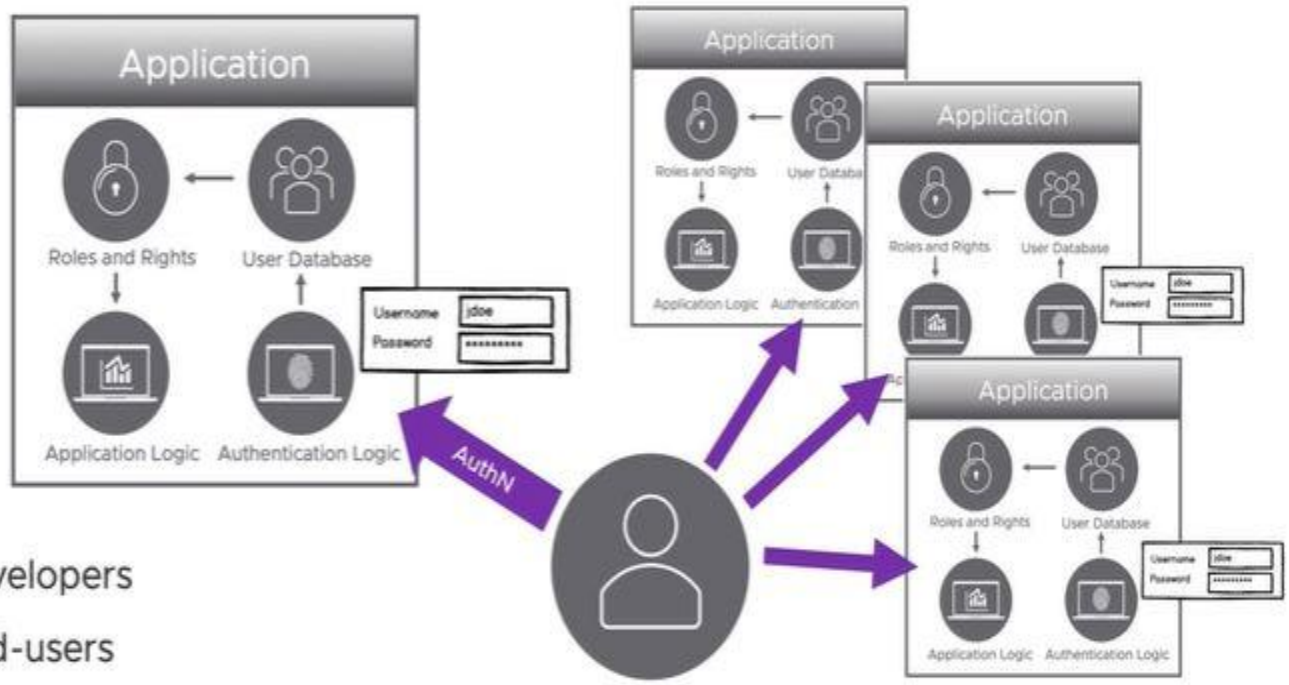
- Take Google for example. Upon logging in to one Google service such as Gmail, you are automatically authenticated to YouTube, Docs, sheets, Google Analytics, and other Google apps.

- Likewise, if you log out of your Gmail or other Google apps, you are automatically logged out of all the apps.

Why SSO?

- Earlier each application had its business logic along with its user database and roles and rights for each user.
- As the number of applications started increasing the complexity of managing each user and applications rights and role also started increasing.
- It became **painful for developer** who mainly cared about business logic is now in charge of protecting the user store.
- It became **painful for the users** to remember so many credentials for each applications often resulting in weak password and reuse of passwords.
- It became **painful for administrators** for provisioning user for each application and also if someone leave they have to de-provision the user from each application.

Why SSO



Painful for developers

Painful for end-users

Painful for the administrators

Different Authentication methods

1. **Username and password:** Username and password authentication is the tried and true method of protecting applications.

- Enhancing the username and password authentication flow can be done by:
  - Enforcing strong password requirements,
  - Forcing password changes every so often,
  - Preventing password reuse etc..

Different Authentication methods

2. **Social Accounts:** Social authentication has gained prominence in the last few years because it allows organizations to authenticate users with existing accounts.

- Social authentication gets its name from the fact that companies that implement this type of authentication usually allow users to login with social network accounts such as
  - Facebook,
  - LinkedIn,
  - Twitter
  - Google etc.

Different Authentication methods

3. **Passwordless:** Here the user simply provides their username and with that info system generate a one time passcode reffered to as OTP and is delivered via mail, SMS or dedicated app .

- The benefits of passwordless authentication are twofold.
  - One, the owner of the system does not have to take the burden of storing and protecting user passwords.
  - Two, users are not required to remember yet another password.

Different Authentication methods

4. **Multifactor Authentication:** Although multifactor authentication is not a type of authentication in the traditional sense, it deserves special mention as it augments existing authentication methods and makes them more secure.

- The most common type of multifactor authentication is two‐factor authentication (2FA), where in addition to your password a second set of credentials like OTP, Security questions etc..

SSO and Identity Federation

- Identity federation and Single Sign On go hand-in-hand.
- Single Sign On enables a user to login with different authentication workflows and access multiple applications. This is possible through **identity federation** and a **centralized authentication server.**
- Identity federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources.

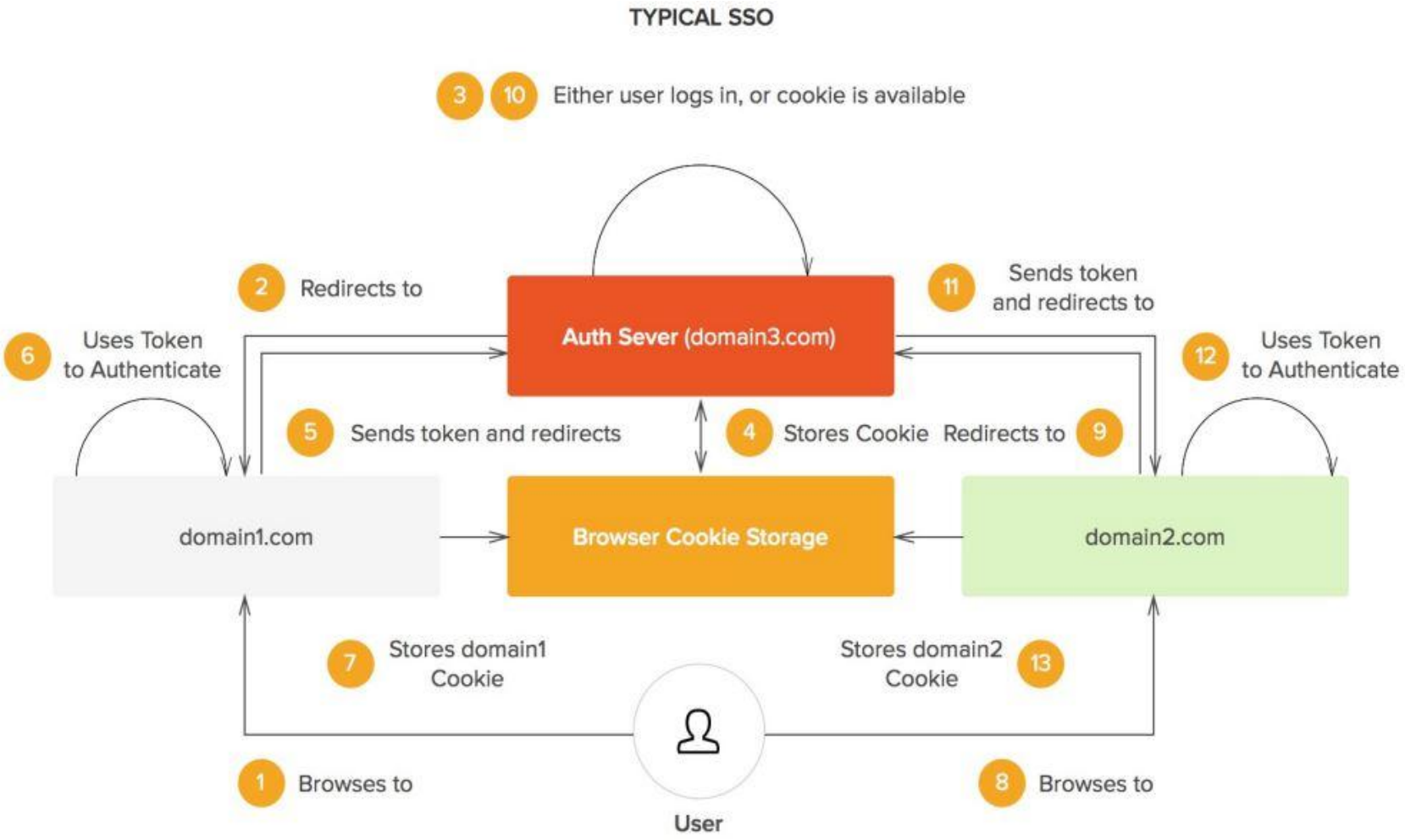
SSO Vs Non SSO system

- In a non-SSO application, a user will login and their credentials will be sent to the backend system for verification. This backend system is usually the actual application.

- In the SSO use case, the user credentials are sent to a centralized authentication server, and upon verification, this centralized server grants the user the right to access the application they are attempting to log in to.

Non SSO scenario

SSO scenario



Identity Protocols and Providers

Protocols

- SAML
- WS-Fedration
- OpenID Connect/ Oauth
- Lightweight Directory Access Protocol (LDAP)
- SCIM

Providers

- Database/Local
- Microsoft-Active Directory, ADFS, Azure AD
- Social Identity Providers
- Jumpcloud

Identity Provider

- The term *Identity Provider*, abbreviated as IdP, refers to a subcategory of IAM solution that is focused on managing core user identities.

- Also known as directory services, the IdP acts as the source of truth for authenticating user identities.

- It lays the foundation of an IT organization's overall identity and Access management infrastructure.

- Other IAM categories and solutions, such as **IDaaS**, PIM/PAM, MFA/2FA, and others are often layered on top of the core IdP

Identity Provider (Contd...)

- **1. Database/Local:** A common way of managing identity is through a local database which is only concerned with users and their roles.

- Organizations requiring full control over their data will often opt for this option for their identity provider.

- Users typically log into the database via username and password authentication.

Identity Provider (Contd...)

2. **Microsoft-Active Directory, Azure AD:** Active Directory is one of the most popular identity providers in the Microsoft Enterprise space.

- Active Directory worked with Windows Server technologies to provide Single Sign On functionality to not just web applications but the entire Windows ecosystem.

- In recent years, Microsoft has begun offering their various online services like Azure Active Directory, bringing their tried and true identity provider to the cloud.

Identity Provider (Contd...)

3. **Social Providers:** Social providers can often make for great identity providers. Social providers, like Facebook or Google, typically make use of the OAuth protocol for managing user identity.

- The benefit of using a large social provider as an identity provider is that these organizations typically have some of the best security standards for user accounts in the world.

Identity Provider (Contd...)

4. **JumpCloud:** JumpCloud is a zero-trust directory platform that customers use to authenticate, authorize, and manage users, devices, and applications.

- They do it all through a common directory in the cloud, instead of through legacy, on-premises IT systems .

- JumpCloud has a global user base of more than 180,000 organizations.

Use Cases of SSO

1. **SSO for Organizations:** From small startup to large enterprise, SSO enables the consolidation of user identity and management.

- Application used like Email, file hosting CRM software, etc.

- Consolidating identity in an organization through SSO will require a centralized identity provider and depending on your existing infrastructure you are likely going to want to use SAML or WS-Federation.

Use Cases of SSO

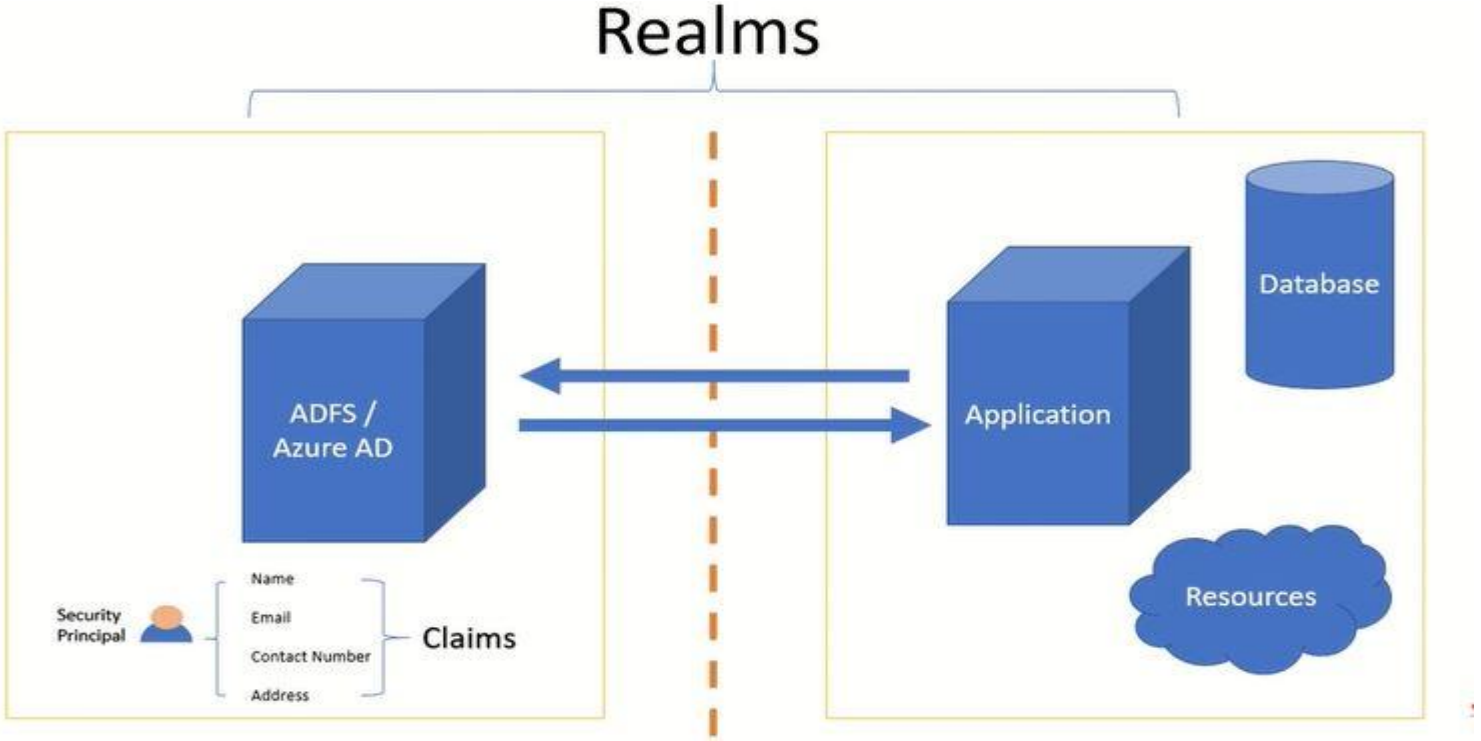
2. **SSO for applications:** If your organization develops applications, Single Sign On can be both a differentiator and a requirement.
   - **Business to Customer (B2C):** Building applications for consumers, such as e-commerce or media applications, means getting the user experience right.
   - **Business to Business (B2B):** The demand for Single Sign On in the B2B space is on the rise. This represents both business opportunity as well as increased revenue potential.
   - **Business to Enterprise (B2E):**Single Sign On is pretty much a requirement when selling to the enterprise. Large enterprises demand governance over their users, and the only way to ensure compliance is through SSO.

What is Federation?

- Federation
  - A collection of realms/domains that have established trust
  - The technology and business arrangements necessary to interconnect users, applications, and systems
- Federated systems can interoperate across organizational and technical boundaries (i.e., various operating systems or security platforms)

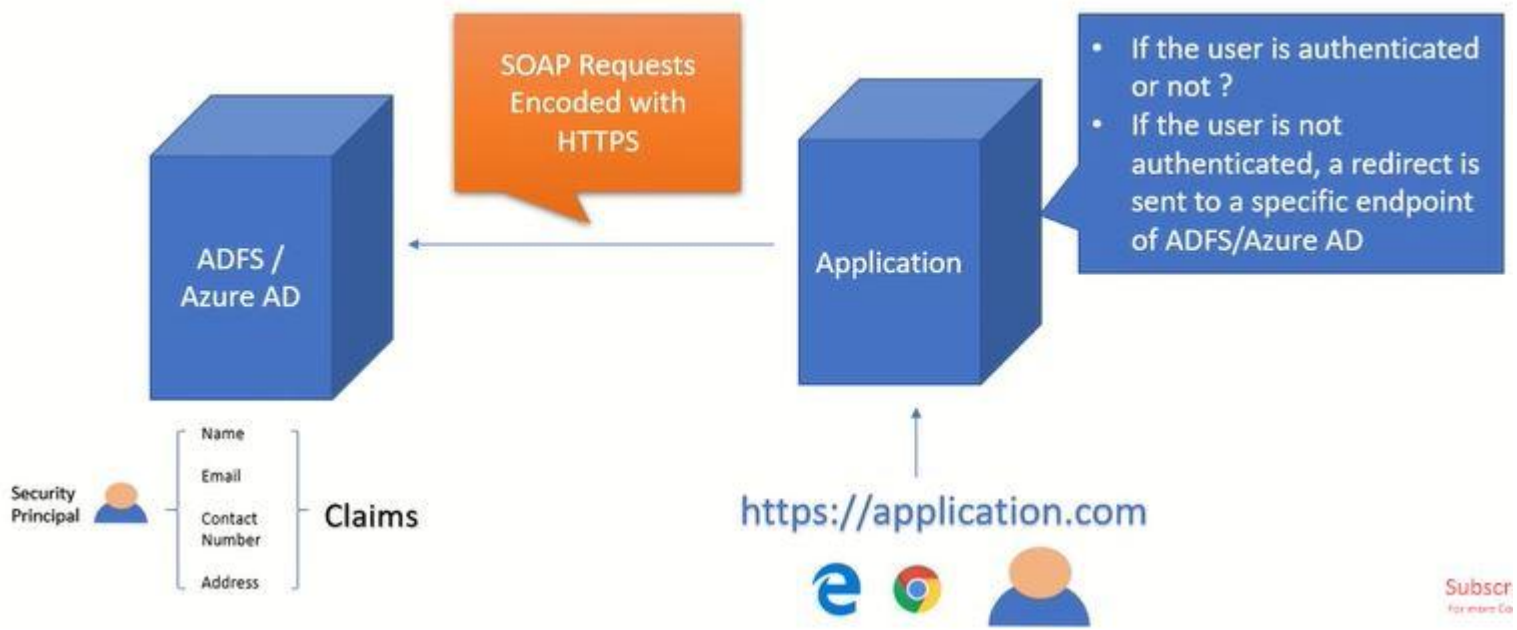
Federation

- Access to protected resources can be granted to ‘security principal’s existing on different realms.



How it works?

- SAML/ WS-fed are the protocol used by the application/service provider and the identity provider to receive and send SOAP request/response in HTTPs.



Federated ATM Network