IDENTITY & ACCESS MGT

Single Sign-On Vs Federated Authentication

Kayathiri Mahendrakumaran Follow

Dec 26, 2020 · 4 min read ★

Fig.1. Login with Passwords

In this article, we will have a quick overview on traditional identity management, drawbacks in it and the remedies.

If you want to create accounts in multiple applications and have to remember the credentials for all accounts. It will be easy to remember credentials for some accounts. **If you have hundreds of accounts, can you remember the credentials?.** No. If you have to maintain 100+ accounts, you may give simple passwords or the same passwords to all accounts. This may result for high Chances of data breaches. And this approach has minimum user experience because you have to remember credentials every time you login. Here the Single sign-on come to play.

What is Single sign-on?

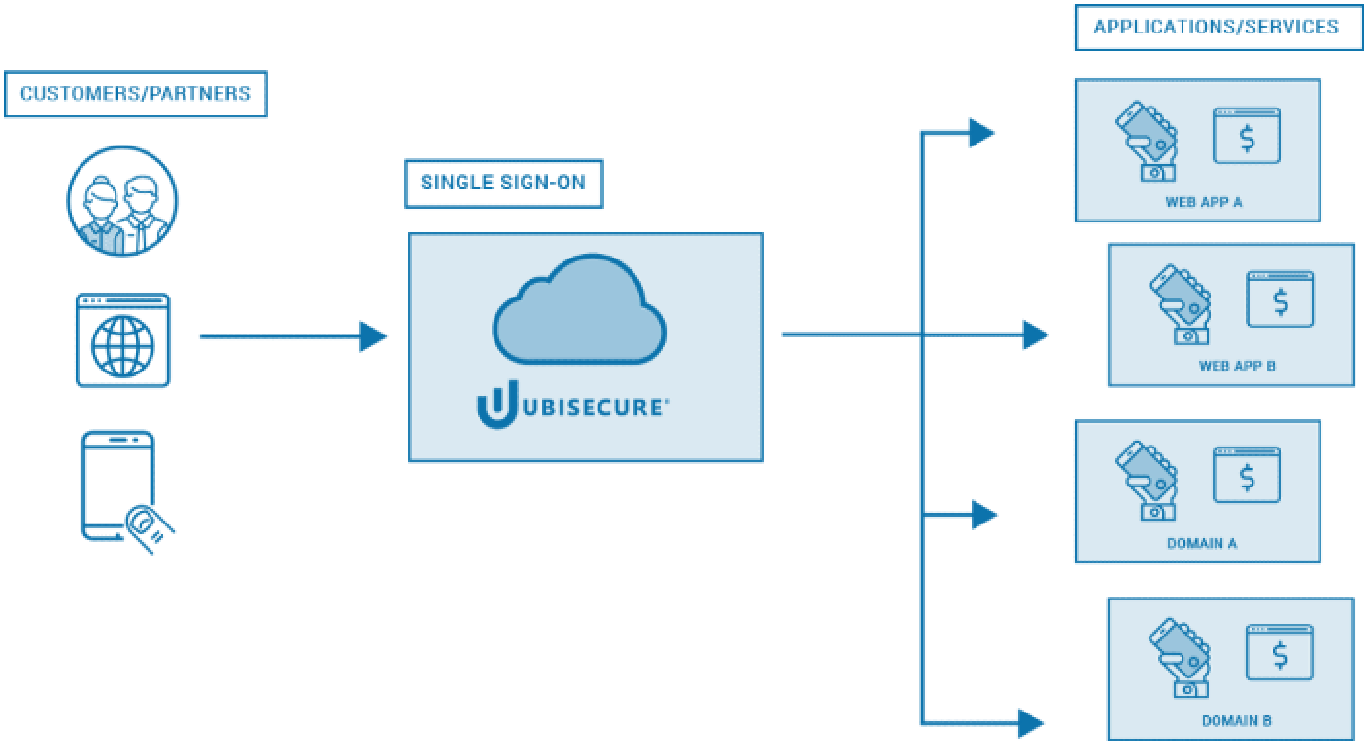

Fig.2. Single Sign-On

Single sign-on (SSO) allows people to login to multiple accounts with only on ID and password. People can login once and access the services multiple times. No need for repeatedly entering the credentials. Just like the name SSO, helps to access various applications with only one credentials. This makes the users to work easily and reduce the overhead of remembering each and every passwords. This service can be used in organizations, enterprises as well as individuals to ease their work and to manage their accounts efficiently. Here, the application server get the credentials of a user from dedicated SSO server. So it prohibits form prompting for the password in the specific session.

Social applications like Facebook, Twitter, Google and LinkedIn implements SSO services in order to allow the users to login to other third party applications using the credentials of social applications. It will be easy and convenience to them but it may be vulnerable to security issues like single point of failure.

Therefore, security professionals say that we have to avoid SSO because if an attacker hacks and get access to credentials of SSO, they can get the access to all other applications.

How does it work?

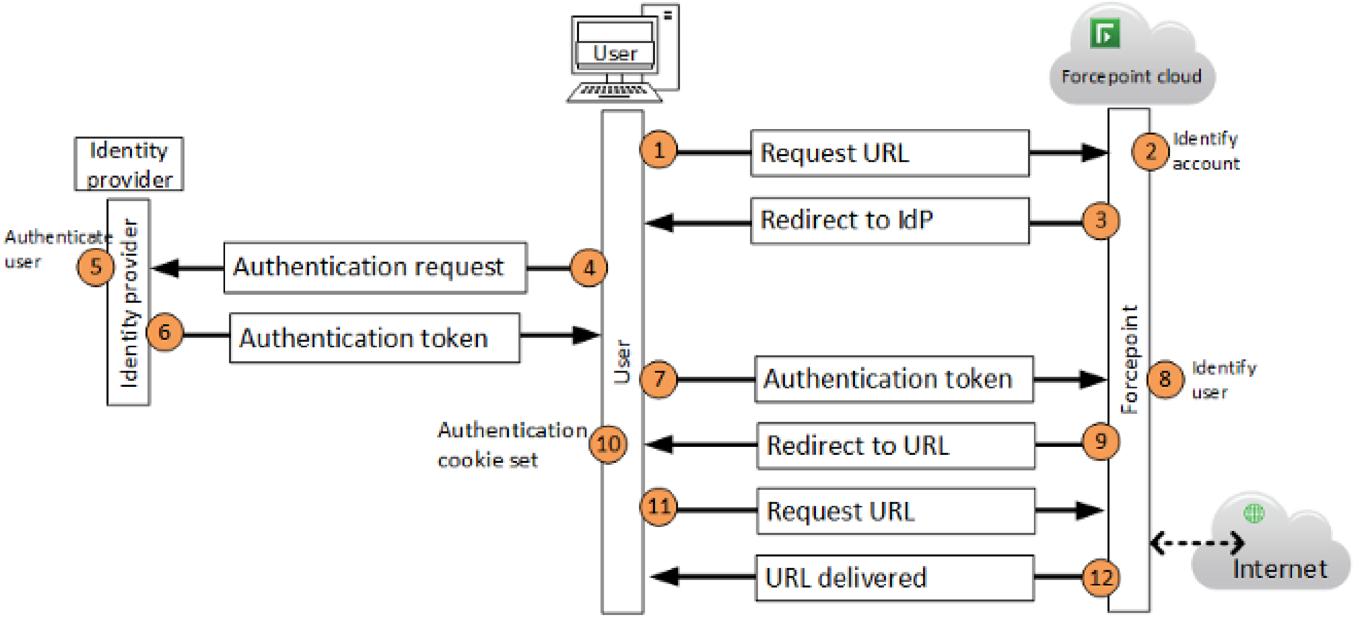

Fig.3. SSO Flow

Think that, you are trying to login or access an application (via service provider- SP), the SP will immediately requests the identity manager or identity provider to authenticate your identification. Then, the identity provider will response to the SP. Finally, the SP will verify the response sent by identity provider and allow you to access the service.

What is Federated Authentication (Federation Identity Management — FIM)

When one server is responsible for authenticating the credentials of a user is known as Federation. Here, one system requests the second system and send the information of the user. The second system will verify the user credentials and sends a message to the first server. So, **does it mean than SSO and Federated Authentication are same?** No, there is a key difference.

There is a small difference between SSO and FIM is SSO authenticate the credentials of the users across numerous systems in an organization but FIM provide the user to access applications across different enterprises with single sign-on. Therefore, we can say that SSO is a function of FIM. However, both these features reduce the obstacles faced by users in user experience.

Components of Federation

Identity Provider (IDP) is one of the component. Application is considered to be as Service Provider (SP). The message that is passed between them is assertion. Assertion will contain all the information required by SP to create a session. These details are signed cryptographically. Therefore, there is a trust between IDP and SP. So, the SP is free and do not interfere in the authentication process. SP will blindly trust IDP and allows the user to access the service if the user is authenticated by IDP.

The first system is called the Identity Provider, or *IDP*. The application is called the Service Provider or *SP*. The message that is sent between the systems is called an *assertion*. The assertion contains the account name of the user along with other attributes that the SP needs to create a user session. It is cryptographically signed so the SP can trust that it came from the right IDP. Notice that the SP has nothing to do with the authentication of the user. It trusts the IDP to take care of that. All the SP cares about is that the user was authenticated properly.

Multiple SPs can be federated with a single IDP. When user try to access an application, IDP will send their identity to that application. So now there is a single point of control for the user.

Advantages

- Reduce the time in entering the password several times.
- Reduce the overhead of users by making the users to remember only few usernames and passwords.
- Can access the 3rd party sites because there is no need to store the credentials externally.

- Provide a seamless processing of accessing service rather than entering passwords repeatedly.
- Leads to fewer complaints or trouble about passwords for IT help desks.

Disadvantages

- Security issues — when an attacker gets the control over SSO credentials, all the accounts can be compromised.
- It does not address certain levels of security each application sign-on may need.
- If availability is lost, then users are locked out of the multiple systems connected to the SSO.
- If unauthorized users gain access, then they could gain access to more than one application.

References

1. https://searchsecurity.techtarget.com/definition/single-sign-on
2. https://www.okta.com/identity-101/federated-identity-vs-sso/
3. https://www.okta.com/blog/2019/05/what-is-federation-and-why-should-your-apps-support-it/

Single Sign On   Federated Identity   Authentication   Federated   Identity Management