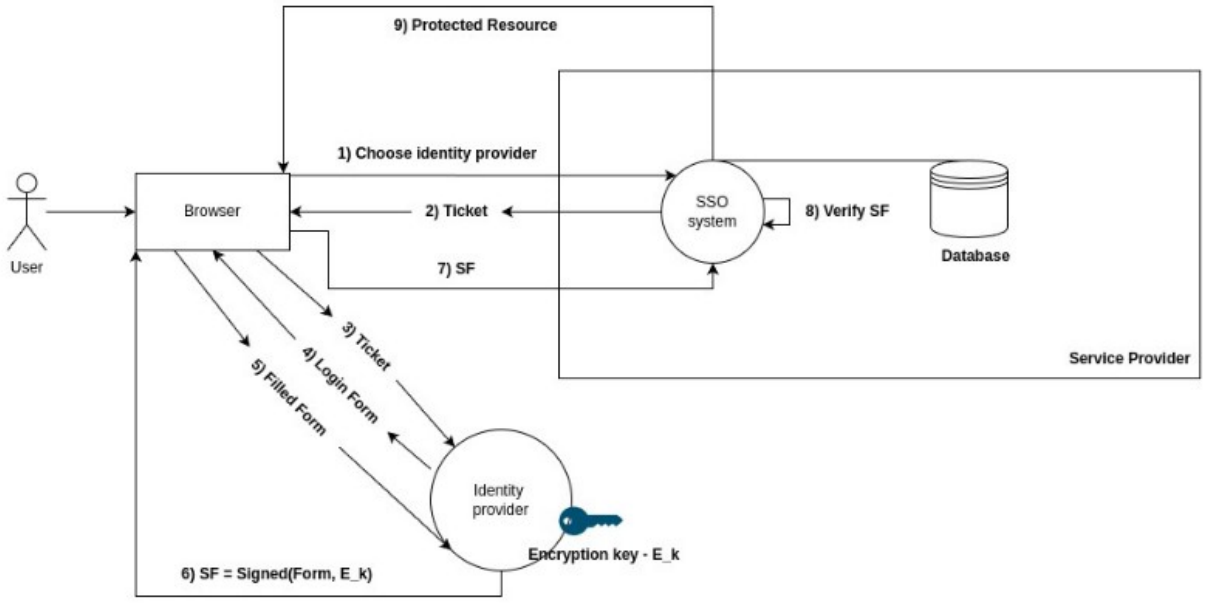
SINGLE SIGN-ON (SSO) authentification system

Types:

- SAML
- OAuth
- OIDC
- Kerberos

Entities:

1. Identity provider
2. Service Provider or information system
3. User browser

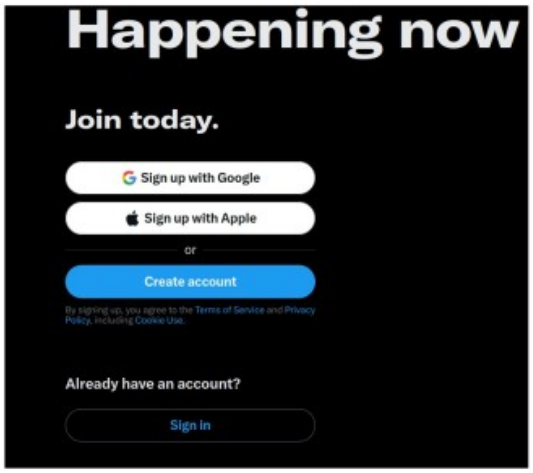


The Single-Sign-On (SSO) authentification process is the process where user identity verification is done through a third party or Identity Provider. In the usual authentification process, user credentials are held directly with the service provider. In SSO setup the credentials are held with the identity provider who identifies the user on behalf of the Service Provider. The Service Provider generates a “ticket” which the user forwards to the identity provider. The result of the authentification process with the Identity Provider is a signed ticket (signature) which ensures the integrity of the message. The Service Provider verifies the signature to verify the integrity requirement or that the message wasn’t tempered along the way. The verification step is done with public key cryptography where the SSO subsystem of the service provider retrieves the public key of the identity provider and compares the hash of the given data with the signature. When the verification process is done, the

protected resource is passed to the user. From the security perspective the SSO system is much more effective when the user has a lot of digital identities and enables more smoother transition between identities. On the other hand, the user puts all his trust in the hand of the single identity provider which in some cases could be bad and could give him information about all the services which user is using. If the identity provider is hacker, that would lead to the leakage of all other services.

How Single Sign in works?

When entering into information system (IS) user has several login options to choose from. He makes a choice, then the IS returns him a ticket which he needs pass to the identity provider. Identity provider are usually Big Tech companies. For example, to enter into X social media we have several options:



We have direct mean to enter into information system or we can use sign in on behalf of the Google or Apple. When we use the login on behalf of some company we are reusing password which is stored on their system.

When we choose one of the option we generate a referral ticket, which is the passed to the identity provider. There we need to pass the credentials, identity provider creates a signature which is then used as the entrance into information system IS.