**SSO – SINGLE SIGN ON**

Single sign-on (SSO) is an identification method that enables users to log in to multiple applications and websites with one set of credentials.

Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials -- for example, a name and password -- to access multiple applications. SSO can be used by enterprises, smaller organizations and individuals to ease the management of various usernames and passwords.

**How single sign-on works**

Single sign-on is a federated identity management (FIM) arrangement, and the use of such a system is sometimes called identity federation. OAuth, which stands for Open Authorization and is pronounced "oh-auth," is the framework that enables an end user's account information to be used by third-party services, such as Facebook, without exposing the user's password.

OAuth acts as an intermediary on behalf of the end user by providing the service with an access token that authorizes specific account information to be shared. When a user attempts to access an application from the service provider, the service provider will send a request to the identity provider for authentication. The service provider will then verify the authentication and log the user in.

**Types of SSO configurations**

Some SSO services use protocols, such as Kerberos, and Security Assertion Markup Language (SAML).

* SAML is an extensible markup language (XML) standard that facilitates the exchange of user authentication and authorization data across secure domains. SAML-based SSO services involve communications among the user, an identity provider that maintains a user directory and a service provider.
* In a Kerberos-based setup, once the user credentials are provided, a ticket-granting ticket (TGT) is issued. The TGT fetches service tickets for other applications the user wishes to access, without asking the user to reenter credentials.
* Smart card-based SSO will ask an end user to use a card holding the sign-in credentials for the first log in. Once the card is used, the user will not have to reenter usernames or passwords. SSO smart cards will store either certificates or passwords.

**Advantages and disadvantages of SSO**

* It enables users to remember and manage fewer passwords and usernames for each application.
* It streamlines the process of signing on and using applications -- no need to reenter passwords.
* It lessens the chance of phishing.
* It leads to fewer complaints or trouble about passwords for IT help desks.