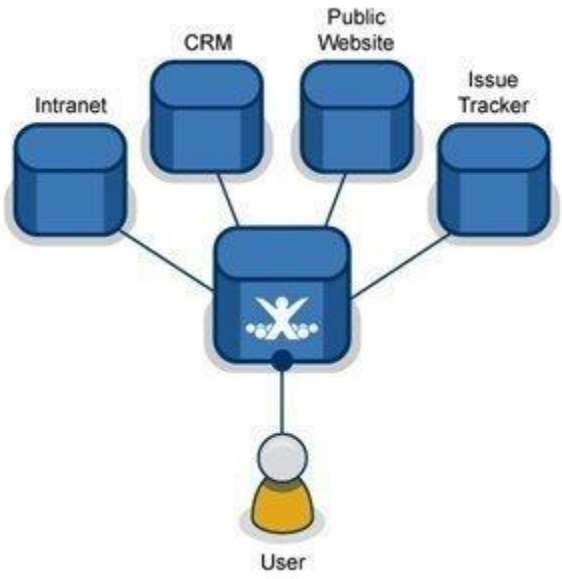
Single Sign-On

Single Sign-On is a concept that allows an end-user to access multiple, related but independent, software applications using a single account. That is, an end-user logs into his/her account only once and then access multiple applications without needing to login again. Single Sign-On is often abbreviated *SSO*.
One the same line, Single Sign-Off is a concept where an end-user logs out from one application and he/she is automatically logged out of all other related applications.

Therefore, an end-user receives only one username-password combination which works effectively across multiple applications. It basically manages identity of end-users in an effective and secure way.

Different applications may use different security mechanism to store user credentials. However, Single Sign-On takes care that irrespective of differences in authentication processes, everything is well translated internally to be in sync with everyone.



Single Sign-On is quite helpful to end users. Few of its major advantages are:

- End user does not have to remember multiple usernames and passwords.
- End user does not have to type-in usernames and passwords every time he/she visits a new application.

- Back-end support can be effectively managed. That is, users won't make multiple support calls for different usernames and passwords.
- The authentication process can be merged into a single component, which acts as a gateway for every other application.

Although many are adapting Single Sign-On in their services, there are few negative impacts.

- Keeping all authentication components and credentials in one place can be risky. If that's hacked or compromised, your access to multiple applications will be open and vulnerable.
- When services make use of Open ID, Google ID or Facebook ID, they rely entirely on them. Giving all data to them can be risky in future.

The two methods utilized by Single Sign-On systems are:

- Password synchronization – The Single Sign-On system *copies* the username and password configuration to each system.
- Centralized account management – Each system is configured to query a central database for userauthentication and authorization.

Single Sign-On systems have the promise of saving IT organizations significant resources in terms of lost user time and reduced password resets. In addition, Single Sign-On systems can significantly increase the security of an IT environment.

Source: http://www.tech-faq.com/single-sign-on.html