

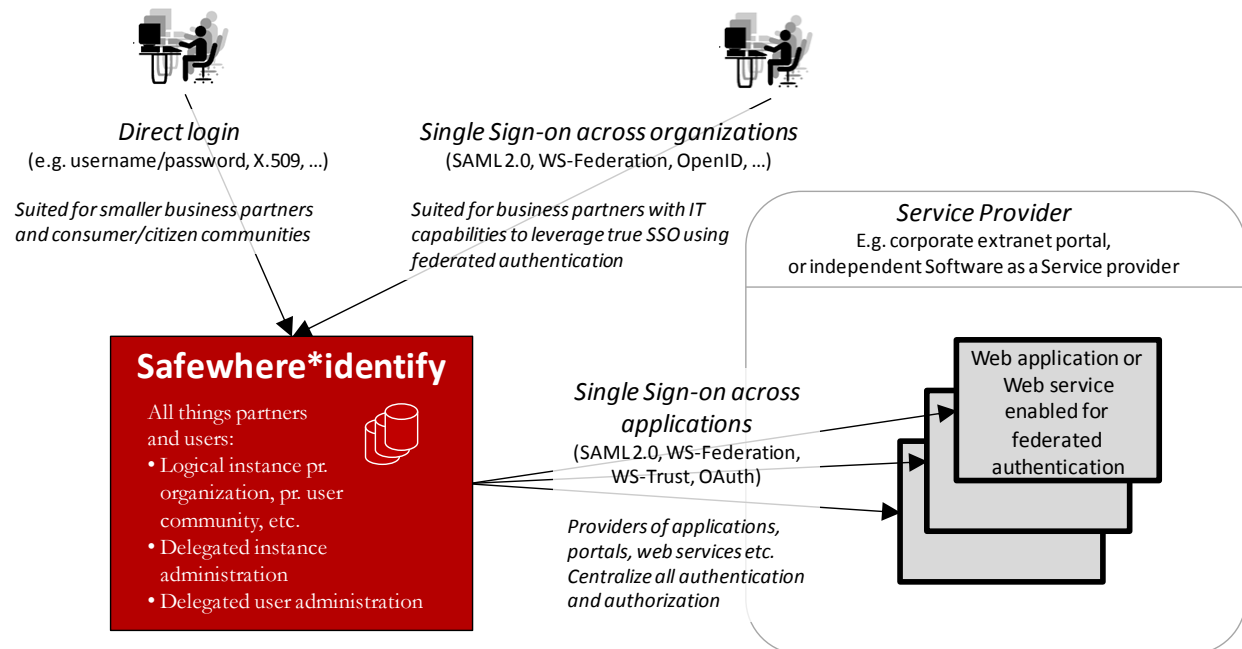
Externalized user administration and identification with **Safewhere*identify**

Safewhere*identify is a new kind of user identification and administration service providing for externalized and seamless authentication and authorization across organizations and the web services consumed.

With Safewhere*identify an organization may handle user identification and administration centrally and external to all web applications and web services. Safewhere*identify supports any kind of authentication including traditional methods such as username/password and X.509 as well as various *identity federation* mechanisms.

Selected benefits and advantages include

- *Self service user administration.* Safewhere*identify provides a separate instance per organization for authentication and maintenance of user attributes. Each instance belongs to, and is administered by, one organization.
- *Externalization of authentication.* Applications and services move all authentication to the Safewhere*identify “identity broker”, which in turn integrates with the desired authentication mechanisms and user databases
- *Application integration.* As more and more of your applications leverage the new identity solution, your users will experience seamless single sign-on across applications. Safewhere*identify provides identity conversion/mapping to successfully transfer identities between applications.



Logical identity flow from users to web applications

- *Provided both “as a service” and as traditional on premise software.* Due to the unique and standards compliant architecture and communication patterns, Safewhere*identify may equally well be leveraged as an external service (Software as a Service) or as software installed in your own infrastructure. Whichever is chosen has no effect on feature set or security.
- *Self registration of organizations and users.* Workflows support the signing of new organizations – e.g. new business partners – as well new uses of each organization. The first requires review and approval of you whereas the latter leverages the distributed nature of user administration and leaves it up to the user’s home organization.

Key capabilities

Safewhere*identify provides a rich set of features with the aim to remove entirely all need for service provider local administration and authentication of users. Key capabilities include

- *User management* including self registration, assignment of attributes including roles and permissions, password management (when required by authentication mechanism), etc.
- *Traditional user authentication.* For external users not ready for federated authentication, Safewhere*identify provides integration to local user account stores, thus allowing for seamless leverage of your existing investments in user directories. Through the published plugin interface, new authentication mechanisms
- *Federated identities.* User identities may be seamlessly and securely transferred from their origin – the place where the user first logged in – to the consuming applications, thereby removing the need for operation and administration of a local user database. This is often referred to as Web SSO
- *Browser based federation.* Safewhere*identify implements a number of federation protocols including SAML 2.0 and WS-Federation for browser based authentication
- *Federated authentication for Web services* – aka. “active” federation – through WS-Federation/WS-Trust and OAuth
- *Claims mapping.* Applications leveraging Safewhere*identify potentially all need different kinds of user attributes, or *claims*, and often with slightly different names and formatting. (E.g. a role to one application is a group to another). Safewhere*identify provides delegated administration of attribute mappings to transparently and correctly transfer identities between applications.

The broader Safewhere advantage

The full *Safewhere Access Management* suite provides a complete solution aimed at removing all access related concerns from web and service architectures.

Using products such as *Safewhere*identify*, *Safewhere*authorize*, and *Safewhere*protect* central access models drive application specific access control policies, which are rigidly enforced by protection agents guarding access to applications and services.

To learn more please contact Safewhere at sales@safewhere.net or call +45 70 225 885.