



Cross-domain AJAX/Flash Single Sign-On (SSO) provides a simplified and secure approach to cross-domain authentication allowing the user to access resources at many service providers through a single login at a centralized identity provider. It is derived from SAML 2.0, but is highly simplified and easy to understand and implement.

When a user client requests a protected resource from a service provider and a security context does not yet exist within the session at the service provider, the service provider saves the original request and responds with a redirect to the *produceArtifact* service of the appropriate identity provider passing the identity of the service provider as a provider identifier. The identity provider saves the provider identifier so that it can be used for cross-domain AJAX/Flash single sign-off and responds with a redirect to the service provider's *consumeArtifact* service with an *artifact* to the user's credentials. The *consumeArtifact* service internally calls the *resolveArtifact* service of the identity provider over a previously authenticated inter-provider session to obtain the authentication credentials and establish a local security context within the service provider. The service provider then restores the original request state and responds with a redirect to the original resource request. The resource is then returned to the user client by the service provider.

