SAML CONFIGURATION FOR SP INITIATED SSO FLOW

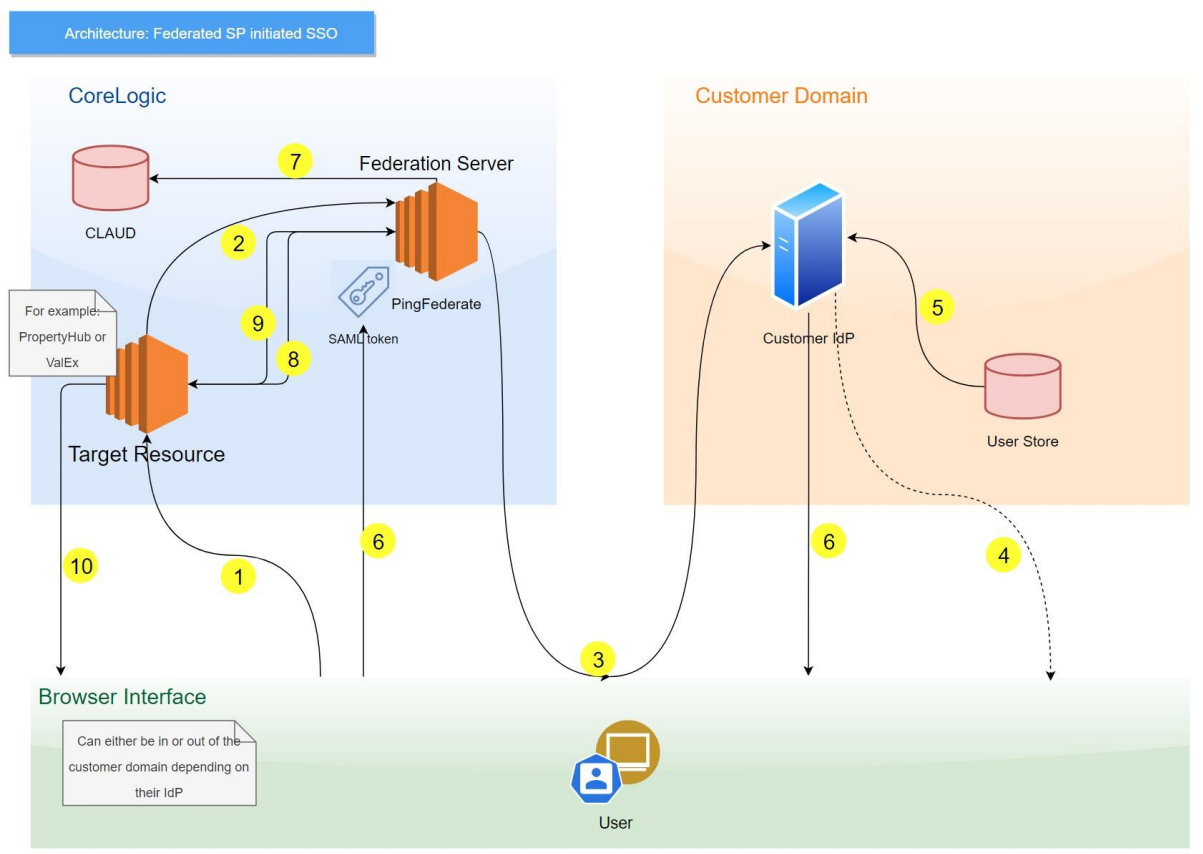
CORELOGIC

Contents

Introduction

SSO is practiced inside an organization (intra-organizational) so that the user can access resources (different web properties and applications) within an organization

Service Provider (SP) initiated SSO involves the SP creating a SAML request, forwarding the user and the request to the Identity Provider (IdP), and then, once the user has authenticated, receiving a SAML response & assertion from the IdP. This flow would typically be initiated by a login button within the SP.



SP (Service Provider) initiated SSO Flow:

1. A user requests access to a protected CoreLogic SP resource, for example: PropertyHub or ValEx.
2. The user is not logged on to the site. The request is redirected to the federation (CoreLogic's PingFederate) server to handle authentication.
3. The SP returns an HTTP redirect (code 302 or 303) or POST containing a SAML request for authentication through the user's browser to the IdP's SSO service.
4. If the user is not already logged on to the IdP site or if re-authentication is required, the IdP asks for credentials (for example, ID and password) and the user logs on.
5. Additional information about the user may be retrieved from the user data store for inclusion in the SAML response. (These attributes are predetermined as part of the federation agreement between the IdP and the

SP). The SAML_SUBJECT is normally set to the email address of the user; this email address is then also used as the user's username.

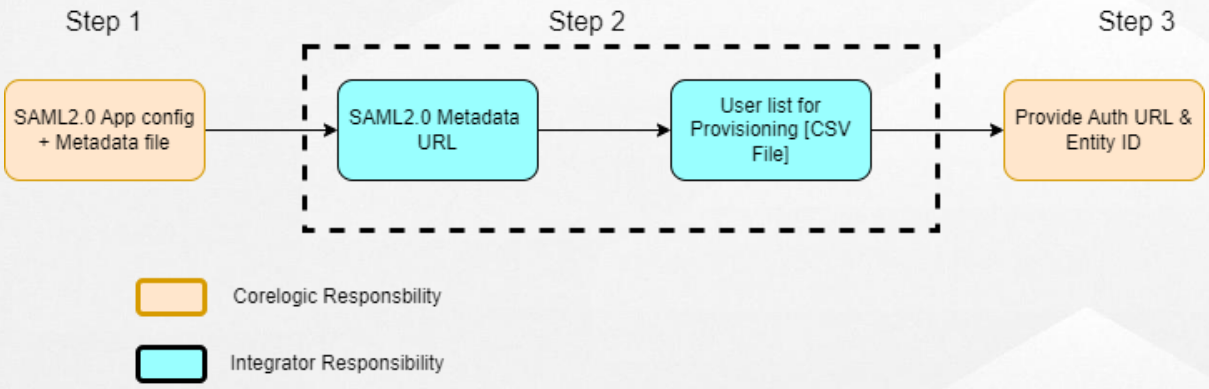
6. The IdP's SSO service returns an HTML form to the browser with a SAML response containing the authentication assertion and any additional attributes. The browser automatically posts the HTML form back to the SP.
7. PingFederate will query a local user management system (Users would need to be setup at CoreLogic side prior to this step – Just in Time provisioning is not supported at the moment – Batch manual processing in place)
8. If the signature and the assertion are valid, PingFederate sends an authorisation code to the target resource.
9. The target resource then uses that authorisation code along with its clientId and secret to get an access, id and refresh token. Ideally that access and refresh token stay on the backend and never goes out to the client browser.
10. The target application then creates a session for the user.

To enable an external Identity Provider to login to our applications, CoreLogic will define an IDP connection for the partner identity system.

Supported identity providers:

Identity systems with SAML 2.0 support - Azure AD, Okta, Auth0, AWS Identity, PingFederate, PingOne, and similar.

Steps to setup SP Initiated flow:



Step 1 – SAML 2.0 Application Configuration

Variables	values
Entity ID for the connection	Starting Value - corelogic.com.au * This is the IdP SAML Application ID, an updated value may be generated when the application is created, confirm via metadata.
Assertion Consumer Service (ACS) URL (aka Reply URL)	**UAT:** https://auth-uat.corelogic.asia/sp/ACS.saml2 **Production:** https://auth.corelogic.asia/sp/ACS.saml2

Sign on URL (Optional)	* Will be configured based on the ACS URL
Relay State (Optional)	Not used for SP initiated flows
Logout URL (Optional)	**UAT:** https://auth-uat.corelogic.asia/idp/startSLO.ping **Production:** https://auth.corelogic.asia/idp/startSLO.ping
SAML Subject Attribute	**email address** ***No additional attributes are required, but may be included if automated provisioning is planned. External SSO identities will be manually provisioned to the CoreLogic identity systems with correct application access.

Optional - certificates if SAML2.0 signing/encryption is enabled.

Step 2 –Identity Provider configures the SAML application

External integrators will configure a SAML2.0 application connected with the appropriate CoreLogic ACS URL.

External Integrator to provide:

1. SAML2.0 Application Metadata URL or Metadata file. [Metadata URL preferred]
2. List of IdP email addresses for batch provisioning into the CoreLogic applications.

Step 3 – Confirmed SP-IDP Sign On

1. CoreLogic to send the partner the confirmed Entity ID to update back to the SAML application config.
2. Confirm the authentication URL(s) (with their PartnerIdP name) and request the external party to test their users with CoreLogic authentication URL.

For example, a Property Hub SSO link for “example_sso_partner_name”:

UAT: https://auth-uat.corelogic.asia/as/authorization.oauth2?client_id=da495393&response_type=code&redirect_uri=https://propertyhub-uat.corelogic.asia/sso&scope=openid%20profile&PartnerIdp=**example_sso_partner_name**

Production:
https://auth.corelogic.asia/as/authorization.oauth2?client_id=da495393&response_type=code&redirect_uri=https://propertyhub.corelogic.asia/sso&scope=openid%20profile&PartnerIdp=**example_sso_partner_name**

Users - Manual Provisioning

At the moment, only manual provisioning is supported from Corelogic and the following file is required to be populated for the user list which need to be provisioned.

Email addr	Firstname	Lastname	StaffID
test@test.	John	Citizen	ABCD1234