**SAML Service Provider**

**Activants Pte Ltd**

**Estimation Effort**

Development of SAML Service Provider with HTTP-Artifact bindings.

|  |  |  |
| --- | --- | --- |
| **S. No** | **Items** | **Man Days** |
| 1 | Function to loads the SP and IDP certificate from file. | Completed |
| 2 | The machine key set is specified so the certificate is accessible to the IIS process. |
| 3 | Function to Create some URLs to identify the service provider to the identity provider. |
| 4 | As we're using the same endpoint for the different bindings, add a query string parameter to identify the binding. |
| 5 | Initialize the IssuerURL |
| 6 | Create new function Create the assertion consumer service URL. |
| 7 | Rather than have different endpoints for each binding we use the same endpoint and identify the binding type by a query string parameter. |
| 8 | Create the authentication request with all the parameters |
| 9 | Append the idp sso URL from web config file. | 1 |
| 10 | Serialize the authentication request to XML for transmission. |
| 11 | Sign the authentication request with x509 Certificate |
| 12 | Generate the SAMLMessageSignature. |
| 13 | Create and cache the relay state so we remember which SP resource the user wishes to access after SSO. |
| 14 | Send the authentication request to the identity provider over the selected binding. | 1 |
| 15 | Create the artifact. |
| 16 | Cache the authentication request for subsequent sending using the artifact resolution protocol. |
| 17 | Send the artifact. |
| 18 | Create function (ArtifactResponder) to receive the artifact | 0.5 |
| 19 | Process the artifact resolve request received from the identity provider in response to the artifact sent by the service provider. |
| 20 | Function to Receive the artifact resolve request. |
| 21 | Get the artifact. |
| 22 | Remove the artifact state from the cache. | 0.5 |
| 23 | Create an artifact response containing the cached SAML message if Http Artifact is null |
| 24 | Send the artifact response. |
| 25 | Store the query string parameter identifying the IdP to SP binding in use. | 1 |
| 26 | Variable to store the query string parameter indicating an error occurred. |
| 27 | Function to Receive the SAML response from the identity provider. |
| 28 | Determine the identity provider to service provider binding type. |
| 29 | We use a query string parameter rather than having separate endpoints per binding. |
| 30 | Receive the SAML response over the specified binding. |
| 31 | Receive the artifact. | 1 |
| 32 | Create an artifact resolve request. |
| 33 | Create an Issuer for Artifact resolver. |
| 34 | Convert artifact resolve to xml |
| 35 | Send the artifact resolve request and receive the artifact response. | 0.5 |
| 36 | Assign the idpArtifactResponderURL from web config |
| 37 | Send the request with artifact Resolve to get the artifact response |
| 38 | Extract the SAML response from the artifact response. |
| 39 | Check if Invalid identity provider to service provider binding is provided. | 1 |
| 40 | Verify the response's signature with X509 certificate |
| 41 | Catch an exception if the SAML response fail to verify |
| 42 | Deserialize the XML. |
| 43 | Check whether the SAML response indicates success or an error and process accordingly. | 1 |
| 44 | Create function to process success SAML response |
| 45 | Extract the asserted identity from the SAML response. |
| 46 | Get the subject name identifier. |
| 47 | Get the originally requested resource URL from the relay state. |
| 48 | Create a login context for the asserted identity. |
| 49 | Redirect to the originally requested resource URL. | 1 |
| 50 | Create a function to process Error SAML Response |
| 51 | Create a function to respond to Single Log out (SLO) |
| 52 | Create a logout request. |
| 53 | Serialize the logout request to XML for transmission. | 1 |
| 54 | Send the logout request to the IDP over HTTP redirect. |
| 55 | Logout locally |
| 56 | Function to Receive the logout request or response. |
| 57 | Create a logout response. | 0.5 |
| 58 | Serialize the logout response for transmission. |
| 59 | Send the logout response over HTTP redirect. |
| 60 | Redirect to the default page. |
|  |  | Approximately (10 days) |

Note: I have no Identity Provider to test my application.

And I will try to complete before the estimations.

Process Flow (SSO)

RESPONSE REDIRECT from CLIENT TO SINGPASS/CORPASS

|  |  |  |
| --- | --- | --- |
| **Client** | **Service Provider** | **Identity Provider** |
| Sign (URL) |  |  |
|  |  | **LoginPage**   * Credentials * Redirect |
|  |  | **SSOService**   * Page\_Load * CreateSAMLResponse * SendSAMLResponse |
|  | AssertionConsumerService   * ProcessSAMLResponse * ReceiveSAMLResponse |  |
|  |  | ArtifactResponder   * Page\_Load * ProcessArtifactResolver |
|  | AssertionConsumerService   * ReceiveSAMLResponse * ProcessSAMLResponse * ProcessSuccessSAMLResponse |  |
| Logged in page |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Service Provider** | **Identity Provider** |
| **Logout (URL)** |  |  |
|  | **Logout page**   * Logout\_function |  |
|  |  | **SLOService**   * Page\_Load * ProcessLogoutRequest * CreateLogoutResponse * SendLogoutResponse |
|  | **SLOService**   * Page\_Load * ProcessLogoutResponse |  |
| **Default Page** |  |  |

IDP

|  |  |
| --- | --- |
| Target: | client URL |
| Saml Response | Destination = Assertion Consumer Service URL(SP)  Issuer = IDP URL |
| SAML Assertion | Issuer = SAML Response. Issuer (IDP) |
|  | Subject  User identity name |
|  | Subject Confirmation  Recipient: Assertion Consumer Service URL(SP) |
|  | Subject Confirmation Data  Recipient: Assertion Consumer Service URL(SP) |
| Add all to Saml assertion. Subject | |
| AuthnStatement |  |
|  | AuthnContext |
| Add all to saml assertions. Statements | |
| Add Saml assertion to saml response. | |
|  |  |
|  |  |

**SP Artifact Resolve**

|  |  |
| --- | --- |
| **subject** | **NameID** |
| **AttributeStatement** | **user’s information**   * **UserInfo**: NRIC/FIN or Foreign ID as “CUPID” attribute * **AuthAccess**: UEN/non-UEN ID * **TPAuthAccess**: 3rd party , can be null if no 3rd party * **Digital Service ID** * **The role the user** * **Sub-UEN** |
|  |  |
|  |  |

**SP(SP/CP) | Assertion Consumer Service | Artifact Response**

|  |  |
| --- | --- |
| **Artifact** **Resolution or THE FINAL RESPONSE.** | |
| Authentication Assertion: |  |
|  | **UserInfo**: (Full Name, account status, User type, etc);  **AuthAccess** **or** **TPAuthAccess**: UEN/non-UEN ID), Digital  Service and Role information of the user. |
| SAML Assertion | **Namespace: urn:oasis:names:tc:SAML:2.0:assertion** |
|  | **saml**: **Issuer**: unique identifier of the identity provider  **ds**: **Signature**:  **saml**: **Subject:**  User NRIC/FIN  **saml**: **Conditions**: which gives the conditions under which the assertion is to be  considered valid  **saml**: **AuthnStatement**: act of authentication  **saml: AttributeStatement** provides the attribute information for the subject  as requested by SP  **saml: Authentication context:** Password Protected Transport/  Mobile Two Factor Unregistered /  Time Sync Token / Software PKI  **Attributes**:   * **UserInfo**: User information * **AuthAccess**: provides roles for authorization at client side. * **TPAuthAccess**: 3rd party attribute.. |