**Activants Pte Ltd Service Provider Application**

**Development Breakdown**

|  |
| --- |
| **Date: 6th Nov 2019** |
| **Technical Requirements**   * Microsoft Visual Studio version: 2019 * Microsoft SQL Server 2017 * Microsoft SQL Server Management Studio (SSMS) v18.4 * Microsoft IIS Server |
| **Project Details**   * Project type: ASP.NET C# MVC project. * ASP.NET Framework Version: 4.7.2 * Entity Framework version: 6.0.0 * ComponentSpace.SAML2 DLL version: 3.4.0.0 (**TRIAL VERSION**) |
| **Project Description**   * Project Name: ActivantsSP (Activants Service Provider) * Project summary: A SAML based Service Provider which takes SAML Request, Authenticates the user from the identity provider and sends back SAML response to clients. |
| **Database created**   * Created new database named as Activants in SQL Server Management Studio (SSMS) * Authentication mode: Windows based authentication * Table and fields are auto created when application starts running. * Tables are used to store User claims, user’s security stamp and username. |
|
|
| **Template Used**   * Default ASP.Net template with Razor Views. |
|
| **Pages Created**   * One About page is created with a login and logout button to initiate the login, display the data and to initiate the Logout option. |
| **Config Files**   * One saml configuration file is created (saml.config) to store the metadata of Identity Provider. |
| **Changes in Web.Config**   * Added identity provider’s identifier in web.cofig file. * Added Database configurations. |
| **DLL file**   * ComponentSpace.SAML2 DLL is used which is trial version. |
| **Controller Created**   * one controller (SamlController) created for SAM request and response. * Consisting of the following main functions |
| **Certificate Folder**   * One new folder (Certificate) created to store Identity’s public key and Service provider’s private and public key. |

|  |
| --- |
| **Date: 7th Nov 2019** |
| **Changes made**   * **Controller**: Change in SingleLogoutService function under SamlController. * **Config**: Change in saml.config file |

|  |
| --- |
| **Date: 8th Nov 2019** |
| **Certificate Folder**   * Installed OpenSSL software for generating new x509 certificates (SP.CER and SP.PFX)   **Issue fixed**   * Cleared SAMLCertificateException   **Deployment in Development Server**   * Successfully deployed Service Provider application in Development Environment. |

|  |
| --- |
| **Date: 11th Nov 2019 & 12th Nov 2019** |
| * Service Provider User Guide * Service Provider Development breakdown * SAML PPT |

**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) |