FEDERATED APPLICATION ONBOARDING

***Identity Provider Data***

|  |
| --- |
| **Identity Provider Data** |
| **Display Name**  | EAD.STS.WA.GOV |
| **Identifier**  | http://ead.sts.wa.gov/adfs/services/trust  |
| **Federation Service Endpoint URL**  | https://ead.sts.wa.gov/adfs/ls/  |
| **Federation Metadata URL** *Contains endpoint/certificate/claim references required for Web application federations with FS– Passive federations.* | https://ead.sts.wa.gov/FederationMetadata/2007-06/FederationMetadata.xml  |
| **WS-MEX URL(WS-MetaDataExchange)** *Contains endpoint/ certificate references required for Web service/active-client federations with FS – active federations.*  | https://ead.sts.wa.gov/adfs/services/trust/mex  |
| **FS Token-Signing Certificate** *Used to validate the authenticity of SAML tokens issued**by FS. Will also provide the certificate upon request.* | **-----BEGIN CERTIFICATE-----****MIIDMTCCAhmgAwIBAgIQVz5UHyLFM6pDf3Sa4PlAtTANBgkqhkiG9w0BAQsFADAm****MSQwIgYDVQQDExtUb2tlblNpZ25pbmctZWFkLnN0cy53YS5nb3YwHhcNMTIxMDAx****MDgwMDAwWhcNMzIxMDAxMDgwMDAwWjAmMSQwIgYDVQQDExtUb2tlblNpZ25pbmct****ZWFkLnN0cy53YS5nb3YwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7****ksGEdMEmk3//GyFUuJN52dt3978jVlq9wB9OmWEYqWDmhGk3VoWDJ2iQVunlbFu6****wxPcuYjXKH87lULvNNGwrvoVORVSg0uw65dMBK3dXbfdPbiLf/LAGkwzOmkfS8OE****eX5LT4bfDFLCDuWThyHNGbiNJYkl4zSHdnmrk4kHUnB2WTJOVLVjFJ+uLAYLvTpO****xVemZCCUYY4Nh7Ox6Tx5FhA0dUY8GPl0J4KYA+Zos+GPUtFann1MO0TZy3zAFI9x****HyYj5rfT4VpX2rN0PHFChvXR/YZ70VMxHrAkbYTT2sXQvknF5QyuQAZ4HM1qgRcF****oIkZ/iN68iths86My5/PAgMBAAGjWzBZMFcGA1UdAQRQME6AEF+Xbral6Q+ZpOl2****ZO9+opmhKDAmMSQwIgYDVQQDExtUb2tlblNpZ25pbmctZWFkLnN0cy53YS5nb3aC****EFc+VB8ixTOqQ390muD5QLUwDQYJKoZIhvcNAQELBQADggEBAFOatP6ptufqLN1j****NggdiowMQoms+wr84ipKizpCtWFTXteGhmy0HVMiCE3u0Sd5xmG0l6qAf0Krmd0a****Y4R+wbtHEgq1/2s/9lmvY5mtKfiQ5I3+Vlmu2TzgCW3ruvhz1ptf6flwlVFfF5wm****2RxaV5R/NKyvCGkphX40hIf1ghK7B+R/xC2M3e+zTSVGYr6DHBfrTDlG/cXdoqAJ****3cG80l1FTK7hqZsJlu/9YAV+xu0K2lVfubu5z3G+zA/SaHqEgow2SJOmkBrfvc90****d0wMMia4B9VwKnUIsoBYn0klUZmv+cZNBW14HyybL/B5G6X1Z/fgQHmvnjluVXT7****XowXE0I=****-----END CERTIFICATE-----** |

OpenID Configuration URL: <https://ead.sts.wa.gov/adfs/.well-known/openid-configuration>

 ***Application Owner Responsibility:***

* To build ADFS 4.0 compatible applications or web services, review Identity Developer Training Kit and Microsoft’s WIF SDK.
* Questions? Contact ServiceDesk@watech.wa.gov

***Required Partner Information***

|  |
| --- |
| **Project / Application Function**  |
| **Description** *Provide the summary of what this application does**.* - *Is this application for POC or Production use?*   |
| **Platform**  | **Examples:**  |
| Provide a description of the application platform and type of federation – SAML, WS-Fed, OAuth. | ACS ADFSv1 ADFSv2 WIF application Azure application SharePoint 2010 site Third-party STS [Specify product name] Windows Phone 7 |
| **Sponsor Details**  |
| **Sponsor**  |
| **Vendor and Agency Contact Information** | **Vendor Contact****Name:** **Email:** **Company:** **Phone:****Agency Contact****Name:****Email:****Agency:****Phone:** |
| **Relying Party Setup Preparation Checklist**  |
| **Display Name** *Provide a user-friendly name to identify the Relying Party*  | **Example:** Agy ApplicationNameWaTech SalesForce |
| **Realm Identifier** ***\*****Text is case-sensitive* *Entity ID of the requestor.****URI of the App making the request for auth.*** | **Examples:** <https://www.contoso.net/> <https://contoso/ClaimsAwareWebsite/>  |
| **Endpoint URL** *Provide the Relying Party application URL or* *WIF/ADFS Fedmetadata.xml if available.****\*****Supports only https****Where does ADFS post the token?*** | **Examples:**https://www.contoso.net/ https://contoso/ClaimsAwareWebsite/ https://www.contoso.net/FederationMetadata/2007-06/FederationMetadata.xml  |
| **Requested Authentication Providers**  | **Examples:**  |
| Specify the authentication sources that your application will be able to consume. * All applications get “AD Authentication by default”
* Additional review/approvals required for Partners, Windows Live ID andFederated auth
 | AD Credentials  |
| **Requested Claims** *Specify the Claims/assertions your application will consume from ADFS**What attributes does the application require in the SAML token?* | **Examples:** Email, UPN, FirstName, LastName, EmployeeId etc.  |
| **Authorization Rules** Specify rules to permit or deny a user or group of users to receive a SAML token for this relying party.  | **Examples:** * Permit all users

Permit only users belonging to security group “Agy\G-S-Agy” (all others will be denied by default)  |
| **Require Token Encryption****This option requires that a certificate is provided by the application.** | Yes/No  |
| **Secure Hash Algorithm** | SHA1/SHA256  |

Want to know more? Check out the ADFS Onboarding Applications Deep-Dive link below:

<https://blogs.technet.microsoft.com/askpfeplat/2015/03/01/adfs-deep-dive-onboarding-applications/>