ADFS Federated Application Onboarding Template

State of Maine's Identity Provider Data:

Microsoft's Identity Provider Data	
Display Name	State of Maine Federation Services
Identifier	http://sts.maine.gov/adfs/services/trust
Federation Service Endpoint URL	https://sts.maine.gov/adfs/ls/idpinitiatedsignon.aspx
Federation Metadata URL *Contains endpoint/certificate/claim references required for Web application federations with Corp STS– Passive federations.*	https://sts.maine.gov/federationmetadata/2007-06/federationmetadata.xml
WS-MEX URL(WS-MetaDataExchange) *Contains endpoint/ certificate references required for Web service/active-client federations with Corp STS – active federations.*	https://sts.maine.gov/adfs/services/trust/mex
STS.maine.gov Token-Signing Certificate *Used to validate the authenticity of SAML tokens issued by Corp STS*	If needed: You have a choice between .cer and .P7b file and .pfx

Application Owner Responsibility:
- Fill out information below and email to: EnterpriseDirectoryServices@maine.gov
- Questions? Contact EnterpriseDirectoryServices@maine.gov

Required Partner Information:

(Some responses will require additional follow-up or approvals from State of Maine.)

Project / Application Function	
Description *Provide the summary of what this application does.* - *Is this application for POC or Production use?*	
Platform *Provide a description of the application platform* *ACS federation requests* • *Applications which need ACS federations for service bus/caching service etc. are allowed and any other ACS tenant request needs to be onboarded to the*	**Examples:** xbxcACS ADFSv2 ADFSv3 WIF application Azure application SharePoint 2010 site

Service Provider (SP) tenant or STS.maine.gov directly.	Third-party STS [*Specify product name*] Windows Phone 7
Sponsor Details	
Service Provider Sponsor Alias	
Vendor Contact Information *For vendor or third-party developed applications*	**Name:** **Email:** **Company:** **Phone:**
Application Support Alias	
Relying Party Setup Preparation Checklist	
Display Name *Provide a user-friendly name to identify the Relying Party*	**Example:** Contoso
Realm Identifier ***Text is case-sensitive***	**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***	**Examples:** https://www.contoso.net/ https://contoso/ClaimsAwareWebsite/ https://www.contoso.net/FederationMetadata/2007-06/FederationMetadata.xml
Requested Authentication Providers *Specify the authentication sources that your application will be able to consume.* • *All applications get "Corp Authentication by default"* • *Additional review/approvals required for Partners, Windows Live ID and Federated auth* *Notes: Windows Live ID auth will not be approved;* • *For POC/Dev applications* • *To access internal applications that can otherwise be accessed via Microsoft AD or Partners account.*	**Examples:** Corporate Credentials Windows Live ID PARTNERS (extranet) user accounts

Requested Claims
Specify the Claims/assertions your application will consume from ADFS
 	
Notes:
• *'tokenGroups' will not be issued; individual group names will be emitted as Group or Role claims*
• *Security groups must be created via http://idweb*
  ○ *Domain Local scope*
  ○ *Redmond domain*
	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. The default Authorization Rule for new Relying Parties is "Deny All" – all authorization logic must be specified by the RP owner.*	**Examples:** • Permit all users Permit only users belonging to security group "SOM\Foo" (all others will be denied by default)
Require Token Encryption	**Yes/No**
Secure Hash Algorithm	**SHA1/SHA256**
Privacy Policies	
Does your application adhere to the terms of http://privacy.microsoft.com/en-ca/fullnotice.mspx?	**Yes/No**