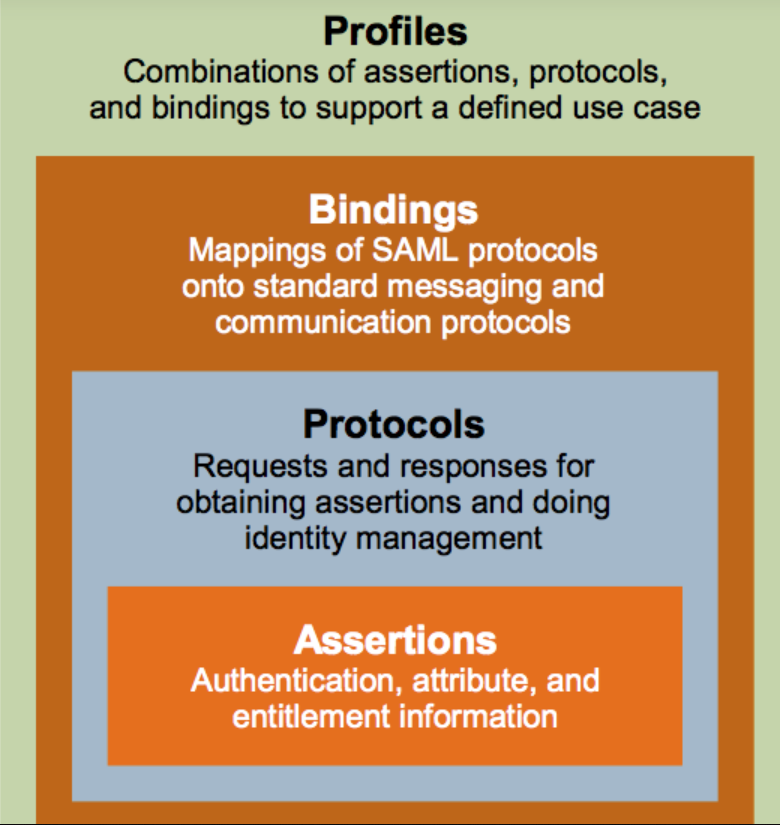
**SDLC**

* **Analysis and user requirements**
* **Design & UI prototype**
* **Coding**
* **Testing**
* **Deployment**
* **Maintenance**

**Important Points:**

* SAML transactions use Extensible Mark-up Language (XML)
* SAML maintains a secure federated identity management system running at IDP and SP
* Both ends need to have the exact configuration for the SAML authentication to work
* **SAML** consists of **three** sets of **components**: assertions, protocols and bindings.
* Does IDP cross verifies the SP with the signature in its local cache or reaching live.
* HTTP post, HTTP artefact, Low level API, High Level API



**Installing**

**Add/Replace ComponentSpace library**

First remove the existing ComponentSpace library

* In Solution Explorer, select the project.
* On the Project menu, choose Add Reference.  
  The Add References dialog box opens.
* Click the tab for a category that contains references you want to remove.
* Select ComponentSpace reference, and click Select to place it in the Selected Components field.
* To remove the selected references, choose Remove.

Then add the new ComponentSpace library

* In Solution Explorer, right-click on the References or Dependencies node and choose Add Reference.
* You can also right-click on the project node and select Add > Reference.
* Click Browse then select ComponentSpace DLL file.

**Add Identity Provider Certificate public key**

* In Solution Explorer, open Certificates folder, open idp.cer file
* Paste the Identity Provider Certificate inside

**Add Service Provider Certificate private key**

* In Windows Explorer, go to the project directory, open Certificate folder
* Replace sp.pfx with your Service Provider Certificate private key
* Make sure the file name still sp.pfx

**Configure SAML request and response**

* In Solution Explorer, open saml.config file
* Fill in the empty values with Service Provider and Identity Provider information

**Add Identity Provider Entity ID to Web.config**

* In Solution Explorer, open Web.config file
* Fill in the empty value for PartnerIdP key with Identity Provider Entity ID

<add key="PartnerIdP" value="YOUR\_IDP\_ENTITY\_ID" />

**Identity Provider Requirements**

Send these information to your Identity Provider to be added into their configuration

* Base URL: "<http://localhost:49864>"
* Assertion Consumer Service endPoint: "/SAMLSP/AssertionConsumerService"
* SLO Service endPoint: "/loginSP"
* SP EntityID: "YOUR\_SP\_ENTITY\_ID"
* SP certificate: "YOUR\_SP\_PUBLIC\_KEY\_CERTIFICATE"

**POINTS**

The private key (ie PFX file) should not be distributed. It's used by their SP site but isn't required by the IdP or any other party.  
We do not enforce the use of a private key.  
The SP doesn't need a private key unless either SAML messages are to be signed or SAML assertions are encrypted.  
If the IdP is using ADFS, the SAML authn requests sent to ADFS don't have to be signed.  
However, if you wish to support SAML logout, ADFS requires all SAML messages to be signed.  
This is a requirement of ADFS. It's not a limitation on our side.  
Therefore, your choices when ADFS is the IdP are:  
1. Don't configure a private key in the SP, don't sign SAML authn requests, but don't support SAML logout.  
2. Configure a private key in the SP, sign SAML authn requests, support SAML logout.

PRIVATE KEY SP

C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys

<?xml version="1.0"?>

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" validUntil="2019-10-10T08:40:02Z" cacheDuration="PT604800S" entityID="http://localhost:49864/loginSP">

<md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

<md:KeyDescriptor use="signing">

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:X509Data>

<ds:X509Certificate></ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</md:KeyDescriptor>

<md:KeyDescriptor use="encryption">

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:X509Data>

<ds:X509Certificate></ds:X509Certificate>

</ds:X509Data>

</ds:KeyInfo>

</md:KeyDescriptor>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:49864/loginSP"/>

<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>

<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://localhost:49864/SAMLSP/AssertionConsumerService" index="1"/>

</md:SPSSODescriptor>

</md:EntityDescriptor>