ComponentSpace SAML for ASP.NET Release Notes

www.componentspace.com

7.3.0 – January 10, 2025

- Use a random number generator rather than GUIDs for IDs.

7.2.0 – November 27, 2024

- Add the KeyEncryptionDigestMethod and KeyEncryptionMaskGenerationFunction configuration properties for the http://www.w3.org/2009/xmlenc11#rsa-oaep and http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p key encryption algorithms.

7.1.0 – July 25, 2024

- When there are multiple pending SAML responses within the one browser session, respond to the most recent first rather than the oldest.
- Support encryption certificates when exporting IdP metadata.

7.0.0 – March 1, 2024

- When importing metadata, default the WantAuthnRequestsSigned and AuthnRequestsSigned flags to false as per the specification.
- Add the methods IsLocalIdentityProvider, IsLocalServiceProvider, GetPartnerIdentityProviderNames and GetPartnerServiceProviderNames to the ISAMLConfigurationResolver interface.
- Add the ISAMLConfigurationNameResolver interface to support Entra ID multi-tenant applications and any other use cases where SAML message issuer names don't map directly to partner configuration names.

6.5.0 – November 7, 2023

- Support certificate file passwords stored in web.config using the PasswordKey property.

6.4.0 – September 7, 2023

- When using the database SSO session store, support automatic and scheduled deletion of expired entries.
- When importing metadata, include the certificate thumbprint in the certificate filename to ensure it's unique as different certificates may have the same subject DN.

6.3.0 – May 19, 2023

- Support extension elements in SAML authn requests via the SSOOptions.
- Fix issue with SAMLServiceProvider.IsSSOCompletionPending.

6.2.0 – March 15, 2023

- Clean up the session state properly as IsSSO was returning true after SLO.
- Add the DisableClearAllSessionsOnLogout flag to configure how multi-session SLO is handled.
- Default the configuration flags SignLogoutRequest, SignLogoutResponse, WantLogoutRequestSigned and WantLogoutResponseSigned to true as these messages must be signed as per the SAML Profiles specification.
- Default the configuration flag SignAssertion to true as per the SAML Profiles specification.

- Default the configuration flags SignAuthnRequest and WantAuthnRequestSigned to true to encourage best security practices.

6.1.0 – January 12, 2023

- When sending a logout request, start with the most recent rather than the oldest session.
- Disable SHA-1 support by default. If required, it can be enabled using the EnableSha1Support configuration flag.

6.0.0 – November 17, 2022

- Support encrypted Name IDs.
- Support multiple pending SAML responses within the one browser session.
- Remove the pre .NET 4.0 framework HttpRequest/HttpResponse based low-level APIs.

5.4.0 – September 7, 2022

- Add SAMLAttribute.ToString(separator) overload.
- If returning attributes in an IDictionary, return multi-values separated by a comma.
- Use the System.Security.Cryptography.Xml update that addresses Microsoft Security Advisory CVE-2022-34716.

5.3.0 – July 5, 2022

- Update the XML schema to support the new XML encryption methods.
- Repackage the XML encryption extensions as NuGet packages.

5.2.0 – April 26, 2022

- Add support for the MySqlConnector database provider.
- Support WebHosting and other Windows certificate stores.

5.1.0 – February 9, 2022

- No longer support .NET 2.0 framework. The minimum support level is .NET 4.0 framework.
- Include Visual Studio 2022 examples solution.
- If WantAssertionOrResponseSigned is set, attempt to verify the SAML assertion signature even if the SAML response signature failed to verify.
- Support specifying the Destination through the SSOOptions.

5.0.0 – October 14, 2021

- For consistency, rename the configuration ID to Name. This only affects multi-tenant configurations.
- Enable entity framework support for the SAML configuration.
- For non-standard platforms using SAMLHttpResponse, add support for the HTTP-Post binding.
- Support extension XML schemas to validate custom SAML attribute value datatypes.
- Default to validating SAML messages against the XML schemas.

- Strong name and allow partially trusted callers for the extension DLLs so they can run in medium trust environments.

4.8.0 – May 21, 2021

- The ResolveToHttps configuration flag should only apply to relative URLs.
- Support IdP-initiated SSO relay state being specified through configuration.

4.7.0 – January 20, 2021

- Set the SSO session store memory cache item priority to NotRemovable.
- Support the recipient field in the SAML assertion being either the entity ID or assertion consumer service URL.
- Add ResolveToHttps configuration to better support SSL terminating load balancers.

4.6.0 – November 19, 2020

- Handle SAML assertions not including a subject.
- Support EC-DSA signature algorithms (http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256 etc).
- For .NET 4.8 builds, use the X509KeyStorageFlags.EphemeralKeySet flag when loading certificates to avoid private key container permission issues.
- Add support for encrypting the Name ID in the logout request.
- Support AES-GCM encryption (http://www.w3.org/2009/xmlenc11#aes256-gcm) through XML encryption extensions.

4.5.0 – October 20, 2020

- Ensure the assertion hasn't expired before adding its ID to the assertion replay check cache.
- Support an optional subject alternative name in CreateSelfSignedCert.
- Refactor the XML encryption class so it's easier to support other algorithms.
- Make it easier to specify a different target for the HTTP Post HTML form.

4.4.0 – September 7, 2020

- Add support for clearing the certificate cache through the ICachedCertificateLoader interface.
- When importing metadata include the certificate thumbprint in the file name for uniqueness.
- Support RSASSA-PSS signature algorithms (http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1 etc).
- Include BEGIN/END CERTIFICATE in CreateSelfSignedCert

4.3.0 – May 7, 2020

- Check the configured use when loading local certificates.
- Change the certificate manager to minimize the number of configuration resolver calls.

4.2.0 – March 20, 2020

- Add SAMLHttpRequest.Headers property.

- Validate decrypted SAML assertions against the SAML XML schemas.
- Remove any -----BEGIN/END CERTIFICATE----- when loading a certificate string.
- Support disabling IdP-initiated SSO.
- Tighten up the InResponseTo checking.

4.1.0 – February 20, 2020

- Allow for long serial numbers when validating SAML metadata against the schema.
- Don't attempt SLO to a partner SP if an SLO URL hasn't been configured.
- Handle a missing User-Agent header when checking for SameSite=None compatibility.
- Include UC Browser on Android compatibility check.
- Don't clear the cookie's secure flag if the connection isn't secure as there might be an SSL terminating load balancer.

4.0.0 – January 7, 2020

- Include a .NET framework v4.8 specific build.
- Set the SAML session cookie SameSite mode to None for all .NET framework builds.
- Support overriding the setting of the SAML session cookie.
- Handle browsers that don't support SameSite=None.
- Support the SAML session cookie being either a session or permanent cookie.
- Support programmatically turning the SAML diagnostics on or off.

3.5.0 – October 7, 2019

- Update the SAML configuration to support any number of certificates.
- Support the import/export of any number of certificates.
- Support separate signature and encryption certificates.
- Enhance the subject confirmation data support.
- Support specifying via the SSO options the subject and conditions to include in the authn request.
- Add the DisableLogoutResponseStatusCheck configuration flag.
- Add the CreateSelfSignedCert example.

3.4.0 – June 12, 2019

- Don't mark the SAML session cookie as secure if not using HTTPS.
- Make authn request scoping information available to the IdP through the SSOOptions.
- Support importing multiple certificates in the MetadataImporter.

3.3.0 – April 2, 2019

- Strong named the assemblies.

3.2.0 – February 15, 2019

- Include the Content-Type header in HTTP-Post to support nosniff.
- Move the JavaScript to after the HTML body for HTTP-Post to support older browsers.
- Support extending the CertificateManager class for custom implementations.

3.1.0 – December 4, 2018

- Add support for the content security policy HTTP header.
- Default the SAML cookie to secure.
- Sign NuGet packages.

3.0.0 – October 18, 2018

- Move to a single NuGet package and use this in the refreshed example projects.
- Provide better support for ISAMLConfigurationResolver implementations when exporting metadata.
- Include partner name in ISAMLObserver methods.
- Add session ID delegate for storing the session ID in a custom cookie.
- Add LocalCertificateKey/PartnerCertificateKey configuration settings to support certificates stored in the Azure key vault.
- Remove basic authentication header support for ECP as this is no longer used.
- Wrap DbCommand creation in a using block to prevent potential resource leaks.
- Implement IDisposable in SAMLHttpRequest and SAMLHttpResponse to dispose of unmanaged resources.
- Default to in-memory cookie based SSO sessions rather than relying on the ASP.NET session.
- Support deletion of SSO sessions.
- Support specifying the AssertionConsumerServiceIndex in the SSO options.

2.8.8 – March 2, 2018

- Support specifying a requested NameID in the authn request through SSO options.
- Support the IdP specifying the authn context programmatically.

2.8.7 – December 22, 2017

- Improve configuration logging.
- When setting SAMLController.Configuration(s), ensure the SAMLConfigurationResolver is refreshed.

2.8.6 – November 1, 2017

- Refactor the ISAMLObserver interface to make it easier to use.
- For security reasons, only allow a single SAML assertion in the SAML response.

2.8.5 – September 12, 2017

- For the .NET 4.6 build, use X509Certificate2.GetRSAPublicKey() as this returns an RSACng.

2.8.4 – August 21, 2017

- Add IConfigurationResolver for dynamic resolution of SAML configuration.
- Change configuration to use lists rather than dictionaries for consistency.
- Make exception constructors public so they may be thrown by custom classes implementing interfaces.

- Enhance SAML metadata import and export.

2.8.3 – August 4, 2017

- In some cases, the .NET framework's SignedXml bug caused SAML assertion signature verification to fail. As an enhanced workaround, first try the original XML element, then the cloned XML element, and finally the cloned element with namespaces declared on the document element. This is an enhancement to the change made in 2.8.1.
- Add support for receiving SAML responses from Postman.
- Include scoping in SSOOptions to support Azure domain hint.
- Add CyclicTraceListener to produce daily logs.
- For .NET frameworks earlier than v4.6.2, perform on the fly conversion of the Cryptographic Service Provider type to 24 to support SHA-256 XML signature generation.

2.8.2 – July 17, 2017

- Default XML encryption to http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p and http://www.w3.org/2001/04/xmlenc#aes256-cbc.
- Add WantAssertionOrResponseSigned configuration flag.
- Add SAMLIdentityProvider.CanSLO and SAMLServiceProvider.CanSLO methods.

2.8.1 – June 26, 2017

- The signature verification change made in 2.7.0 meant some signatures correctly verified but others did not. This is a bug in Microsoft's SignedXml class. To work around this and support all scenarios, try the signature verification first without cloning namespaces and then with cloning namespaces.
- Add LocalCertificateString, PartnerCertificateString etc to the configuration to make it easier to load certificates from a database.

2.8.0– June 9, 2017

- Support RSACng in .NET 4.6.
- Include nupkg for each version of the DLL.
- Switch to semantic versioning (Major.Minor.Patch).

2.7.0.0 – May 22, 2017

- Add .NET 4.6 version of the DLL to support Cryptographic New Generation (CNG) which is required for Hardware Security Modules (HSM). This means private keys are accessed using the X509Certificate2 GetRSAPrivateKey extension method.
- Have SAMLServiceProvider.ReceiveSSO also return the AuthnContext.
- Support specifying the certificate store name.

2.6.0.21 – March 21, 2017

- Add support for AuthnContextComparison configuration.
- Add support for configuring tertiary certificates.

2.6.0.20 – March 13, 2017

- Add support for Visual Studio 2017

2.6.0.19 – February 20, 2017

- Uri.ToString() behaviour has changed between .NET releases. Avoid these issues by using Uri.OriginalString instead.

2.6.0.18 – December 30, 2016

- Added more XML signature logging.
- Copyright updated to 2017.

2.6.0.17 – October 6, 2016

- Don't set the RequestAuthnContext comparison to minimum but instead default to exact.
- Fix bug with metadata import and SecondaryLocalCertificateStoreLocation attribute.
- Add more example configurations including OneLogin, PingOne, Bitium, Centrify, Freshdesk, Zendesk.

2.6.0.16 – August 26, 2016

- Support sending relay state on logout with the high-level API.
- Add extra checking when receiving SAML messages.
- When exporting metadata set the SPSSODescriptor's AuthnRequestsSigned correctly.
- Expose the schema warnings and errors as properties to the SAMLSchemaValidationException.
- Add SAMLController.Uninitialize method so SAML configuration may be reloaded.
- Add WSO2 identity server example configuration.
- Improve support for dynamic configuration changes including not loading certificates until required and making certificate caching optional.
- Add OWIN examples.

2.6.0.15 – June 27, 2016

- Support multiple certificates as well as separate signature and encryption certificates.
- Don't include null SSOOptions.RequestedAuthnContext.
- Include support for Facebook at Work.
- Check there's a signing key for XML signature generation.
- Fix the MySQL provider name as the case was wrong.
- Include SLO support for Okta.
- Don't restrict the authn context and name ID format to the standard values in the configuration schema.
- SingleLogoutService methods for HTTP-Redirect need to specify the signature algorithm.

2.6.0.14 – June 3, 2016

- Add support for checking the destination field.

- Add support for checking the recipient field.
- Fix bug with SubjectConfirmationData.IsWithinTimePeriod.
- Add AuthnContext check.
- Add extra logging for failed signature generation/verification.
- Strip any Unicode BOM character from the XML.
- If there's a single SAML configuration use “default” only if no ID is specified.
- Default the digest method depending on the specified signature method.
- When importing metadata, if two certificates, use the signing certificate.
- Add WantDigestMethod and WantSignatureMethod so these may be checked against incoming signatures.
- Default to SHA-256 signatures.
- Add XMLSignatureDescriptions.SHA2Enabled to allow disabling of SHA-2 support.

2.6.0.13 – February 25, 2016

- Add support for validating SAML messages against the XML schemas.
- Fix bug with FIPs support – SHA-256, SHA-384 and SHA-512 now work with FIPs enabled or disabled.
- When a response is pending, check the response type as well.

2.6.0.12 – February 4, 2016

- Support multiple requested authn contexts in the SSO options.
- Update SAMLHttpResponse for sending SAML messages through non-standard methods.
- Change license expiry message.
- Add PartnerIdentityProviders and PartnerServiceProviders elements so configuration isn’t element order sensitive.
- Add SAMLConfigurations element so multiple configurations may be specified.
- Rename SAMLResponse.GetAssertion to SAMLResponse.GetUnsignedAssertion to avoid confusion.

2.6.0.11 – December 29, 2015

- When registering for SHA-256, SHA-384 and SHA-512 support, use the FIPS compliant SHA256CryptoServiceProvider rather than SHA256Managed etc.
- Update copyright to 2016.

2.6.0.10 – November 16, 2015

- Allow for no partner providers when exporting metadata.

2.6.0.9 – October 8, 2015

- Handle empty audience restriction.
- Allow the database column names to be changed.

2.6.0.8 – August 3, 2015

- Minor updates to the logging.

- If there's no NotOnOrAfter value then use a default when adding to the replay detection cache.
- Improve the way SSO session IDs are supported by using delegates.
- Add support for SHA-384 and SHA-512 XML signatures and automatically register these algorithms.

2.6.0.7 – July 14, 2015

- Include RequestedAuthnContext in SSOOptions.
- Add SAMLIdentityProvider.SendSSO overload that takes an assertionConsumerServiceUrl.
- Support current user certificate store location.
- Include IsPassive in SSOOptions.
- Add SAMLIdentityProvider.SendSSO overload that takes a SAML status.
- Update for Visual Studio 2015.

2.6.0.6 – June 3, 2015

- Fix a bug when sending a logout response with a non-default signature algorithm.
- Add GetPartnerPendingResponse API.

2.6.0.5 – May 8, 2015

- AuthnContextDecl should be anyType not anyURI.
- Add extra methods to ISAMLObserver to permit the modification of the SAML assertion, SAML message and destination URL.
- Fix a bug when serializing the SignLogoutResponse configuration to XML.
- Made <ServiceProvider> AssertionConsumerServiceUrl optional.

2.6.0.4 – March 6, 2015

- Add IssuerFormat, DisableAssertionReplayCheck, DisableTimePeriodCheck and DisablePendingLogoutCheck to the SAML configuration.
- AssertionConsumerServiceUrl should be optional in the SAML configuration.
- Added SAMLHttpRequest, SAMLHttpResponse and associated classes to support communications through non-standard methods.
- Add more trace around configuration, session and ID cache database usage.
- Update configuration schema to specify authentication context and name ID format types.

2.6.0.3 – February 23, 2015

- Fix bug when processing logout response.
- Fix bug in validation against SAML schema.

2.6.0.2 – February 9, 2015

- Work around issue with .NET 2.0 VirtualPathUtility.ToAbsolute and query string parameters.

2.6.0.1 – January 23, 2015

- Add AllowCreate and SPNameQualifier properties to SSOOptions.
- For FIPS compilance, use SHA256CryptoServiceProvider rather than SHA256Managed in .NET 4.0.
- Allow SAML configuration file specification through SAMLConfigFile app setting in web.config.

2.6.0.0 – November 21, 2014

- Diagnostics trace to include exception stack trace.
- Add SAMLIdentityProvider.InitiateSSO override to directly specify the assertion consumer service URL and thereby overriding the configuration.
- Add SAMLServiceProvider.InitiateSSO override to directly specify the SSO service URL and thereby overriding the configuration.
- For consistency, rename SSOSessionStore to HttpSSOSessionStore.
- Modify configuration from CertificateFile to LocalCertificateFile and PartnerCertificateFile to make it clearer and also to support specifying a different LocalCertificateFile for each partner. This makes it easier to manage rolling over to a new local certificate in a staged manner.
- Strip Unicode left-to-right marker characters from certificate serial numbers etc that appear when pasted from the Windows Certificates snap-in.
- Move certificate classes to separate namespace.
- By default, monitor SAML configuration file changes.
- Update copyright to 2015.

2.5.0.20 – October 15, 2014

- Add DatabaseSSOSessionStore for storing SSO session data in a custom database.
- Add date to diagnostics trace.
- The DatabaseIDCache should return false if the ID is a duplicate rather than throwing an exception.

2.5.0.19 – August 13, 2014

- Add SingleLogoutServiceResponseUrl configuration attribute.

2.5.0.18 – August 1, 2014

- Add IsSSOPending and IsSLOPending methods.

2.5.0.17 – July 18, 2014

- Minor changes to SAMLConfiguration.Current to make its use more consistent.
- Sign MSIs with new certificate.

2.5.0.16 – May 30, 2014

- Add ProviderName configuration attribute.
- Include a SAMLConfiguration.Current setter and make setting the configuration programmatically easier.

- Minor updates associated with Visual Studio 2013 static code analysis.
- Don't verify signatures unless they have to be even if a signature is present.

2.5.0.15 – April 25, 2014

- Add ISSOSessionState to make it easier to store session state outside the ASP.NET session.
- Automatically load the saml.config on demand rather than in the static initializer.
- Add SAMLErrorStatusException.

2.5.0.14 – April 4, 2014

- Set the default logout binding type for the partner provider configuration.
- Automatically load the saml.config file if it exists.
- Add OverridePendingAuthnRequest configuration parameter.
- Reorganize exceptions.
- Add SSOOptions to high-level API.

2.5.0.13 – March 3, 2014

- Add RequestedAuthnContext configuration parameter.

2.5.0.12 – December 7, 2013

- Add ForceAuthn configuration parameter.

2.5.0.11 – November 23, 2013

- Digest and signature methods should be part of partner not local provider configuration.
- Fix bug in ManageNameIDRequest.ToXml.

2.5.0.10 – November 11, 2013

- Fix bug in SLO with multiple SPs.

2.5.0.9 – October 18, 2013

- Add SAMLConfiguration.Load(filename) and Unload methods.
- If the DatabaseIDCache.Add fails, throw an exception.
- Add the TraceLevel configuration property.
- Support different certificates for the local identity provider and service provider.
- Support specifying the ACS URL in SAMLServiceProvider.InitiateSSO.
- Add ImportMetadata and ExportMetadata.

2.5.0.8 – October 2, 2013

- Add the DisableInResponseToCheck configuration attribute.
- Add serialization constructors for exceptions.
- Support comma separator for duration fractional seconds.
- Add ISAMLObserver.OnSAMLAssertionSent and OnSAMLAssertionReceived.

2.5.0.7 – September 4, 2013

- Add SAMLIdentityProvider.SendSSO overload to allow for sending an error status.
- Set the default clock skew in the high-level API to 3 minutes.
- Synchronize the configuration loading to support SharePoint web parts etc where there's no convenient place to load the configuration.
- Add support for multi-tenancy applications.
- Add the DisableAudienceRestrictionCheck configuration attribute.

2.5.0.6 – July 16, 2013

- Support Issuer in SAML assertion.
- Include the SAML response error status in the exception.
- The configuration's SingleSignOnServiceUrl should be optional.
- Add DisableInboundLogout and DisableOutboundLogout configuration parameters.
- Add overloads to the high level API to specify name format for SAML attributes.
- Support XML node lists as attribute values.
- Support nil attribute value.

2.5.0.5 – July 1, 2013

- Accept logout request and permit logout response in the high-level API even if the partner no longer has a session.
- Support InResponseTo in the subject confirmation data.
- Add ISAMLObserver to support audit etc.

2.5.0.4 – June 14, 2013

- Add support in the high-level API for the service provider to send relay state.
- Add support for Office 365.

2.5.0.3 – June 3, 2013

- Add better support for custom configuration eg in a database.
- Fix empty attribute statement bug.

2.5.0.2 – May 23, 2013

- Add support for database ID cache.
- Allow configuration to be set programmatically rather than through saml.config.
- Add support for XML attributes in high-level API.

2.5.0.1 – May 6, 2013

- Add support for certificate management via configuration.
- Add support for SLO in the high-level API.

2.5.0.0 – April 13, 2013

- Add the SAML high-level API to simplify the SSO interface.
- Add SubjectConfirmationData.IsWithinTimePeriod methods.
- Fix the bug when adding XML signatures to the XML (only showed up in Mono).

2.4.0.17 – February 22, 2013

- Add convenience method for retrieving issuer from SAML response.

2.4.0.16 – February 8, 2013

- Add convenience methods for extracting SAML assertions.
- Add overloads for decrypting SAML assertions.

2.4.0.15 – January 21, 2013

- Add overloads for .NET 4 to take either HttpRequestBase or HttpRequest etc.

2.4.0.14 – January 14, 2013

- When decrypting a SAML assertion to XML prepare it for signature verification.

2.4.0.13 – October 31, 2012

- Fix bug with encryption method namespace in metadata key descriptor.

2.4.0.12 – September 21, 2012

- With the XSW attack fix, copy SAML messages from the SOAP message otherwise signature verification fails.

2.4.0.11 – August 23, 2012

- Fix XSW attack vulnerabilities from On Breaking SAML paper.

2.4.0.10 – August 14, 2012

- Add AttributeQueryRequester.SendAttributeQueryReceiveResponseBySOAP overload.
- Add support for creating post data for use in web browser control in thick client.

2.4.0.9 – June 12, 2012

- Add support for retrieving attributes by friendly name.

2.4.0.8 – April 20, 2012

- Fix bug adding accept header for PAOS binding.

2.4.0.7 – March 30, 2012

- For FIPS compliance, use Aes instead of Rijndael in .NET 4.0.

2.4.0.6 – January 20, 2012

- Include support for .NET 4 and ship a separate DLL.
- Add SAML.HttpContext so the HttpContextBase can be set when testing with mock objects.

2.4.0.5 – December 30, 2011

- Fix schema validation bug.

2.4.0.4 – December 16, 2011

- The EncryptionMethod element is optional but if present the Algorithm attribute is mandatory. A specific check is made and exception thrown if the Algorithm attribute is not present.

2.4.0.3 – November 1, 2011

- Build both .NET 2.0 and .NET 4.0 DLLs. The .NET 4 version uses the HttpRequestBase and HttpResponseBase classes etc.

2.4.0.2 – October 14, 2011

- Add Issuer.GetIssuer convenience method.
- Relax parsing of query string parameters as sometimes relay state isn't properly encoded.
- Add EntitiesDescriptor.GetEntityDescriptor.

2.4.0.1 – October 6, 2011

- Use HttpResponse.AddHeader instead of HttpResponse.Headers.Add as this isn't supported on IIS 6.

2.4.0.0 – September 26, 2011

- Add SAML.MillisecondPrecision property to turn on/off millisecond precision for date/times.

2.3.0.19 – August 8, 2011

- Fix XmlEncryption.GetEncryptedKey to use the URI when retrieving the key and also handle no key info in the encrypted data.
- Add ArtifactResolver.SendRequestReceiveResponse overload that takes a WebRequest.
- Add Decrypt methods that take dataEncryptionMethod parameter only without requiring keyEncryptionMethod.

2.3.0.18 – August 1, 2011

- Add convenience methods for determining artifact type.
- More precisely retrieve message from ArtifactResolve.
- Call PrepareForSignatureVerification on the message contained in the ArtifactResponse so signatures verify correctly.

2.3.0.17 – July 25, 2011

- Add support for http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p key encrypting algorithm.
- Add extra methods for retrieving artifacts.

2.3.0.16 – May 11, 2011

- Fix attribute serialization problem.

2.3.0.15 – February 1, 2011

- Set ID in metadata ready for signing.

2.3.0.14 – January 17, 2011

- Set content type to text/xml in SOAPBinding.SendResponse.

2.3.0.13 – January 7, 2011

- Add IsAttributeValueSerializerRegistered.

2.3.0.12 – January 5, 2011

- A null inclusiveNamespacesPrefixList means default not no list.

2.3.0.11 – December 4, 2010

- Add support for SHA-256 to HTTP/Redirect.

2.3.0.10 – December 1, 2010

- Add support for SHA-256 signatures.

2.3.0.9 – November 18, 2010

- Round times to milliseconds.

2.3.0.8 – November 10, 2010

- Trim inner text and attributes so whitespace isn't included when parsing XML.

2.3.0.7 – October 21, 2010

- Fix bug in DateTime conversion.

2.3.0.6 – September 24, 2010

- Reduce the risk of XML DOS attacks.
- Fix bug in Extensions which was using the wrong namespace.

2.3.0.5 – August 20, 2010

- Have the dataEncryptionMethod parameter to XmlEncryption.Decrypt only override the EncryptedData.EncryptionMethod if it isn't present.

2.3.0.4 – July 28, 2010

- Set the XmlResolver property in XmlDocument to null to attempt to avoid permissions errors when not in full trust mode eg SharePoint.

2.3.0.3 – July 2, 2010

- Fix bug in ArtifactResolve using wrong XML prefix.

2.3.0.2 – June 9, 2010

- Fix signature verification failure on signed response containing signed assertion generated by Java. The response signature verified but the assertion signature didn't. This appears to be a .NET SignedXml issue related to namespaces but it's not clear exactly what the cause is. As a workaround XmlSignature.PrepareForSignatureVerification has been defined to move namespace declarations to the document element. Signature verification now works for Java and .NET generated signatures. Also signature verification was modified to not set the KeyInfo in the SignedXml but instead use the appropriate CheckSignature overload.

2.3.0.1 – June 8, 2010

- Support KeyInfoRetrievalMethod on decryption.

2.3.0.0 – April 26, 2010

- Add ToString methods for SAMLAssertion etc.
- Add serialization support for SAMLAssertion.
- Add IsLicensed method for determining if evaluation or licensed version.
- Add support for supplying KeyInfo when encrypting SAML assertions, attributes etc.
- Add support for authentication, attribute and assertion query profiles and name identifier management and mapping profiles.

2.2.0.13 – March 22, 2010

- Add support for adding arbitrary KeyInfo when encrypting XML.

2.2.0.12 – March 16, 2010

- Add more trace.

2.2.0.11 – March 5, 2010

- Add ServiceProvider.ReceiveArtifactByHTTPArtifact.

2.2.0.10 – February 25, 2010

- Add trace to dump out HTTP requests.

2.2.0.9 – February 8, 2010

- Add convenience methods for setting attribute values.
- Add IdP discovery policy support.

2.2.0.8 – February 1, 2010

- Add SubjectConfirmationData constructors to accept not before/not on or after and timespan arguments.
- Add support for including attribute value type.

2.2.0.7 – November 20, 2009

- Add GetAttributes and GetAttributeValue methods.

2.2.0.6 – September 25, 2009

- Fix bug in SubjectConfirmationData.

2.2.0.5 – September 1, 2009

- Add more error checking and tracing around HTTP redirect query string parsing.

2.2.0.4 – August 9, 2009

- Fix bug if pass null attribute value to SAMLAttribute constructor.

2.2.0.3 – July 9, 2009

- Don't include the AssertionConsumerServiceIndex or AttributeConsumingServiceIndex in the AuthnRequest if they haven't been set.
- Use correct inclusive namespace prefix lists when signing.

2.2.0.2 – July 3, 2009

- SAMLAssertion.Find must copy the elements otherwise signature validation fails.

2.2.0.1 – June 19, 2009

- Fix bug in SAMLAssertion.ToXml which incorrectly placed the signature at the end of the assertion.

2.2.0.0 – June 15, 2009

- Allow inclusive namespace prefix list to be optional, specified or default when generating signatures.

2.1.0.5 – May 22, 2009

- Add SAMLValidator for validation against XML schema and an example project.

2.1.0.4 – February 11, 2009

- For POST binding allow writing POST data to a stream.

2.1.0.3 – October 9, 2008

- Detect encryption key size mismatches.

2.1.0.2 – October 2, 2008

- Fix bug with 128 and 192 bits AES keys.

2.1.0.1 – September 16, 2008

- Fixed bug with NameIDType's SPProvidedID name.

2.1.0.0 – August 29, 2008

- Add metadata support.
- Add support for additional encryption algorithms.

2.0.0.9 – July 4, 2008

- Fix serialization bug in EncryptedElementAbstract.

2.0.0.8 – April 25, 2008

- Add ParseHttpRedirectUrl OpenSAML example.
- Change URL encoding to use upper case (eg %2F instead of %2f) as lower case caused problems with OpenSAML.

2.0.0.7 – April 21, 2008

- Add Shibboleth and OpenSAML examples.
- Fix problems found during testing – Booleans can be 0 and 1, HTTP redirect signature verification error.
- Add support for extra encrypted key format.
- Add single logout support.

2.0.0.6 – April 8, 2008

- Serialize Booleans as “true” and “false” rather than “True” and “False”.

2.0.0.5 – April 1, 2008

- Fix bug with EncryptedAssertion deserialization.

2.0.0.4 – March 24, 2008

- Fix assertion signature bug found when adding AssertionExample project.

2.0.0.3 – March 19, 2008

- Fix relaystate bug.

2.0.0.2 – March 10, 2008

- Fix URL encoding bug.
- Add XML encryption support.

2.0.0.1 – August 1, 2007

- Initial release.

AES-GCM Extension

2.11.0 – January 10, 2025

- Update package dependencies.

2.10.0 – November 27, 2024

- Update package dependencies.

2.9.0 – July 25, 2024

- Update package dependencies.

2.8.0 – March 1, 2024

- Update package dependencies.

2.7.0 – November 7, 2023

- Update package dependencies.
- Switch from Portable.BouncyCastle to BouncyCastle.Cryptography NuGet package.

2.6.0 – September 7, 2023

- Update package dependencies.

2.5.0 – May 19, 2023

- Update package dependencies.

2.4.0 – March 15, 2023

- Update package dependencies.

2.3.0 – January 12, 2023

- Update package dependencies.

2.2.0 – November 17, 2022

- Update package dependencies.

2.1.0 – September 7, 2022

- Update package dependencies.

2.0.0 – July 5, 2022

- Ship as a NuGet package.

1.1.0 – November 19, 2021

- Reference the latest SAML library.

1.0.0 – October 20, 2020

- Initial release.

RSA-OAEP Extension

2.11.0 – January 10, 2025

- Update package dependencies.

2.10.0 – November 27, 2024

- Remove the .NET framework limitations by moving to BouncyCastle.
- Update package dependencies.

2.9.0 – July 25, 2024

- Update package dependencies.

2.8.0 – March 1, 2024

- Update package dependencies.

2.7.0 – November 7, 2023

- Update package dependencies.

2.6.0 – September 7, 2023

- Update package dependencies.

2.5.0 – May 19, 2023

- Update package dependencies.

2.4.0 – March 15, 2023

- Update package dependencies.

2.3.0 – January 12, 2023

- Update package dependencies.

2.2.0 – November 17, 2022

- Update package dependencies.

2.1.0 – September 7, 2022

- Update package dependencies.

2.0.0 – July 5, 2022

- Ship as a NuGet package.

1.1.0 – November 19, 2021

- Reference the latest SAML library.

1.0.0 – October 20, 2020

- Initial release.