# SAML Security Processing

## Introduction

This document summarizes the security processing in the ComponentSpace SAML products when acting as either the identity provider or service provider.

## SAML SSO - Identity Provider

The following sections summarize the security processing when acting as the identity provider during SAML SSO.

### Receiving an Authn Request

1. A SAML message is received correctly as per the SAML HTTP Bindings specification.
2. Check that the SAML message is well formed XML and an authn request.
3. Validate the authn request against the SAML XML schemas. This check may be disabled by setting the DisableSchemaCheck configuration property.
4. Check that the issuer matches one of the configured partner service providers.
5. Verify the signature if the WantAuthnRequestSigned configuration property is true.
6. Check the digest algorithm if the WantDigestAlgorithm configuration property is set.
7. Check the signature algorithm if the WantSignatureAlgorithm configuration property is set.
8. Check that the destination field matches the identity provider's name or identity provider's SSO service URL. This check may be disabled by setting the DisableDestinationCheck configuration property.
9. Check the assertion consumer service URL against the ValidAssertionConsumerServiceUrls configuration property.

### Sending a SAML Response

1. Check that a SAML authn request was previously received for SP-initiated SSO.
2. Sign the SAML assertion if the SignAssertion configuration property is set.
3. Encrypt the SAML assertion if the EncryptAssertion configuration property is set.
4. Sign the SAML response if the SignSamlResponse configuration property is set.

## SAML SSO - Service Provider

The following sections summarize the security processing when acting as the service provider during SAML SSO.

### Sending an Authn Request

1. Sign the authn request if the SignAuthnRequest configuration property is set.

### Receiving a SAML Response

1. A SAML message is received correctly as per the SAML HTTP Bindings specification.
2. Check that the SAML message is well formed XML and a SAML response.

3. Validate the SAML response against the SAML XML schemas. This check may be disabled by setting the DisableSchemaCheck configuration property.
4. Check that the issuer matches one of the configured partner identity providers.
5. Verify the SAML response signature if the WantSAMLResponseSigned configuration property is true.
6. Check the digest algorithm if the WantDigestAlgorithm configuration property is set.
7. Check the signature algorithm if the WantSignatureAlgorithm configuration property is set.
8. Check that the destination field matches the service provider's name or service provider's assertion consumer service URL. This check may be disabled by setting the DisableDestinationCheck configuration property.
9. Check the InResponseTo field. This check may be disabled by setting the DisableInResponseToCheck configuration property.
10. Check if IdP-initiated SSO. The DisableIdPInitiatedSso configuration property disables IdP-initiated SSO.
11. Check the success status.
12. Check that the SAML response contains one and only one SAML assertion.
13. Decrypt the SAML assertion if the WantAssertionEncrypted configuration property is set.
14. The SAML assertion must be well formed XML.
15. Validate the SAML assertion against the SAML XML schemas. This check may be disabled by setting the DisableSchemaCheck configuration property.
16. Verify the SAML assertion signature if the WantSAMLResponseSigned configuration property is true.
17. Check for assertion replay. This check may be disabled by setting the DisableAssertionReplayCheck configuration property.
18. Check that the recipient field matches the service provider's name or service provider's assertion consumer service URL. This check may be disabled by setting the DisableRecipientCheck configuration property.
19. Check that the assertion is within the NotBefore/NotOnOrAfter interval. This check may be disabled by setting the DisableTimePeriodCheck configuration property.
20. Check the audience restriction field matches the service provider's name. This check may be disabled by setting the DisableAudienceRestrictionCheck configuration property.
21. Check the authentication context field against the configured ExpectedAuthnContext. This check may be disabled by setting the DisableAuthnContextCheck configuration property.

## SAML SLO – Identity or Service Provider

The following sections summarize the security processing when acting as the identity provider or service provider during SAML logout.

### Receiving a SAML Logout Message

1. A SAML message is received correctly as per the SAML HTTP Bindings specification.
2. The SAML message must be well formed XML and a SAML logout request or response.
3. Validate the SAML logout message against the SAML XML schemas. This check may be disabled by setting the DisableSchemaCheck configuration property.
4. Check that the issuer matches one of the configured partner providers.

5. If a logout request, check that inbound logout is permitted. The DisableInboundLogout configuration property disables inbound logout.
6. Verify the signature if the WantLogoutRequestSigned/WantLogoutResponseSigned configuration property is true.
7. Check the digest algorithm if the WantDigestAlgorithm configuration property is set.
8. Check the signature algorithm if the WantSignatureAlgorithm configuration property is set.
9. If a logout response, confirm that a logout request was previously sent. This check may be disabled by setting the DisablePendingLogoutCheck configuration property.
10. If a logout response, check the InResponseTo field. This check may be disabled by setting the DisableInResponseToCheck configuration property.
11. If a logout response, check that the issuer matches the configured partner name from which a response is pending.
12. If a logout response, check whether the status is success. This check may be disabled by setting the DisableLogoutResponseStatusCheck configuration property.

## Sending a SAML Logout Message

1. Check that there's a partner provider to logout. The DisableOutboundLogout configuration property disables outbound logout.
2. Encrypt the logout request Name ID if the EncryptLogoutNameID configuration property is set.
3. Sign the logout request/response if the SignLogutRequest/SignLogoutResponse configuration property is set.