****

**Test Plan for Kantara Initiative – SAML2INT Profile** **Test Criteria**

**Version:**        1.1

**Date:**              2015-03-27

**Editor:**          Raj Srinivas, 8kMiles Inc.

 Lena Kannappan 8kMiles Inc.

**Contributors:**

The full list of contributors can be referenced here:

http://kantarainitiative.org/confluence/display/iopwg/Participant+Roster

**Status:** This document is a**Kantara Initiative Interoperability Work Group**

**(IOPWG) Final Report**, and has been approved by the IOPWG and Leadership Council.

(See section 3.9 and 4 of the Kantara Initiative Operating Procedures.)

**Abstract:**

This document describes the test steps to achieve the Kantara Initiative Interoperability

Certification designation for SAML2INT profile.

**Filename:**       Kantara\_Initiative\_SAML2INT\_Test\_Plan\_Final\_Report\_v1.1.pdf

**Notice:**

This document has been prepared by Participants of Kantara Initiative. Permission is

hereby granted to use the document solely for the purpose of implementing the

Specification. No rights are granted to prepare derivative works of this Specification.

Entities seeking permission to reproduce portions of this document for other uses must

contact Kantara Initiative to determine whether an appropriate license for such use is

available.

Implementation or use of certain elements of this document may require licenses under

third party intellectual property rights, including without limitation, patent rights. The

Participants of and any other contributors to the Specification are not and shall not be

held responsible in any manner for identifying or failing to identify any or all such third

party intellectual property rights. This Specification is provided "AS IS," and no

Participant in Kantara Initiative makes any warranty of any kind, expressed or implied,

including any implied warranties of merchantability, non-infringement of third party

intellectual property rights, and fitness for a particular purpose. Implementers of this

Specification are advised to review Kantara Initiative„s website

[(http://www.kantarainitiative.org/)](http://www.kantarainitiative.org/) for information concerning any Necessary Claims

Disclosure Notices that have been received by the Kantara Initiative Board of Trustees.

Copyright: The content of this document is copyright of Kantara Initiative. © 2010

Kantara Initiative.

**Contents**

**Contributors:.............................................................................................................................** [**1**](#1)

[**Abstract:**](#1)[**.....................................................................................................................................**](#1) [**1**](#1)

[**1**](#6)    [**INTRODUCTION**](#6)[**..............................................................................................................**](#6) [**5**](#6)

[1.1](#6)   [Overview](#6) [of](#6) [Test](#6) Plan....................................................................................................  [5](#6)

[1.2](#6)   [SAML2INT](#6) Profile [.............................................................................................................](#6)

[**2**](#6)  [**TEST**](#14)[**CASES**](#14)[**....................................................................................................................**](#14) [**5**](#14)

[2.1](#14)   [Overview](#14) [of](#14) [Test](#14) [Case](#14) [Description](#14) [.............................................................................](#14) [5](#14)

[2.2](#14)   [Test](#14) [Cases](#14) [Associated](#14) [with](#14) SAML2INT Profile......................................................  [5](#14)

[2.2.1](#15)       [Test](#15) [Case](#15) [SAML2INT-1:](#15) Production of IOP-compliant Metadata [...... ...........](#15) [6](#15)

[2.2.2](#17)       Test Case SAML2INT-2 – Consumption of IOP-compliant Metadata ........... [6](#17)

[2.2.3](#20)       Test Case SAML2INT-3 - Support for "Metadata Extension for Entity Attributes" Profile  [.............................](#20) [7](#20)

[2.2.4](#23)        Test Case SAML2INT-4 - Publication [................................](#23) [8](#23)

[2.2.5](#27)        Test Case SAML2INT-5 - Confirm support for NameIDPolicy of 'persistent' & 'transient'..........................................................................  [9](#27)

[2.2.6](#17)       Test Case SAML2INT-6 - IDP Discovery .......  [10](#17)

[2.2.7](#20)        Test Case SAML2INT-7 - AuthnRequest with HTTP-REDIRECT Binding Only [.............................](#20) [11](#20)

[2.2.8](#23)        Test Case SAML2INT-8 - Support for AssertionConsumerServiceURL and ProtocolBinding [................................](#23) [11](#23)

[2.2.9](#27)        Test Case SAML2INT-9 - Non-Support for Scoping element in AuthnRequest by IDPs that act as a proxy..........................................................................  [12](#23)

[2.2.10](#20)      Test Case SAML2INT-10 - Support for only POST Binding communication of SAML Response by IDP to SP [.............................](#20) [16](#20)

[2.2.11](#23)       Test Case SAML2INT-11 - Support for Signed Assertions in SAML Response  [................................](#23) [17](#23)

[2.2.12](#27)        Test Case SAML2INT-12 - Support for UnSolicited SAML Response by the SP..........................................................................  [18](#27)

[2.2.13](#27)       Test Case SAML2INT-13 - Support for presence of exactly one Assertion, one AuthnStatement, zero or one AttributeStatement in SAML Response and non-presence of BaseID or EncryptedID in Subject ..........................................................................  [19](#27)

[**3**](#6)[**REFERENCES**](#78)[**.................................................................................................................**](#78) [**20**](#78)

[3.1](#78)   [Normative](#78) [References](#78) [..................................................................................................](#78) [20](#78)

[3.2](#79)   [Non-Normative](#79) [References](#79) [..........................................................................................](#79) [21](#79)

**1   INTRODUCTION**

**1.1**     **Overview of Test Plan**

This document is the Kantara Initiative SAML 2.0 Test Criteria Test Plan, which contains

the scope of the technical requirements for Kantara Initiative certification of SAML2INT

profile. This document is intended to be publicly viewable through the Kantara Initiative website

as well as prospective test participants. The document is reviewed and authored by the

Interoperability Work Group (IOPWG) of Kantara Initiative.

The contents of this document include the test cases for SAML2INT Profile certification as well as

additional technical information relevant to testing.

**1.2**     **SAML2INT Profile**

The SAML2INT Profile is a conformance profile developed by the Kantara Initiative

eGovernment Work Group. The test cases within this test plan to achieve SAML2INT

certification are based on the requirements stated in the SAML2INT profile. The SAML2INT

profile and other associated documents should be consulted for further explanation of the

eGov requirements.

http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG\_SAML2.0\_INT\_SSO+Deployment+Profile\_v0.1.pdf

**2   TEST CASES**

**2.1**     **Overview of Test Case Description**

Each test case is setup with the first part listing an overview of the test steps in the test

case. The second part describes the details of the individual test steps to carry out the test

case. The test step overview lists the sequence of test steps along with a general

description of the message or action or configuration setting required. The test step

details provide more information on the expected test steps.

**2.2   Test Cases Associated with SAML2INT Profile**

In order to achieve certification in SAML2INT Profile Conformance

Mode, the associated test cases must be completed. The test cases are described in the following sections.

**2.2.1 Test Case SAML2INT-1 - Production of IOP-compliant Metadata**

**Scope**

Verify the ability to produce metadata conformant to the

Metadata IOP.**[MetaIOP]**

**Preconditions**

Implementation configured sufficiently to produce metadata identifying its signing, TLS,

and encryption keys.

Details of expected md:KeyDescriptor content available to tester

**Conformance Mode: SAML2INT**

**Test Sequence**

**Step 1. Access published metadata**

The metadata produced by the implementation is obtained.

CONFIRM: The metadata has an md:IDPSSODescriptor (if the producer of

the metadata is an IDP)

CONFIRM: The contents of the md:SingleSignOnService element(s) matches

the expected output (if the producer of the metadata is an IDP)

CONFIRM: The metadata has an md:SPSSODescriptor (if the producer of

the metadata is a SP)

CONFIRM: The contents of the md:AssertionConsumerService element(s) matches

the expected output (if the producer of the metadata is a SP)

CONFIRM: The content(s) of the md:KeyDescriptor element(s) matches the

expected output.

**2.2.2 Test Case SAML2INT-2 – Consumption of IOP-compliant Metadata**

**Scope**

Verify the ability to consume metadata conformant to the

Metadata IOP.**[MetaIOP]**

**Preconditions**

Implementation configured sufficiently to produce metadata identifying its signing, TLS,

and encryption keys.

Details of expected md:KeyDescriptor content available to tester

**Conformance Mode: SAML2INT**

**Test Sequence**

**Step 1. Access published metadata**

The metadata produced by the implementation is obtained.

CONFIRM: The metadata has an md:IDPSSODescriptor (if the producer of

the metadata is an IDP)

CONFIRM: The contents of the md:SingleSignOnService element(s) matches

the expected output (if the producer of the metadata is an IDP)

CONFIRM: The metadata has an md:SPSSODescriptor (if the producer of

the metadata is a SP)

CONFIRM: The contents of the md:AssertionConsumerService element(s) matches

the expected output (if the producer of the metadata is a SP)

CONFIRM: The content(s) of the md:KeyDescriptor element(s) matches the

expected output.

**2.2.3 Test Case SAML2INT-3 - Support for "Metadata Extension for Entity**

**Attributes" Profile**

**Scope:**

Test SP acceptance of SSO based on IdP metadata extension content**[MetaAttr]**

The proposed tag would be an attribute named

"urn:oasis:names:tc:SAML:attribute:assurance-certification" and would appear as follows

**[IAP]:**

<EntityDescriptor  entityID="https://idp.example.org/SAML"

...   >

<Extensions>

<attr:EntityAttributes

xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute">

<saml:Attribute

NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"

Name="urn:oasis:names:tc:SAML:attribute:assurance-

certification">

<saml:AttributeValue>

http://foo.example.com/assurance/loa1

</saml:AttributeValue>

</saml:Attribute>

</attr:EntityAttributes>

</Extensions>

<IDPSSODescriptor...>

...

</IDPSSODescriptor>

</EntityDescriptor>

**Preconditions:**

SP configured with metadata for candidate IdP containing acceptable LOA "tag".

SP configured with metadata for candidate IdP not containing acceptable LOA "tag".

SP configured to require presence of "tag" in metadata for IdPs before it will accept SSO

from them.

**Conformance Mode: SAML2INT**

**Test Sequence**

**Step 1. Verify use of acceptable IdP**

SP-initiated or IdP-initiated SSO is used to produce an assertion response from the

candidate IdP.

CONFIRM: SSO is successful.

**Step 2. Verify non-use of unacceptable IdP**

SP-initiated or IdP-initiated SSO is used to produce an assertion response from the

candidate IdP.

CONFIRM: SSO is unsuccessful based on the policy requiring the tag.

**2.2.4 Test Case SAML2INT-4 - Publication**

**Scope:**

Publication (and maintenance) of metadata via Well-Known-Location resolution profile.

**Preconditions:**

An http/https entityID defined that is suitable for dereferencing

Appropriate configuration of that entityID is completed

Multiple details of configuration are available to tester (location of a profile endpoint, a

key descriptor, etc.)

Any pre-publishing step required is completed

**Conformance Mode: SAML2INT**

**Test Sequence**

**Step 1. Access published metadata**

The entityID is dereferenced to obtain the metadata document.

CONFIRM**:** The metadata is available, and correctly reflects the entityID

accessed, and is returned with the correct MIME type

(application/xml+samlmetadata). The configuration details expected are found in

the metadata.

**Step 2. Alter metadata and republish**

Alter the configuration (changing an endpoint, a key descriptor, etc.) and republish, then

repeat the first test.

CONFIRM**:** As in (1), but also that the implementation did not require a restart or

disruption of service.

**2.2.5 Test Case SAML2INT-5 - Confirm support for NameIDPolicy of 'persistent'**

**& 'transient'**

**Scope:**

Verify SP possibility to specify values of 'persistent' & 'transient' for the NameIDPolicy

element in an AuthnRequest

**Preconditions:**

Metadata exchanged and imported

SP and IDP configured to use HTTP-Redirect binding for AuthnRequest

**Conformance Mode: SAML2INT**

**Test sequence**

**Step 1. Trigger SP-initiated single sign-on using the HTTP-Redirect binding,**

**specifying at SP that the returned identifier be**

**'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent'.**

CONFIRM: SP offers capability for specifying name identifier format of

"urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"

**Step 2. Observe HTTP redirect parameters and decode the SAMLRequest value**

**using the DEFLATE algorithm reversal.**

CONFIRM: presence of element "NameIDPolicy" with value

"urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" on element

<samlp:AuthnRequest>

**Step 3. Authenticate to IDP using test account**

**Step 4. Observe response message**

CONFIRM**:** NameID supplied according to NameIDPolicy specified in

AuthnRequest

**Repeat** above test sequence for 'urn:oasis:names:tc:SAML:2.0:nameid-

format:transient'.

**2.2.6 Test Case SAML2INT-6 - IDP Discovery**

**Scope:**

Verify that during web-based SSO that a SP is able to establish an IDP associated with

the user.

**Preconditions:**

Exchange and import metadata for SP (including extension element for the discovery‟s

response) and IDP

**Conformance Mode: SAML2INT**

**Test Sequence**

**Step 1. Trigger the SP to redirect the user agent to the discovery service with an**

**HTTP GET request.**

CONFIRM: SP capability for specifying policy of

"urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol:single"

**Step 2. Allow user to interact with discovery service to select an IDP by having**

**default setting of <IsPassive> to “false”.**

**Step 3. The discovery service responds by redirecting the user agent back to the**

**requesting service provider with an HTTP GET request at the location supplied in**

**the <return> parameter in the original request and/ or discovery response element**

**of the metadata.**

CONFIRM: SP recognizes the identifier for the selected Identity Provider

**Step 4. IdP is reconfigured with <IsPassive> set to “true”. CDC is deleted.**

**Step 5. User attempts to interact with discovery service and select IDP but**

**<isPassive> set to "true" prevents interaction with the user.**

CONFIRM: SP returns no IDP selection

**2.2.7 Test Case SAML2INT- 7 – AuthnRequest with HTTP-REDIRECT Binding Only**

**Scope:**

Verify SP possibility to specify values other than HTTP-REDIRECT binding in AuthnRequest.

**Preconditions:**

Metadata exchanged and imported

SP and IDP configured to use HTTP-Redirect binding for AuthnRequest

**Conformance Mode: SAML2INT**

**Test sequence**

**Step 1. Trigger SP-initiated single sign-on using the HTTP-POST binding,**

**specifying that a particular AssertionConsumerServiceURL be called using a**

**specified ProtocolBinding i.e HTTP-POST Binding.**

CONFIRM**:** SP offers capability for specifying the AssertionConsumerService

URL

CONFIRM**:** SP offers capability for specifying the ProtocolBinding to be used

**Step 2. Observe IDP to check if it accepts an AuthnRequest with HTTP-POST binding**

CONFIRM: IDP error code to the SP’s AuthnRequest

**2.2.8 Test Case SAML2INT- 8 –Support for AssertionConsumerServiceURL and**

**ProtocolBinding**

**Scope:**

Verify possibility to specify, and presence of, the AuthnRequest attributes

AssertionConsumerServiceURL, ProtocolBinding and non-presence of Subject

**Preconditions:**

Metadata exchanged and imported

Service provider metadata contains indexed AssertionConsumerService entries

SP and IDP configured to use HTTP-Redirect binding for AuthnRequest

**Conformance Mode: SAML2INT**

**Test sequence**

**Step 1. Trigger SP-initiated single sign-on using the HTTP-Redirect binding,**

**specifying that a particular AssertionConsumerServiceURL be called using a**

**specified ProtocolBinding.**

CONFIRM**:** SP offers capability for specifying the AssertionConsumerService

URL

CONFIRM**:** SP offers capability for specifying the ProtocolBinding to be used

**Step 2. Observe HTTP redirect parameters and decode the SAMLRequest value**

**using the DEFLATE algorithm reversal.**

CONFIRM**:** presence of attribute "AssertionConsumerServiceURL" with the

URL specified in step 1 as value, on element <samlp:AuthnRequest>

CONFIRM**:** presence of attribute "ProtocolBinding" with the URL specified in

step 1 as value, on element <samlp:AuthnRequest>. This MUST be “HTTP-POST

binding” as the SP expects IDP to return a SAML Response by HTTP-POST Binding.

CONFIRM**:** absence of attribute "Subject” on element <samlp:AuthnRequest>

**2.2.9 Test Case SAML2INT- 9 – Non-Support for Scoping element in AuthnRequest by IDPs that act as a proxy**

**Scope:** Check for the non-presence of Scoping element in AuthnRequest

**Preconditions:**

Metadata exchanged and loaded

Encryption disabled

User Identities Not Federated

**Conformance Modes: SAML2INT**

**Background on IdP Proxy**

Refer to Section 3.4.1.5 of [SAMLCore] for more background. The IdP Proxy feature

requires two IdP implementations and one SP implementation. Let us assume we have participants A

and B and let us assume that IdPA and SPB are the implementations under test:

To complete this Test Case, the IdP under test(IdPA) must receive an authentication request for

a User it can not authenticate but a User that the supporting IdP(IDPB) can authenticate. This

coordination of User accounts must be done prior to executing the test case.

**Step 1: ProxyCount=0**

Description: SP sets ProxyCount=0 where proxy is disallowed.

SP CONFIRM: SP has disallowed proxy.

**Step 2: AuthnRequest from SP to IdPA, Redirect Binding, Federate**

Description: User/SP attempts Single Sign-On with Persistent Name Identifier to

Federate with AllowCreate is set to TRUE. SP communication to the IdPA for the SAML

Authentication Request is through HTTP Redirect binding. IdPA does not recognize User

and thus can not authenticate user.

IdPA CONFIRM: ProxyCount is set to 0.

IdPA CONFIRM: AuthnRequest does not contain the Scope element.

IdPA CONFIRM: User is not authenticated.

**Step 3: Response Failure**

Description: Being unable to authenticate User, IdPA returns SAML Response with error

indicating AuthnRequest failed.

SP CONFIRM: IdPA returns SAML Response indicating authentication error.

**Step 4: ProxyCount is Removed and IdP List is set**

Description: SP removes ProxyCount where proxy is allowed. SP configures <IdPList>

to include IdPB.

SP CONFIRM: SP has removed ProxyCount to allow proxy.

SP CONFIRM: SP has set <IdPList> to include IdPB.

**Step 5: AuthnRequest from SP to IdPA, Redirect Binding, Federate**

Description: User/SP does Single Sign-On with Persistent Name Identifier to Federate

with AllowCreate is set to TRUE. SP communication to the IdPA for the SAML

Authentication Request is through HTTP Redirect binding. IdPA does not recognize User

but recognizes it can proxy the AuthnRequest to IdPB.

IdPA CONFIRM: ProxyCount is not set.

IdPA CONFIRM: User is not authenticated.

IdPA CONFIRM: AuthnRequest contains <IdPList> which includes IdPB.

IdPA CONFIRM: AuthnRequest does not contain Scope element

**Step 6: AuthnRequest from IdPA to IdPB, Redirect Binding, Federate**

Description: IdPA proxies AuthnRequest to IdPB through HTTP Redirect binding.

IdPB CONFIRM: Receives AuthnRequest from IdPA.

IdPB CONFIRM: ProxyCount is set to 0.

IdPB CONFIRM: <IdPList> includes IdPB.

IdPB CONFIRM: AuthnRequest does not contain Scope element

**Step 7: Assertion Response from IdPB to IdPA, POST binding**

Description: User provides assigned credentials to IdPB for authentication. IdPB provides

assertion of User and returns a signed SAML Response message to IdPA through HTTP

POST binding.

IdPA CONFIRM: Receives SAML Response through HTTP POST binding.

IdPA CONFIRM: Valid assertion is returned from IdPB.

IdPA CONFIRM: <AuthnStatement> contains <AuthenticatingAuthority>

referencing IdPB.

**Step 8: Assertion Response from IdPA to SP, POST binding**

Description: IdPA inserts assertion of User it received from IdPB and returns a signed

SAML Response message to SP through HTTP POST binding.

SP CONFIRM: Receives SAML Response through HTTP POST binding.

SP CONFIRM: Valid assertion is returned from IdPA.

SP CONFIRM: <AuthnStatement> contains <AuthenticatingAuthority>

referencing IdPB.

**Step 9: SLO Request, IdP-Initiated, Redirect Binding**

Description: IdPA logs out User session. IdPA sends a signed LogoutRequest message to

SP using HTTP Redirect binding.SP logs out User session. SP returns a signed

LogoutResponse message to IdPA using HTTP Redirect binding.

IdPA CONFIRM: User logged out at IdPA.

SP CONFIRM: Receives signed LogoutRequest through HTTP Redirect binding.

SP CONFIRM: User logged out at SP.

IdPA CONFIRM: Receives signed LogoutResponse through HTTP Redirect

binding.

**Step 10: ProxyCount=1 and IdP List is set**

Description: SP makes ProxyCount set to 1. SP configures <IdPList> to include IdPB.

SP CONFIRM: SP sets ProxyCount to 1.

SP CONFIRM: SP has set <IdPList> to include IdPB.

**Step 11: AuthnRequest from SP to IdPA, Redirect Binding, Federate**

Description: User/SP does Single Sign-On with Persistent Name Identifier to Federate

with AllowCreate is set to TRUE. SP communication to the IdPA for the SAML

Authentication Request is through HTTP Redirect binding. IdPA does not recognize User

but recognizes it can proxy the AuthnRequest to IdPB.

IdPA CONFIRM: ProxyCount is set to 1.

IdPA CONFIRM: User is not authenticated.

IdPA CONFIRM: AuthnRequest contains <IdPList> which includes IdPB.

IdPA CONFIRM: AuthnRequest does not contain Scope element

**Step 12: AuthnRequest from IdPA to IdPB, Redirect Binding, Federate**

Description: IdPA proxies AuthnRequest to IdPB through HTTP Redirect binding.

IdPB CONFIRM: Receives AuthnRequest from IdPA.

IdPB CONFIRM: ProxyCount is set to 0.

IdPB CONFIRM: <IdPList> includes IdPB.

IdPB CONFIRM: AuthnRequest does not contain Scope element

**Step 13: Assertion Response from IdPB to IdPA, POST binding**

Description: User provides assigned credentials to IdPB for authentication. IdPB provides

assertion of User and returns a signed SAML Response message to IdPA through HTTP

POST binding.

IdPA CONFIRM: Receives SAML Response through HTTP POST binding.

IdPA CONFIRM: Valid assertion is returned from IdPB.

IdPA CONFIRM: <AuthnStatement> contains <AuthenticatingAuthority>

referencing IdPB.

**Step 14: Assertion Response from IdPA to SP, POST binding**

Description: IdPA inserts assertion of User it received from IdPB and returns a signed

SAML Response message to SP through HTTP POST binding.

SP CONFIRM: Receives SAML Response through HTTP POST binding.

SP CONFIRM: Valid assertion is returned from IdPA.

SP CONFIRM: <AuthnStatement> contains <AuthenticatingAuthority>

referencing IdPB.

**Step 15: SLO Request, IdP-Initiated, Redirect Binding**

Description: IdPA logs out User session. IdPA sends a signed LogoutRequest message to

SP using HTTP Redirect binding.SP logs out User session. SP returns a signed

LogoutResponse message to IdPA using HTTP Redirect binding.

IdPA CONFIRM: User logged out at IdPA.

SP CONFIRM: Receives signed LogoutRequest through HTTP Redirect binding.

SP CONFIRM: User logged out at SP.

IdPA CONFIRM: Receives signed LogoutResponse through HTTP Redirect

binding.

**2.2.10 Test Case SAML2INT- 10 – Support for only POST Binding communication of SAML Response by IDP to SP**

**Scope:**

Verify acceptance of POST Binding only in AuthnRequest

**Preconditions:**

Metadata exchanged and imported

Service provider metadata contains indexed AssertionConsumerService entries

SP and IDP configured to use HTTP-Redirect binding for AuthnRequest

IDP configured to return SAML Response to SP in POST Binding

**Conformance Mode: SAML2INT**

**Test sequence**

**Step 1. Trigger SP-initiated single sign-on using the HTTP-Redirect binding,**

**specifying that a particular AssertionConsumerServiceURL be called using a**

**HTTP-REDIRECT ProtocolBinding.**

CONFIRM**:** SP offers capability for specifying the AssertionConsumerService

URL

CONFIRM**:** SP offers capability for specifying the ProtocolBinding (HTTP-REDIRECT in this case) to be used

**Step 2. Observe HTTP redirect parameters and decode the SAMLRequest value**

**using the DEFLATE algorithm reversal.**

CONFIRM**:** presence of attribute "AssertionConsumerServiceURL" with the

URL specified in step 1 as value, on element <samlp:AuthnRequest>

CONFIRM**:** presence of attribute "ProtocolBinding" with the URL specified in

step 1 as value, on element <samlp:AuthnRequest>. This for testing purposed can be “HTTP-Redirect binding” as the SP expects IDP to return a SAML Response by HTTP-Redirect Binding.

CONFIRM**:** absence of attribute "Subject” on element <samlp:AuthnRequest>

**Step 3. Error accepting/responding to the SAML Request by the IdP**

CONFIRM**:** Error at the IDP responding to the <samlp:AuthnRequest> (as the IDP is configured to respond only in POST binding and not Redirect binding). Observe the error message.

**2.2.11 Test Case SAML2INT- 11 – Support for Signed Assertions in SAML Response**

**Scope:**

Verify presence of signed Assertion in SAML Response

**Preconditions:**

Metadata exchanged and imported

Service provider metadata contains indexed AssertionConsumerService entries

SP and IDP configured to use HTTP-Redirect binding for AuthnRequest

IDP configured to return SAML Response to SP in POST Binding

**Conformance Mode: SAML2INT**

**Test sequence**

**Step 1. Trigger SP-initiated single sign-on using the HTTP-Redirect binding,**

**specifying that a particular AssertionConsumerServiceURL be called using a**

**specified ProtocolBinding.**

CONFIRM**:** SP offers capability for specifying the AssertionConsumerService

URL

CONFIRM**:** SP offers capability for specifying the ProtocolBinding to be used

**Step 2. Observe HTTP redirect parameters and decode the SAMLRequest value**

**using the DEFLATE algorithm reversal.**

CONFIRM**:** presence of attribute "AssertionConsumerServiceURL" with the

URL specified in step 1 as value, on element <samlp:AuthnRequest>

CONFIRM**:** presence of attribute "ProtocolBinding" with the URL specified in

step 1 as value, on element <samlp:AuthnRequest>. This MUST be “HTTP-POST

binding” as the SP expects IDP to return a SAML Response by HTTP-POST Binding.

CONFIRM**:** absence of attribute "Subject” on element <samlp:AuthnRequest>

**Step 3. Authenticate to IDP using test account**

**Step 4. Observe response message**

CONFIRM**:** Presence of a valid Assertion that is signed

CONFIRM**:** Verification of the signature by the SP

**2.2.12 Test Case SAML2INT- 12 – Support for UnSolicited SAML Response by the SP**

**Scope:**

Verify receipt of Unsolicited SAML Response with an Assertion in it

**Preconditions:**

Metadata exchanged and imported

Service provider metadata contains indexed AssertionConsumerService entries

IDP configured to return SAML Response to SP in POST Binding

**Conformance Mode: SAML2INT**

**Test sequence**

**Step 1. Trigger IDP-initiated single sign-on, specifying a particular AssertionConsumerServiceURL**

CONFIRM**:** IDP offers capability for specifying the AssertionConsumerService

URL

**Step 2. Authenticate to IDP using test account**

**Step 3. Observe response message**

CONFIRM**:** one Assertion in SAML Response

CONFIRM**:** one AuthnStatement within the Assertion

CONFIRM**:** zero or one AttributeStatement within the Assertion

CONFIRM**:** absence of BaseID or EncryptedID under Subject element.

**2.2.13 Test Case SAML2INT- 13 –Support for presence of exactly one Assertion, one AuthnStatement, zero or one AttributeStatement in SAML Response and non-presence of BaseID or EncryptedID in Subject**

**Scope:**

Verify presence of one Assertion, AuthnStatement and AttributeStatement in SAML Response Verify absence of BaseID or EncryptedID in Subject element of the SAML Response

**Preconditions:**

Metadata exchanged and imported

Service provider metadata contains indexed AssertionConsumerService entries

SP and IDP configured to use HTTP-Redirect binding for AuthnRequest

IDP configured to return SAML Response to SP in POST Binding

**Conformance Mode: SAML2INT**

**Test sequence**

**Step 1. Trigger SP-initiated single sign-on using the HTTP-Redirect binding,**

**specifying that a particular AssertionConsumerServiceURL be called using a**

**specified ProtocolBinding.**

CONFIRM**:** SP offers capability for specifying the AssertionConsumerService

URL

CONFIRM**:** SP offers capability for specifying the ProtocolBinding to be used

**Step 2. Observe HTTP redirect parameters and decode the SAMLRequest value**

**using the DEFLATE algorithm reversal.**

CONFIRM**:** presence of attribute "AssertionConsumerServiceURL" with the

URL specified in step 1 as value, on element <samlp:AuthnRequest>

CONFIRM**:** presence of attribute "ProtocolBinding" with the URL specified in

step 1 as value, on element <samlp:AuthnRequest>. This MUST be “HTTP-POST

binding” as the SP expects IDP to return a SAML Response by HTTP-POST Binding.

CONFIRM**:** absence of attribute "Subject” on element <samlp:AuthnRequest>

**Step 3. Authenticate to IDP using test account**

**Step 4. Observe response message**

CONFIRM**:** NameID supplied according to NameIDPolicy specified in

AuthnRequest

CONFIRM**:** one Assertion in SAML Response

CONFIRM**:** one AuthnStatement within the Assertion

CONFIRM**:** zero or one AttributeStatement within the Assertion

CONFIRM**:** absence of BaseID or EncryptedID under Subject element.

**3**     **REFERENCES**

**3.1**     **Normative References**

**[ExcXMLCan]** John Boyer et al, “Exclusive XML Canonicalization Version 1.0, W3C

Recommendation”, W3C (July 2002), <http://www.w3.org/TR/xml-exc-c14n/>

**[IAP]** OASIS Committee Draft, Identity Assurance Profiles, Version 1.0, September 2009.

[http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.pdf)

[01.pdf](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.pdf)

**[MetaIOP]** OASIS Committee Specification, SAML V2.0 Metadata Interoperability Profile

Version 1.0, August 2009. [http://docs.oasis-open.org/security/saml/Post2.0/sstc-](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf)

[metadata-iop.pdf](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf)

**[SAMLAuthnCxt]** J. Kemp et al, “Authentication Context for the OASIS Security

Assertion Markup Language (SAML) V2.0,” OASIS SSTC (March 2005),

<http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>

**[SAMLBind]** Scott Cantor et al, “Bindings for the OASIS Security Assertion Markup

Language (SAML) V2.0,” OASIS SSTC (March 2005), [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)

[open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)

**[SAMLConf]** Prateek Mishra et al, “Conformance Requirements for the OASIS Security

Assertion Markup Language (SAML) V2.0,” OASIS SSTC (March 2005).

<http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>

**[SAMLCore]** S. Cantor et al, “Assertions and Protocols for the OASIS Security

Assertion Markup Language (SAML) V2.0,” OASIS SSTC (March 2005),

<http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

**[SAMLErrata]** Jahan Moreh, “Errata for the OASIS Security 2 Assertion Markup

Language (SAML) V2.0, Working Draft 28,” OASIS SSTC (May 8, 2006),

[http://www.oasis-open.org/committees/download.php/18070/sstc-saml-errata-2.0-](http://www.oasis-open.org/committees/download.php/18070/sstc-saml-errata-2.0-draft-28.pdf)

[draft-28.pdf](http://www.oasis-open.org/committees/download.php/18070/sstc-saml-errata-2.0-draft-28.pdf)

**[SAMLMeta]** S. Cantor et al, “Metadata for the OASIS Security Assertion Markup

Language (SAML) V2.0,” OASIS SSTC (March 2005), [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

[open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

**[MetaAttr]** OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity

Attributes Version 1.0, August 2009. [http://docs.oasis-](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf)

[open.org/security/saml/Post2.0/sstc-metadata-attr.pdf](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf)

**[SAMLMetaExt]** Tom Scavo et al, “Metadata Extension for SAML V2.0 and V1.x

Query Requesters”, OASIS SSTC (Nov 2007), http://docs.oasis-

open.org/security/saml/Post2.0/sstc-saml-metadata-ext-query-os.pdf

**[SAMLProf]** S. Cantor et al, “Profiles for the OASIS Security Assertion Markup

Language (SAML) V2.0,” OASIS SSTC (March 2005), [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.)

[open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.)

**[SAMLSec]** Frederick Hirsch et al, “Security and Privacy Considerations for the OASIS

Security Assertion Markup Language (SAML) V2.0,” OASIS SSTC (March

2005), <http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf>

**[SAML2INT]**  Andreas Akre Solberg et al, “SAML2.0 INT SSO Deployment Profile”,

Kantara Initiative (December 2011), http://kantarainitiative.org/confluence/download/attachments/41649836/FIWG\_SAML2.0\_INT\_SSO+Deployment+Profile\_v0.1.pdf

**3.2**     **Non-Normative References**

**[ICAM]** J. Bradley et al, Federal Identity, Credentialing, and Access Management

Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-on

(SSO) Profile (2010)

<http://www.idmanagement.gov/documents/SAML_20_SSO_Profile_Draft.doc>

**[INC]** InCommon Assurance Technical Procedures

<http://www.incommonfederation.org/assurance/technical_procedures.cfm>

**[NZ]** New Zealand Government Authentication Context Profiles

www.authentication.govt.nz/pub/igovt-ils-authncontext.pdf