Cross Operation of Single Sign-On, Federation, and Identity Web Services Frameworks

Version: 1.1

Editors:
Sampo Kellomäki, Symlabs, Inc.

Contributors:
Conor Cahill, Intel
Rob Lockhart, IEEE-ISTO
Guillermo Lorenzo, Symlabs, Inc.
Paul Madsen, NTT
Greg Whitehead, Hewlett-Packard

Abstract:

As standards evolve, both in versions and in scope, it is necessary to adopt newer technologies. This poses problems in terms of already-provisioned federations as well as in using combinations of frameworks that were not foreseen at the time when the specifications were written.

This technote provides pragmatic solutions for these situations, providing equivalence or interoperability of Name IDs as well as specifying how all known combinations of SSO assertions and bootstraps are represented.

Filename: liberty-cross-framework-v1.1.pdf

Notice

This document has been prepared by Sponsors of the Liberty Alliance. 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 the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Sponsors 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 the Liberty Alliance makes any warranty of any kind, express 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 the Liberty Alliance Project's website (http://www.projectliberty.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance Management Board.

Liberty Alliance Project
Licensing Administrator
c/o IEEE-ISTO
445 Hoes Lane
Piscataway, NJ 08855-1331, USA
info@projectliberty.org

Contents

1. Introduction

As standards evolve, both in versions and in scope, it is necessary to adopt newer technologies. This poses problems in terms of already-provisioned federations as well as in using combinations of frameworks that were not foreseen at the time when the specifications were written.

This technote provides specific solutions to these advanced problems. For introductory material, see [LibertyIDWS-FGuide10].

1.1. Notational Conventions

In case of disagreement between the present document and any guidelines or [XML] schema descriptions, this document is prescriptive. Any published errata is hereby incorporated to this document by reference and as such is normative.

The key words "MUST," "MUST NOT," "REQUIRED," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" in this specification are to be interpreted as described in IETF [RFC2119].

2. Name ID Compatibility Between SAML 1.x, ID-FF 1.x, and SAML 2.0

SAML assertions are the basis of most modern Single Sign-On (SSO) and Federation Frameworks. There is a frequent need to migrate already-existing federations between the different versions of SAML assertions or, indeed, serve from the same federation database, both SAML 2.0 [SAMLCore2] and SAML 1.1 [SAMLCore] assertions, simultaneously, as would be necessary in heterogeneous environments of partners supporting different versions of SAML.

Historically, Liberty ID-FF and, lately, SAML 2.0 have evolved towards a better understood and more coherent Name ID, or *pseudonym*, format and management system. The SAML 2.0 incarnation represents the current culmination of this evolution. While the Name ID format varies between SAML versions and while the additional semantics attached by various Liberty ID-FF versions vary, as well, it is possible to define a least common denominator format. In this discussion, we are mainly concerned with pseudonyms because they are characteristically used in federation databases. Other formats, such as temporary Name IDs, do not present similar problems.

By adopting the conventions described below, it is possible to support many types of federation protocols from one federation database.

2.1. An Introduction to Name IDs

A SAML 1.1 <**NameIdentifier**> carries `NameQualifier` and `Format` [XML] attributes. See [SAMLCore] Section 2.4.2.2 "Element <**NameIdentifier**>," p. 18.

A SAML 2.0 <**NameID**>, which is of XSD type `NameIDType`, carries `NameQualifier`, `SPNameQualifier`, `Format`, and `SPProvidedID` [XML] attributes. See [SAMLCore2], Section 2.2.2 "Complex Type NameIDType," p. 13.

Liberty ID-FF 1.2 [LibertyProtSchema], Section 3.1.11.1 "Deprecation of ID-FF 1.1 Name Identifier Practices," discusses some problems that older versions of the specifications have with respect to Name IDs.

2.2. NameQualifiers Across Versions

For each federation, the IdP always assigns a Name ID for the Principal, but it is qualified by the namespace of the SP towards which the Principal is federated. By convention, the namespace qualification is expressed by carrying the Provider ID or Entity ID of the SP, or the *affiliation* to which the SP belongs, in the `NameQualifier`. Both versions of SAML assertions work the same in this regard.

Versions of ID-FF prior to 1.2 did not support affiliations and did not require any *NameQualifier* to be specified, but, unfortunately, allowed it to be specified without specifying what the allowable values were. If an old federation has a nonstandard `NameQualifier`, then that should be kept in a database and reproduced when using Liberty ID-FF 1.0 or 1.1 protocols. However, when talking Liberty ID-FF 1.2 or SAML 2.0 protocol, the old `NameQualifier` MUST be ignored and the Provider ID or Entity ID used instead.

For each federation, it is possible for the SP to register an additional Name ID, which will be sent back to the SP whenever the IdP talks to the SP about the given federation. However, Liberty ID-FF 1.2 and SAML 2.0 behave differently in this regard. In SAML 2.0, the SP Name ID is always carried in `SPProvidedID`, which can be namespace-qualified using `SPNameQualifier`, which contains the affiliation ID of the SP, if any, or, otherwise, the entity ID of the SP.

ID-FF 1.x extended the SAML Subject to add an `IDPProvidedNameIdentifier` element in addition to <**NameIdentifier**>. In the case where there is no SP-provided Name ID, then both `Subject`/`NameIdentifier` and `Subject`/`IDPProvidedNameIdentifier` are the IdP-provided Name ID. In the case where there is an SP-provided Name ID, it goes in Subject/`NameIdentifier` and Subject/`IDPProvidedNameIdentifier` is the IdP-provided Name ID.

In SAML 1.1, there is no special way to express the SP-registered Name ID. By convention, in communications towards the SP, the <**NameIdentifier**> contains (properly namespace-qualified) the SP-registered Name ID, if any, or, otherwise, the IdP-assigned Name ID. In communications towards the IdP, the <**NameIdentifier**> always carries the IdP-assigned Name ID.

`NameQualifier` and `Format` in an ID-FF SP-provided Name ID is discarded when translating to SAML 2.0 unless they happen to correspond to the SAML 2.0-specified values. Clearly, this could be problematic and, practically, it restricts interoperability to the cases where implementations are not dependent on these values being preserved. ID-FF 1.x deployments that are using these features may need to take the step of updating their federations to be SAML 2.0-compatible before attempting migration or interoperability.

In various versions of Liberty ID-FF, different rules, which may or may not differ from the base convention, apply to what is appropriate to carry in the <**NameIdentifier**> when using the Name ID Registration protocol. Understanding these is left as an exercise to the reader.

> **Conclusion**: NameQualifiers are interoperable between SAML 2.0, Liberty ID-FF 1.2, and SAML 1.1. Earlier versions of Liberty ID-FF require special case treatment.

2.3. Name ID Formats

In SAML, a Name ID may have different formats. Of interest here is the *pseudonymous* format, a.k.a. *persistent* format. SAML 1.1 [SAMLCore], Section 7.3 "NameIdentifier Format Identifiers," p. 49, does not specify this format, but Liberty ID-FF 1.2 [LibertyProtSchema], Section 3.2.2.3 "SubjectType and Related Types," p. 18, specifies `urn:liberty:iff:nameid:federated` and, in Section 3.2.1.1 "Element <**AuthnRequest**>," p. 14, a corresponding <**NameIDPolicy**> enumerator `federated`. SAML 2.0 [SAMLCore2], Section 8.3.7 "Persistent Identifier," p. 79, specifies `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` and also specifies, in Section 3.4.1.1 "Element <**NameIDPolicy**>," p. 50, that the same enumerator is used as `NameIDPolicy`.

We adopt the convention that `urn:liberty:iff:nameid:federated` and `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` are treated synonymously such that if a federation database has a Name ID in the former format, it MUST be reported in SAML 2.0 transactions as the latter format, and if a database has a Name ID in the latter format, it MUST be reported in SAML 1.1 or Liberty ID-FF transactions as the former format.

We also adopt the convention that ID-FF 1.2 `urn:liberty:iff:nameid:one-time` is mapped to `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` and vice versa, as needed.

Both versions of SAML specify the Name ID as `xs:string`, thus, the actual value of the Name ID does NOT have compatibility issues. However, we RECOMMEND that Name IDs be URIs for improved compatibility and be restricted to the character set of safe base 64 encoding [RFC3548] for maximum compatibility.

> **Conclusion**: Name ID Formats are interoperable by treating *federated* (ID-FF) and *persistent* (SAML 2.0) as equivalent.

3. Independence of SSO (a.k.a. Federation) Framework from WS Framework

3.1. Guidance for Cross Use of SSO and WS Frameworks

Single Sign-On (SSO) frameworks (often referred to as Federation Frameworks), such as SAML 2.0 [SAMLCore2] and Liberty ID-FF 1.2 [LibertyProtSchema], are nearly entirely disjoint from Identity Web Services frameworks such as Liberty ID-WSF 1.0, ID-WSF 1.1 [LibertyIDWSFGuide10], and ID-WSF 2.0 [LibertyIDWSFGuide]. The only connection occurs when, as part of an SSO, a *discovery bootstrap* is conveyed. Therefore, it is desirable to decouple the choice of SSO framework from the choice of Identity Web Services frameworks.

Each framework makes an independent choice of the version of SAML assertions that is used within its own sphere. A different version can be profitably used in each sphere, thus all combinations in the accompanying table are valid. However, Liberty ID-FF 1.2 with ID-WSF 2.0, but only using SAML 1.1 assertions for both, is NOT valid. Similarly, SAML 2.0 with ID-WSF 1.1, but only using SAML 2.0 assertions for both, is not valid.

Table 1. Valid Combinations of Frameworks and SAML versions: SSO Assertion Version (Bootstrap Assertion Version)

	ID-WSF 1.1	**ID-WSF 2.0**
SAML 2.0 protocol	SAML 2.0 (SAML 1.1)	SAML 2.0 (SAML 2.0)
Liberty ID-FF 1.2	SAML 1.1 (SAML 1.1)	SAML 1.1 (SAML 2.0)

The SSO operation results in a Federation framework-dependent version of a SAML assertion that carries an ID-WSF version-dependent SAML assertion. All versions of SAML assertions support attribute statements and an attribute statement[1] is capable of carrying an arbitrary payload. There is no problem in the inner assertion being of a different version than the assertion carrying the attribute statement. Implementations wishing to support cross operation will simply need to support multiple versions of SAML.

3.2. Trivial Interoperability

Interoperability of Liberty ID-FF 1.2 with Liberty ID-WSF 1.1 is described in [LibertyDisco12], Section 6 "SAML AttributeDesignator for Discovery ResourceOffering."

Interoperability of Liberty ID-FF 1.2 and SAML 2.0 with Liberty ID-WSF 2.0 is described in [LibertyDisco].

3.3. Interoperability Between SAML 2.0 SSO and Liberty ID-WSF 1.1

It turns out that Liberty ID-WSF 1.1 in [LibertyDisco12], Section 6 "SAML AttributeDesignator for Discovery ResourceOffering," p. 23, appears to have an unnecessary restriction hampering interoperability in that the namespace prefix `saml:` actually is bound to SAML 1.1. There is no need to make this restriction.

To carry a Liberty ID-WSF 1.1 bootstrap in a SAML 2.0 SSO assertion, the following convention is adopted.

- The `Attribute/@Name` MUST be "`urn:liberty:disco:2003-08:DiscoveryResourceOffering`."
- The `Attribute/@NameFormat` MUST be "`urn:oasis:names:tc:SAML:2.0:attrname-format:uri`."
- One or more **<AttributeValue>** elements MUST be included and each of them MUST contain a single **<ResourceOffering>** (usually referring to a Discovery Service).

[1] For ID-WSF 1.x, the security token is carried in `Advice`, not in the attribute value.

- The **<ResourceOffering>** that is inside the **<AttributeStatement>** may contain **<CredentialRef>** elements referring to credentials that are necessary to access the service. These IDs SHOULD resolve to an [XML] element contained within the `Advice` element of the SSO assertion.

Example

```
<saml2:Attribute
   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
   Name="urn:liberty:disco:2003-08:DiscoveryResourceOffering">
  <sb1:ResourceOffering> ... </sb1:ResourceOffering>
</saml2:Attribute>
```

> **Conclusion**: Interoperability is achieved by treating SAML 1.1 `AttributeName` and `AttributeNamespace` fields as SAML 2.0 `Attribute/@Name` and `Attribute/@NameFormat` fields, respectively. The bootstrap attribute name value and format value are determined by the respective Liberty ID-WSF specifications.

3.4. General Interoperability Between SSO and ID-WSF

In general, any SSO protocol that can carry generic attributes can be used with ID-WSF by embedding the bootstrap as an attribute. The attribute name and name format should respect what is defined in respective ID-WSF bootstrap specifications.

For the specific case of ID-WSF 1.x, where the credential is not carried in an attribute but rather in the `Advice`, the putative SSO - ID-WSF cross operation scheme needs to specify a specific solution such as a special `credential` attribute.

For those developing new such mappings, please keep the Liberty Alliance up to date on such through Liberty's [LibertyFeedback] process. Such submissions will be reviewed in light of adding them here.

4. Using ID-WSF 1.x Service Specifications with ID-WSF 2.0

ID-WSF 1.x service specifications may be readily adapted for use within the ID-WSF 2.0 framework by following the guidelines in this chapter.

4.1. ResourceIDs

When constructing messages according to the ID-WSF 1.x service specification, use urn:liberty:isf:implied-resource for the ResourceID. In the case that the service specification makes ResourceID optional, and defaults to urn:liberty:isf:implied-resource, then the ResourceID element should be omitted.

4.2. Action URIs

For each message defined by the service specification, construct the action URI for that message by taking the namespace qualified name of the message element (i.e., the element that will be placed in the SOAP Body) and concatenating the namespace with the element name, separated by ":".

4.3. DST 2.0 Subscriptions

DST 2.0 Subscription elements use the ID-WSF 1.1 ServiceInstanceUpdate structure to describe NotifyTo and NotifyEndedTo endpoints. When using DST 2.0 Subscription elements within the ID-WSF 2.0 framework, use the following mapping to/from the ID-WSF 2.0 EndpointReference representation of the endpoints:

- EPR/Address = ServiceInstanceUpdate/Endpoint
- EPR/Metadata/SecurityContext/SecurityMechID = ServiceInstanceUpdate/SecurityMechID
- EPR/Metadata/SecurityContext/Token = ServiceInstanceUpdate/Credential

4.4. Example – Personal Profile Service

For the ID-WSF 1.x Personal Profile service, the action URIs would be:

- urn:liberty:id-sis-pp:2003-08:Query
- urn:liberty:id-sis-pp:2003-08:QueryResponse
- urn:liberty:id-sis-pp:2003-08:Modify
- urn:liberty:id-sis-pp:2003-08:ModifyResponse

and a Query request might look like:

```
<S:Envelope xmlns:S="...">
   <S:Header>
      <sbf:Framework version="2.0"/>
      <wsa:MessageID xmlns:wsa="...">...</wsa:MessageID>
      <wsa:Action xmlns:wsa="...">urn:liberty:id-sis-pp:2003-08:Query</wsa:Action>
      <sb:Sender xmlns:sb="..." providerID="http://wsc.com"/>
      <wsse:Security>
         ...
      </wsse:Security>
   </S:Header>
   <S:Body>
      <pp:Query xmlns:pp="urn:liberty:id-sis-pp:2003-08:Query">
         <pp:QueryItem itemID="1">
            <pp:Select>/pp:PP/pp:CommonName/pp:CN</pp:Select>
         </pp:QueryItem>
      </pp:Query>
   </S:Body>
</S:Envelope>
```

5. Examples

The following two examples illustrate different combinations of Federation Frameworks and ID Web Services Frameworks. They also show how a Federation Frameworks can simultaneously support both ID Web Services Frameworks by simply returning two bootstraps.

5.1. SAML 2.0 SSO with ID-WSF 1.1 and 2.0 Bootstraps

```
<sa:Assertion
   xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="ARFAmaI5TXCcPKchcZ_R"
   IssueInstant="2006-03-10T01:31:12Z"
   Version="2.0">
   <sa:Issuer
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
      https://s-ps.liberty-iop.org:8881/idp.xml
   </sa:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <ds:Reference URI="#ARFAmaI5TXCcPKchcZ_R">
            <ds:Transforms>
               <ds:Transform Algorithm="w3:xmldsig#enveloped-signature"/>
               <ds:Transform Algorithm="w3:xml-exc-c14n#"/>
            </ds:Transforms>
         </ds:Reference>
         <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
         <ds:DigestValue>2siB09gKiQ3b9CimyCt8uHgxFXM=</ds:DigestValue>
      </ds:SignedInfo>
      <ds:SignatureValue>ZI0Vz...HrUu2o=</ds:SignatureValue>
   </ds:Signature>
   <sa:Subject>
      <sa:NameID
         Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
         NameQualifier="https://s-ps.liberty-iop.org:8881/idp.xml">
         PGCTWDfZmWApzRT_ZeOB4</sa:NameID>
      <sa:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
         <sa:SubjectConfirmationData
            NotOnOrAfter="2006-03-10T01:41:11Z"
            Recipient="https://s-ps.liberty-iop.org:8843/SP-A"/>
      </sa:SubjectConfirmation>
   </sa:Subject>
   <sa:Conditions NotBefore="2006-03-10T01:26:12Z" NotOnOrAfter="2006-03-10T01:41:12Z">
      <sa:AudienceRestriction>
         <sa:Audience>https://s-ps.liberty-iop.org:8843/sp.xml</sa:Audience>
      </sa:AudienceRestriction>
   </sa:Conditions>
   <sa:AuthnStatement AuthnInstant="2006-03-10T01:31:12Z" SessionIndex="1141954271-1">
      <sa:AuthnContext>
         <sa:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password
         </sa:AuthnContextClassRef>
      </sa:AuthnContext>
   </sa:AuthnStatement>
   <sa:AttributeStatement>

<!-- ID-WSF 1.1 Bootstrap -->

      <sa:Attribute
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
         Name="urn:liberty:disco:2003-08:DiscoveryResourceOffering">
         <sa:AttributeValue>
            <disco:ResourceOffering
               xmlns:disco="urn:liberty:disco:2003-08"
               entryID="2">
               <disco:ResourceID>
```

```
                  https://s-ps.liberty-iop.org/profiles/WSF1.1/RID-DISCO-sue
               </disco:ResourceID>
               <disco:ServiceInstance>
                  <disco:ServiceType>urn:liberty:disco:2003-08</disco:ServiceType>
                  <disco:ProviderID>https://s-ps.liberty-iop.org:8881/idp.xml</disco:ProviderID>
                  <disco:Description>
                     <disco:SecurityMechID>
                        urn:liberty:security:2005-02:TLS:Bearer
                     </disco:SecurityMechID>
                     <disco:Endpoint>https://s-ps.liberty-iop.org:8881/DISCO-S</disco:Endpoint>
                  </disco:Description>
               </disco:ServiceInstance>
               <disco:Abstract>Symlabs Discovery Service Team G</disco:Abstract>
            </disco:ResourceOffering>
         </sa:AttributeValue>
      </sa:Attribute>

<!-- ID-WSF 2.0 Bootstrap -->

      <sa:Attribute
         Name="urn:liberty:disco:2005-11:DiscoveryEPR"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
         <sa:AttributeValue>
            <wsa:EndpointReference xmlns:wsa="http://www.w3.org/2005/08/addressing" entryID="2">
               <wsa:Address>https://s-ps.liberty-iop.org:8881/DISCO-S</wsa:Address>
               <wsa:Metadata>
                  <disco:Abstract xmlns:disco="urn:liberty:disco:2005-11">
                     Symlabs Discovery Service Team G
                  </disco:Abstract>
                  <disco:ProviderID xmlns:disco="urn:liberty:disco:2005-11">
                     https://s-ps.liberty-iop.org:8881/idp.xml
                  </disco:ProviderID>
                  <disco:ServiceType xmlns:disco="urn:liberty:disco:2005-11">
                     urn:liberty:disco:2005-11
                  </disco:ServiceType>
                  <disco:SecurityContext xmlns:disco="urn:liberty:disco:2005-11">
                     <disco:SecurityMechID>
                        urn:liberty:security:2005-02:TLS:Bearer
                     </disco:SecurityMechID>
                     <sec:Token>
                        <sa:Assertion
                           ID="CREDJjxfYtEabJY0VD5Mbf42"
                           IssueInstant="2006-03-10T01:31:12Z"
                           Version="2.0">
                           <sa:Issuer
                              Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                              https://s-ps.liberty-iop.org:8881/idp.xml
                           </sa:Issuer>
                           <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                              <ds:SignedInfo>
                                 <ds:CanonicalizationMethod
                                    Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                 <ds:SignatureMethod
                                    Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                                 <ds:Reference URI="#CREDJjxfYtEabJY0VD5Mbf42">
                                    <ds:Transforms>
                                       <ds:Transform Algorithm="w3:xmldsig#enveloped-signature"/>
                                       <ds:Transform
                                          Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                    </ds:Transforms>
                                    <ds:DigestMethod
                                       Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                    <ds:DigestValue>/AHzzZvqRH/su5755Tb3OGmE8M4=</ds:DigestValue>
                                 </ds:Reference>
                              </ds:SignedInfo>
                              <ds:SignatureValue>rABK91+l...N/CuiM=</ds:SignatureValue>
                           </ds:Signature>
```

```
                        <sa:Subject>
                           <sa:NameID
                              NameQualifier="https://s-ps.liberty-iop.org:8881/idp.xml">
                              915YxgPo2hrUzzq_hPtOzGSJ9StANPPCh5YweHbxxCE=
                           </sa:NameID>
                           <sa:SubjectConfirmation
                              Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
                        </sa:Subject>
                        <sa:Conditions
                           NotBefore="2006-03-10T01:26:12Z" NotOnOrAfter="2006-03-10T01:41:12Z">
                           <sa:AudienceRestriction>
                              <sa:Audience>
                                 https://s-ps.liberty-iop.org:8843/sp.xml
                              </sa:Audience>
                           </sa:AudienceRestriction>
                        </sa:Conditions>
                     </sa:Assertion>
                  </sec:Token>
               </disco:SecurityContext>
            </wsa:Metadata>
         </wsa:EndpointReference>
      </sa:AttributeValue>
   </sa:Attribute>

</sa:AttributeStatement>
</sa:Assertion>
```

5.2. ID-FF 1.2 SSO with ID-WSF 1.1 and 2.0 Bootstraps

```
<saml:Assertion
   xmlns:lib="urn:liberty:iff:2003-08"
   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   AssertionID="ARFAHo2R6kXmv9W9XrQM"
   InResponseTo="RaUb5vfg_19khwnR4F0mW"
   IssueInstant="2006-03-10T02:41:05Z"
   Issuer="https://s-ps.liberty-iop.org:8881/idp.xml"
   MajorVersion="1"
   MinorVersion="2"
   xsi:type="lib:AssertionType">
   <saml:Conditions
      NotBefore="2006-03-10T02:39:05Z"
      NotOnOrAfter="2006-03-11T02:41:05Z">
      <saml:AudienceRestrictionCondition>
         <saml:Audience>
            https://s-ps.liberty-iop.org:8843/sp.xml
         </saml:Audience>
      </saml:AudienceRestrictionCondition>
   </saml:Conditions>
   <saml:AuthenticationStatement
      AuthenticationInstant="2006-03-10T02:41:05Z"
      AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
      SessionIndex="1141958463-1"
      xsi:type="lib:AuthenticationStatementType">
      <saml:Subject
         xsi:type="lib:SubjectType">
         <saml:NameIdentifier
            Format="urn:liberty:iff:nameid:federated"
            NameQualifier="https://s-ps.liberty-iop.org:8843/sp.xml">PFAXR79p6NFy72j_nS7Xt
         </saml:NameIdentifier>
         <saml:SubjectConfirmation>
            <saml:ConfirmationMethod>
               urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
         </saml:SubjectConfirmation>
         <lib:IDPProvidedNameIdentifier
```

```
            Format="urn:liberty:iff:nameid:federated"
            NameQualifier="https://s-ps.liberty-iop.org:8843/sp.xml">
            PFAXR79p6NFy72j_nS7Xt
         </lib:IDPProvidedNameIdentifier>
      </saml:Subject>
   </saml:AuthenticationStatement>
   <saml:AttributeStatement xsi:type="lib:AttributeStatementType">
      <saml:Subject xsi:type="lib:SubjectType">
         <saml:NameIdentifier
            Format="urn:liberty:iff:nameid:federated"
            NameQualifier="https://s-ps.liberty-iop.org:8843/sp.xml">PFAXR79p6NFy72j_nS7Xt
         </saml:NameIdentifier>
         <saml:SubjectConfirmation>
            <saml:ConfirmationMethod>
               urn:oasis:names:tc:SAML:1.0:cm:bearer</saml:ConfirmationMethod>
         </saml:SubjectConfirmation>
         <lib:IDPProvidedNameIdentifier
            Format="urn:liberty:iff:nameid:federated"
            NameQualifier="https://s-ps.liberty-iop.org:8843/sp.xml">PFAXR79p6NFy72j_nS7Xt
         </lib:IDPProvidedNameIdentifier>
      </saml:Subject>

<!-- ID-WSF 1.1 Bootstrap -->

      <saml:Attribute
         AttributeName="DiscoveryResourceOffering"
         AttributeNamespace="urn:liberty:disco:2003-08">
         <saml:AttributeValue>
            <disco:ResourceOffering
               xmlns:disco="urn:liberty:disco:2003-08" entryID="2">
               <disco:ResourceID>
                  https://s-ps.liberty-iop.org/profiles/WSF1.1/RID-DISCO-sue
               </disco:ResourceID>
               <disco:ServiceInstance>
                  <disco:ServiceType>
                     urn:liberty:disco:2003-08</disco:ServiceType>
                  <disco:ProviderID>
                     https://s-ps.liberty-iop.org:8881/idp.xml</disco:ProviderID>
                  <disco:Description>
                     <disco:SecurityMechID>urn:liberty:security:2005-02:TLS:Bearer
                     </disco:SecurityMechID>
                     <disco:Endpoint>
                        https://s-ps.liberty-iop.org:8881/DISCO-S
                     </disco:Endpoint>
                  </disco:Description>
               </disco:ServiceInstance>
               <disco:Abstract>Symlabs Discovery Service Team G</disco:Abstract>
            </disco:ResourceOffering>
         </saml:AttributeValue>
      </saml:Attribute>

<!-- ID-WSF 2.0 Bootstrap -->

      <saml:Attribute
         AttributeName="urn:liberty:disco:2005-11:DiscoveryEPR"
         AttributeNamespace="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
         <saml:AttributeValue>
            <wsa:EndpointReference
               xmlns:wsa="http://www.w3.org/2005/08/addressing" entryID="2">
               <wsa:Address>
                  https://s-ps.liberty-iop.org:8881/DISCO-S</wsa:Address>
               <wsa:Metadata>
                  <disco:Abstract
                     xmlns:disco="urn:liberty:disco:2005-11">
                     Symlabs Discovery Service Team G</disco:Abstract>
                  <disco:ProviderID
                     xmlns:disco="urn:liberty:disco:2005-11">
```

```
                    https://s-ps.liberty-iop.org:8881/idp.xml</disco:ProviderID>
                 <disco:ServiceType
                    xmlns:disco="urn:liberty:disco:2005-11">urn:liberty:disco:2005-11
                 </disco:ServiceType>
                 <disco:SecurityContext xmlns:disco="urn:liberty:disco:2005-11">
                    <disco:SecurityMechID>urn:liberty:security:2005-02:TLS:Bearer
                    </disco:SecurityMechID>
                    <sec:Token>
                       <sa:Assertion
                          xmlns:sa="urn:oasis:names:tc:SAML:2.0:assertion"
                          ID="CRED7I6vzj8rGuoATD1QAYZG"
                          IssueInstant="2006-03-10T02:41:04Z"
                          Version="2.0">
                          <sa:Issuer
                             Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                             https://s-ps.liberty-iop.org:8881/idp.xml
                          </sa:Issuer>
                          <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                             <ds:SignedInfo>
                                <ds:CanonicalizationMethod
                                   Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                <ds:SignatureMethod
                                   Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                                <ds:Reference URI="#CRED7I6vzj8rGuoATD1QAYZG">
                                   <ds:Transforms>
                                      <ds:Transform
                                         Algorithm="http://www.w3.org/2000/09/xmldsig
#enveloped-signature"/>
                                      <ds:Transform
                                         Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                   </ds:Transforms>
                                   <ds:DigestMethod
                                      Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                   <ds:DigestValue>sQhsTDCk24L7QIqePR7va4BX4z4=</ds:DigestValue>
                                </ds:Reference>
                                <ds:SignatureValue>kmlM...N/F2Y=</ds:SignatureValue>
                             </ds:SignedInfo>
                             <sa:Subject>
                                <sa:NameID
                                   NameQualifier="https://s-ps.liberty-iop.org:8881/idp.xml">
                                   gXw_-3PgHN7cTS4cxli17vFEGngSmfULfFHqJZnr_0Q=
                                </sa:NameID>
                                <sa:SubjectConfirmation
                                   Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
                             </sa:Subject>
                             <sa:Conditions
                                NotBefore="2006-03-10T02:36:04Z"
                                NotOnOrAfter="2006-03-10T02:51:04Z">
                                <sa:AudienceRestriction>
                                   <sa:Audience>
                                      https://s-ps.liberty-iop.org:8843/sp.xml
                                   </sa:Audience>
                                </sa:AudienceRestriction>
                             </sa:Conditions>
                          </ds:Signature>
                       </sa:Assertion>
                    </sec:Token>
                 </disco:SecurityContext>
              </wsa:Metadata>
           </wsa:EndpointReference>
        </saml:AttributeValue>
     </saml:Attribute>

  </saml:AttributeStatement>
</saml:Assertion>
```

References

Normative

[LibertyDisco] Hodges, Jeff, Cahill, Conor, eds. "Liberty ID-WSF Discovery Service Specification," Version 2.0, Liberty Alliance Project (30 July, 2006). *http://www.projectliberty.org/specs*

[LibertyDisco12] Sergent, Jonathan, eds. "Liberty ID-WSF Discovery Service Specification," Version 1.2, Liberty Alliance Project (12 December 2004). *http://www.projectliberty.org/specs/*

[LibertyProtSchema] Cantor, Scott, Kemp, John, eds. "Liberty ID-FF Protocols and Schema Specification," Version 1.2-errata-v3.0, Liberty Alliance Project (14 December 2004). *http://www.projectliberty.org/specs*

[RFC2119] S. Bradner "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, The Internet Engineering Task Force (March 1997). *http://www.ietf.org/rfc/rfc2119.txt*

[RFC3548] Josefsson, S., eds. (July 2003). "The Base16, Base32, and Base64 Data Encodings," RFC 3548, The Internet Engineering Task Force *http://www.ietf.org/rfc/rfc3548.txt*

[SAMLCore] Hallam-Baker, Phillip, Maler, Eve, eds. (05 November 2002). "SAML Core Assertions and Protocols," SAML V1.0, OASIS Standard, Organization for the Advancement of Structured Information Standards *http://www.oasis-open.org/specs/index.php#samlv1.0*

[SAMLCore2] Cantor, Scott, Kemp, John, Philpott, Rob, Maler, Eve, eds. (15 March 2005). "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0," SAML V2.0, OASIS Standard, Organization for the Advancement of Structured Information Standards *http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf*

[XML] Bray, Tim, Paoli, Jean, Sperberg-McQueen, C. M., Maler, Eve, Yergeau, Francois, eds. (04 February 2004). "Extensible Markup Language (XML) 1.0 (Third Edition)," Recommendation, World Wide Web Consortium *http://www.w3.org/TR/2004/REC-xml-20040204*

Informative

[LibertyFeedback] Champagne, Darryl, Lockhart, Rob, eds. (2003). "Provide Comments and Questions about Liberty Specifications," Release 1.0, Liberty Alliance Project *http://www.projectliberty.org/specs/specs_comments_questions.asp*

[LibertyIDWSFGuide10] Weitzel, David, eds. (22 May 2005). "Liberty ID-WSF Implementation Guideline," Draft v1.0-12, Liberty Alliance Project *http://www.projectliberty.org/specs/*

[LibertyIDWSFGuide] Weitzel, David, eds. "Liberty ID-WSF Implementation Guide," Version 2.0-02, Liberty Alliance Project (13 January, 2005). *http://www.projectliberty.org/specs*