OMA Network Identity Web Service Framework

Candidate Version 1.0 – 20 Dec 2005

Open Mobile Alliance

OMA-TS-OWSER_NI_WSF-V1_0-20051220-C

Contents

1. SCOPE 5
2. REFERENCES 6
   2.1 NORMATIVE REFERENCES 6
   2.2 INFORMATIVE REFERENCES 7
3. TERMINOLOGY AND CONVENTIONS 8
   3.1 CONVENTIONS 8
   3.2 DEFINITIONS 8
   3.3 ABBREVIATIONS 10
4. INTRODUCTION 11
   4.1 OWSER CORE WEB SERVICES WITHOUT OWSER NETWORK IDENTITY 11
   4.2 WEB SERVICES USING OWSER NETWORK IDENTITY 12
      4.2.1 Accessing a User's Identity Attributes 12
      4.2.2 Single Signon in a Liberty enabled Web Services Environment 14
5. DESCRIPTION OF FUNCTIONAL ELEMENTS 17
   5.1 SERVICE PROVIDER 17
   5.2 IDENTITY PROVIDER 17
   5.3 DISCOVERY SERVICE 17
   5.4 ATTRIBUTE PROVIDER 17
6. DESCRIPTION OF PROCEDURES 19
   6.1 ATTRIBUTE QUERY 19
      6.1.1 Attribute Query using PAOS 20
   6.2 ATTRIBUTE MODIFICATION 20
   6.3 USAGE DIRECTIVES 21
   6.4 INTERACTION SERVICE 22
      6.4.1 Interaction Redirect 23
   6.5 BOOTSTRAPPING IDENTITY BASED WEB SERVICES FRAMEWORK 23
      6.5.1 Discovery Service Bootstrap 24
      6.5.2 Authentication Service 24
      6.5.3 SSO Service 24
   6.6 DISCOVERY SERVICE 24
      6.6.1 Discovery Lookup 25
      6.6.2 Discovery Update 26
   6.7 LUAD 27
      6.7.1 LUAD acting as WSC 27
      6.7.2 LUAD acting as WSP 27
   6.8 SECURITY 28
      6.8.1 Authentication 28
      6.8.2 Confidentiality and Privacy 28
      6.8.3 Authorization 29
      6.8.4 Message Correlation 29
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 30
   A.1 APPROVED VERSION HISTORY 30
   A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY 30
APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) 31
   B.1 IDP 31
   B.2 DS 31
   B.3 SP 32
   B.4 LUAD WSC 32
   B.5 LUAD WSP 32
   B.6 AP 33
   B.7 IS 33

Figures

Figure 1: Web Service Interactions enabled by OWSER Core specification in the absence of NI Protocols and Services 11

Figure 2: interactions needed to access a user's identity attributes at an Attribute Provider 13

Figure 3: Authentication Service and the SSOS 15

Figure 4: Attribute Query 19

Figure 5: Attribute Modification 21

Figure 6: Usage Directive 22

Figure 7: Interaction Service 23

Figure 8: Interaction Redirect 23

Figure 9: Illustration of Calendar Service Instance hosting Calendar resource for Various Principals 24

Figure 10: Illustration of different resources for a specific Principal 25

Figure 11: Discovery Lookup 26

Figure 12: Discovery Update 27

Tables

Table 1: SCR for IdP 31

Table 2: SCR for DS 31

Table 3: SCR for SP 32

Table 4: SCR for LUAD WSC 32

Table 5: SCR for LUAD WSP 33

Table 6: SCR for AP 33

Table 7: SCR for IS 33

1. Scope

This document is part of a series of documents [OWSER NI FF], [OWSER NI AD] [OWSER NI WSF] that specifies components of the OMA Web Services Network Identity Enabler (OWSER NI).

"OMA Web Services Network Identity Enabler (OWSER NI): Architecture" [OWSER NI AD] is informative and describes the architecture of a technical solution to the requirements in [NI RD] based on the Liberty Alliance Identity Federation Framework and Identity Web Services Framework

"OMA Network Identity Federation Framework" document [OWSER NI FF] provides the specifications of the components needed to leverage Identity Federation in a Liberty-enabled Web services environment

This document namely, "OMA Network Identity Web Services Enabler: (OWSER NI): Identity Web Services Framework " [OWSER NI WSF] provides the specification of the components needed to fulfil the requirements in [NI-RD] related to accessing user-related attributes (e.g., user location, presence status etc.) in a privacy-protected manner in a Liberty-enabled Web Services Environment. This document is intended to provide normative guidance to designers of OMA Network Identity Web Services and implementers thereof.

2. References

2.1 Normative References

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, URL:http://www.openmobilealliance.org/

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997, URL:http://www.ietf.org/rfc/rfc2234.txt

[RFC2828] "Internet Security Glossary," R. Shirey, May 2000, URL:http://www.ietf.org/rfc/rfc2828.txt

[Liberty-IDFF-Protocols-Schema] "Liberty ID-FF Protocols and Schema Specification," Version 1.2, Liberty Alliance Project.

[Liberty-IDWSF-DST] "Liberty ID-WSF Data Services Template Specification," Version 1.1, Liberty Alliance Project.

[Liberty-IDWSF-Interaction-Svc] "Liberty ID-WSF Interaction Service Specification," Version 1.1, Liberty Alliance Project.

[Liberty-IDWSF-Soap-Binding] "Liberty ID-WSF SOAP Binding Specification," Version 1.2, Liberty Alliance Project.

[Liberty-Paos] "Liberty Reverse HTTP Binding for SOAP Specification," Version 1.1, Liberty Alliance Project.

[Liberty-IDWSF-Disco] "Liberty ID-WSF Discovery Service Specification," Version 1.2, Liberty Alliance Project.

[Liberty-IDWSF-Client-Profiles] "Liberty ID-WSF Profiles for Liberty Enabled User Agents and Devices," Version 1.1, Liberty Alliance Project.

[Liberty-IDWSF-Security-Mechanisms] "Liberty ID-WSF Security Mechanisms," Version 1.2, Liberty Alliance Project.

[Liberty-IDWSF-AuthnSSO] "Liberty ID-WSF Authentication Service and Single Sign-On Service Specification," v1.1, Liberty Alliance.

[NI-RD] "MWS Identity Management Requirements", OMA Web Services Enabler Release V1.0, Approved Enabler, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[OWSER1.0] "OMA Web Services Enabler Release V1.0", Approved Enabler, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[OWSER1.0-NI] "OMA Web Services Enabler (OWSER) Network Identity Specifications", OMA Web Services Enabler Release V1.0, Approved Enabler, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[OWSER Core] "OMA Web Services Enabler (OWSER): Core Specifications", OMA Web Services Enabler Release V1.0, Approved Enabler, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[OWSER NI FF] "OMA Web Services Network Identity Enabler (OWSER NI): Federation Framework ", OMA Web Services Network Identity Enabler (OWSER NI), Draft Enabler, Open Mobile Alliance, URL:http://www.openmobilealliance.org/

[OWSER NI WSF] "OMA Web Services Network Identity Enabler (OWSER NI): Identity Web Services Framework", OMA Web Services Network Identity Enabler (OWSER NI), Draft Enabler, Open Mobile Alliance, URL:http://www.openmobilealliance.org/

[OMADict] "Dictionary for OMA Specifications", Version 2.1, 14 September2004, URL: http://www.openmobilealliance.org

[wss-sms] Hallam-Baker, Phillip, Kaler, Chris, Monzillo, Ronald, Nadalin, Anthony, eds. (January, 2004). "Web Services Security: SOAP Message Security," OASIS Standard V1.0 [OASIS 200401], Organization for the Advancement of Structured Information Standards *http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf*

2.2 Informative References

[OWSER NI AD] "OMA Web Services Network Identity Enabler (OWSER NI): Architecture", OMA Web Services Network Identity Enabler (OWSER NI), Draft Enabler, Open Mobile Alliance, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

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

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Attribute	An Attribute is a characteristic that describes a Principal.
Attribute Provider	A special type of Service Provider, whose service is to provide Attributes about a Principal. In this document an Attribute provider is an ID-WSF-enabled Web Service Provider
Attribute Sharing	See Attribute Transfer.
Attribute Transfer	Transmission of a Principal’s Attribute from an Entity (i.e. an Attribute Provider) that manages it, on behalf of the Principal, to an Entity that requests it (e.g. a Service Provider).
Authentication	The process of verifying an Identity claimed by (or for) a Principal.
Authentication Assertion	An Assertion that can be sent from one Identity Provider (or an Identity Broker) to another Provider, which describes a successful Authentication of a Principal. An Authentication Assertion may also contain information such as for how long the Assertion is valid. An Authentication Assertion will also often include an Authentication Context, to notify the Provider what form of Authentication was used.
Authentication Context	The set of parameters (time, location, transaction value, etc.) within which a specific Authentication instance is acceptable, emphasising that a single Authentication instance may need to be re-established, perhaps with different mechanisms or classes of mechanisms, when some parameter changes.
Authentication Service	See ID-WSF Authentication Service.
Authorisation	A right or permission that is granted to a system Entity to access a system resource, or the process of granting the right or permission [RFC 2828].
Business Agreeement	Business agreements are formal agreements (contracts) between parties in the Identity Management Circle of Trust, documenting binding commitments between the parties with respect to aspects such as mutual confidence (e.g. business standards, minimum requirements, certifications and audits supported), risk management (e.g. dissimination of knowledge and use of best practices), liabilities (e.g. defined liability, dispute resolution) and compliance (e.g. general compliance, privacy issues).”
Circle of Trust	One or more service providers and identity providers that have business relationships and operational agreements, and with whom users can transact business in a secure and apparently seamless environment.
Data Service Template	See ID-WSF Data Service Template.
De-Federation	A reversal of the process of Federation of two Accounts (belonging to the same Principal), or termination of the state of Identity Federation. De-Federation usually involves an exchange of messages among the systems which established the Identity Federation.
Discovery	A mechanism that allows requestors to discover resources and how to access those resources.
Discovery Service	The Discovery Service allows requesters to discover resource offerings [Liberty-IDWSF-Disco]
End User	An End User is a (human) user of a service. An End User is therefore a subset of the term Principal.
Federation	The binding of two or more Accounts (within an Authentication Domain or a Circle of Trust, where one of the Accounts is at an IDP) for a given Principal. Federation does not imply that Identity Attributes are being shared – it is simply a joining of two or more Accounts (e.g. for Single Sign On), after which Attributes could then be shared.

Entity	A thing with distinct existence. In this document the term Principal is regularly used as a subset of Entity, more specific to the Entities involved in an Identity Management enabler.
Identifier	A reference that uniquely maps to an Identity. One or more Identifiers are among the characteristics that define an Identity.
Identity	The characteristics by which an Entity or person is recognised or known.
Identity Provider	A special type of Service Provider role that creates, maintains, and manages Identity information for Principals, and can provide an Authentication Assertion to other Service Providers within an Authentication Domain (or even a Circle of Trust).
ID-WSF Authentication Service	The ID-WSF Authentication Service is a specification that allows generic identity authentication information exchange over SOAP in order to implement a WSC/WSP peer to peer authentication.
ID-WSF Enabled Web Service Provider	A Web Service provider that supports the Liberty ID-WSF protocols as specified in this specification.
ID-WSF Data Service Template	The ID-WSF Data Service Template is a specification that defines common data access protocols to allow querying and modifying arbitrary data items according to the application (e.g. an application may simply use or extend the DST protocol to provide a basic query/modify interface to application clients without having to design or code such functionality itself).
ID-WSF Discovery Service	The ID-WSF Discovery Service is a specification that enables various entities (e.g. service providers) to dynamically discover a principal's registered services. Given the type of service desired, the Discovery Service responds with a service description containing WSDL for the desired identity service, provided that permissions set by the Principal allow the disclosure of these resources to the relevant entity. The Discovery Service can also function as a security token service, issuing security tokens to the requester that the requester will use in the request to the discovered identity service.
ID-WSF Interaction Service	The ID-WSF Interaction Service is a specification that allows an identity service to interact with the owner of a requested resource that it is exposing, in order to collect attribute values, or to obtain permission to share the data with a Web Services Consumer.
ID-WSF Security Mechanisms	The ID-WSF Security Mechanisms is a specification that describes profiles and requirements for securing the discovery and use of web services. It includes security requirements to both protect privacy, and to ensure integrity and confidentiality of messages between service providers.
ID-WSF SOAP Binding	The ID-WSF SOAP Binding provides a SOAP-based invocation framework for identity services. This binding does not specify any contents for the SOAP body itself, but offers an extensibility model by defining headers addressing message exchange specifics (i.e. consent claims, affiliation declaration, etc)
Interaction Service	See ID-WSF Interaction Service.
LUAD	"User agents and devices that send or consume protocol messages specified in the ID-WSF (or ID-FF) specifications are called *Liberty enabled User Agents and Devices*. The defining characteristic of a LUAD is that it is closely associated with one user (or a few users, such as a family)." [Liberty-IDWSF-Client-Profiles]
Principal	An entity that has an identity, that is capable of providing consent and other data, and to which authenticated actions are done on its behalf. Examples of principals include an individual end user, a group of end users, a corporation, service enablers / applications, system entities and other legal entities. [OMADict]
Pseudonym	An arbitrary name assigned by the Identity Provider or Service Provider to identify a Principal to a given relying party, so that the name has meaning only in the context of the relationship between the relying parties.
Resource Offering	A resource offering is the association of a resource and a service instance. This association is necessary as there is a many-to-many relationship between resources and service instances. A single service instance may serve many resources. For example, a personal profile service provider would typically serve up many profiles behind a single service instance, as having a separate protocol endpoint for each profile would be impractical. [Liberty-IDWSF-Disco].
Security Mechanisms	See ID-WSF Security Mechanisms.

Service Instance	A service instance is a running Web Service at a distinct protocol endpoint [Liberty-IDWSF-disco].
Service Provider	An Entity that provides services and/or goods to Principals.
Single Log Out	The ability for End Users to properly terminate all open connections, active services or relationships associated with a Single Sign On (SSO) Session, with one logout process.
Single Sign On	The ability to use an Authentication Assertion from one Provider (an Identity Provider or an Identity Broker) at another Provider, in order to ease the burden (for a Principal) of having to authenticate to each Provider separately within a single Session.
SOAP Binding	See ID-WSF SOAP Binding.
Trust	The extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions. [source:RFC2828]
Web Service Provider	See [OWSER Core]
WS-Security	WS-Security describes enhancements to SOAP messaging to provide *quality of protection* through message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies.

3.3 Abbreviations

AP	Attribute Provider
IdP	Identity Provider
ID-FF	Identity Federation Framework
ID-WSF	Identity Web Services Framework
IS	Interaction Service
NI	Network Identity
OMA	Open Mobile Alliance
OSE	OMA Service Environment
OWSER	OMA Web Services Enabler Release
SASL	Simple Authentication and Security Layer
SP	Service Provider
WSC	Web Service Consumer
WSP	Web Service Provider
WSR	Web Service Requester

4. Introduction

4.1 OWSER Core Web Services Without OWSER Network Identity

The OWSER Enabler Release includes a Core specification defining standard protocols to be used in interactions between Web Service Requestors and Web Service Providers including an XML Message Envelope (SOAP) , a Web Services Registry access protocol (UDDI) and mechanisms for encapsulating security tokens as header elements in a SOAP message envelope (OASIS Web Services. Security)

The diagram in Figure 1 and associated flows illustrate the Web Service interactions enabled by the OWSER Core specification in the absence of Network Identity protocols and services

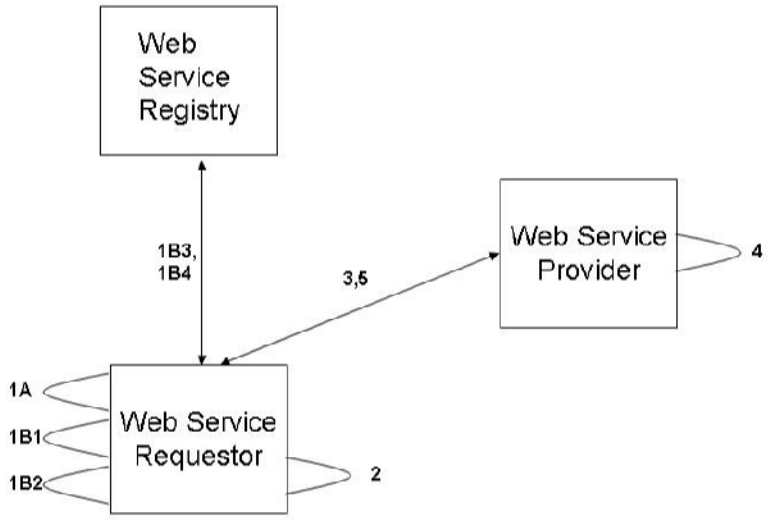

Figure 1: Web Service Interactions enabled by OWSER Core specification in the absence of NI Protocols and Services

The execution flow for diagram above follows.

1. Web Service Requestor determines how to locate and interact with a Web Service Provider

    1 A) Web service requestor uses out-of-band information, such as local configuration information to identify a particular Web Service provider, or

    1 B) Web Service Requestor uses a Web Services Registry to locate a Web Service Provider offering the desired service.

1B1. Web service requestor uses out-of-band information, such as local configuration information to identify a particular Web service Registry.

1B2. Web Service Requester populates a UDDI Query message

1B3. Web Service Requestor sends the query message to the Registry

1B4. Web Service registry returns a response message containing information enabling the Web Services Requestor to locate and communicate with a Web Service Provider offering the desired service

2. Web Service Requester populates a message described with WSDL that is conformant to the SOAP/HTTP content described, encapsulates a security token in a SOAP header as specified by the OWSER Core to populate the requester identity and credentials.

3. Web Service Requestor sends the message to the Web Service Provider.

4. The Web Service Provider receives the messages, extracts and processes the security token contained in the security header in order to authenticate the user, performs its function and populates the response message with the attribute information.

5. The response message is returned to the Web Service Requester.

Note: this example is simplified for clarity, and does not reflect elements such as encryption, signing, proxies and other elements or functions that are covered by OWSER Core.

4.2 Web Services using OWSER Network Identity

The foundations of Network Identity are laid down in the OWSER V1.0 Network Identity specifications, based on the Liberty Alliance Identity Federation Framework (ID-FF) which define a distinguished Service provider, the Identity Provider, and associated protocols , (Identity Federation, Name Registration) that together enable management of Federated user identities across multiple Service Providers within a Circle of Trust while allowing users to manage and control the identifiers by which they are known at any individual Service Provider (thus protecting the user's privacy across multiple, independent interactions with multiple Service Providers). The OSWER V1.0 Network Identity specifications also define Single Signon services that leverage Identity Federation to allow users of Web-based Application Service Providers to authenticate to multiple such Services Providers within a Circle of Trust via the sharing an of an authentication event at a trusted party (the Identity Provider).

This specification builds on those foundations by providing additional mechanisms, based on the Liberty Alliance Identity Web Services Framework (ID-WSF) and conformant to the OWSER core specifications that enable applications to leverage Federated Identity and Single Signon in Web Service interactions between WSRs and WSPs and to provide seamless access to users' identity attributes in a privacy-protected manner in a Liberty enabled Web Services environment. This specification defines a class of Web Service Provider, an Attribute Provider, and associated protocols used to manage access to users' identity attributes (subject to user consent). A distinguished Attribute Provider, the ID-WSF Discovery Service, enables discovery by a WSR of the Attribute Providers capable of providing identity attributes associated with a particular user and optionally, provides assertions than can be used by WSRs in subsequent Web service interactions with those Attribute Providers.

4.2.1 Accessing a User's Identity Attributes

The diagram in Figure 2 and associated flows describe the interactions needed to access a user's identity attributes at an Attribute Provider

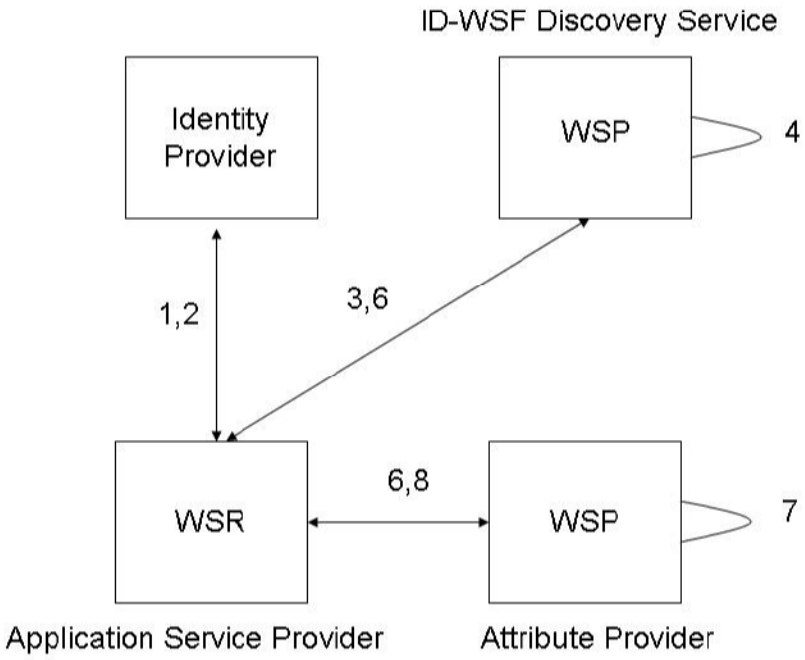

Figure 2: interactions needed to access a user's identity attributes at an Attribute Provider

The execution flow for diagram above follows.

1. WSR authenticates the user by issuing an ID-FF authentication request to the IdP.

> Note: The ID-FF authentication request utilizes redirection through the application client as described in detail in the OWSER v1.0 Network Identity specifications and OWSER Network Identity Phase 2 Architecture document. The details are not repeated here.

2 IdP returns an ID-FF SAML assertion authenticating the user to the WSR and a ID-WSF resource offering for the user's ID-WSF Discovery Service

3. WSR uses the resource offering and SAML Assertion provided by the IdP to bind and authenticate to the user's ID-WSF Discovery Service and request a ID-WSF resource offering and SAML Assertion for an Attribute Provider capable of providing the desired user Identity Attributes.

4. ID-WSF Discovery Service authenticates the WSR and populates a response message containing a ID-WSF resource offering and SAML assertion for an Attribute Provider capable of providing the desired user Attributes.

5. ID-WSF Discovery Service returns the response message to the WSR

6. WSR uses the resource offering and SAML assertion provided by the ID-WSF Discovery Service to authenticate to the attribute Provider and request the desired Attributes

7. Attribute Provider authenticates the WSR and populates a response message containing the desired Attributes

8. Attribute Provider returns the Response to the WSR

Note: this example is simplified for clarity, and does not reflect elements such as encryption, signing, proxies and other elements or functions that are covered by Liberty specifications.

4.2.2 Single Signon in a Liberty enabled Web Services Environment

For a Liberty enabled Web Services environment, a Liberty IdP can offer Single sign-on (SSO) services to a Web Service Requester (WSR) by supporting the ID-WSF Authentication Service and the ID-WSF Single Sign-on Service. Note that a WSR cannot use the Liberty ID-FF SSO service of OWSER 1.0 NI directly, as these were designed for a browser-based environment, where the SSO to a Service Provider (SP) was achieved through browser redirection of the authentication request.

In the absence of the browser redirection feature, a WSR authenticates directly with the IdP and convey the results of this authentication event to any SP (WSP) it interacts with within the Circle of Trust. The IdP must support the Liberty ID-WSF Authentication Service, which uses the standard SASL protocols to implement authentication exchanges.

The result of the authentication includes a resource offering to an ID-WSF Single Sign-on Service (SSOS). The WSR then interacts with the SSOS to obtain appropriate credentials to interact with any WSP within the Circle of Trust. The authentication request/response information in this interaction with the SSOS is exactly the same as that for browser based SSO, only the encapsulating protocol and transfer mechanisms are different.

One option, for a Liberty ID-WSF enabled WSR, is where the SSOS returns the resource offering for a special WSP, the Discovery Service for a Principal's attributes. This DS may, in turn, be queried to obtain the resource offering for the WSP hosting the resource corresponding to a particular attribute.

Note that the ID-WSF Authentication Service and SSOS are available to any WSR for interactions that need not be related to accessing a user's identity attributes.

Note also that this solution continues to preserve the user's privacy through the use of anonymous or pseudonymous name identifiers valid at a specific WSP. Such identifiers were set at the time of identity federation.

The use of the Authentication Service and the SSOS is described below in Figure 3.

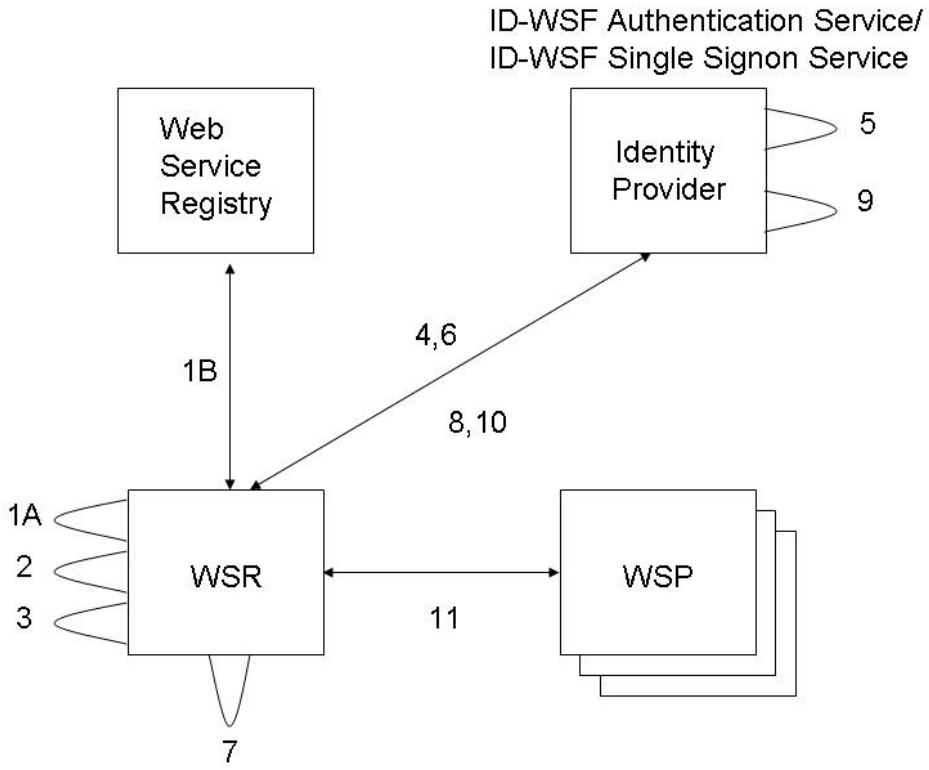

Figure 3: Authentication Service and the SSOS

The execution flow for diagram above follows.

1 WSR determines how to locate and interact with a Web Service Provider.

> 1A. Web service requestor uses out-of-band information, such as local configuration information to identify a particular Web Service provider, or
>
> 1B. Web Service Requestor uses a Web Services Registry to locate a Web Service Provider offering the desired service
>
> Note: The detailed interactions for 1B are identical for those described for 1B in section 4.2 and are not repeated here.

2 WSR uses out-of-band information, such as local configuration information to identify an ID-WSF Authentication Service.

3. WSR populates an ID-WSF Authentication Service Request as needed to acquire a security token enabling it to authenticate to the ID-WSF SSOS service.

4. WSR sends the authentication request to the ID-WSF Authentication Service.

5. ID-WSF Authentication Service validates the Authentication Request and populates an Authentication Response .containing a security token enabling the WSR to authenticate to the ID-WSF SSOS.

6. ID-WSF Authentication Service returns the Authentication Reponses to the WSR.

7. WSR populates an ID-WSF SSOS request including a SOAP Header containing the token obtained from the ID-WSF Authentication Service and a SOAP body containing an ID-FF Authentication Request.

.8. WSR sends a request to the ID-WSF SSOS asking for an assertion enabling to it interact with the WSP

9. ID-WSF SSOS validates the request and populates a SOAP response message containing an ID-FF authentication response

10. ID-WSF SSOS returns the response message to the WSR

11. WSR sends the request to the WSP and receives a response.

> Note: The details of this interaction are identical to those described in bullets 2-5 in section 4.1 above and are not repeated here.

Note: this example is simplified for clarity, and does not reflect elements such as encryption, signing, proxies and other elements or functions that are covered by Liberty specifications.

5. Description of Functional Elements

5.1 Service Provider

As defined in Section 3.2, a Service Provider is "an entity that provides services and/or goods to Principals."

A Service Provider may act as a Web Services Requestor (WSR) in its interaction with an Attribute Provider that is acting as a Web Services Provider (WSP). In such a case, the Service Provider may use the Attribute Query mechanism to request attributes from the Attribute Provider. When a Service Provider makes an attribute query to an Attribute Provider using the <Query> element, the Service Provider MAY include a <UsageDirective> header that indicates its policies for handling the attributes. The Service Provider may also use the Attribute modification mechanism to modify attributes pertaining to a Principal at the Attribute Provider.

A Service Provider may also take on the role of a LUAD Web Service Consumer (WSC) when it resides on a Liberty User Agent and Device (LUAD).

The Service Provider may also belong to an affiliation.

5.2 Identity Provider

As defined in Section 3.2, an Identity Provider is a "special type of Service Provider role that creates, maintains, and manages Identity information for Principals, and can provide an Authentication Assertion to other Service Providers within an Authentication Domain (or even a Circle of Trust)."

When Identity Federation for a specific Principal occurs between a Service Provider and an Identity Provider, then Single Sign On is possible for that Principal.

5.3 Discovery Service

As defined in Section 3.2, the Discovery Service "allows requesters to discover resource offerings."

When a Service Provider wishes to determine the Attribute Provider(s) hosting required resource(s) on behalf of a specific Principal, it MAY contact a Discovery Service to obtain such information. The Discovery Service MAY also provide the requesting Service Provider with necessary credentials needed to access the Attribute Provider.

In order to obtain information on suitable resource offerings, a requester needs to initiate a discovery lookup procedure at the Discovery Service. In order to insert, delete or modify Resource Offerings at a Discovery Service, a Discovery Update procedure needs to be initiated at the Discovery Service.

5.4 Attribute Provider

As defined in Section 3.2, an Attribute Provider is "a special type of Service Provider, whose service is to provide Attributes about a Principal."

An Attribute Provider may act as a Web Services Provider (WSP) in its interaction with a Service Provider that is acting as a Web Services Requester (WSR). In such a case, when the Service Provider uses the Attribute Query mechanism to request attributes from the Attribute Provider, the Attribute Provider may respond with the attributes requested. When the Attribute Provider responds to the Service Provider with a <QueryResponse> element, the Attribute Provider MAY include a <UsageDirective> header that indicates its policies for subsequent use of the released attributes.

When the Service Provider uses the Attribute modification mechanism to modify attributes pertaining to a Principal at the Attribute Provider, the Attribute Provider responds with a modification response message.

The Attribute Provider may be hosted on a device that does not support a HTTP server, or that is not generally reachable or addressable from the Internet, in which case the PAOS mechanism may be used to retrieve attributes from the Attribute Provider.

6. Description of Procedures

6.1 Attribute Query

In order to query an Attribute Provider, a Service Provider MAY use the mechanisms specified in the Liberty Data Service Template (DST) [Liberty-IDWSF-DST]. When this is the case, the Service Provider MUST use the <Query> element, and the Attribute Provider MUST use the <QueryResponse> element in its response to the Service Provider.

The elements of the DST as specified in [Liberty-IDWSF-DST] are not intended to be used as standalone messages. Rather, the DST provides template XML that an application MAY use in WSDL to implement query/modify semantics.

The Figure 4 below illustrates this message exchange.

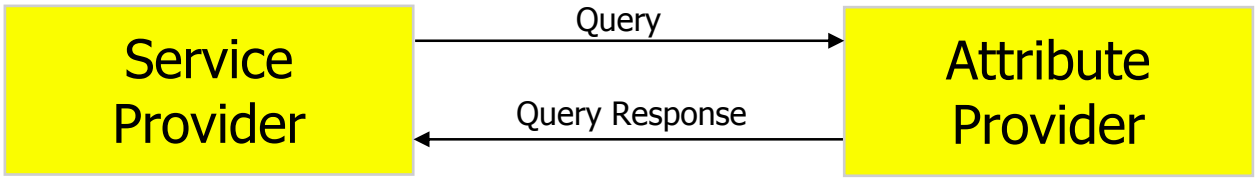

Figure 4: Attribute Query

The schema and usage of the <Query> element MUST be as described in Section 3.2.1 of [Liberty-IDWSF-DST]. The schema and usage of the <QueryResponse> element MUST be as described in Section 3.2.2 of [Liberty-IDWSF-DST]. The processing rules for the <Query> and <QueryResponse> elements MUST be as described in Section 3.2.3 of [Liberty-IDWSF-DST].

Below, we include an example of a <Query>. The resource is identified by the ResourceID `http://OWSER-attribute-provider.com/u6gh8jlx90bt8h1o`. The query is for the name and home address of the resource.

```
<Query>
   <ResourceID>http://OWSER-attribute-provider.com/u6gh8jlx90bt8h1o</Resource ID>
   <QueryItem itemID="name">
      <Select>/pp:PP/pp:CommonName</Select>
   </QueryItem>
   <QueryItem itemID="home">
      <Select>/pp:PP/pp:AddressCard[pp:AddressType="urn:liberty: id-sis-pp:addrType:home"]</Select>
   </QueryItem>
</Query>
```

Below, we include an example of a <QueryResponse> to the above <Query>. The resource's common name is returned as Dr. Genie Wunderkid, with an alternative common name being Dr. Genie Wunder. The resource's address is also provided.

```
<QueryResponse>
   <Status code="OK"/>
   <Data itemIDRef ="name">
      <CommonName>
         <CN>Genie Wunderkid</CN>
         <AnalyzedName nameScheme="firstlast">
            <FN>Genie</FN>
            <SN>Wunderkid</SN>
            <PersonalTitle>Dr.</PersonalTitle>
         </AnalyzedName >
         <AltCN>Genie Wunder</AltCN>
      </CommonName>
   </Data>
   <Data itemIDRef="home">
      <AddressCard id='9812'>
         <AddressType>urn:liberty:id-sis-pp:addrType:home<AddressType>
```

```
        <Address>
           <PostalAddress>c/o Senthil Sengodan$12278 Scripps Summit Drive</PostalAddress>
           <PostalCode>92131-2341</PostalCode>
           <L>San Diego</L>
           <ST>ca</ST>
           <C>us</C>
        </Address>
      </AddressCard>
   </Data>
</QueryResponse>
```

6.1.1 Attribute Query using PAOS

An attribute query MAY be done using the reversed HTTP binding for SOAP, as specified in [Liberty-Paos]. When this is the case, the procedures specified in [Liberty-Paos] MUST be followed.

Examples of scenarios where the reversed HTTP binding for SOAP may be used are:

- The attribute provider is hosted on a device that supports a HTTP client but not a HTTP server. This may be the case when the device is resource constrained.
- The attribute provider is hosted on a device that is not generally addressable or reachable from the Internet.

As described in Section 7 of [Liberty-Paos], two message exchange patterns are supported:

1. In the request-response message exchange pattern, a PAOS-enabled user agent sends a HTTP request to a HTTP server, which then sends the SOAP request in the HTTP response. The user agent sends the SOAP response in a second HTTP request. When the request-response message exchange pattern is used, the procedures specified in Section 8 of [Liberty-Paos] MUST be followed.
2. In the response message exchange pattern, a PAOS-enabled user agent sends a HTTP request to a HTTP server, which then sends the SOAP response in the HTTP response. When the response message exchange pattern is used, the procedures specified in Section 9 of [Liberty-Paos] MUST be followed.

An example of the request-response message exchange pattern is as follows. A user agent on a mobile device sends a HTTP request to a HTTP server in order to purchase an item. In the HTTP response message, the HTTP server includes a SOAP request for the credit card number of the user. The user agent, acting as the attribute provider for the credit card attribute, issues a new HTTP request to the HTTP server, in which it sends the SOAP response message containing the credit card number. The HTTP server responds with a 200 OK message.

An example of the response message exchange pattern is as follows. A user wishes to poll a messaging service for confirmation of message delivery. In order to do so, the user agent sends a HTTP request to the HTTP server hosting the messaging the service, inquiring about the message delivery confirmation. The HTTP response from the HTTP server contains a SOAP response message containing information confirming the message delivery.

6.2 Attribute Modification

In order to modify an attribute stored at an Attribute Provider, a Service Provider MAY use the mechanisms specified in the Liberty Data Service Template (DST) [Liberty-IDWSF-DST]. When this is the case, a Service Provider MUST use the <Modify> element, and the Attribute Provider MUST use the <ModifyResponse> element in its response to the Service Provider.

The elements of the DST as specified in [Liberty-IDWSF-DST] are not intended to be used as standalone messages. Rather, the DST provides template XML that an application MAY use in WSDL to implement query/modify semantics.

The Figure 5 below illustrates this message exchange.

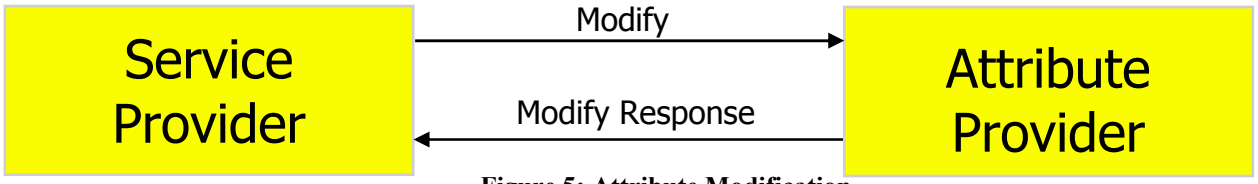

Figure 5: Attribute Modification

The schema and usage of the <Modify> element MUST be as described in Section 3.3.1 of [Liberty-IDWSF-DST]. The schema and usage of the <ModifyResponse> element MUST be as described in Section 3.3.2 of [Liberty-IDWSF-DST]. The processing rules for the <Modify> and <ModifyResponse> elements MUST be as described in Section 3.3.3 of [Liberty-IDWSF-DST].

The example below depicts how an address is inserted or modified in a personal profile stored at profile.MobileOperator.com.

```
<Modify>
   <ResourceID>http://profile.MobileOperator.com/8fhelk9savbq4p0j</ResourceID>
   <Modification overrideAllowed="True">
      <Select>/pp:PP/pp:AddressCard[pp:AddressType= 'urn:liberty:id-sis-pp:addrType:home']</Select>
      <NewData>
         <AddressCard id='45387'>
            <AddressType>urn:liberty:id-sis-pp:addrType:home</AddressType>
               <Address>
                  <PostalAddress>Sophie Wunderkid$1234 Wonderland Drive</PostalAddress>
                  <PostalCode>12345-1234</PostalCode>
                  <L>Olympia</L>
                  <ST>CA</ST >
                  <C>us</C>
               </Address>
         </AddressCard>
      </NewData>
   </Modification>
</Modify>
```

6.3 Usage Directives

When a Service Provider makes an attribute query to an Attribute Provider using the <Query> element, the Service Provider MAY include a <UsageDirective> header that indicates its policies for handling the attributes. When the Attribute Provider responds to the Service Provider with a <QueryResponse> element, the Attribute Provider MAY include a <UsageDirective> header that indicates its policies for subsequent use of the released attributes. Thus, the <UsageDirective> header in the <Query> element describes intended usage of the attributes, while the <UsageDirective> header in the <QueryResponse> element describes the required usage of the attributes by the recipient.

When a <UsageDirective> header is included, the procedure described in Section 6.6 of [Liberty-IDWSF-Soap-Binding] MUST be followed. Examples of usage directives may be found in Section 6.6.3 of [Liberty-IDWSF-Soap-Binding].

The Figure 6 below illustrates the optional usage directive header being included in the Query message from the Service Provider to the Attribute Provider. It also depicts the optional usage directive header being included in the Query Response message from the Attribute Provider to the Service Provider.

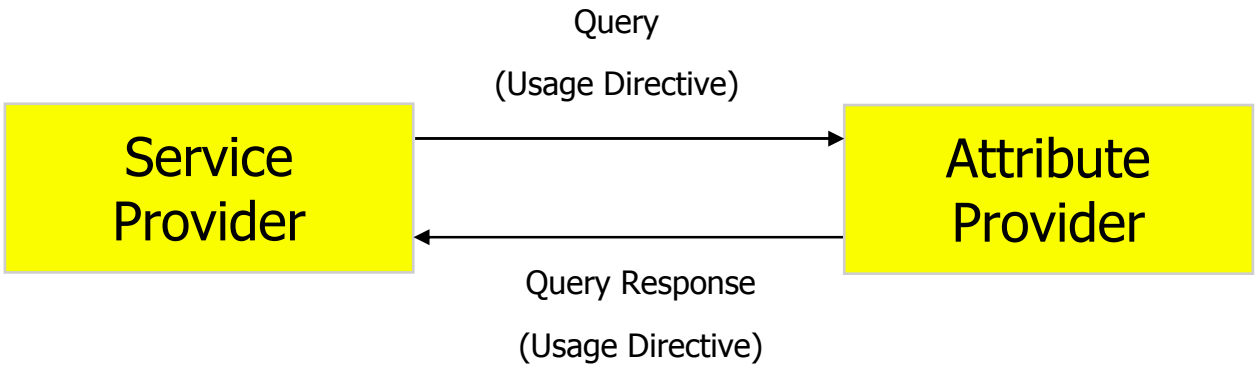

Figure 6: Usage Directive

The schema below taken from [Liberty-IDWSF-Soap-Binding] provides an example of a UsageDirective header. As seen in the example below, the usage directive indicates that the usage of the attribute must be compliant with EU usage directive regulations.

```
<UsageDirective id="directive1000" ref="#datarequest001" S:mustUnderstand="1">
   <cot:PrivacyPolicyReference xmlns:cot="http://circle-of-trust.com/isf">
      http://circle-of-trust.com/policies/eu-compliant
   </cot:PrivacyPolicyReference>
</UsageDirective>
```

6.4 Interaction Service

An Attribute Provider may use an Interaction Service to query a Principal, by sending an <InteractionRequest> element to the Interaction Service, which after interacting with the Principal responds with an <InteractionResponse> element. The Figure 7 below illustrates this message exchange for the case where a Service Provider queries an Attribute Provider.

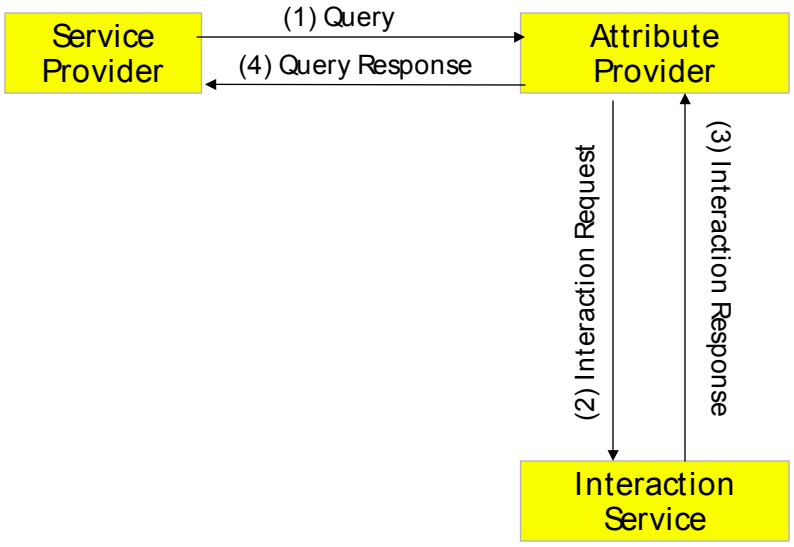

Figure 7: Interaction Service

The Interaction Request MUST follow the description in Section 5.1 of [Liberty-IDWSF-Interaction-Svc], and the Interaction Response MUST follow the description in Section 5.2 of [Liberty-IDWSF-Interaction-Svc].

6.4.1 Interaction Redirect

When an Attribute Provider (acting as the Web Service Provider) wishes to request the Service Provider (acting as the Web Service Requester) to redirect the Principal to a URL at the Attribute Provider, the mechanism specified in Section 4 of [Liberty-IDWSF-Interaction-Svc] MUST be adhered to. As shown in Figure 8, the RedirectRequest element is used for this purpose, and indicates to the Service Provider to redirect the Principal. After the necessary information has been obtained by the Attribute Provider, the Attribute Provider redirects the Principal back to the Service Provider.

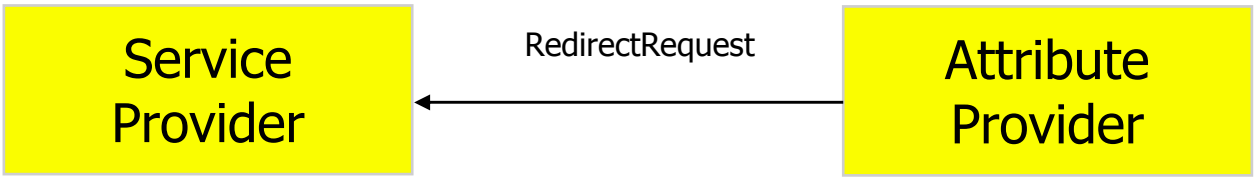

Figure 8: Interaction Redirect

6.5 Bootstrapping Identity based Web Services Framework

In order to access the Identity based Web Services Framework, two mechanisms are provided:

- The Discovery Service bootstrap

- Authentication Service and SSO Service

6.5.1 Discovery Service Bootstrap

The Discovery Service Bootstrap is a mechanism by which an Identity Provider can provide a Service Provider with resource offerings needed to contact a Discovery Service, by leveraging the Identity Federation Framework. When the Discovery Service Bootstrap is supported, the mechanisms specified in Section 6 of [Liberty-IDWSF-Disco] MUST be adhered to.

6.5.2 Authentication Service

The Authentication Service is a mechanism by which an Identity Provider can provide a Service Provider with resource offerings needed to contact other Providers including the Discovery Service. When the Authentication Service is supported, the mechanisms specified in Section 5 of [Liberty-IDWSF-AuthnSSO] MUST be adhered to.

6.5.3 SSO Service

When the SSOS is supported, the mechanisms specified in Section 6 of [Liberty-IDWSF-AuthnSSO] MUST be adhered to.

6.6 Discovery Service

When a Service Provider wishes to determine the Attribute Provider(s) hosting required resource(s) on behalf of a specific Principal, it MAY contact a Discovery Service to obtain such information. The Discovery Service MAY also provide the requesting Service Provider with necessary credentials needed to access the Attribute Provider.

The Discovery Service allows requesters to discover resource offerings. A resource offering is the association of a resource and a service instance. A service instance is a running Web Service at a distinct protocol endpoint. This association is necessary as there is a many-to-many relationship between resources and service instances. A single service instance may serve many resources. For example, a personal profile service provider would typically serve up many profiles behind a single service instance.

The Figure 9 below illustrates a Calendar Service Instance hosting the Calendar resource for various Principals (P1,P2,P3,P4,P5,P6). The various resource offerings, denoting the association of the calendar resource for each of the Principals with the Calendar Service Instance, are also depicted in the figure. In this specific case, there are six resource offerings.

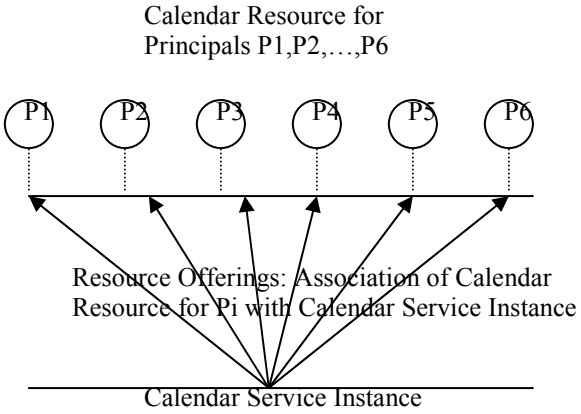

Figure 9: Illustration of Calendar Service Instance hosting Calendar resource for Various Principals

The Figure 10 below depicts a single service instance hosting three different resources, namely Calendar, Contact Book and Personal Profile, for a specific Principal P1. The various resource offerings, denoting the association of the resources for the specific Principal with the common Service Instance, is also depicted in the figure. In this specific case, there are three resource offerings.

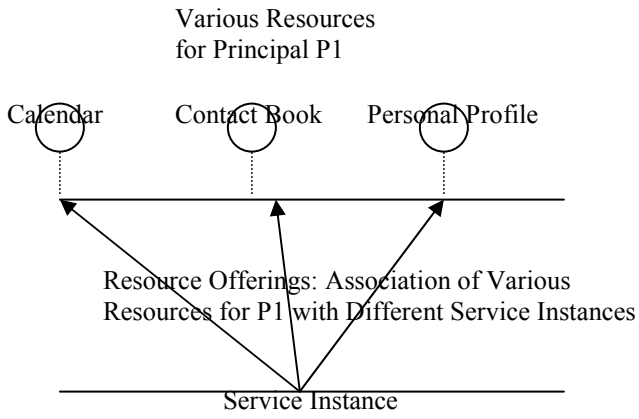

Figure 10: Illustration of different resources for a specific Principal

The schema below provides an illustration of a Resource Offering as the association between a Resource (depicted by ResourceID) and a ServiceInstance. In the example below, the ResourceOffering element has two child elements, the ResourceID and the ServiceInstance elements. The uri http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs in the ResourceID element denotes a specific Principal's Calendar resource. The ServiceInstance element describes the service type, the service provider ID and a description of the service itself.

```
<ResourceOffering xmlns="urn:liberty:disco:2003-08">
   <ResourceID>http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs</ResourceID>
   <ServiceInstance xmlns="urn:liberty:disco:2003-08">
      <ServiceType>urn:CalendarService:2003-08</ServiceType>
      <ProviderID>http://CalendarServiceProvider.com/</ProviderID>
      <Description>
         <SecurityMechID>urn:liberty:security:2003-08:TLS:SAML</SecurityMechID>
         <Endpoint>https://soap.CalendarServiceProvider.com/soap/</Endpoint>
      </Description>
   </ServiceInstance>
</ResourceOffering>
```

6.6.1 Discovery Lookup

In order to obtain information on suitable resource offerings, a requester needs to initiate a discovery lookup procedure. The procedure described in Section 5.1 of [Liberty-IDWSF-Disco] MUST be followed. As indicated in the Figure 11 below, a requestor sends a Query message to the Discovery Service, which responds using a Query Response message.

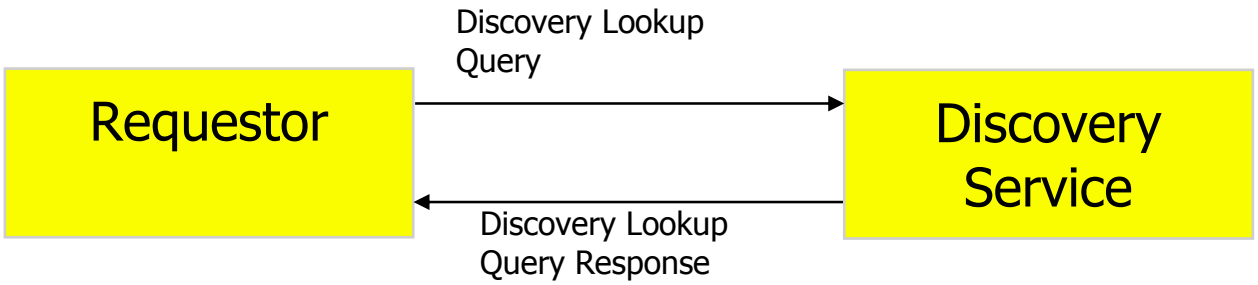

Figure 11: Discovery Lookup

The Discovery Lookup Query message from the Requestor to the Discovery Service MUST adhere to the specifications in Section 5.1.1 of [Liberty-IDWSF-Disco]. The Discovery Lookup Query contains the ResourceID element, which indicates to the Discovery Service the specific resource(s) being requested.

The example below shows a Discovery Lookup Query schema.

```
<Query xmlns="urn:liberty:disco:2003-08">
   <ResourceID> http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs</disco:ResourceID>
   <RequestedServiceType>
      <ServiceType> urn:CalendarService:2003-08</disco:ServiceType>
   </RequestedServiceType>
</Query>
```

The Discovery Lookup QueryResponse message from the Discovery Service to the Requestor MUST adhere to the specifications in Section 5.1.2 of [Liberty-IDWSF-Disco]. The Discovery Lookup QueryResponse message contains the ResourceOffering element(s) that satisfy the query.

The example below shows a Discovery Lookup QueryResponse schema.

```
<QueryResponse xmlns="urn:liberty:disco:2003-08">
   <ResourceOffering xmlns="urn:liberty:disco:2003-08">
      <ResourceID>http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs</ResourceID>
      <ServiceInstance xmlns="urn:liberty:disco:2003-08">
         <ServiceType>urn:CalendarService:2003-08</ServiceType>
         <ProviderID>http://CalendarServiceProvider.com/</ProviderID>
         <Description>
            <SecurityMechID>urn:liberty:security:2003-08:TLS:SAML</SecurityMechID>
            <Endpoint>https://soap.CalendarServiceProvider.com/soap/</Endpoint>
         </Description>
      </ServiceInstance>
   </ResourceOffering>
</QueryResponse>
```

6.6.2 Discovery Update

In order to insert, delete or modify Resource Offerings at a Discovery Service, a Discovery Update procedure needs to be initiated. The procedure described in Section 5.2 of [Liberty-IDWSF-Disco] MUST be followed. As indicated in the Figure 12 below, the initiator sends a Discovery Update Modify message to the Discovery Service, which in turn sends a Discovery Update ModifyResponse message back to the initiator.

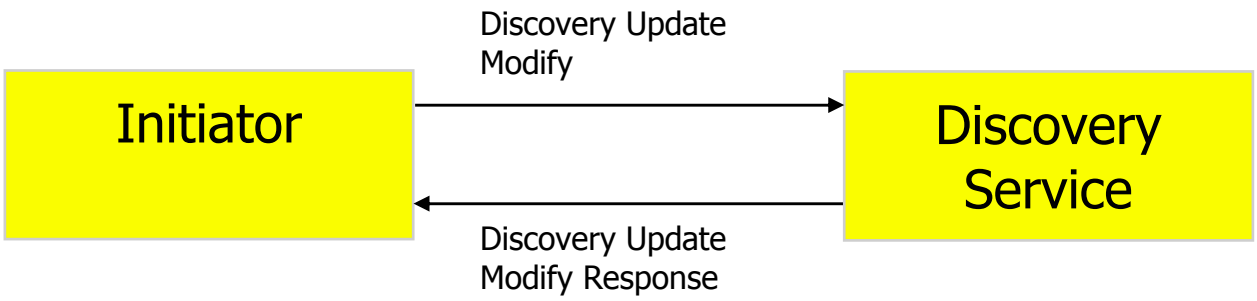

Figure 12: Discovery Update

The Discovery Update Modify message from the Initiator to the Discovery Service MUST be as specified in Section 5.2.1 of [Liberty-IDWSF-Disco], while the Discovery Update ModifyResponse message from the Discovery Service to the Initiator MUST be as specified in Section 5.2.2 of [Liberty-IDWSF-Disco].

An example of Discovery Update Modify and ModifyResponse are included below.

```
<Modify xmlns="urn:liberty:disco:2003-08">
   <ResourceID>http://example.com/disco/d0CQF8elJTDLmzEo</disco:ResourceID>
   <InsertEntry>
      <ResourceOffering xmlns="urn:liberty:disco:2003-08">
         <ResourceID>http://CalendarServiceProvider.com/profiles/l4m0B82k15csaUxs</ResourceID>
         <ServiceInstance xmlns="urn:liberty:disco:2003-08">
            <ServiceType>urn:CalendarService:2003-08</ServiceType>
            <ProviderID>http://CalendarServiceProvider.com/</ProviderID>
            <Description>
               <SecurityMechID>urn:liberty:security:2003-08:TLS:SAML</SecurityMechID>
               <Endpoint>https://soap.CalendarServiceProvider.com/soap/</Endpoint>
            </Description>
         </ServiceInstance>
      </ResourceOffering>
   <AuthenticateRequester descriptionID Refs="saml"/>
   <AuthorizeRequester descriptionIDRefs="samlclientTLS"/>
   </InsertEntry >
   <RemoveEntryentryID="1"/>
</Modify>


<ModifyResponse xmlns="urn:liberty:disco:2003-08" new EntryIDs="2">
   <Status code="OK"/>
</ModifyResponse>
```

6.7 LUAD

It is possible that a Web Service Consumer (WSC) or a Web Service Provider (WSP) is associated with one or a few users, rather than many users. User agents and devices hosting such WSCs or WSPs are known as Liberty enabled User Agents and Devices (LUAD). When this is the case, the mechanisms specified in [Liberty-IDWSF-Client-Profiles] MUST be adhered to.

6.7.1 LUAD acting as WSC

When a LUAD acts as a WSC, the mechanisms specified in Section 3 of [Liberty-IDWSF-Client-Profiles] MUST be adhered to. A LUAD WSC may not be associated with a browsing session.

6.7.2 LUAD acting as WSP

When a LUAD acts as a WSP, the mechanisms specified in Section 4 of [Liberty-IDWSF-Client-Profiles] MUST be adhered to.

6.8 Security

6.8.1 Authentication

Two types of authentication mechanisms are specified in order to accommodate various deployment scenarios - Peer Entity authentication and Message Authentication.

- **Peer Entity Authentication**: When a Web Services Requestor (WSR) interacts directly with a Web Services Provider (WSP), the Provider may use the communication channel authentication feature to convey its identity. A candidate mechanism is SSL3.0/TLS1.0 client-side X.509 v3 certificate based authentication. When communicating Providers use Peer Entity Authentication, the procedures specified in Section 6.2 of [Liberty-IDWSF-Security-Mechanisms] MUST be adhered to. The null and peer entity authentication mechanisms, as specified in Section 6.2 of [Liberty-IDWSF-Security-Mechanisms] MUST be supported.

- **Message authentication:** When a WSR interacts with a WSP via one or more active intermediaries (e.g. proxy), the Provider may explicitly convey its identity to the recipient. Two types of message authentication MAY be supported:

    - X.509 v3 Certificate Message Authentication
    - SAML Assertion Message Authentication

  When communicating Providers use Message Authentication, the procedures specified in Section 6.3 of [Liberty-IDWSF-Security-Mechanisms] MUST be adhered to. The null and bearer message authentication mechanisms, as specified in Section 6.3 of [Liberty-IDWSF-Security-Mechanisms] MUST be supported.

6.8.2 Confidentiality and Privacy

Confidentiality and privacy mechanisms are needed to guarantee that transported information will only be understandable by the authorised parties. Confidentiality mechanisms are provided at multiple levels, namely transport, message and resource identifier level. Such mechanisms MUST adhere to Section 5 of [Liberty-IDWSF-Security-Mechanisms].

- **Transport Layer Channel Protection**: When the communicating providers interact directly without any active intermediary (e.g. proxy), then transport layer protection mechanism can insure integrity and confidentiality of messages exchange. Suitable SSL/TLS cipher-suites MUST be used to achieve transport layer channel protection. As specified in Section 5.1 of [Liberty-IDWSF-Security-Mechanisms], the following SSL/TLS cipher-suites SHOULD be used:

    - TLS_RSA_WITH_RC4_128_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_CBC_SHA
    - TLS_DHE_DSS_WITH_AES_CBC_SHA

  Other protocols such as Kerberos and IPSEC MAY be used as long as they provide an equivalent level of protection.

- **Message Confidentiality Protection**: In the presence of active intermediaries (e.g. proxy, gateway, broker) the integrity and confidentiality of message exchanges between communicating Providers MUST be assured at the message level. In this case communicating peers MUST protect sensitive information from unauthorized entities. As specified in Section 5.2 of [Liberty-IDWSF-Security-Mechanisms], to fulfil this requirement, peers MUST use the confidentiality mechanisms specified in [wss-sms] to encrypt the child elements of the SOAP body.

- **Identifier Privacy Protection**: When information conveyed by a trusted authority for consumption by the invoked services contains privacy sensitive data (e.g. federate name space identifier), such information MUST be

protected from untrusted intermediary entities. The encryption of the Name Identifier and/or the URI mechanism MUST be available. The procedures specified in Section 5.3 of [Liberty-IDWSF-Security-Mechanisms] MUST be adhered to.

6.8.3 Authorization

In order to generate, convey and consume authorization information, the procedures specified in Section 8 of [Liberty-IDWSF-Security-Mechanisms] MUST be adhered to. The authorization mechanisms rely upon XML schema support, in order to foster conveyance of authorization information within a given message exchange. These include proxy schema for conveying the identity of a proxy, session context to convey session status from an entity to another, and resource access to convey information regarding the accessing entity and the resource for which access is being attempted.

6.8.4 Message Correlation

The messages exchanged between participants of the protocol MAY require assurance that a response correlates to its request. In order to do this, the Request may include a correlation element in the message header in order to address this issue. The mechanisms specified in [Liberty-IDWSF-Soap-Binding] MUST be adhered to.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-OWSER-NI-Phase2-V1_0-20050204-D	08 Feb 2005	5, 6	Created table of contents for sections 5 & 6, based on document: OMA-MWS-2004-0058R02-TechhnologyforIDManagementReq
OMA-TS-OWSER-NI-Phase2-V1_0-20050324-D	March 24, 2005	6	Added contents from Doc 31R01
OMA-TS-OWSER-NI-Phase2-V1_0-20050331-D	March 31, 2005	1,6	Added contents from Doc 42
OMA-TS-OWSER-NI-Phase2-V1_0-20050519-D	May 19, 2005	3,5	Added contents from Doc 50R1
OMA-TS-OWSER-NI-Phase2-V1_0-20050615-D	June 15, 2005	4	Added contents from Doc 58
OMA-TS-OWSER-NI-WSF-V1_0-20050616-D	June 15, 2005	6	Added contents from Doc55R03 Affiliation and Proxying sections moved to NI-FF spec
OMA-TS-OWSER-NI-WSF-V1_0-20050808-D	August 8, 2005	1	Modified Scope section
OMA-TS-OWSER-NI-WSF-V1_0-20050822-D	August 22, 2005	4,5,6,B.6	Added contents from Doc 69R02 and 81R01
OMA-TS-OWSER-NI-WSF-V1_0-20051103-D	Nov 03, 2005	All	Corrected References. Corrected cross-references.
Candidate Version OMA-TS-OWSER-NI-WSF-V1_0	20 Dec 2005		Status changed to Candidate by TP TP ref # OMA-TP-2005-0396-OWSER_NI_V1_0_for_Candidate_approval

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [IOPPROC].

B.1 IdP

Item	Function	Reference	Status	Requirement
NI-IdP-001	Bootstrapping Identity Based Web Services Framework	6.5	M	NI-IdP-002 OR NI-IdP-003
NI-IdP-002	DS Bootstrap	6.5.1	O	
NI-IdP-003	Authentication Service	6.5.2	O	
NI-IdP-004	SSO Service	6.5.3	O	
NI-IdP-005	Basic Security Mechanisms	6.8	M	NI-IdP-006
NI-IdP-006	Authentication	6.8.1	M	
NI-IdP-007	Confidentiality	6.8.2	O	
NI-IdP-008	Authorization	6.8.3	O	

Table 1: SCR for IdP

B.2 DS

Item	Function	Reference	Status	Requirement
NI-DS-001	Discovery Service	6.6	M	NI-DS-002 AND NI-DS-003
NI-DS-002	Discovery Lookup	6.6.1	M	
NI-DS-003	Discovery Update	6.6.2	M	
NI-DS-004	Interaction Service	6.4	O	NI-DS-005
NI-DS-005	Interaction Redirect	6.4.1	O	
NI-DS-006	LUAD	6.7	O	NI-DS-007
NI-DS-007	LUAD as DS	6.7.3	O	
NI-DS-008	PAOS	6.1.1	O	
NI-DS-009	Basic Security Mechanisms	6.8	M	NI-DS-010
NI-DS-010	Authentication	6.8.1	M	
NI-DS-011	Confidentiality	6.8.2	O	
NI-DS-012	Authorization	6.8.3	O	

Table 2: SCR for DS

B.3 SP

Item	Function	Reference	Status	Requirement
NI-SP-001	Attribute Query	6.1	O	
NI-SP-002	Attribute Modification	6.2	O	
NI-SP-003	Usage Directives	6.3	O	
NI-SP-004	Discovery Lookup	6.6.1	O	
NI-SP-005	Interaction Redirect	6.4.1	O	
NI-SP-006	PAOS	6.1.1	O	
NI-SP-007	Basic Security Mechanisms	6.8	M	NI-SP-008
NI-SP-008	Authentication	6.8.1	M	
NI-SP-009	Confidentiality	6.8.2	O	
NI-SP-010	Authorization	6.8.3	O	

Table 3: SCR for SP

B.4 LUAD WSC

Item	Function	Reference	Status	Requirement
NI-SP-001	Attribute Query	6.1	O	
NI-SP-002	Attribute Modification	6.2	O	
NI-SP-003	Usage Directives	6.3	O	
NI-SP-004	Discovery Lookup	6.6.1	O	
NI-SP-005	Interaction Redirect	6.4.1	O	
NI-SP-006	Basic Security Mechanisms	6.8	M	NI-SP-007
NI-SP-007	Authentication	6.8.1	M	
NI-SP-008	Confidentiality	6.8.2	O	
NI-SP-009	Authorization	6.8.3	O	
NI-SP-010	Authentication Service	6.5.2	M	
NI-SP-011	SSO Service	6.5.3	O	

Table 4: SCR for LUAD WSC

B.5 LUAD WSP

Item	Function	Reference	Status	Requirement
NI-SP-001	Attribute Query	6.1	O	
NI-SP-002	Attribute Modification	6.2	O	
NI-SP-003	Usage Directives	6.3	O	

Item	Function	Reference	Status	Requirement
NI-SP-004	Discovery Lookup	6.6.1	O	
NI-SP-005	Interaction Service	6.4	O	
NI-SP-006	PAOS	6.1.1	O	
NI-SP-007	Basic Security Mechanisms	6.8	M	NI-SP-008
NI-SP-008	Authentication	6.8.1	M	
NI-SP-009	Confidentiality	6.8.2	O	
NI-SP-010	Authorization	6.8.3	O	

Table 5: SCR for LUAD WSP

B.6 AP

Item	Function	Reference	Status	Requirement
NI-AP-001	Attribute Query	6.1	O	
NI-AP-002	Attribute Modification	6.2	O	
NI-AP-003	Usage Directives	6.3	O	
NI-AP-004	Interaction Service	6.4	O	
NI-AP-005	Interaction Redirect	6.4.1	O	
NI-AP-006	Basic Security Mechanisms	6.8	M	NI-AP-007
NI-AP-007	Authentication	6.8.1	M	
NI-AP-008	Confidentiality	6.8.2	O	
NI-AP-009	Authorization	6.8.3	O	

Table 6: SCR for AP

B.7 IS

Item	Function	Reference	Status	Requirement
NI-IS-001	Interaction Service	6.4	M	NI-IS-002
NI-IS-002	Interaction Redirect	6.4.1	M	
NI-IS-003	Basic Security Mechanisms	6.8	M	NI-IS-004
NI-IS-004	Authentication	6.8.1	M	
NI-IS-005	Confidentiality	6.8.2	O	
NI-IS-006	Authorization	6.8.3	O	

Table 7: SCR for IS