OMA Web Services Network Identity Architecture

Approved Version 1.0 – 28 Mar 2006

Open Mobile Alliance

OMA-AD-OWSER_NI-V1_0-20060328-A

Contents

1. SCOPE (INFORMATIVE) 4
2. REFERENCES 5
2.1 NORMATIVE REFERENCES 5
2.2 INFORMATIVE REFERENCES 5
3. TERMINOLOGY AND CONVENTIONS 7
3.1 CONVENTIONS 7
3.2 DEFINITIONS 7
3.3 ABBREVIATIONS 9
4. INTRODUCTION (INFORMATIVE) 10
4.1 PLANNED PHASES 10
5. ARCHITECTURAL MODEL 11
5.1 DEPENDENCIES 11
5.2 ARCHITECTURAL DIAGRAM 12
5.3 FUNCTIONAL COMPONENTS AND INTERFACES 13
5.3.1 Description of Interfaces 13
5.4 FLOWS 15
5.4.1 Single Circle of Trust 16
5.4.2 Interconnected Circles of Trust 18
5.4.3 Shared Circle of Trust 20
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 24
A.1 APPROVED VERSION HISTORY 24

Figures

Figure 1: High Level ID-WSF Architecture 12
Figure 2: High Level Flow 15
Figure 3: Message Flows within a single CoT 18
Figure 4: Interconnection between two CoTs 20
Figure 5: Shared CoT 22

1. Scope (Informative)

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): Identity Web Services Framework " [OWER 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.

"OMA Web Services Network Identity Enabler (OWSER NI): 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 Web Services Network Identity Enabler (OWSER NI): Architecture" document [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

2. References

2.1 Normative References

[OSE] "OMA Service Environnent"
URL: http://www.openmobilealliance.org/

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

[OWSER NI WSF] "OMA Web Services Network Identity Enabler (OWSER NI): Identity Web Services Framework ", Open Mobile Alliance, 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

[NI-RD] "MWS Identity Management Requirements", OMA Web Services Enabler Release V1.1, 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/

2.2 Informative References

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

[ID-FF] "Liberty ID-FF Architecture Overview: Version 1.2," URL:

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

[ID-WSF] "Liberty ID-WSF Web Service Framework Overview, Version 1.0", September 2004. URL:http://www.projectliberty.org

[Liberty-IDFF-ProtocolsSchema] "Liberty ID-FF Protocols and Schema Specification," Version 1.2 http://www.projectliberty.org

[Liberty-Metadata] "Liberty Metadata Description and Discovery Specification," Version 1.0, http://www.projectliberty.org

[Liberty-InteractionService] "ID-WSF Interaction Service," April 2003, URL:http://www.projectliberty.org

[Liberty-IDWSF-Security-Mechanisms] "Liberty ID-WSF Security Mechanisms," Version 1.0, URL: http://www.projectliberty.org

[Liberty-IDWSF-DST] "Liberty ID-WSF Data Services Template Specification," Version 1.0, URL:http://www.projectliberty.org

[Liberty-IDWSF-SOAPBinding "Liberty ID-WSF SOAP Binding Specification," Version 1.0, URL:http://www.projectliberty.org

[Liberty-IDWSF-Disco-Svc] "Liberty ID-WSF Discovery Service Specification," Version 1.0, URL:http://www.projectliberty.org

[Liberty-IDFF-Authn-Context] "Liberty ID-FF Authentication Context Specification,: Version 1.2 URL:http://www.projectliberty.org

[Liberty-IDWSF-Client-Profiles] "Liberty ID-WSF Profiles for Liberty-enabled User Agents and Devices," version 1.0 http://www.projectliberty.org

[Liberty-IDWSF-Authn] "Liberty ID-WSF Authentication Service and Single Sign-on Service Specification," Version 1.0, URL:http://www.projectliberty.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.

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

Assertion	A statement about a Principal.
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 event is acceptable, emphasising that a single authentication event 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 Agreement	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. dissemination 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	See ID-WSF Discovery Service.
End User	An individual who uses services and content [OMADict]

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	**Entity**: **1** : The information transferred as the payload of a request or response. **2** : A distinct component of a service architecture [OMADict]. 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 recognized 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 [OWSER NI ….]
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 Data Service Template 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.
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.
Security Mechanisms	See ID-WSF Security Mechanisms.
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 that 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]
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.
Web Service Provider	See [Owser Core]

3.3 Abbreviations

AP	Attribute Provider
DST	Data Services Template
IdP	Identity Provider
ID-FF	Identity Federation Framework
ID-WSF	Identity Web Services Framework
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

4. Introduction (Informative)

This document describes the logical entities and interfaces needed to support the discovery and use of Web Services for accessing end-user related attributes in a privacy-protected manner. Attributes are data about or related to an end user such as personal information, preferences, capabilities etc. It is expected that such information about an individual will be distributed amongst different parties (called attribute providers), such as an individual's bank, employer, personal devices, mobile operator etc. Many services are enhanced if such information can be used (with the user's permission) by a service provider to personalize or make more efficient the end-user experience. Some widely used examples of such attributes in an OMA context are the location or the presence status of a mobile subscriber.

The OMA Web Services Network Identity Enabler Release (OWSER NI) has chosen to address this area in two specifications:,

- The OMA Network Identity Federation Framework [OWSER NI FF] fulfils requirements (see [NI-RD]) for identity federation based on the Liberty Alliance Identity Federation Framework [ID-FF].
- The OMA Network Identity Web Services Framework [OWSER NI WSF] fulfils the remaining 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

In an OMA environment, a relevant example to illustrate the typical scenarios addressed by this architecture is the need to access a subscriber's location information to provide a Find Nearest____ service. Such information may be offered by a (location) attribute provider through a Web service interface. In such a case, the service provider offering the overall service may need to access the attribute data (in this case, location) at the attribute provider, a mobile operator. These two providers do not have a shared identity for the end user (more formally, a Principal) through which the former may request some attribute data from the latter. In fact, it is possible that the Principal may not even have an identity associated with the overall service provider, as this may be a one-time access or an anonymous access. However, if the Principal has federated his identity at the service provider and attribute provider with that at an Identity Provider, which provides authentication services for both of them, it is possible for the overall service provider to be given access to the pseudonym by which the identity provider and the attribute provider refer to the same Principal This pseudonym, encrypted to prevent disclosure to the Service Provider and suitably protected against replay attacks, is sufficient to allow the Service Provider to refer to the Principal when requesting attribute information.

The identity federation techniques specified in [OWSER NI FF] therefore provide one of the tools to enable services such as attribute sharing. In the simplified discussion above, not all the other features for such attribute sharing have been discussed. For instance, service providers need to discover what attributes related to a Principal are available and where the corresponding data may be accessed. Also, in the course of accessing such attribute data, a Principal may need to be contacted to obtain permission to share such data, or directives may need to be passed that describe how such data may be used. The specification of such capabilities is addressed in [OWSER NI WSF].

This document presents an overview of the architecture and interfaces required to support the requirements related to privacy-protected attribute sharing, which is based on the Liberty Alliance Identity Web Services Framework [ID-WSF], as well as additional identity-federation features (e.g., affiliations, chain of authentications) of Liberty Alliance [ID-FF] .

4.1 Planned Phases

EDNote: This section will be populated as the specification work progresses

5. Architectural Model

5.1 Dependencies

The technical solution to the MWS Network Identity requirements in [NI-RD], whose architecture is described below, is based on specifications provided by the Liberty Alliance. This section briefly describes the Liberty specifications on which that solution depends. Subsequent sections describe the architecture of that solution in detail.

Mechanisms for establishing, maintaining and verifying trust relationships between multiple Service Providers and Identity Providers both within a single Circle of Trust and across Multiple Circles of Trust are based on [Liberty-IDFF-ProtocolsSchema] and [Liberty-Metadata].

Mechanisms for end users to provide consent to release their identity attributes are provided by the Liberty Interaction Service [Liberty-InteractionService].

Security Mechanisms for conveying artifacts e.g., a security token, needed to establish and verify trust and protect these artifacts during transmission are described in [Liberty-IDWSF-Security-Mechanisms].

Interfaces to query and update attributes in an attribute provider are provided by the Liberty Data Services Template [Liberty-IDWSF-DST].

Interfaces to discover an attribute provider or providers hosting the identity attributes for a specific user (principal) are provided by the Liberty Discovery Service [Liberty-IDWSF-Disco-Svc].

SOAP bindings for message exchanges in Liberty protocols are specified in [Liberty-IDWSF-SOAPBinding].

An authentication protocol and the use of the protocol to interact with a Liberty Identity Provider and Single Sign-on Service are defined in [Liberty-IDWSF-Authn]

Profiles describing how user agents such as personal computers and mobile devices can host Liberty-enabled WSCs and/or WSPs are provided in [Liberty-IDWSF-Client-Profiles]

Mechanisms for conveying authentication context information between Liberty entities are described in [Liberty-IDFF-Authn-Context]

The OWSER NI specification's use of the Liberty Alliance specifications listed above will reuse the technologies specified in the OWSER Core Specification [OWSER Core]. The OWSER NI specification will collectively provide additional services and protocols beyond those described in [OWSER Core] that can be used to provide access to user-related attributes in a privacy protected manner.

The architecture described in this document satisfies the design principles for the OSE as follows:

- An implementation MUST specify or reference one or more interfaces for its intrinsic functionality that will be used to interface to (i.e. invoke) its functions

The NI Architecture documents multiple interfaces required to provide access to identity attributes in a privacy-protected manner. Details are provided in subsequent sections.

- ·If an implementation depends on already defined OMA functions, it MUST identify which other enablers' intrinsic functionality it will invoke to perform these already-defined OMA functions.

The NI solution whose architecture is described here relies on protocols and services defined in the OWSER Core Specification [OWSERCore].

- ·An implementation MUST specify or reference only the functions, protocols and invocations that are essential (i.e. core) to its purpose.

The protocols and services described in this document are all related to identity and access to identity-related attributes in a Liberty enabled Web Services environment and collectively provide a solution to the NI requirements in [NI-RD]. Details are provided in subsequent sections.

5.2 Architectural Diagram

The Liberty Alliance Project addresses a broad set of requirements around Network Identity.

Liberty's architecture provides the ability to protect the Principal's privacy at various SPs in their interactions with the Principal. This is done through the provisioning of pseudonyms for the Principal at each SP anchored at a distinguished Service Provider, called the Identity Provider in the Liberty architecture, who is the entity that can map each pseudonym to a specific individual. Thus, SPs only have to manage identity information local to their own user community and do not have to maintain linkages to all other SPs with whom the Principal may have a relationship (existing or in the future).

In addition to minimising the need for a SP to maintain multiple relationships, identity federation with an IdP also allows valuable add-on services to a SP, such as a Single SignOn service provided by the Identity Provider. The core feature of Liberty's ID-WSF is a means for a SP to find a particular Principal's Attribute Providers, and permit the sharing of attributes with the SP based on the Principal's consent. An SP, given the distinguished name Attribute Provider, provides some information (attributes) about the Principal (subject to his consent) to other SPs. This is done by leveraging the Identity Provider's special role of mapping the Principal's pseudonym at each SP using ID-FF, because the Liberty model is based on SPs interacting with.each other about a specific Principal without explicitly sharing an identifier.

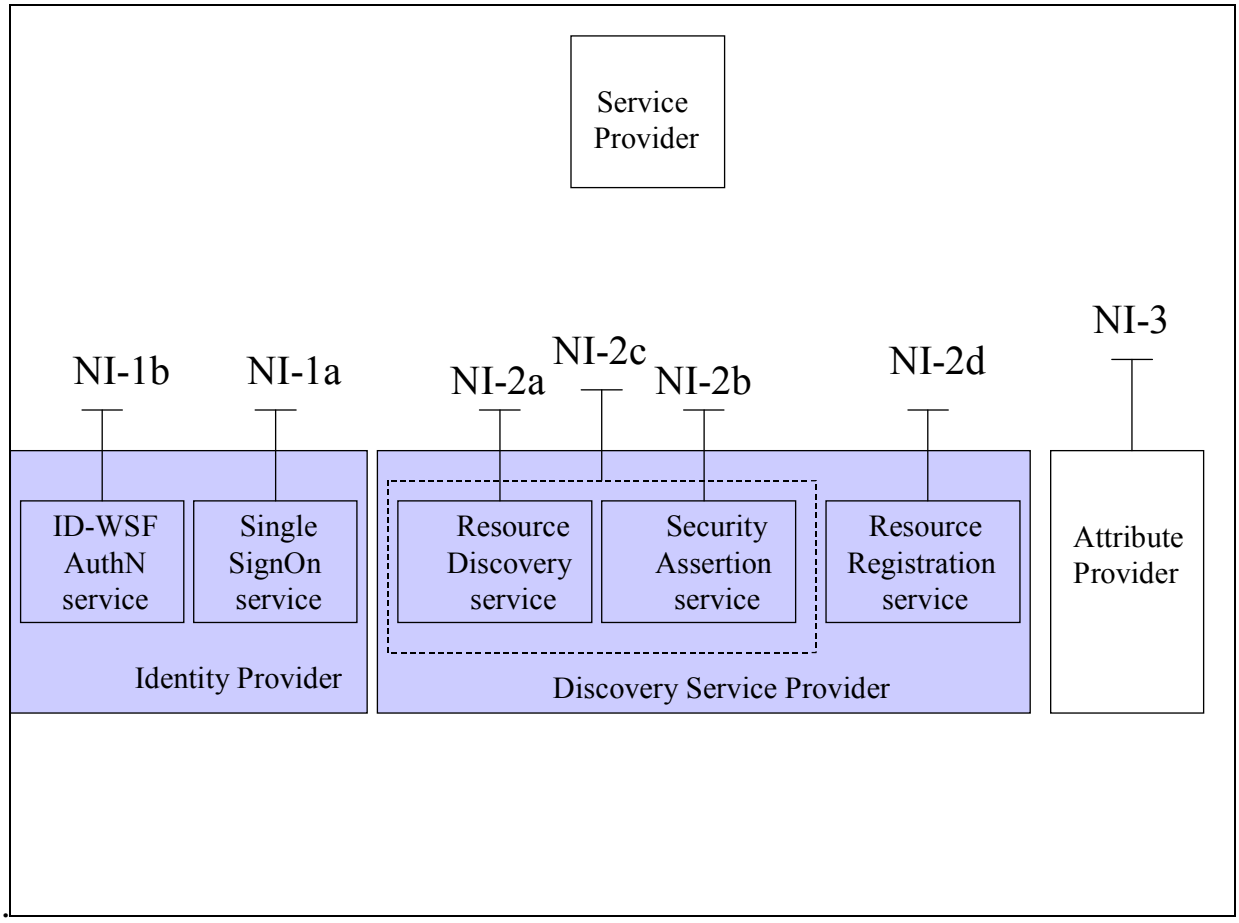

Figure 1: High Level ID-WSF Architecture

The interfaces are described in section 5.3.

5.3 Functional Components and Interfaces

5.3.1 Description of Interfaces

5.3.1.1 Interface NI-1: Service Provider - Identity Provider

The NI-1 interface supports communication between a service provider and the identity provider. The NI-1 interface uses protocols defined in ID-FF, as described in [OWSER NI FF], as well as additions described below to support ID-WSF. This interface consists of the following services.

5.3.1.1.1 NI-1a: Single Signon Service

The functions provided by this interface are:

- The retrieval by an SP of an Authentication Assertion about an existing authenticated session at the IdP involving a particular Principal's federated identity
    - see [OWSER NI FF] for browser based interactions between a client and an SP
    - defined in ID-WSF for Liberty ID-WSF-enabled Web Service clients
- Setting the Authentication Context about acceptable authentication assertions related to the Principal
- Single Sign Out (see OWSER NI FF])

To support ID-WSF based interactions, the response from the Identity Provider to the Service provider with an authentication assertion may also contain "bootstrap" information consisting of a SOAP endpoint enabling the Service Provider to locate the Principal's Discovery Service Provider.

This bootstrap information may contain the name identifier by which the Principal is known to the IdP and the DS. This name identifier may be secured so that it is not visible to or modifiable by the SP.

5.3.1.1.2 NI-1b: ID-WSF Authentication Service

The interface provides the facility for a Web Service Requester to create an authenticated session at an IdP. Information about this authenticated session is used by a non-browser/Web Service client to invoke the Single SignOn service

5.3.1.1.3 Interface NI-2: Service Provider - Discovery Service

The NI-2 interface supports communication between a service provider and the discovery service. The NI-2 interface uses protocols defined in ID-WSF. The NI-2 interface is comprised of the following services.

5.3.1.1.4 Service NI-2a

The functions provided by this service are:

- Discovery of attribute providers for a given principal.

5.3.1.1.5 Service NI-2b

The functions provided by this service are:

- Obtaining an authorization token for a particular Principal's Attribute Providers

  NOTE: How the Discovery Service implements authorization decisions are out of scope of the NI specifications.

5.3.1.1.6 Service NI-2c

The functions provided by this service are:

- Discovery of Attribute Providers for a given principal.

and optionally,

- Provides authorization tokens for a particular Principal's Attribute Providers.

NI-2c provides a composition of services NI-2a and NI-2b that allows a requestor to discover Attribute Providers and obtain authorization tokens in a single request operation.

5.3.1.1.7 Service NI-2d

The functions provided by this service are:

- Registration of attribute services (Resource Offerings) for a given principal.

5.3.1.1.8 Interface NI-3: Service Provider - Attribute Provider

The NI-3 interface supports communication between the service provider and any attribute provider. The NI-3 interface uses protocols defined in ID-WSF. The NI-3 interface is:

- The service to create, read, write, update, and delete Attributes
- User Interaction Service, by which a Principal's consent is requested prior to attribute sharing

5.4 Flows

The general architecture and flow for a simple example of a user request to an ID-WSF-enabled application is as follows.

Note: Unlabelled arrows are out-of-scope of the OWSER Network Identity specifications

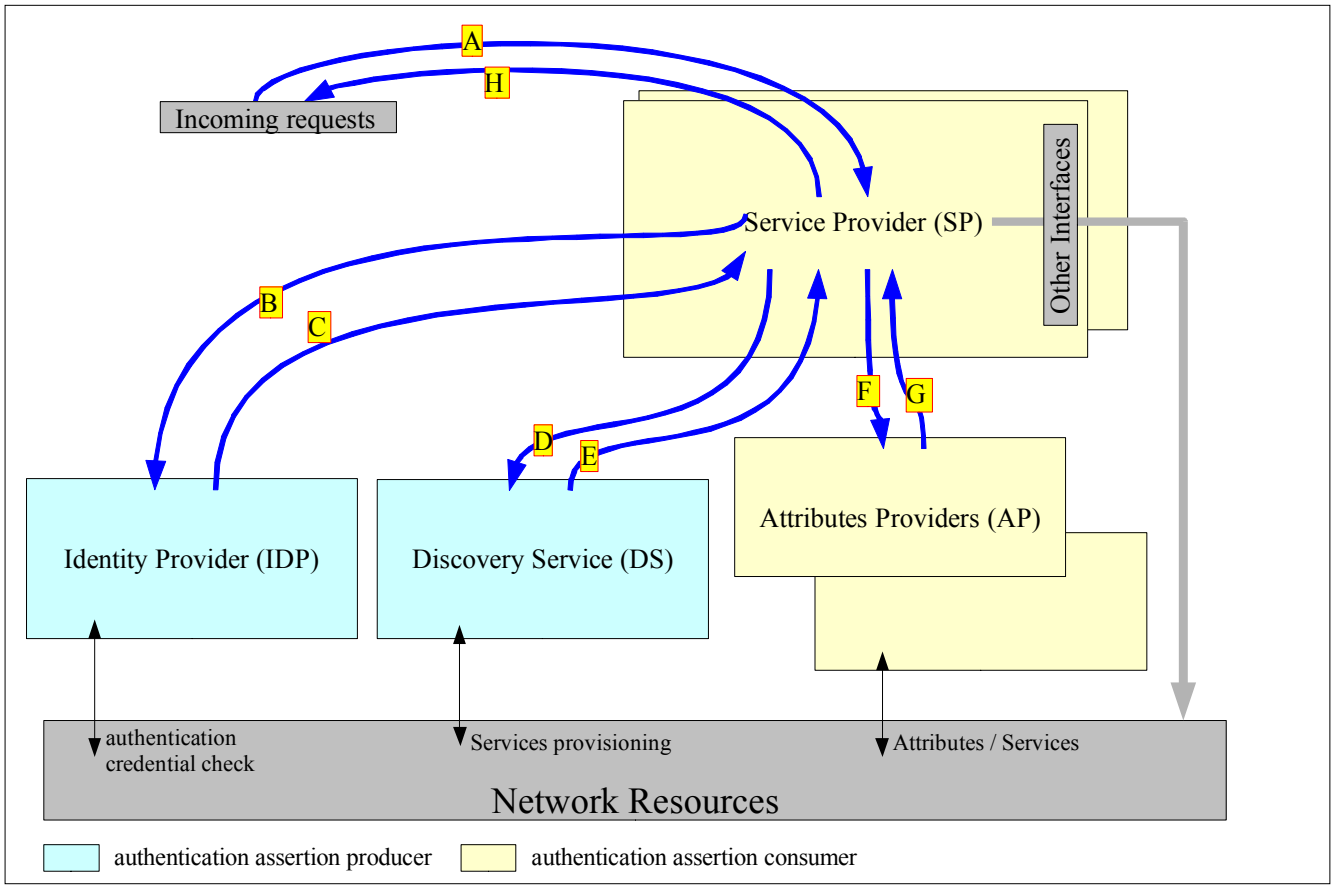

Figure 2: High Level Flow

- **A** - A Principal ("User/Equipment") initiates a request.
- **B** - The Application, at a SP, checks the Principal's authentication status with the Identity provider.
- **C** – The Identity provider responds to the request with an authentication assertion describing the Principal's authentication status, and optionally with the bootstrap information necessary to access the Principal's Discovery Service. Note that the IdP issues authentication assertions as well as handles the authentication context which identifies the strength and other parameters related to the authentication event.

  NOTE: When no valid SSO context for the Principal at the SP is available, the Principal needs to be authenticated at the IdP so that a valid SSO session can be established.. The specific authentication mechanism on which an authentication assertion is based is not part of Liberty specifications and it is usually delegated to a subpart (e.g., RADIUS IP/MSISDN or LDAP Login/Password check).
- **D** – The Service Provider (in the role of a WSC) uses the bootstrap information from step C to query the Principal's discovery service for a specific Attribute Provider for that Principal.

- **E** – The Discovery Service returns an authorization assertion which can be used by the SP to access the Attribute Provider.
- **F** - The Service Provider requests attributes, or actions on attributes from the Principal's attribute Provider. .
- **G** - The Attribute Provider returns the requested information,

(There may be an additional step – not shown in the figure - when the Principal is queried for consent to release attribute information.)

- **H** – The SP responds to the Principal's request.

In order to highlight the ID-WSF architecture and show where and how the major components of the architecture are activated, we will use three simple scenarios:

1. A single CoT, where a user is buying a ring tone from his mobile phone.
2. An interaction between two CoTs, that illustrates how one might build convergence between fixed and mobile services, with a user listening to his mobile voicemail from his fixed-line phone.
3. A shared CoT, where users belonging to multiple operators use a common webmail/portal interface from either their mobile phones or Internet/DSL connections.

These three scenarios are representative of the three main classes of typical requirements for telecoms operators and have enough complexity to show how the major elements of Liberty ID-WSF can be activated.

Note: All these flow make the assumption that following pre-requirements are fulfilled:

- A business agreement exists between an Identity Provider, Service Provider and Attribute Provider.
- A federation has already occurred between the Identity Provider, Service Provider and the Attribute providers

5.4.1 Single Circle of Trust

In this case the service provider is part of the operator CoT, which means that the service provider accepts the operator IdP as being its authentication authority. The fact that the service provider sits within the operator domain or is outsourced to an external partner does not change anything in the flow. The Liberty architecture makes the assumption that the IdP and the service providers, while belonging to the same CoT, need not belong to the same security domain, in order to allow each actor to structure its business and security environment as it sees fit.

The Ringtone Service Provider, Messaging Attribute Provider and Payment Attribute Provider entities in the flows below are used for illustrative purposes and are not specified by OWSER.

User flow:

- browses to his phone operator's portal and click on "Ringtone services"
- selects a ring tone for purchase and clicks on "Buy Now".
- receives a request for consent from his operator for payment.
- receives the ringtone through an SMS/MMS message

Technical flow:

(a) User starts browsing the Ringtone-SP (service provider) anonymously (i.e., he does not log in).

(b) When he clicks on "Buy Now", the Ringtone-SP redirects the user to the IdP for authentication.

(c) The Identity Provider authenticates the user (e.g., by checking the user's IP address at a RADIUS server).

(d) The IdP returns, via a redirection at the user's browser, an authentication assertion verifying his authenticated status and bootstrap information enabling the Ringtone-SP to invoke the user's Discovery Service, to the Ringtone-SP.

(e) The Ringtone-SP queries the DS (discovery service) for the user's ID-WSF enabled Payment Service (attribute provider), and receives the information needed to interact with that Payment Service

(f) The Ringtone-SP sends a Web Service request to the user's ID-WSF enabled Payment Service to receive payment for the ringtone.

(g) In this case payment requires the user's consent, so the user's ID-WSF enabled Payment Service returns a "MUST-INTERACT" SOAP Fault, the details of which contain a URL where the user's browser should be redirected, to the Ringtone-SP.

(h) The Ringtone-SP returns an HTTP redirect response to redirect the the user's browser to his ID-WSF enabled Payment Service for consent (using the URL obtained in (g)).

(i) The user's ID-WSF enabled Payment Service negotiates consent with the user using HTTP request/response protocols.

(j) The Principal's ID-WSF enabled Payment Service returns an HTTP redirect response to redirect the user's browser back to theRingtone-SP.

(k) The Ringtone-SP sends (again) a Web Service request to the user's ID-WSF enabled Payment Service to receive payment for the ringtone.

(l) The user's ID-WSF enabled Payment Service accepts the payment request from Ringtone-SP and charges the user's account (this invocation of the Payment-AP succeeds because user consent was obtained in (i) above)..

(m) The user's ID-WSF enabled Payment Service returns the payment status to Ringtone-SP.(

(p) The Ringtone-SP returns the ringtone and payment status to the user.

Note: Obviously exchanges can vary significantly depending on the deployment options. For example, the Ringtone application could discover, via a single request, both the Principal's Payment and the Messaging services, or the ringtone application could be run by an entity trusted by the Principal, in which case it could directly handle the consent for payment on behalf on the Principal

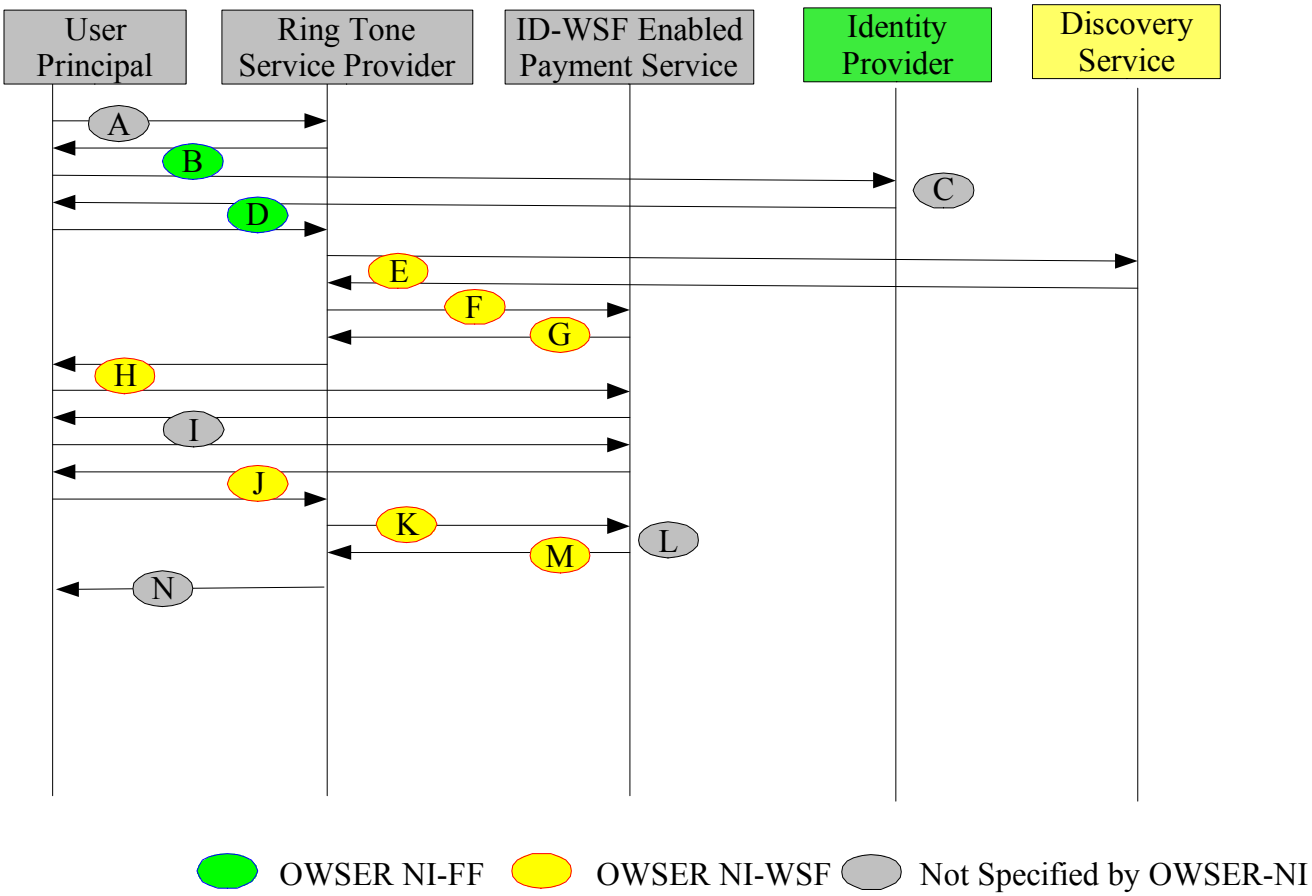

Figure 3: Message Flows within a single CoT

5.4.2 Interconnected Circles of Trust

Seamless interconnection has proven to be a key element in building global business. Two extremely successfully examples are:

- Banking: The ability to retrieve money from your bank account from any ATM interconnected to the global banking network.
- GSM roaming:, The ability to make/receive calls anywhere in the world owing to interconnection agreements between your home and visited networks.

Within today Telecoms business environment, interconnection between CoTs can be used for driving convergence of: fixed phone, Internet, Mobile, TV, Etc. or to interconnect two countries operators in a roaming context. More generally interconnection of CoTs is needed each time you want/need to allow users authenticated within an alien CoT to use one or more of your services such as the case of roaming where you might want a roaming user to consume services from a local CoT while not having a permanent identity in the visited CoT.

Interconnection between two (or more) CoTs introduces the concept of the Proxy IdP bridging two circles of trust. In this case, the user logs into the internet and then needs access to mobile services. The example shows how a user could listen to his mobile voicemail from his fixed-line Internet connection. As mobile and Internet subscription are independent, the user belongs to two independent CoTs and has a valid identity within both of them:

- In the mobile CoT the user is identified by MSISDN.

- In fixed CoT, the users access the Internet access via an ISP, and provides a username/password pair to establish an identity.

The Portal Service Provider, Messaging Attribute Provider and Web Voicemail Service Provider entities in the flows below are used for illustrative purposes and are not specified by OWSER.

User flow:

- connects to her ISP's Internet portal
- provides her Internet username/password

Technical flow:

(a) User browses to an Internet Portal-SP from his ISP's Internet Portal

(b) The Portal-SP redirects the user to the ISP (acting in the role of an IdP) for authentication.

(c) The ISP-IdP authenticates the user (e.g., by a login/password LDAP check to a subscriber database)

(d) Internet-IdP redirects authenticated user with authentication response toward Internet PortalSP.

(e) The Internet Portal-SP replies to the user (at this point user is authenticated within the ISP's CoT).

(f) User clicks on his mobile web Voicemail URL and is directed to Voicemail-SP within mobile CoT.

(g) Mobile Voicemail-SP needs to authenticate the user and redirects her to mobile-IdP.

(h) The Mobile-IdP cannot authenticate the user because she did not access the VoiceMail-SP via the mobile infrastructure (no MSISDN is available)

(i) The Mobile-IdP, acting as an SP in the CoT managed by IdP-ISP redirects the user to ISP-IdP for authentication (proxy authentication)

(j) ISP-IdP constructs an Authentication Assertion (no additional checks are necessary because the user has previously authenticated to the ISP-IdP.)

(k) The ISP-IdP redirects the user to the mobile-IdP and, in the process, returns the Authentication Assertion from (j) to the Mobile-IdP

(l) Mobile-IdP constructs an Authentication Assertion by mapping the user's identity at ISP-IdP (obtained from the Authentication assertion provided to it by SP-IdP in (k)) into the user's identity at Mobile IdP.

(m) Mobile-IdP redirects the authenticated user to the Voicemail-SP and, in the process, returns the Authentication Assertion from (k) as well as bootstrap information enabling the Voicemail-SP to invoke the user's Discovery Service, to the Voicemail-SP.

(n) Voicemail-SP queries the user's Discovery Service for the ID-WSF enabled Messaging Service and receives the information needed to interact with that Message AP

(o) Voicemail-SP requests and receives the user's voicemail messages from the user's ID-WSF enabled Messaging Service

(p)Voicemail-SP provides Mobile Voice Messages to the user

Note:

1. *Interconnection of CoTs is not limited to two CoTs. In fact there are no l hard limits on the number of interconnected CoTs. The only requirement for CoTs interconnection is to trust ,from a business agreement point of view, the authentication provided by an alien CoT for user asking a service within your own CoT.*

2. *Steps (i-k) is where the proxy id is established between the two circles of trust.*

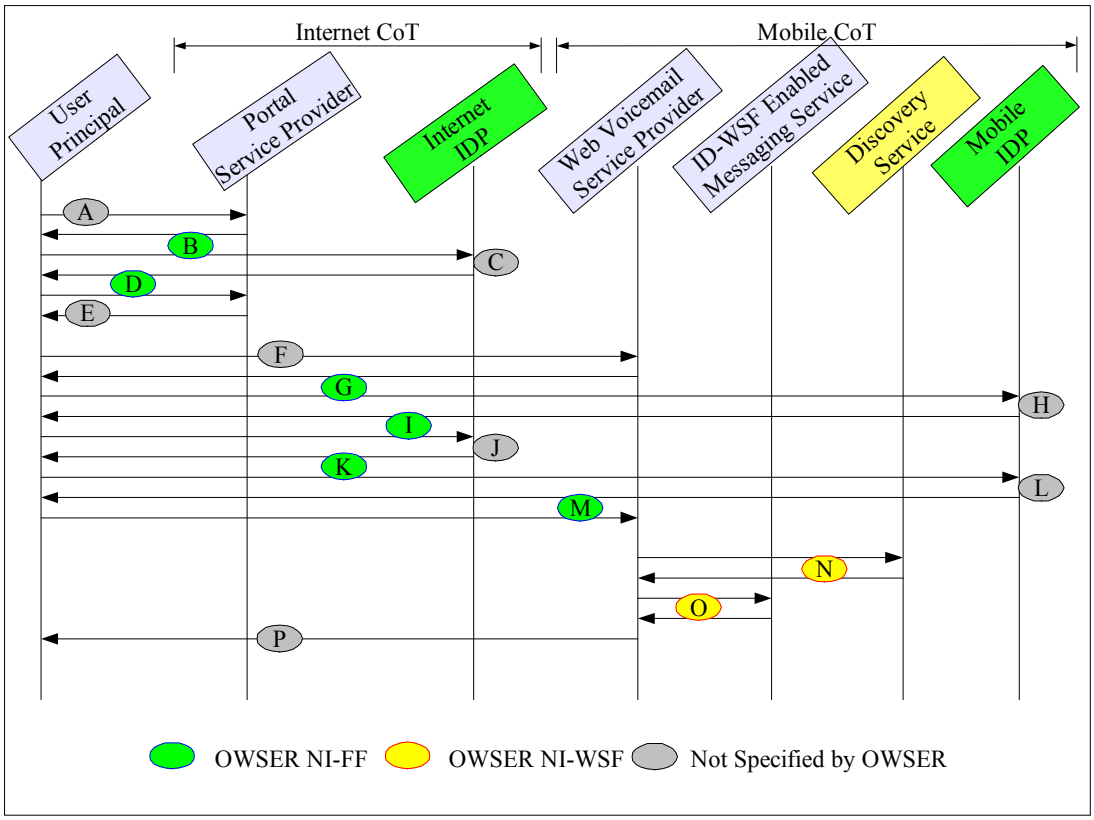

Figure 4: Interconnection between two CoTs

5.4.3 Shared Circle of Trust

This scenario is an extension of CoT interconnection scenario, in which a CoT is established to handle shared services that will be consumed by users from other CoTs. As in the interconnected CoTs scenario, this scenario utilizes proxy authentication, In the shared CoTs scenario not only does an SP (indirectly via IdP proxies) rely on Authentication Assertions generated in a "foreign" CoT, but also we expect to rely on someone else's attributes provider to handle full service to customers. Typically services like payment, charging, geolocation, personal profile, etc. remain attached to origin user's CoT, while some others like mobile portal, shopping, game, etc. will be hosted within the shared CoT. A typical use case for this would be to have a common pan European mobile portal infrastructure with attached services shared in between many country operators from a same mother company.

The example shows how a user could use a mobile webmail service implemented at a global European level to send an MMS from his mobile phone utilising his account at a "regional" or "country" operator.

The Mobile Webmail Service Provider, Messaging Service , Contact Book Attribute Provider and Payment Service entitles in the flows below are used for illustrative purposes and are not specified by OWSER.

User flow

- takes a picture with his phone.
- Invokes the mobile webmail browser application.
- logs onto global shared webmail service using SSO (user transparent)
- Selects a recipient address from his address book (eventually stored at country level).
- chooses a picture from his phone memory
- Gives consent for payment and sends mail (see illustration for a possible mobile consent+send GUI scenario).

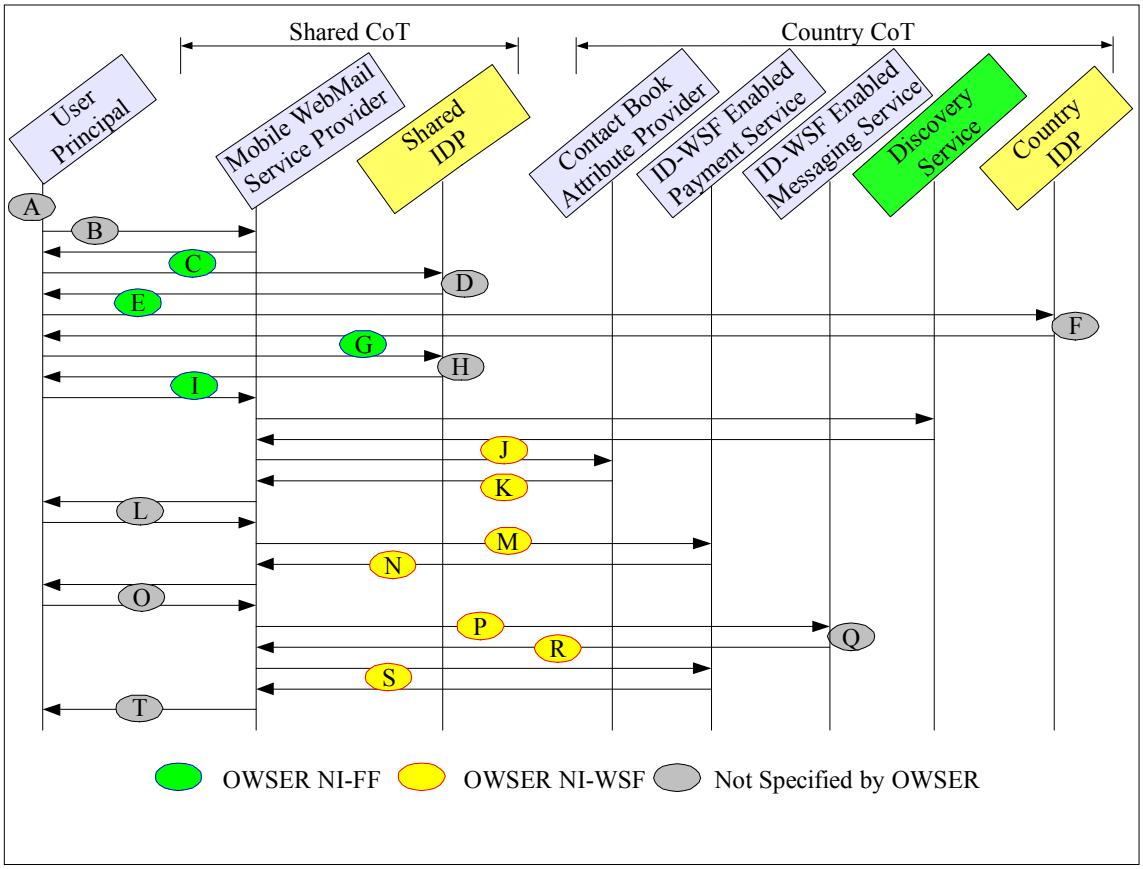

Figure 5: Shared CoT

Technical flow:

(a) Picture was taken and is stored on the phone.

(b) User connects from a pre-provision URL on shared Webmail-SP.

(c) Webmail-SP redirects user to the shared-IdP for authentication.

(d) Shared-IdP cannot authenticate the user (no way to check the user MSISDN).

(e) Shared-IdP redirects the user to country-IdP for proxy authentication (IdP discovery could use e.g. IP address ranges for such a discovery)

(f) County-IdP constructs an Authentication Assertion (no additional checks are needed because the user has previously authenticated when he connected to the country mobile network .e.g. via a check of IP/MSISDN at a Radius Server).

(g) Country-IdP redirects the authenticated user to the shared-IdP and, in the process, returns the Authentication Assertion from (f) as well as bootstrap information required to invoke the user's country Discovery Service, to the Shared-IdP.

(h) Shared-IdP constructs an Authentication Assertion by mapping the user's identity at country-IdP (obtained from the Authentication assertion provided to it by Country-IdP in flow (g)) into the user's identity at Shared-IdP.

(i) Shared-IdP redirects the authenticated user to the Webmail-SP and, in the process, returns the Authentication Assertion from (h) as well as the bootstrap information enabling the Webmail-SP to invoke the user's Discovery Service (obtained during proxy authentication in flow g) , to the Webmail-SP

(j) Shared webmail-SP queries the user's country-DS and requests the user's ContactBook-AP, the users' Messaging-AP and the user's Charging-AP. For each requested Attribute Provider, Country-DS returns the information needed by WebMail –SP to invoke that AP

(i) Shared Webmail-SP retrieves a list of potential MMS recipients from the user's ContactBook-SP.

(l) Shared Webmail-SP prompts the user to select a recipient and prepares an MMS message to send to that recipient.

(m) Shared Webmail-SP sends a request for payment to the user's Country ID-WSF enabled Payment Service.

(n) User's Country ID-WSF enabled Payment Service returns a MUST-INTERACT response to Webmail-SP indicating that the user must provide his consent in order for the payment request can be honored

(o) User gives provides consent out-of-band by sending email (cf: illustration 3 for user flow).

(p) Mobile Webmail-SP sends a request to the User's Messaging-AP requesting that the MMS be sent to the recipient.

(q) User's ID-WSF Enabled Messaging Service uploads the MMS and sends it to the recipient.

(r) User's responds to Webmail-SP indicating that the message has been sent

(s) Mobile Webmail-SP sends a payment request to the user's Country ID-WSF enabled Payment Service (this charging is now possible because user gave his consent in previous step).

(t) Webmail-SP returns final status to user.

Note:

- In this scenario, the user never authenticates directly at the shared CoT level, though this is possible using the same mechanism described in previous transversal CoTs example. One scenario for doing so would have the user authenticate in proxy mode when coming from a mobile and to authenticate directly at the shared level when coming from Internet.
- In order not to overload the example scenario, payment has been kept very simple and does not use money pre-reservation.
- It is part of the business process how to decide whether consent is required from the user for the purchase in (f).

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-AD-OWSER_NI-V1_0-20060328-A	28 Mar 2006	Version 1.0 Approved TP ref erence OMA-TP-2006-0097-OWSER_NI_v1_0_for_final_approval