MWS Identity Management Requirements

OMA-RD_MWS_NI-V1_0-20031120-A

Open Mobile Alliance

OMA-RD_MWS_NI-V1_0-20031120-A

This document is considered confidential and may not be disclosed in any manner to any non-member of the Open Mobile Alliance™, unless there has been prior explicit Board approval.

This document is a work in process and is not an approved Open Mobile Alliance™ specification. This document is subject to revision or removal without notice. No part of this document may be used to claim conformance or interoperability with the Open Mobile Alliance specifications.

The Open Mobile Alliance™ assumes no responsibility for errors or omissions in this document. In no event shall the Open Mobile Alliance be liable for any special, indirect or consequential damages or any damages whatsoever arising out of or in connection with the use of this information.

This document is not an Open Mobile Alliance™ specification, is not endorsed by the Open Mobile Alliance and is informative only. This document is subject to revision or removal without notice. No part of this document may be used to claim conformance or interoperability with the Open Mobile Alliance specifications.

Open Mobile Alliance™ members have agreed to use reasonable endeavors to disclose in a timely manner to the Open Mobile Alliance the existence of all intellectual property rights (IPR's) essential to the present document. However, the members do not have an obligation to conduct IPR searches. The information received by the members is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at http://www.openmobilealliance.org/ipr.html. Essential IPR is available for license on the basis set out in the schedule to the Open Mobile Alliance Application Form.

No representations or warranties (whether express or implied) are made by the Open Mobile Alliance™ or any Open Mobile Alliance member or its affiliates regarding any of the IPR's represented on this "OMA IPR Declarations" list, including, but not limited to the accuracy, completeness, validity or relevance of the information or whether or not such rights are essential or non-essential.

This document is available online in PDF format at http://www.openmobilealliance.org/.

Known problems associated with this document are published at http://www.openmobilealliance.org/.

Comments regarding this document can be submitted to the Open Mobile Alliance™ in the manner published at http://www.openmobilealliance.org/documents.html.

Contents

1. Scope (Informative)

This document lists the requirements generated by the OMA Mobile Web Services (MWS) Working Group in the area of Identity Management.

2. References

2.1 Normative References

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

2.2 Informative References

[UML]	*'UML Distilled'*, 2nd Edition, by Martin Fowler, Addison-Wesley, 2000
[USECASES]	*'Use Cases'*, by Daryl Kulak and Eamonn Guiney, Addison-Wesley, 2000
[Liberty1.1-Glossary]	"Liberty Architecture Glossary: Version 1.1," January 2003. 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.

3.2 Definitions

Account	A formal business agreement for providing regular dealings and services between a Principal and Providers. (Source: [Liberty1.1-Glossary])
Address	For the purposes of this discussion, address refers to a URI.
Affiliation	A set of Service Providers that have a business relationship amongst them, so that each service provider may be able to obtain benefits of being part of the affiliation.
Attribute	A distinct characteristic of a Principal. A Principal’s attributes are said to describe it.
Attribute Broker	An entity that receives attribute requests and aggregates attribute responses on behalf of multiple attribute providers. The attribute broker and attribute provider adhere to mutually established policies, and permissions of the Principal.
Attribute Class	A predefined set of attributes.
Attribute Provider	An entity that provides attribute information. It is a Web Service that hosts Principal’s attributes.
Authentication Assertion	Conveying information about a successful act of authentication that took place for a Principal.
Business relationship	This is a formal agreement between two entities (such as between two Providers), and may include an establishment of trust between the entities as well as a description of liability aspects between them.
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.
De-federate	To eliminate linkage between Principal’s identities at an Identity Provider and a Service Provider.
Delegation	Permission necessary to authorize an entity to act on behalf of a Principal.
Direct Trust	It is when a relying party accepts as true all (or some subset of) the claims in the token sent by the requestor. (usage of token needs clarification)
Discovery Service	An identity service that allows requestors to discover resources.
Federate	To link or bind two or more entities together.
Identity	The essence of an entity and often described by its characteristics. (Source: [Liberty1.1-Glossary])
Identity Provider	An entity that creates, maintains and manages identity information for Principals and provides an authentication assertion to other service providers within a circle of trust.
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 user, a group of individuals, a corporation, service enablers/applications, system entities and other legal entities. (Source: [Liberty1.1-Glossary])
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.
Single Sign-On (SSO)	It is an optimization of the authentication sequence to ease the burden of repeating actions placed on the Principal. It is the ability to use proof of an existing authentication

session with Provider A to create a new authentication session with Provider B.

State Information that is created and stored at the time of identity federation.

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]

Usage Directive A directive describing the allowable usage of released attributes by the recipient.

3.3 Abbreviations

AP	Attribute Provider
IdP	Identity Provider
SP	Service Provider
SSO	Single Sign On

4. Introduction (Informative)

This document lists the requirements generated by the OMA Mobile Web Services (MWS) Working Group in the area of Identity Management.

5. Use Cases (Informative)

The following use cases were created by OMA's Mobile Web Services (MWS) Working Group in the area of Identity Management. These use cases were used to derive the Identity Management requirements.

5.1 Single Sign On

5.1.1 Introduction

The purpose of this use case is to illustrate how single sign on technology can simplify a business transaction from a terminal user's point of view. Typically, when using mobile services today, a user needs to authenticate by logging in using a combination of username and password. While this works for personal computers with full keyboard, it is often tedious for mobile terminals with numeric keypads. Single sign on makes use of mobile services easier by reducing the number of keystrokes required to use a service.

5.1.2 Basic Use Case

5.1.2.1 Short Description

In this use case, user uses his mobile terminal to access a movie ticket service, selects a movie he wishes to see, downloads an electronic ticket to his terminal, and pays for it. This electronic movie ticket may be e.g. a barcode in an MMS message that can be printed or scanned or an electronic ticket that can be verified via bluetooth.

The main point of this use case is single sign on (SSO) feature. User does not need to authenticate himself to the service provider, because is using an external identity provider, which provides his credentials to the service provider. Thus less input (i.e. key strokes) is required from the user to use the service.

Additionally, single sign on service may host profile information on user's favourite services such as payment service, so required user input can be further simplified.

In this use case, it is assumed that movie ticket service provider is a service that requires users to have an account and authenticate themselves to provide customized service.

5.1.2.2 Actors

- User – end user using a mobile device
- Identity provider –operator or service provider offering single sign on service
- Movie ticket service provider. Service provider providing downloadable movie tickets.
- Payment service provider - an entity providing a payment service credit card

5.1.2.3 Pre-conditions

- User has created an account with an identity provider
- User has an account with the movie ticket service provider
- Service provider has made necessary arrangements (business and technical) with identity provider to use single sign on provided by identity provider
- User has activated his/her account with movie ticket service provider to use single sign on based on his account with the identity provider
- Identity provider has authenticated user.

5.1.2.4 Post-conditions

- A ticket has been downloaded to user's terminal.
- A billing record has been placed on payment service records

5.1.2.5 Normal Flow

- User accesses movie ticket service provider's service using the browser on his terminal
- User browses available movies, and finds a movie he is interested in
- User selects theater and time that are suitable, and indicates to movie ticket service provider that he wishes to purchase a ticket
- Movie ticket service provider seamlessly authenticates user using identity provider.
- User selects a payment method
- User enters necessary payment information (e.g. credit card number and expiration date)
- Movie ticket service provider asks user to confirm purchase
- A movie ticket is downloaded to user's terminal

5.1.2.6 Alternative Flow

An identity provider may also host a repository of a user's favourite services, such as payment service. In this case, movie ticket service provider and identity provider can directly negotiate payment service provider, and transaction is further simplified from the user's point of view.

- User accesses movie ticket service provider's service using the browser on his terminal
- User browses available movies, and finds a movie he is interested in
- User selects theater and time that are suitable, and indicates to movie ticket service provider that he wishes to purchase a ticket
- User is seamlessly authenticated Movie ticket service provider seamlessly authenticates user using identity provider
- Ticket provider requests user's payment method/information from identity provider which is also acting as profile provider
- Movie ticket service provider asks user to confirm purchase
- A movie ticket is downloaded to user's terminal

5.1.2.7 Operational and Quality of Experience Requirements

- **Privacy protection.** Single sign on technology must protect user's privacy, and not reveal any more personal data to movie ticket service provider than is needed to provide the service, and user has given his consent to. For example, one of the primary requirements is that two different service providers should not be able to collude and determine that it is the same user that visited their sites. The name identifier associated with the same user at two different service providers should be different.
- **Allow use from multiple devices**. Single sign should not be dependent on any cookies – i.e. it SSO to a service should work even though using a new mobile device for the first time.
- **Performance.** Single sign on must have high enough performance so that it does not deteriorate user experience.
- **Ease of initial setup.** Initial setup of the single signon mechanism and the user profile info and privacy settings must be simple enough that users will make use of these capabilities.

5.1.3 Technical Analysis

Ticket purchase using single sign on type of authentication is divided into five operations. Each of the operations illustrates a potentially reusable functionality that is logically separate.

- ***Content selection*** allows user to browse available content (content name, price, size etc) and make a selection.
- **User authentication** using single sign on technology.
- ***Payment method selection***. Allows user to select a preferred payment method from a list of methods that the movie ticket service provider accepts.
- With ***Content download*** movie ticket service provider can reliably deliver content to a terminal.
- ***Payment service***. Technology movie ticket service provider needs in order to receive payments for the content.

5.1.3.1 Refined use case

Java download is divided into five operations. Each of the operations illustrates a potentially reusable functionality that is logically separate.

- ***Content selection*** allows user to browse available content (content name, price, size etc) and make a selection.
- ***User authentication*** allows service provider to authenticate user.
- ***Payment method selection***. Allows user to select a preferred payment method from a list of methods that the movie ticket service provider accepts.
- With ***Content download*** movie ticket service provider can reliably deliver content to a terminal.
- ***Payment service***. Technology movie ticket service provider needs in order to receive payments for the content.

5.1.3.1.1 Content Selection

Function	This building block allows user to browse and select content that he/she wishes to download.
Input dataset	-
Output dataset	A unique pointer to content (e.g. URI)
Pre-condition	User has connection to movie ticket service provider
Post-condition	Terminal knows a unique pointer (e.g. URI) to the content the user wishes to download

5.1.3.1.2 User Authentication

Function	User identification based on his credentials
Input dataset	User credentials in the form of e.g. user name & password, X.509 certificate
Output dataset	User identity
Pre-condition	A trust relationship exists between user and identity provider
Post-condition	Service Provider has knowledge of user identity.

5.1.3.1.3 Payment method selection

Function	User selects a payment method from a list of possible payment methods.
Input dataset	List of possible payment methods
Output dataset	Payment method and details for billing
Pre-condition	User has connection to movie ticket service provider, and movie ticket service provider has authenticated user/terminal. User and movie ticket service provider have negotiated list of possible payment methods.
Post-condition	Movie ticket service provider has knowledge of the payment method user prefers, and required information to bill the user (e.g. account number).

5.1.3.1.4 Reliable Content download

Function	This operation provides a reliable file download from movie ticket service provider to mobile terminal
Input dataset	A pointer to the content user wishes to download.
Output dataset	-
Pre-condition	Existing connection from terminal to provider Terminal knows the pointer to the content user wishes to download
Post-condition	Content is downloaded from movie ticket service provider to terminal. Terminal and movie ticket service provider reliably share the status whether the download was successful.

5.1.3.1.5 Payment Service

Function	This technology building block enables a movie ticket service provider to bill the user via operator billing system or an external payment service provider.
Input dataset	A description of the delivered service and the amount to be billed, User billing information
Output dataset	Whether billing was successful Necessary references for book keeping
Pre-condition	User has indicated payment method approved amount to be charged
Post-condition	A billing record has been placed on the payment provider’s billing system.

The following operations have been defined in UC-4 Java Download:

- Content selection
- Payment method selection.

- Content download
- Payment service.

5.1.3.2 Gap and Overlap Analysis

Single sign on plays a crucial role for mobile services take-off. OMA currently does not have a single sign on technology. In the market place there are several single sign on vendors – most of which are not based on open standards, and thus should not be endorsed by OMA.

Of the existing single sign on technologies the following are both open and satisfy the requirements for privacy

- Liberty Alliance project specification v1.0 (www.projectliberty.org//)

5.2 Federation, Defederation and Single Logout

5.2.1 Introduction

The benefits of Single Sign On (SSO) were highlighted in Section 5.1. With SSO, a user authenticated at an Identity Provider (IdP) is able to obtain seamless access to service providers (SP) that the user has federated his account with. This decreases the need for repeated user authentication at various sites, thereby enhancing the overall user experience.

This use case describes various other aspects surrounding SSO. Specifically, this use case discusses:

- federation of a user's account at an IdP with that at an SP
- de-federation of an existing federation
- single logout (SLO) of a user

5.2.2 Basic Use Case

5.2.2.1 Short Description

Consider the case where a user has an account with an Operator (acting as an Identity Provider) and the user is currently authenticated with the Operator. The Operator has entered into business agreements with several service providers, so that the user's account at the Operator may potentially be linked (or federated) with the user's account at the service provider, if the user so desires. The Operator and the set of service providers that the Operator has entered into an agreement with, are said to belong to the same authentication domain. One of the service providers in the same authentication domain as the Operator is a movie ticket service provider that requires user authentication prior to the user being able to browse (portions of) the site.

Federation of user accounts

When the user visits the movie ticket service provider site, the movie ticket service provider determines that the user has an account with the Operator. The movie ticket service provider prompts the user whether the user would like to simplify his authentication process by federating his account at the movie ticket service provider with his account at the Operator. Since the mobile user would like to obtain the benefits of Single Sign On (SSO), the user consents to such federation. The movie ticket service provider contacts the Operator requesting that the user's account at the movie ticket service provider be federated with the user's account at the Operator. The movie ticket service provider includes an optional name identifier (say Bob-123) that it would like the Operator to refer to the user as, when the Operator subsequently contacts the movie ticket service provider about the user. Note that the user may be known by a different identity (say, BostonBob) to the Operator. Upon receiving the federation request from the movie ticket service provider, the Operator prompts the user to verify that the user would like to federate his account at the Operator with his account at the movie ticket service provider. After obtaining the user's consent, the Operator federates the user accounts of the user. The Operator then sends a federation response message to the movie ticket service provider indicating successful federation. Had the movie ticket service provider not included the optional name identifier (Bob-123) for the user in the federation request message, the Operator would have generated a random name identifier (say, abxv) that it conveys in the federation response message, so that the user is always referred to as abxv when the Operator is communicating with the movie ticket service provider. The user's account at the Operator has now been federated with the user's account at the movie ticket service provider.

When the same user subsequently federates his account at the Operator with his account at another service provider, the name identifier user to refer to the user is different. The advantage of this is that different service providers will not be able to collude, and determine the usage patterns of the user. This protects the privacy of the user.

De-Federation of federated accounts

After the user has federated his account at the Operator with his account at the movie ticket service provider, at some future point in time, the user decides to de-federate these accounts. In other words, the user does not want to link these two accounts any more to use the benefits of SSO. This could be either because the user wishes to explicitly authenticate himself to the movie ticket service provider, or because the movie ticket service provider has left the authentication domain of the Operator thereby necessitating de-federation. The former case is termed user-initiated de-federation, while the latter case is termed network-initiated de-federation.

With user-initiated de-federation, the user is currently authenticated with the Operator. The user then explicitly requests the Operator to de-federate his account with the movie ticket service provider. The Operator sends a de-federate request message to the movie ticket service provider, requesting that the movie ticket service provider de-federate the user's account at the movie ticket service provider with the user's account at the Operator. The movie ticket service provider completes the de-federation and acknowledges this in a response to the Operator. The Operator then completes the de-federation and sends an acknowledgement to the user confirming successful de-federation of the user's account at the Operator with the user's account at the movie ticket service provider.

With network-initiated de-federation, since the Operator and the movie ticket service provider are no longer in the same authentication domain (having terminated their business agreement), each of them independently de-federates the user's account and independently notifies the user of such de-federation.

Single Logout (SLO) of federated accounts

The user is currently authenticated at the Operator, and the user has also federated his account at the Operator with his account at the movie ticket service provider. The user may or may not be authenticated at the movie ticket service provider, either directly or by means of the movie ticket service provider having received an authentication assertion from the Operator. The user then sends a single logout (SLO) request message to the Operator, requesting that the user be logged out at the Operator and at the movie ticket service provider. Note that the user may send a more generic single logout request message requesting that the user be logged out at the Operator and at all service providers that the user has federated his account with. The Operator sends a request message to the movie ticket service provider requesting that the user be logged out. If the user is currently authenticated at the movie ticket service provider, the movie ticket service provider logs the user out, and sends a response to the Operator confirming such logout. The Operator also logs the user out at the Operator. The Operator then sends a response message to the user confirming successful logout at the Operator and at the movie ticket service provider.

5.2.2.2 Actors

- User – end user using a mobile device
- Operator – Operator acting as Identity Provider (IdP)
- Movie ticket service provider – service provider providing downloadable movie tickets to authorized users.

5.2.2.3 Pre-conditions

- User has an account with the Operator.

- User has an account with the movie ticket service provider.
- User is currently authenticated at the Operator.

In addition to this, additional pre-conditions for de-federation and Single Logout (SLO) are:

- User's account at the Operator is federated with the user's account at the movie ticket service provider.

5.2.2.4 Post-conditions

The post-condition for federation is :

- User's account at the Operator is federated with the user's account at the movie ticket service provider. This ensures that the user can seamlessly access the movie ticket service provider site.

The post-condition for de-federation is:

- The user's account at the Operator has been de-federated with the user's account at the movie ticket service provider. The user no longer has seamless access to the movie ticket service provider's site, and has to explicitly authenticate with the movie ticket service provider in order to access the site.

The post-condition for Single Logout (SLO) of a federated user is:

- User has been successfully logged out of the Operator and the movie ticket service provider sites.

5.2.2.5 Normal Flow

Federation of user accounts

The normal flow for federation of the user account at the Operator with the user account at the movie ticket service provider is as follows:

1. User browses the movie ticket service provider site, which requires that the user be authenticated prior to the user being able to browse (restricted portions of) the site.
2. Since the movie ticket service provider is in the same authentication domain as the Operator, it determines that the user has an account with the Operator. How this is done is the "Introduction" problem, and there are a few ways of achieving this.
3. The movie ticket service provider prompts the user whether he would like to federate his account at the movie ticket service provider with his account at the Operator, so that the user may be able to benefit from SSO.
4. The user responds with a confirmation that he would like to federate his accounts.
5. The movie ticket service provider sends a federation request to the Operator requesting that the user's account at the movie ticket service provider be federated with the user's account at the Operator. The movie ticket service provider may optionally include a name identifier that identifies the user at the movie ticket service provider.
6. Since the user is already authenticated at the Operator, the Operator prompts the user whether he would like to federate his account at the Operator with his account at the movie ticket service provider.
7. After obtaining a positive response from the user, the Operator federates the user accounts, and sends a federation response message to the movie ticket service provider confirming federation.
8. The movie ticket service provider completes federation of the user's accounts at its site, and sends a message to the user confirming the federation of the user's account at the Operator with the user's account at the movie ticket service provider.

User Initiated de-federation of federated accounts

The normal flow for user-initiated de-federation of a user account at the Operator that is federated with a user account at the movie ticket service provider is as follows:

1. Mobile user that is currently authenticated at the Operator requests the Operator to de-federate his account at the Operator with his account at the movie ticket service provider.

2. Operator sends a de-federate request message to the movie ticket service provider, requesting de-federation of the user’s account at the Operator with the user’s account at the movie ticket service provider.

3. After completing such de-federation, the movie ticket service provider responds to the Operator confirming the de-federation.

4. The Operator then de-federates the accounts at his site, and sends a confirmation back to the user, confirming that the user’s account at the Operator has been de-federated with the user’s account at the movie ticket service provider.

Network Initiated de-federation of federated accounts

The normal flow for network-initiated de-federation of a user account at the Operator that is federated with a user account at the movie ticket service provider is as follows. This is likely triggered because the movie ticket service provider has terminated his business agreement with the Operator, and hence is no longer in the same authentication domain as the Operator:

1. Movie ticket service provider sends a notification to the user indicating that his account at the Operator has been de-federated with his account at the movie ticket service provider.

2. Operator sends a notification to the user indicating that his account at the Operator has been de-federated with his account at the movie ticket service provider.

Single Logout (SLO) of federated user accounts

The normal flow for single logout (SLO) of federated user accounts is as follows:

1. User that is currently authenticated at the Operator requests to the Operator that the user be logged out of the Operator and movie ticket service provider sites. Note that the user may or may not be currently authenticated at the movie ticket service provider site.

2. The Operator logs the user out of the Operator site.

3. Operator sends a request to the movie ticket service provider, requesting that the user be logged out of the site.

4. After logging the user out (if the user is currently logged in), the movie ticket service provider confirms the logout in a response to the Operator.

5. The Operator sends a confirmation message to the user, confirming that the user has been successfully logged out of the Operator and the movie ticket service provider site.

5.3 Single Sign On with Authentication Context

5.3.1 Introduction

The benefits of Single Sign On (SSO) were highlighted in Section 5.1. With SSO, a user authenticated at an Identity Provider (IdP) is able to obtain seamless access to service providers (SP) that the user has federated his account with. This decreases the need for repeated user authentication at various sites, thereby enhancing the overall user experience.

In many cases, the service provider may not be content with any form of authentication that the IdP uses to authenticate the user, but may request a specific form of authentication to be used. The SP may also request that the IdP re-authenticate the user irrespective of whether the IdP previously authenticated the user or not. Such context surrounding the authentication of the user at the IdP is collectively referred to as the authentication context. Hence, authentication context captures such concepts as:

- Ability of an SP to request an IdP to authenticate the user using a certain class of authentication mechanisms.
- Ability of an SP to request an IdP to authenticate the user using a specific authentication mechanism.
- Ability of an SP to request an IdP to re-authenticate the user even if the user has been authenticated by the IdP.

Ability of an SP to request an IdP to re-authenticate the user if the user has been authenticated by the IdP before a certain time (i.e., aged authentication).

5.3.2 Basic Use Case

5.3.2.1 Short Description

Consider the case where a user's account at an Operator (acting as an Identity Provider) is federated with the user's account at a movie ticket service provider (acting as a service provider.) The user is currently authenticated at the Operator, and the Operator has used a username-password based mechanism to authenticate the user. The user decides to browse the movie ticket service provider site, and the site requires that the user be authenticated before the user can browse (restricted portions of) the site.

The movie ticket service provider requests an authentication assertion from the Operator, so that it may allow access to the user to browse its site. Certain forms of authentication (of the user by the Operator) are acceptable to the movie ticket service provider, one of which is a username-password based authentication. The movie ticket service provider includes an authentication context in the authentication request message, indicating the acceptable forms of authentication. In the Authentication response message that the Operator sends back to the movie ticket service provider, the Operator includes an authentication context, which captures the fact that the user was authenticated by the Operator by means of a username-password based mechanism.

Subsequently, when the user decides to purchase a movie ticket, the movie ticket service provider wishes to re-authenticate the user. The movie ticket service provider sends another authentication request message to the Operator. The authentication context in the authentication request message indicates that the movie ticket service provider would like the Operator to re-authenticate the user irrespective of whether the user was authenticated by the Operator in the past. Upon receiving the authentication request message with the authentication context in it, the Operator re-authenticates the mobile user. The Operator then sends an authentication assertion back to the movie ticket service provider, and includes an authentication context, which states that the user was re-authenticated by the Operator. The movie ticket service provider then permits the user to continue with the purchase of the movie ticket. Note that one of the advantages of the Operator re-authenticating the user instead of the movie ticket service provider authenticating the user, is that the user only needs to know/remember his username-password at the Operator (thereby simplifying the user's overall experience.)

5.3.2.2 Actors

- User – end user using a mobile device
- Operator – Operator acting as Identity Provider (IdP)
- Movie ticket service provider – service provider providing downloadable movie tickets to authorized users.

5.3.2.3 Pre-conditions

- User has an account with the Operator.
- User has an account with the movie ticket service provider.
- User's account at the Operator is federated with the user's account at the movie ticket service provider.
- User is currently authenticated at the Operator by means of a username-password mechanism.

5.3.2.4 Post-conditions

The post-condition for the first authentication request is :

1. Mobile user is allowed seamless access to the movie ticket service provider's site.

The post-condition for the second authentication request is:

2. Mobile user is allowed seamless access to continue with the purchase of the movie ticket at the movie ticket service provider's site.

5.3.2.5 Normal Flow

The normal flow is as follows:

1. User browses the movie ticket service provider site, which requires that the user be authenticated prior to the user being able to browse (restricted portions of) the site.
2. Movie ticket service provider sends an authentication request message to the Operator, requesting an authentication assertion for the user. An authentication context has been included in the authentication request message, wherein the movie ticket service provider specifies the acceptable forms of authentication (one of which is username-password).
3. Since the user has been authenticated by the Operator using a username-password based mechanism, the Operator sends an authentication assertion back to the movie ticket service provider. This authentication assertion includes an authentication context wherein the Operator states that the authentication mechanism used to authenticate the user was a username-password based mechanism.
4. Upon receiving the authentication assertion, the user is allowed seamless access to the movie ticket service provider's site.
5. After browsing the site for a while, the user decides to purchase a ticket from the site.
6. The movie ticket service provider requires the user to be re-authenticated prior to any ticket purchase. Hence, the movie ticket service provider sends another authentication request message to the Operator. An authentication context is included in this request, which states that the movie ticket service provider would like the Operator to re-authenticate the user, irrespective of whether the Operator had authenticated the user in the past.
7. Upon receiving the authentication request, the Operator prompts the user for authentication.
8. The user re-authenticates using his username-password at the Operator.
9. After successfully re-authenticating the user, the Operator sends an authentication assertion back to the movie ticket service provider. The authentication assertion contains an authentication context that states that the Operator has re-authenticated the user using a username-password based mechanism.
10. Upon receiving the authentication assertion with an acceptable authentication context, the movie ticket service provider lets the user continue with the purchase of the movie ticket.

5.4 Delegation of Authority to Federate Identities

5.4.1 Introduction

There are many scenarios where a user delegates his authority for federating the user's accounts, to an Identity Provider (IdP) so that the IdP may be able to federate the user's accounts on his behalf. The IdP does not require the user to authenticate at the time of federation, so that the user could be off-line when the IdP is federating on behalf of the user. Such scenarios are typically found in the enterprise or B2B area:

- Employees in an enterprise delegate their authority to the employer (Information Technology team) to federate their accounts on their behalf. Such delegation of authority typically happens as part of the employment contract. The advantage of federating the user’s account at the employer with that at other partner sites (e.g. 401(K), benefits etc.) of the employer, is that once the user has logged into the corporate network, he is allowed seamless access to his other sites (e.g. 401(K), benefits etc.) Subsequently, in order to provide seamless access to sites such as the 401(K) plan, benefits plan etc., the employer decides to federate the user’s account with the employer to the user’s account with the 401(K) plan site and the benefits plan site. In this scenario, the employer is acting as the IdP, while the 401(K) plan site and the benefits plan site are acting as the service provider.

- In a B2B scenario, a mega-portal connects suppliers to consumers. Each of the consumers has an account with the mega-portal, which is acting as the Identity Provider. At the time of account creation, the consumer delegates authority to the mega-portal to federate the consumer’s account at the mega-portal with the consumer’s account at each supplier that the mega-portal has a relationship with. Federating the consumer’s account at the mega-portal with that at the suppliers, allows the consumer to authenticate once with the mega-portal and obtain seamless access to the suppliers’s sites. With such delegation of authority, as suppliers keep changing, the consumer does not have to explicitly federate and de-federate his accounts, but the mega-portal handles this instead. This provides a seamless user experience to the consumer.

The purpose of presenting this use case to OMA is to illustrate the benefits of a user delegating authority for federation of the user’s accounts to his Identity Provider. Operators acting as IdPs can typically benefit from such a scenario.

5.4.2 Basic Use Case

5.4.2.1 Short Description

Consider the case where a mobile Operator offers a service so that a certain class of its subscribers (say, gold class customers) have free access to various network games provided by game providers that are partners of the Operator. The user may pay a higher monthly subscription fee in order to make use of this offering by the Operator. In order to provide the benefits of Single Sign On (SSO) to the user, it is useful to federate the user’s account at the Operator with his accounts at the various game providers. When this is done, the mobile user that is currently authenticated by the Operator would have seamless access to the games provided by each game provider. We saw the benefits of SSO in Section 5.1.

The purpose of this use case is to highlight the fact that it would be beneficial to the user if he does not have to explicitly federate his account at the Operator with his accounts at each game provider. Instead, the user could delegate such authority to the Operator, so that the Operator could federate the user’s accounts on behalf of the user. In order to do this, the user’s contract with the Operator for this gaming service gives the Operator authority to perform such federation on behalf of the user.

After a new subscriber joins such a plan, the Operator sends a federate request message to each game provider requesting that the user’s account at the Operator be federated with the user’s account at the game provider. The Operator is able to identify himself to the game provider by strong means (e.g. digital signatures), and vice versa. Such federation of the user’s accounts could happen when the user is not currently online, i.e., when the mobile user is not currently authenticated to the Operator.

When a new game provider enters into a partnership with the Operator and joins this program, the Operator needs to federate the accounts of each user in this program with an account at the new game provider. The Operator initiates a federate request (typically a bulk federate request, whereby multiple user accounts can be federated at the same time) to the game provider in order to federate the user account at the Operator with the user account at the game provider.

Similarly, when a game provider that is currently participating in the program decides to terminate its contract with the Operator and is no longer part of the program, the Operator needs to de-federate the accounts of the users with this game provider. The Operator sends a bulk de-federate request message to the game provider requesting that it de-federate the accounts of the listed users. After doing so, the game provider responds with an acknowledgement.

5.4.2.2 Actors

- User – end user using a mobile device
- Operator – Operator acting as Identity Provider (IdP)
- GameProvider1 – service provider providing game service to authorized users.
- GameProvider2 – service provider providing game service to authorized users.

5.4.2.3 Pre-conditions

- User has an account with the Operator.
- User has delegated authority to the Operator to federate the user's account at the Operator with game providers that the Operator has an agreement with.
- User is not currently authenticated with the Operator.

5.4.2.4 Post-conditions

The post-condition for federation of a new subscriber is :

- User's account at the Operator is federated with that at each game provider that the Operator has a partnership with, as part of this program. This ensures that the user can seamlessly access any game at any game provider site that is in partnership with the Operator.

The post-condition for bulk federation of all user accounts with a new game provider is:

- The accounts of all users in the program have been federated with that at the new game provider that joined the program. Each user in the program is allowed seamless access to the new game provider's site.

The post-condition for de-federation of a user's account with all game providers (likely because the user terminated his subscription to this program with the Operator) is:

- User's account at the Operator has been de-federated with the user's account at each game provider, so that the user is no longer able to have seamless access to the game provider sites.

The post-condition for bulk de-federation of all user accounts with a particular game provider (likely because this game provider terminated its participation in the program) is:

- User accounts at the Operator have been de-federated with the user accounts at the particular game provider, so that the users are no longer able to have seamless access to the particular game provider site.

5.4.2.5 Normal Flow

Federation of a new subscriber

The normal flow for federation between the user account at the Operator and that at the game provider is as follows:

1. Operator (rather the Web service at the Operator) sends a federate request to the game provider (rather the Web service at the game provider) requesting that the user account at the Operator be federated with the user account at the game provider.
2. Game provider verifies the identity of the Operator.
3. Game provider federates the user account at the Operator with the user account at the game provider. (Note that this could mean the creation of new accounts at the game provider for the users.)
4. Game provider responds to the Operator with a federation response message.

Bulk federation with a new game provider

The normal flow for bulk federation of all user accounts (participating in the program) at the Operator with corresponding accounts at a new game provider that recently joined the program is as follows:

1. Operator (rather the Web service at the Operator) sends a bulk federate request to the new game provider (rather the Web service at the game provider) requesting that the user accounts at the Operator be federated with the corresponding user accounts at the game provider.
2. Game provider verifies the identity of the Operator.
3. Game provider federates the user accounts of the various users at the Operator with the corresponding user account at the game provider. (Note that this could mean the creation of new accounts at the game provider for the users.)
4. Game provider responds to the Operator with a federation response message

De-federation of a user account with all game providers

The normal flow for de-federating a user account with all game providers (likely because the user terminated his participation in the program) is as follows:

1. Operator (rather the Web service at the Operator) sends a de-federate request to each game provider (rather the Web service at each game provider) requesting that the user account at the Operator be de-federated with the user account at the game provider.
2. Game provider verifies the identity of the Operator.
3. Game provider de-federates the user account at the Operator with the user account at the game provider.
4. Game provider responds to the Operator with a de-federation response message

Bulk de-federation of all user accounts with a game provider

The normal flow for bulk de-federation of all user accounts with a certain game provider (likely because the game provider terminated his participation in the program) is as follows:

1. Operator (rather the Web service at the Operator) sends a bulk de-federate request to the particular game provider (rather the Web service at each game provider) requesting that each of the user accounts at the Operator be de-federated with the user account at the game provider.
2. Game provider verifies the identity of the Operator.
3. Game provider de-federates the user accounts at the Operator with the user account at the game provider.
4. Game provider responds to the Operator with a de-federation response message

5.5 Identity Broker

5.5.1 Introduction

The relevance of Single Sign On (SSO) to OMA was discussed in Section 5.1. One of the pre-conditions there was that the service provider (movie ticket service provider) and the Identity Provider had made the necessary arrangements (both technical and business) in order to federate a user’s accounts. In a deployment scenario where there may exist several Identity Providers, a Service Provider may have to enter into a business agreement with many Identity Providers. This may not be desirable from the Service Provider’s viewpoint.

In order to alleviate this problem, the notion of an Identity Broker is introduced. In such a scenario, the Service Provider may enter into a business agreement with an Identity Broker, which may subsequently enter into business agreements with one or more Identity Providers. Thus, from the Service Provider’s perspective, it only needs to enter into a business agreement with an Identity Broker, instead of entering into a business agreement with several Identity Providers.

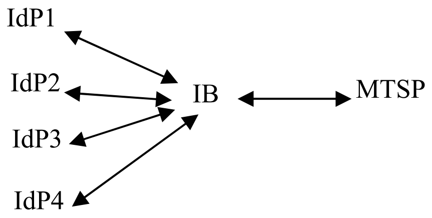
The reader is also encouraged to read the use case in Section 5.10, where the concept of Identity Broker is also introduced.

5.5.2 Basic Use Case

5.5.2.1 Short Description

This use case is similar to the use case described in Section 5.1 in that it illustrates SSO, with the difference being that the movie ticket service provider (acting as the service provider) and the Identity Provider do not share a business arrangement among themselves. Instead, the Movie Ticket Service Provider enters into a business agreement with an Identity Broker, which in turn, enters into a business agreement with several Identity Providers.

The figure below illustrates the scenario. The Movie Ticket Service Provider (denoted as MTSP) has a business agreement with an Identity Broker, which in this scenario is shown as IB. The Identity Broker, in turn, has business agreements with four Identity Providers denoted as IdP1, IdP2, IdP3 and IdP4.



Consider the case where the User1 has an account with IdP1, User2 has an account with IdP2, User3 has an account with IdP3, and User4 has an account with IdP4.

Consider now that User1 visits the Movie Ticket Service Provider (MTSP) site. Since the MTSP does not have a business relationship with IdP1 but has a business relationship with the Identity Broker IB, the MTSP contacts the IB for possible federation of the user's account at the MTSP with the user's account at an Identity Provider. The IB determines that User1 has an account at IdP1, and hence forwards the federation request to IdP1. Upon federating the User1's identity at IdP1 with the User1's identity at the MTSP, IdP1 sends a federation response to IB, which then forwards it to the MTSP.

After such federation, User1 would be able to utilize the benefits of Single Sign-On (SSO). Consider the case where User1 subsequently visits the MTSP site. The MTSP site then sends an Authentication request message to the IB, which forwards it to IdP1. If User1 is already authenticated at IdP1, then IdP1 sends an Authentication assertion to IB, which forwards it to the MTSP. The User1 is then able to seamlessly log into the MTSP site. Note that when the IB forwards messages between the MTSP and the IdP, it could potentially make modifications such as adding its signature, adding its assertion etc.

Similarly, when a User2 who has an account at IdP2 visits the MTSP, the IB acts as a broker between the MTSP and IdP2. And so on, for User3 and User4. In each of these cases, since the user does not have to explicitly enter the authenticating information, the overall user experience is enhanced.

5.5.2.2 Actors

- User – end user using a mobile device
- Identity Broker – Entity acting as a broker between a Service Provider and an Identity Provider
- IdP – Identity Provider
- Movie ticket service provider – Service provider providing downloadable movie tickets.

5.5.2.3 Pre-conditions

- User has an account with IdP, which is acting as an identity provider
- User has an account with the movie ticket service provider (MTSP), which is acting as a service provider.
- User does not have an account with Operator 2, which is acting as an IdP and is located both in Authentication Domains 1 and 2.
- The Movie Ticket Service provider has made necessary arrangements (business and technical) with the Identity Broker (IB), so that the IB can act as a broker between the MTSP and other Identity Providers (such as IdP).
- The IdP has made necessary arrangements (business and technical) with the Identity Broker (IB), so that the IB can act as a broker between the IdP and various service providers (such as MTSP).
- IdP has currently authenticated the mobile user.

5.5.2.4 Post-conditions

- User's account at the movie ticket service provider is federated with the user's account at the IdP, so that the user is subsequently able to utilize SSO benefits.
- Movie ticket service provider receives an authentication assertion from IB, after the IB receives an authentication assertion from the IdP.

5.5.2.5 Normal Flow

Federation:

- User accesses movie ticket service provider's service using the browser on his terminal. The movie ticket service provider requires user authentication prior to the user being able to browse (restricted portions of the) site.
- Movie ticket service provider User iscannot find an IdP within its authentication domain that the user has an account with.
- Movie ticket service provider sends a federation request to the Identity Broker (IB) requesting federation of the user's account.
- After determining that the user has an account at IdP, the IB sends a federation request to the IdP.
- The IdP obtains the user's consent for federation, and subsequently federates the accounts. The IdP then sends a federation response back to the IB.
- The IB then sends a federation response back to the MTSP.

Single Sign On (SSO):

The additional pre-condition here is that the user's account at the MTSP has been federated with the user's account at the IdP.

- User accesses movie ticket service provider's service using the browser on his terminal. The movie ticket service provider requires user authentication prior to the user being able to browse (restricted portions of the) site.
- Movie ticket service provider User iscannot find an IdP within its authentication domain that the user has an account with.
- Movie ticket service provider sends an authentication request to the Identity Broker (IB) requesting authentication of the user's account.

- After determining that the user has an account at IdP, the IB sends an authentication request to the IdP.
- Since the user is already authenticated at the IdP, the IdP sends an authentication assertion back to the IB.
- The IB then sends an authentication response back to the MTSP.

5.6 Federation, Single Sign On and Attribute Sharing with Affiliations

5.6.1 Introduction

There are many cases where an alliance among different entities exists in such a fashion that, for certain functions, they appear as a single entity to the end-user. In other words, the different entities or companies in the alliance are no longer relevant to the end-user, but the end-user is merely interested in the services that the entity has to offer as a collective unit.

Consider the following alliances:

- Alliance among airline carriers – such as Star Alliance (with United Airlines, Lufthansa and other airline carriers as members) or One World Alliance (with American Airlines, Finnair and other airline carriers as members.)
- Alliance between an airline carrier, a car rental company and a hotel chain. For instance, United Airlines has a partnership with Hertz car rentals.
- Alliance between a health benefits provider, a 401(K) benefits provider and an Employee Stock Options Provider – via an employer's portal.

Use cases in Section 5.1 and 5.7 describe cases where the user experience is enhanced by the use of SSO between a service provider and an identity provider, and by the use of profile sharing between a service provider and an attribute provider, respectively. In each of these use cases, the service provider acted as an independent entity. However, in the case of alliances, as mentioned above, it is sufficient for the service provider to merely act as an entity that is part of the alliance, and not as an independent entity. This makes the user experience better.

The purpose of presenting this use case to OMA is to illustrate the benefits of (1) a user federating his account at an IdP with not just a single SP, but with an affiliation of SPs instead, and (2) profile sharing between an attribute provider and an affiliation of SPs. One of the main advantages of a user federating his account at an IdP with an entire affiliation is that the user does not need to have an individual account at each member of the affiliation, nor does the user need to individually federate his accounts at each member of the affiliation with that at the IdP.

5.6.2 Basic Use Case

5.6.2.1 Short Description

The user has an account with an Operator, which acts as an Identity Provider (IdP). The user also has an account with a site discountAirlineTickets.com that sells airline tickets. The site discountAirlineTickets.com is a member of a travel affiliation called discountAlliance, which has two other members – discountCarRentals.com and discountHotels.com. Using his mobile device, the user decides to browse the site discountAirlineTickets.com for airline ticket prices and suitable travel itineraries.

Federation with an affiliation: When the user starts to browse the site discountAirlineTickets.com, the site needs to authenticate the user. The site discountAirlineTickets.com realizes that the user experience can be simplified if the user's account at discountAirlineTickets.com is federated with that at the Operator. The site discountAirlineTickets.com also realizes that since it is a member of the affiliation discountAlliance, the user experience can be further enhanced if the federation is done not to discountAirlineTickets.com but to the affiliation as a whole. The main reason for this enhanced user experience is that when the user, at a later time, browses another member of the affiliation discountAlliance (say, the site discountHotels.com), this member does not require the user to have a separate account and does not need the user to separately federate the user's account with this site. Instead, the federation with the affiliation facilitates SSO for this site as well. Hence, there are advantages to federation with an affiliation, rather than individual federation with each member of the affiliation.

So, when the user browses the site discountAirlineTickets.com, it prompts the user whether he would like to simplify his experience by federating his account at the Operator with that at the affiliation discountAlliance. The user wishes to know who the members of the affiliation discountAlliance are, and obtains this information either from the Operator or from discountAirlineTickets.com. After obtaining the information (either from the Operator or from discountAirlineTickets.com) that the other two members of discountAlliance are discountCarRentals.com and discountHotels.com, the user federates his account at the Operator with the affiliation discountAlliance. The user is then able to browse the site discountAirlineTickets.com.

SSO for affiliation: Once the user has federated his account at the Operator with the affiliation discountAlliance, he is able to seamlessly browse any of the other sites without further federation. Consider the case where the user browses the site discountCarRentals.com. Since discountCarRentals.com is a member of the affiliation discountAlliance, it requests an authentication assertion from the Operator based on the fact that it is a member of the affiliation discountAlliance. Upon receiving the authentication assertion, the mobile user is seamlessly authenticated and is able to browse the site discountCarRentals.com. Note that discountCarRentals.com did not have an explicit federation of the user's account with that at the Operator, but was able to authenticate the user on the basis of the federation between the user's account at Operator 1 and the affiliation discountAlliance (which was earlier established by discountAirlineTickets.com.)

Profile Sharing for affiliation: Consider the case where the user stores his residential address at attribute provider attributeProvider.com. The user sets the permissions associated with these attributes in such a manner that any member of the affiliation discountAlliance can request the attributes. When a member of the affiliation (say, discountHotels.com) requests the residential address of the user from attributeProvider.com, the requestor discountHotels.com identifies itself as being a member of the affiliation discountAlliance. Since the user has set his permissions to release the attribute when any member of the affiliation discountAlliance makes the request, attributeProvider.com release the user's residential address to discountHotels.com. The advantages of such profile sharing with an affiliation are clear, including:

- User does not have to explicitly set permissions for each member of the affiliation discountAlliance at attributeProvider.com.
- User may need only one account for the entire affiliation.
- User may have a contract or trust relationship with the affiliation, without necessarily knowing each member of the affiliation separately.

5.6.2.2 Actors

- User – end user using a mobile device
- Operator – Operator acting as Identity Provider (IdP) and offering SSO service and discovery service
- DiscountAirlineTickets.com – Service Provider that sells airline tickets.
- DiscountCarRentals.com – Service Provider that makes car rental reservations.
- DiscountHotels.com – Service Provider that makes hotel reservations.
- DiscountAlliance – Affiliation service containing three service providers, namely, DiscountAirlineTickets.com, DiscountCarRentals.com and DiscountHotels.com.
- AttributeProvider.com – attribute provider that provides the user's residential address information upon proper authorization.

5.6.2.3 Preconditions

- User has an account with the Operator.
- User is authenticated at the Operator.

- User has an account with the affiliation discountAlliance.
- The affiliation discountAlliance consists of three entities – discountAirlineTickets.com, discountCarRentals.com and discountHotels.com.
- The affiliation discountAlliance has made necessary arrangements (business and technical) with the Operator to use single sign on provided by the Operator.
- User has stored his hotel and room preference information at the attribute provider attributeProvider.com.
- The attribute provider attributeProvider.com has registered with Operator 1 to provide discovery service.

5.6.2.4 Postconditions

The post-condition for federation is :

3. User's account at the Operator is federated with affiliation discountAlliance. This ensures that the user can seamlessly browse any site that is a member of the affiliation discountAlliance.

The post-condition for SSO is:

4. User is allowed seamless access to any site (say, discountCarRentals.com) that is a member of the affiliation discountAlliance.

The post-condition for attribute/profile sharing is:

5. User's residential address information stored at attributeProvider.com is seamlessly provided to discountHotels.com, on the basis that discountHotels.com is a member of the affiliation discountAlliance.

5.6.2.5 Normal Flow

Federation with an affiliation

The normal flow for federation between the user account at the Operator and the affiliation discountAlliance is as follows:

5. User begins to browse a portion of the site discountAirlinesTickets.com that requires user authentication.
6. discountAirlinesTickets.com prompts the user whether the user would like to federate his account at the Operator (acting as the IdP) with the affiliation discountAlliance, which discountAirlinesTickets.com is a member of.
7. User receives the list of entities (discountAirlinesTickets.com, discountCarRentals.com and discountHotels.com) comprising the affiliation discountAlliance from either discountAirlinesTickets.com or from the Operator.
8. User agrees to federate his account at the Operator with the affiliation discountAlliance.

SSO with an affiliation

The normal flow for SSO in the case of affiliation discountAlliance is as follows. Note that it is assumed that the user has already federated his account at the Operator with the affiliation discountAlliance:

1. User begins to browse a portion of the site discountCarRentals.com that requires user authentication.
2. Since discountCarRentals.com is a member of the affiliation discountAlliance, it requests an authentication assertion from the Operator by identifying itself as a member of the affiliation discountAlliance. Note that this could be done by means of signing the request with a private key, for which the corresponding public key is tied to the affiliation by means of a certificate.
3. After discountCarRentals.com obtains a valid authentication assertion from the Operator, the user is allowed seamless access to browse discountCarRentals.com

Profile/attribute sharing with an affiliation

The normal flow for profile sharing with discountHotels.com as a member of the affiliation discountAlliance is as follows:

1. User begins to browse a portion of the site discountHotels.com
2. discountHotels.com obtains an authentication assertion from the Operator by identifying itself as a member of the affiliation discountAlliance, after which the user is provided seamless access to the site.
3. discountHotels.com requires the residential address of the user, and it discovers from the Operator that attributeProvider.com hosts this information for the user.
4. discountHotels.com requests the residential address information of the user from attributeProvider.com, and identifies itself as a member of the affiliation discountAlliance.
5. Since discountHotels.com is a member of the affiliation discountAlliance, and since the user has authorized the release of his residential address information to any member of the affiliation discountAlliance, discountHotels.com obtains these attributes from attributeProvider.com.

5.7 Seamless Attribute Transfer

5.7.1 Introduction

The purpose of this use case is to illustrate how identity services can simplify a business transaction from a terminal user's point of view. Typically, when using mobile services today, a user needs to enter his profile information, such as zip code (location), payment information, shipping address etc. This is often tedious for mobile terminals with numeric keypads. Identity services facilitate obtaining such profile information in a seamless manner, and makes the use of mobile services easier by reducing the number of keystrokes required to use a service.

5.7.2 Basic Use Case

5.7.2.1 Short Description

In this use case, the user sets up several of his attributes at an Attribute Provider (AP). Storing such attributes at an attribute provider constitutes storing a portion of the user profile at the attribute provider. The user also associates permission to the attributes that it stores at AP. These permissions state the conditions under which the AP can release the user attribute to the requestor, and the usage of these attributes by the requestor once it obtains them. The main benefit of storing such user attributes at an attribute provider is that the user need not be prompted for these attributes. Instead, the requestor could seamlessly obtain them from the Attribute Provider. This makes the mobile user experience better.

In the use case that we describe, the Location Attribute Provider (AP) has the current location information of the mobile user, and the user has also associated permissions with these attributes. The user does not have to use his mobile terminal to set such attributes or permissions at the Location AP, but could potentially use a Personal Computer or other user-input friendly devices for this purpose. The user is assumed to have an account with an Identity Provider (such as an Operator) and also an account with a movie ticket service provider. The user has also federated his accounts at the Operator and at the movie ticket service provider, so that the movie ticket service provider can receive assertions from the Operator. Moreover, the Location AP and the Operator also have a business agreement so that the Operator can provide discovery service for the Location AP to an authorized requestor that is requesting the user's location attributes.

With these in place, on a certain day when the mobile user is authenticated with the Operator, the mobile user browses the movie ticket service provider's site in order to purchase a movie ticket. Since the movie ticket service provider requires users to have an account and authenticate successfully prior to providing any service, the movie ticket service provider requests and obtains an authentication assertion from the Operator. The mobile user is now seamlessly authenticated at the movie ticket service provider. The movie ticket service provider also wishes to determine the current location of the mobile user, so that the movie ticket provider could customize the view seen by the mobile user. For instance, the movie ticket service provider may be able to provide the mobile user with discount coupons of partners that are in the vicinity of the mobile user's current location. The movie ticket service provider then contacts the Operator requesting information on the Location Attribute Provider (AP) for the mobile user. (Note that this request could be in conjunction with the request for an authentication assertion.) After the Operator provides the movie ticket service provider with the address of the Location AP, the movie ticket service provider requests the Location AP for the current location of the mobile user. After checking the permissions that the user had associated with the location information, the Location AP releases this information to the movie ticket service provider. Based on this information, the movie ticket service provider is able to provide customized service (e.g. discount coupons of nearby merchants etc.) to the mobile user.

5.7.2.2 Actors

- User – end user using a mobile device
- Identity provider – operator or service provider offering single sign on service and discovery service of attribute providers
- Movie ticket service provider – Service provider providing downloadable movie tickets.
- Attribute provider – an entity providing location information of user to authorized requestors

5.7.2.3 Pre-conditions

- User has an account with the Operator (acting as an identity provider)
- User has an account with the movie ticket service provider
- Movie ticket service provider has made necessary arrangements (business and technical) with the Operator to use single sign on provided by identity provider
- User has federated his account at the movie ticket service provider with his account at the Operator, so that the movie ticket service provider can receive authentication assertions from the Operator.
- Identity provider has authenticated user.
- Location information of user is obtained from the Location Attribute Provider (AP), and the user has set permissions for the release of his location information to authorized requestors.
- User has federated/linked his account at Location AP with that at the Operator so that the Operator may provide discovery service of the Location AP to authorized requestors.

5.7.2.4 Post-conditions

- The user is able to access the movie ticket service provider site, as the movie ticket service provider receives the required authentication assertion from the Operator.
- The user's location information has been obtained by the movie ticket service provider from the Location AP.
- The movie ticket service provider provides the mobile user with a customized view based on his current location (e.g. relevant discount coupons based on location of user may have been downloaded to user's terminal.)

5.7.2.5 Normal Flow

1. User accesses movie ticket service provider's service using the browser on his mobile terminal.
2. Since movie ticket service provider requires user authentication prior to accessing the site, the movie ticket service provider requests and obtains an authentication assertion from the Operator. Upon obtaining the authentication assertion, the user is allowed seamless access to the movie ticket service provider's site.

3. Since the movie ticket service provider wishes to obtain the current location information of the mobile user, it requests the Operator (acting as a discovery service) for the address of the Location AP associated with the user. Note that this request can happen in conjunction with the request for an authentication assertion.

4. Upon receiving the address of the Location AP from the Operator, the movie ticket service provider requests the Location AP for the current location of the mobile user.

5. The Location AP checks the permissions set by the user, and upon determining that the movie ticket service provider is authorized to obtain the user's location information, releases the user's location information to the movie ticket service provider.

6. Upon obtaining the current location information of the mobile user, the movie ticket service provider is able to provide a customized view to the user. Relevant discount coupons of partner merchants in the vicinity of the user's current location are downloaded to user's terminal.

7. The user continues to browse the movie ticket service provider site.

5.7.2.6 Alternative Flows

In this section, we describe several alternative flows, which need to be considered with this use case:

5.7.2.6.1 Alternative Flow 1: Missing Attribute Value, AP contacts user

In this alternative flow, the desired attribute value (current location information) is not present at the Location AP. Consequently, the movie ticket service provider redirects the user to the Location AP, so that the user could input the desired attribute value, after which the user is redirected back to the movie ticket service provider.

Items 1 through 4 are identical to Normal Flow, after which we have:

5. The Location AP determines that the user's location was last updated at a time that is longer than that desirable to the movie ticket service provider. After providing this "outdated" location information that is available to it, the Location AP indicates to the movie ticket service provider that it does not have the current location information of the user (updated within the desired time window), as desired by the movie ticket service provider. Note that the location AP checks permissions to ensure that the movie ticket service provider is authorized to receive the user's location information.

6. Movie ticket service provider seamlessly redirects user to the Location AP, where user is able to enter his current GPS location.

7. Location AP sends the latest location information (as entered by the user) to the movie ticket service provider.

8. Location AP seamlessly redirects the user back to the movie ticket service provider.

After this, follow item 6 in Normal Flow.

5.7.2.6.2 Alternative Flow 2: Missing Attribute Value, SP contacts user

This use case is similar to Alternative Flow 1, in that the desired attribute value (current location information) is not present at the Location AP. However, rather than redirect the user to the Location AP, the movie ticket service provider itself obtains the current location information from the user, and updates the Location AP with this latest information. Such a scenario may be desirable when the movie ticket service provider does not wish to hand over the user to another entity, which in this case is the Location AP.

Items 1 through 4 are identical to Normal Flow, after which we have:

5. The Location AP determines that the user's location was last updated at a time that is longer than that desirable to the movie ticket service provider. After providing this "outdated" location information that is available to it, the Location AP indicates to the movie ticket service provider that it does not have the current location information of the user (updated within the desired time window), as desired by the movie ticket service provider. Note that the

location AP checks permissions to ensure that the movie ticket service provider is authorized to receive the user's location information.

6. Movie ticket service provider prompts the user to enter his current GPS location.
7. The movie ticket service provider sends this latest location information (as entered by the user) to the Location AP.

After this, follow item 6 in Normal Flow.

5.7.2.6.3 Alternative Flow 3: Unknown Permission, SP contacts user

In this use case, the Location AP is unable to determine whether the user has authorized it to release the location information to the requesting movie ticket service provider. Consequently, the Location AP indicates to the movie ticket service provider that it does not know the permissions set by the user regarding release of the location information to the movie ticket service provider, following which the movie ticket service provider prompts the user for the required permissions, and forwards this permission to the Location AP.

Identical to Normal Flow items 1 through 4, after which:

5. The Location AP checks permissions associated with the release of location information to the movie ticket service provider, and determines that it is unaware of these permissions.
6. Location AP indicates unknown permission status to the movie ticket service provider
7. Movie ticket service provider queries the user for permission, and forwards this permission to the Location AP.
8. Upon obtaining the desired permissions, the Location AP releases the mobile user's current location to the mobile service provider.

After this, follow Item 6 of Normal Flow.

5.7.2.6.4 Alternative Flow 4: Unknown Permission, AP contacts user

This use case is identical to that of Alternative Flow 3, in that the Location AP is unable to determine the permission associated with the release of the user's location information to the movie ticket service provider. The difference in this case is that it is the Location AP that contacts the user to determine the permissions, instead of the movie ticket service provider contacting the user for the permissions (as was done in Alternative Flow 3).

Identical to Normal Flow items 1 through 4, after which:

5. The Location AP checks permissions associated with the release of location information to the movie ticket service provider, and determines that it is unaware of these permissions.
6. Location AP queries the user for permissions associated with the movie ticket service provider's request indicates unknown permission status to the movie ticket service provider
7. Upon obtaining the desired permissions from the user, the Location AP releases the mobile user's current location to the mobile service provider.

After this, follow Item 6 of Normal Flow.

5.8 Seamless Attribute Transfer with Usage Directives

5.8.1 Introduction

The purpose of this use case is to illustrate the concept of usage directives when service providers request user attributes from attribute providers. By usage directives, we mean the directives on how an attribute that has been released to a requestor may be used by that requestor.

As discussed in Section 5.7, when user attributes are transferred directly from an attribute provider to a service provider without the user explicitly inputting this information using his input-constrained numeric keypad, the overall user experience is enhanced. In this use case, we refine the use case of Section 5.7 to include usage directives. In other words, when the service provider requests a user attribute from the attribute provider, it also includes an indication of how it would use the attributes once it receives them. The attribute provider then releases the attributes to the requesting service provider only if the specified usage directive in the request complies with the usage directive policy that the user has established for the attributes at the attribute provider.

5.8.2 Basic Use Case

5.8.2.1 Short Description

This use case is an enhancement to the use case described in Section 5.7, with the difference being that usage directives associated with attributes are included in this use case. However, we describe the scenario completely here for the sake of completion.

In this use case, the user sets up several of his attributes at an Attribute Provider (AP). The user also associates permission to the attributes that it stores at AP. These permissions state the conditions under which the AP can release the user attribute to the requestor, and the usage of these attributes by the requestor once it obtains them. The attribute provider only releases a user's attribute if the access control policy at the AP allows it to do so, as well as when the usage directive in the request message satisfies the usage directive policy specified by the user. The main benefit of storing such user attributes at an attribute provider is that the user need not be prompted for these attributes. Instead, the requestor could seamlessly obtain them from the Attribute Provider. This makes the mobile user experience better. In this use case, we will focus on the usage directive component.

In the use case that we describe, the Location Attribute Provider (AP) has the current location information of the mobile user, and the user has also associated permissions with these attributes. Permissions associated with a user attribute constitute both access control policies as well as usage directives. The user does not have to use his mobile terminal to set such attributes or permissions at the Location AP, but could potentially use a Personal Computer or other user-input friendly devices for this purpose. The user is assumed to have an account with an Identity Provider (such as an Operator) and also an account with a movie ticket service provider. The user has also federated his accounts at the Operator and at the movie ticket service provider, so that the movie ticket service provider can receive assertions from the Operator. Moreover, the Location AP and the Operator also have a business agreement so that the Operator can provide discovery service for the Location AP to an authorized requestor that is requesting the user's location attributes.

With these in place, on a certain day when the mobile user is authenticated with the Operator, the mobile user browses the movie ticket service provider's site in order to purchase a movie ticket. Since the movie ticket service provider requires users to have an account and authenticate successfully prior to providing any service, the movie ticket service provider requests and obtains an authentication assertion from the Operator. Upon receiving a successful authentication assertion from the Operator, the mobile user is seamlessly authenticated at the movie ticket service provider. The movie ticket service provider also wishes to determine the current location of the mobile user, so that the movie ticket provider could customize the view seen by the mobile user. In addition, the movie ticket service provider may be able to provide the mobile user with discount coupons of partners that are in the vicinity of the mobile user's current location. The movie ticket service provider then contacts the Operator requesting information on the Location Attribute Provider (AP) for the mobile user. (Note that this request could be in conjunction with the request for an authentication assertion.) After the Operator provides the movie ticket service provider with the address of the Location AP, the movie ticket service provider requests the Location AP for the current location of the mobile user. The movie ticket service provider also includes the usage directives in the request. These usage directives specify the intended usage of these attributes by the movie ticket service provider once it receives them. After checking that the usage directives in the request are compliant with those specified by the user's usage directives policy, and after checking the access control policy associated with the release of the attribute, the Location AP releases this information to the movie ticket service provider. Based on this information, the movie ticket service provider is able to provide customized service (e.g. discount coupons of nearby merchants etc.) to the mobile user.

The focus of this use case, as stated earlier, then is to highlight the aspects of usage directives.

5.8.2.2 Actors

- User – end user using a mobile device

- Operator – Entity acting as an Identity Provider and offering single sign on service and discovery service of attribute providers
- Movie ticket service provider – Service provider providing downloadable movie tickets.
- Attribute provider – an entity providing location information of user to authorized requestors

5.8.2.3 Pre-conditions

- User has an account with the Operator (acting as an identity provider)
- User has an account with the movie ticket service provider
- Movie ticket service provider has made necessary arrangements (business and technical) with the Operator to use single sign on provided by identity provider
- User has federated his account at the movie ticket service provider with his account at the Operator, so that the movie ticket service provider can receive authentication assertions from the Operator.
- Operator has authenticated user.
- Location information of user is obtained from the Location Attribute Provider (AP), and the user has set permissions (i.e., both access control and usage directives policies) for the release of his location information to authorized requestors.
- User has federated/linked his account at Location AP with that at the Operator so that the Operator may provide discovery service of the Location AP to authorized requestors.

5.8.2.4 Post-conditions

- The user is able to access the movie ticket service provider site, as the movie ticket service provider receives the required authentication assertion from the Operator.
- The user’s location information has been obtained by the movie ticket service provider from the Location AP.
- The movie ticket service provider provides the mobile user with a customized view based on his current location (e.g. relevant discount coupons based on location of user may have been downloaded to user’s terminal.)

5.8.2.5 Normal Flow

1. User accesses movie ticket service provider’s service using the browser on his mobile terminal.
2. Since movie ticket service provider requires user authentication prior to accessing the site, the movie ticket service provider requests and obtains an authentication assertion from the Operator. Upon obtaining the authentication assertion, the user is allowed seamless access to the movie ticket service provider’s site.
3. Since the movie ticket service provider wishes to obtain the current location information of the mobile user, it requests the Operator (acting as a discovery service) for the address of the Location AP associated with the user. Note that this request can happen in conjunction with the request for an authentication assertion.
4. Upon receiving the address of the Location AP from the Operator, the movie ticket service provider requests the Location AP for the current location of the mobile user. Movie ticket service provider includes the usage directives for the requested attribute.
5. The Location AP checks the permissions set by the user. This includes comparing the usage directives specified by the movie ticket service provider in the request with the usage directive policy specified by the user for the Location attribute stored at Location AP.
6. Upon determining that the movie ticket service provider is authorized to obtain the user’s location information, releases the user’s location information to the movie ticket service provider. While checking usage directives (that

are part of permissions, along with accesss control) the Location AP ensures that the usage directive specified by the movie ticket service provider in the request is compliant with the usage directive policy specified by the user for the Location attribute.

7. Upon obtaining the current location information of the mobile user, the movie ticket service provider is able to provide a customized view to the user. Relevant discount coupons of partner merchants in the vicinity of the user's current location are downloaded to user's terminal.

8. The user continues to browse the movie ticket service provider site.

5.8.2.6 Alternative Flows

5.8.2.6.1 Alternative Flow 1: Usage Directive Policy Not Satisifed, and Request Denied

Items 1 through 5 are identical to the normal flow, as described in Section 5.8.2.5.. After that, the flow is as follows:

1. Location AP denies the request since the attribute usage in the request does not satisfy the usage directive policy specified by the user.

2. Movie ticket service provider sends a new request for the location information, and includes a modified usage directive parameter in the request.

3. Location AP checks the usage directive in the request with the usage directive policy specified by the user.

After this, the flow follows Item 6 of the normal flow, as described in Section 5.8.2.5.

5.8.2.6.2 Alternative Flow 2: Usage Directive Policy Not Satisifed, Request Denied, Allowed Usage Directives Specified

Items 1 through 5 are identical to the normal flow of the basic use case, as described in Section 5.8.2.5.. After that, the flow is as follows:

1. Location AP denies the request since the attribute usage in the request does not satisfy the usage directive policy specified by the user. The Location AP includes the list of acceptable usage directives.

2. Movie ticket service provider sends a new request for the location information, and includes a modified usage directive parameter in the request based on the list of acceptable usage directives that it received from the Location AP.

3. Location AP checks the usage directive in the request with the usage directive policy specified by the user.

After this, the flow follows Item 6 of the normal flow, as described in Section 5.8.2.5.

5.9 Anonymous Attribute Sharing

5.9.1 Introduction

There are many scenarios where a service provider requires access to certain attributes associated with a user, while not knowing the identity of the user. For instance, there may be a case where a service provider may require the zip code of a user in order to properly greet the user (e.g., Good Morning or Good Evening). In another case, a service provider may require the language preference of the user in order to display the text in the appropriate language. In either of these cases, and in many other such cases, the service provider does not need to know the identity of the user, but merely needs access to the user's attributes.

This use case describes the transfer of such anonymous attributes from an attribute provider to the service provider. When this is done, the user experience is enhanced because the mobile user does not have to tediously enter the requested information using his input-constrained keypad.

5.9.2 Basic Use Case

5.9.2.1 Short Description

Consider the case where a user has an account with an Operator (acting as an Identity Provider.) The user is also currently authenticated with the Operator. The user stores the zip code of his residential address and his language preference at a certain Attribute Provider 1 (AP1). The zip code of the user's current location may be obtained from a Location Attribute Provider (AP). The user has set the appropriate permissions for the release of his attributes stored at AP1 and Location AP. The user has linked his account at the Operator with his account at AP1 and the Location AP, so that the Operator can provide a requesting entity with discovery service for AP1 and the Location AP.

The user uses his mobile terminal to access a service provider, CustomizedWeather.com, that provides weather information. The service provider, CustomizedWeather.com, requires the user's current and permanent zip code, as well as the user's language preference in order to provide the user with a customized weather report. Note that CustomizedWeather.com does not care about the identity of the user. This means that if the same mobile user revisited CustomizedWeather.com, there is no way for CustomizedWeather.com to identify that it is the same user browsing its site (unless cookies are stored.)

When the mobile user browses CustomizedWeather.com, it contacts the Operator in order to obtain the address of the attribute provider that stores the user's current and permanent zip code, as well as the user's language preference. Since the Operator has authenticated the mobile user, the Operator knows the identity of the user, and hence is able to determine the suitable attribute providers that store this information (since the Operator acting as IdP also provides discovery service). The Operator indicates to CustomizedWeather.com that the user's permanent zip code and language preference can be obtained from AP1, while the user's current zip code can be obtained from Location AP. CustomizedWeather.com then requests the user's permanent zip code and language preference from AP1, and requests the user's current zip code from Location AP. AP1 and Location AP check the permissions associated with these attributes, and release the attributes to CustomizedWeather.com. Note that throughout this entire flow, CustomizedWeather.com has no idea about the identity of the user. One may also note that CustomizedWeather.com does not require the user to have an account with it.

Since such anonymous attributes are seamlessly transferred from an attribute provider (AP1 or Location AP) to the service provider (CustomizedWeather.com), the mobile user does not need to manually enter this information using his input-constrained numeric keypad. This then enhances the overall mobile user experience.

5.9.2.2 Actors

- User – end user using a mobile device
- Operator – Mobile operator acting as an Identity Provider (IdP) and offering single sign on service and discovery service
- CustomizedWeather.com – Service provider providing customzed weather information.
- Attribute Provider 1 – an entity providing user's permanent zip code and language preference information
- Location AP – an entity providing the user's current zip code

5.9.2.3 Pre-conditions

- User has an account with an Operator (acting as an identity provider and providing discovery service)
- Operator has authenticated the user.
- User has stored his permanent zip code and language preference at Attribute Provider 1 (AP1).
- User's current zip code information is obtained from Location AP.
- User has federated/linked his account at AP1 (and Location AP) with that at the Operator so that the Operator may provide discovery service for the user's attributes stored at AP1 (and Location AP).
- User does not necessarily have an account with CustomizedWeather.com.

5.9.2.4 Post-conditions

- The user’s permanent zip code and language preference information have been obtained by CustomizedWeather.com from AP1.
- The user’s current zip code has been obtained by CustomizedWeather.com from the Location AP.
- CustomizedWeather.com provides a customized view of the user’s weather – both at the user’s current location as well as at the user’s permanent location – using the user’s preferred language.

5.9.2.5 Normal Flow

1. User accesses CustomizedWeather.com service using the browser on his terminal
2. CustomizedWeather.com requires the user’s current and permanent zip code as well as the user’s language preference in order to provide the user a customized weather report.
3. CustomizedWeather.com contacts the Operator to determine the attribute providers that store the user’s current and permanent zip code and the user’s language preference.
4. Since the Operator has already authenticated the user, the Operator knows the identity of the user, and the location of the attribute providers that store the user’s attributes.
5. Operator responds to CustomizedWeather.com that AP1 provides the permanent zip code and language preference information of the user, while Location AP provides the current zip code of the user.
6. CustomizedWeather.com requests permanent zip code and language preference information from AP1, and current zip code information from Location AP.
7. After ensuring that the user permissions allow the release of such information, AP1 releases the permanent zip code and language preference information to CustomizedWeather.com, and Location AP releases the current zip code information to CustomizedWeather.com.
8. CustomizedWeather.com provides a customized view based on the zip code and language preference of the user.

5.10 Interaction Across Authentication Domains

5.10.1 Introduction

The relevance of Single Sign On (SSO) to OMA was discussed in Section 5.1. One of the pre-conditions there was that the service provider (movie ticket service provider) and the Identity Provider (Operator 1) had made the necessary arrangements (both technical and business) in order to federate a user’s accounts. In other words, one could consider the movie ticket service provider and Operator 1 to belong to the same authentication domain.

However, there are also scenarios where the service provider (movie ticket service provider) and the Identity Provider (Operator 1) have not made any business arrangements in order to federate a user’s accounts. In other words, one could consider the movie ticket service provider and Operator 1 to belong to different authentication domains. In such a scenario where the movie ticket service provider and Operator 1 belong to different authentication domains, the user experience is enhanced when Operator 2 residing in the same authentication domain as the movie ticket service provider can introduce the movie ticket service provider and Operator 1 to each other. When this happens, it is possible to federate the user account at Operator 1 in one Authentication Domain with the user account at the movie ticket service provider in another Authentication Domain. Operator 2, that is present in both authentication domains, introduces Operator 1 and the movie ticket service provider.

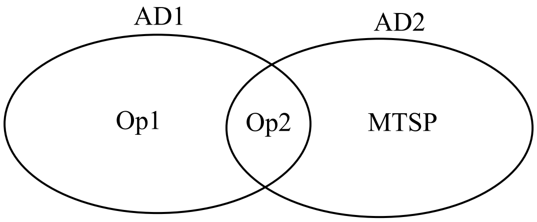
This enhances the overall user experience since the mobile user does not have to explicitly enter his authentication information at the movie ticket service provider. Instead, the movie ticket service provider is able to obtain the authentication assertion from Operator 1. We discuss this use case here.

5.10.2 Basic Use Case

5.10.2.1 Short Description

This use case is similar to the use case described in Section 5.1 in that it illustrates SSO, with the difference being that the movie ticket service provider (acting as the service provider) and Operator 1 (acting as the Identity Provider) belong to different authentication domains. An authentication domain comprises entities that share a business arrangement among themselves.

The figure below illustrates the scenario. Operator 1 (denoted as Op1) belongs to Authentication Domain 1 (denoted as AD1), while the Movie Ticket Service Provider (denoted as MTSP) belongs to Authentication Domain 2 (denoted as AD2). Operator 2 (denoted as Op2) belongs to both authentication domains.



The user has an account with Operator 1, and the user is currently authenticated with Operator 1. The user also has an account with the movie ticket service provider. The user, however, does not have an account with Operator 2.

The mobile user is currently browsing the movie ticket service provider site, which requires the user to be authenticated prior to the user being able to browse the site (or certain portions of the site). Instead of the user providing authentication information to the movie ticket service provider, if the movie ticket service provider obtained an authentication assertion from a trusted entity, then the overall user experience is enhanced. This is because the mobile does not have to enter tedious authentication information using his input-constrained numeric keypad. Thus, the main point of this use case is the single sign on (SSO) feature.

When the mobile user browses the movie ticket service provider, the movie ticket service provider tries to determine an Identity Provider (IdP) that the user has an account with, and which the movie ticket service provider has a business arrangement with. In other words, the movie ticket service provider tries to determine an IdP within its Authentication Domain AD2 that the user has an account with. Upon finding no such IdP, the movie ticket service provider sends an authentication request to Operator 2, which is an IdP belonging to two or more authentication domains. In this case, Operator 2 is located both in AD1 as well as AD2. Also, there is an IdP in AD1 (which is Operator 1) with which the user has an account, and is currently logged in. Since Operator 2 is in the same authentication as Operator 1, it is able to determine that the user has an account with Operator 1. Operator 2 then responds to the movie ticket service provider (MTSP) with the location of Operator 1. The MTSP sends a federation request to Operator 1 indicating that Operator 2 introduced it. Operator 1 then contacts Operator 2 and requests it to validate the MTSP. Upon receiving such a validation, Operator 1 responds to the MTSP with a federation response indicating successful federation of the user account at Operator 1 with the user account at the MTSP. Since an authentication assertion is included as part of the federation response, the MTSP has successfully federated and authenticated the mobile user, and the mobile user is able to browse the MTSP site.

Since the user does not have to explicitly enter the authenticating information, the overall user experience is enhanced.

5.10.2.2 Actors

- User – end user using a mobile device

- Operator 1 – Entity acting as an IdP and offering single sign on service, and which is located in Authentication Domain 1
- Operator 2 – Entity acting as an IdP and which is located in both Authentication Domains 1 and 2
- Movie ticket service provider – Service provider providing downloadable movie tickets.

5.10.2.3 Pre-conditions

- User has an account with Operator 1, which is acting as an identity provider and is located in Authentication Domain 1
- User has an account with the movie ticket service provider, which is acting as a service provider and is located in Authentication Domain 2.
- User does not have an account with Operator 2, which is acting as an IdP and is located both in Authentication Domains 1 and 2.
- The Movie Ticket Service provider has made necessary arrangements (business and technical) with Operator 2 to use single sign on provided by Operator 2.
- Operator 2 (acting as a service provider) has made necessary arrangements (business and technical) with Operator 1 (acting as an IdP) to use single sign on provided by Operator 1.
- Operator 1 has currently authenticated the mobile user.

5.10.2.4 Post-conditions

- User's account at the movie ticket service provider is federated with the user's account at Operator 1.
- Movie ticket service provider receives an authentication assertion from Operator 1, and the mobile user is then able to seamlessly browse the mobile ticket service provider site.

5.10.2.5 Normal Flow

- User accesses movie ticket service provider's service using the browser on his terminal. The movie ticket service provider requires user authentication prior to the user being able to browse (restricted portions of the) site.
- Movie ticket service provider User iscannot find an IdP within authentication domain 2 that the user has an account with.
- Movie ticket service provider sends an authentication request to Operator 2 (acting as an IdP within authentication domain 2).
- Since Operator 2 is also a member of Authentication Domain 1, it determines that the user has an account and is currently authenticated at Operator 1 (within Authentication Domain 1).
- Operator 2 responds to the movie ticket service provider with the address of Operator 1. Based on the fact that the movie ticket service provider and Operator 2 are in the same authentication domain, movie ticket service provider decides to trust the introduction of Operator 1 by Operator 2.
- The movie ticket service provider sends a federation request to Operator 1, requesting to federate the user's account at Operator 1 with the user's account at the movie ticket service provider. The movie ticket service provider indicates that it was introduced by Operator 2.
- Operator 1 contacts Operator 2, which validates the introduction.
- Operator 1 sends a federation response to the movie ticket service provider indicating successful federation of the user's account at Operator 1 with the user's account at the movie ticket service provider. Operator 1 sends this

response based on the validation of the introduction by Operator 2, which is in the same authentication domain as Operator 1.

- The authentication assertion is sent as part of the federation response, and the mobile user is allowed seamless access to the movie ticket provider site.

5.11 Human Resource Provider Identity Management

5.11.1 Introduction

The purpose of this use case is to illustrate how Identity Management (including single sign on) technology can be used to simplify a businesses ability to provide services to a broad set of clients/customers in the dynamic world of e-business. Within the Web Services paradigm, there are combinations of service providers and service requesters. In a B2B environment, different components are coupled to provide business transactions. The components need to be able to provide direct services or be part of a workflow. An end user can be a service requester or a "service" can itself be both a provider of a service to an end user and a requester of a service from a peer.

The goal of this usecase is to illustrate that both B2C and B2B environments need the same security and identity support (the B2C may be a subset of the B2B mostly driven by resource constraints in the B2C case). For web services to be consistent across both types of deployment the management and use of identity information within the web services model must be extensible and scalable.

5.11.2 Basic Use Case

5.11.2.1 Short Description

A Human Resources (HR) department of CompanyA is providing a portal service for employees, retirees, and perhaps even beneficiaries. The HR service provides a variety of identity management services to its end users, including providing single sign-on to multiple benefits-provider companies. The 401K provider(SafeInvestmentInc), the health insurance provider(XYZHealthCare), and other provider companies have agreed to trust the HR service to provide end user authentication (the HR-auth-svc). The solution, cannot require any client-side software beyond a standard HTTP 1.1browser, nor can we require any special hardware (e.g., we cannot require smart cards and card readers). Although one-time-password tokens are being investigated, the initial deployment remains with userids & passwords to authenticate this population. The solution needs to allow for the migration to new authentication mechanisms and supporting a number of types of mechanisms (since there will always be a migration).

Another goal for the corporate intranet portal is to display content seamlessly between internal and 3rd party computer systems. To achieve this goal, the corporate IT team would like to pull in content from the benefits provider based on the user permissions and preferences managed by HR's identity management services. When the user chooses to view content regarding their benefits, the corporate IT team would like the user to stay on the corporate portal with a consistent look and feel of the web site. The IT department is using Web Services to handle this content pull, along with the appropriate security across domains due to the sensitive nature of the data.

In addition to end users accessing these web services via the computers at their desks (and on the company intranet), a user can also log onto the companies portal from a mobile device either within the companies intranet or from the internet. The services that a user is allowed to select from are the ones that have established business relationships with CompanyA and that CompanyA and the provider (i.e., SafeInvetstmentInc) has determined the user is allowed to access. The selection of services can be determined by the business not necessarily only selected by the user.

Each year CompanyA also negotiates new contracts with its providers. When CompanyA changes providers new service providers may appear and others disappear. Employees change their status (retire, etc) frequently and new employees are hired/fired regularly. Retirees needs to access their benefits packages from sources outside the companies intranet, i.e.PCs at public libraries. The management of these federated-network identities may be added to the existing employee administration or may be outsourced to a third party but the identity management provider must have identification/authentication capabilities for up to 100,000+ retirees and perhaps another 100,000+ beneficiaries.

A user can also access specific services by directly accessing the provider company service (SafeInvestmentInc) at any of the provider companies portals/web sites if a trust agreement is in place between the two service providers. if an employee of CompanyA logs on at a provider site, there needs to be some means for the end user to indicate its home domain so the end user (an employee of CompanyA) will be redirected to the HR companies authentication site, and then redirected back to the provider site after successful authentication.

The 401K provider() needs to follow federal policy guidelines for privacy and uses an employee ID to identify the requester of its services.

The health insurance provider needs to follow the HIPPA guidelines and a different set of privacy constraints. The health insurance provider (sponsored by CompanyA) also offers health club credits to encourage healthy living. This is a benefit for active employees only. The employee must select this option under its insurance options. The service issues "vouchers" for employees to use at local health clubs. The vouchers are purchased by the employee(but allow the employee to access the health club for ½ price). The employee must use their own credit card to purchase the vouchers. There is also a service to find health clubs by location (both home and travelling).

A new provider of life insurance needs to be added to the HR Portal. Half of the 401K customers are already enrolled because they are also 401k customers. These employees will not get a new id, but use their 401K ids.

An employee is on his way home from his divorce proceedings and wants to change the life insurance beneficiary from his ex-wife to his daughter and access the HR portal on his cell phone.

5.11.2.2 Basic Flow

5.11.2.2.1 End user

An end user (at his/her home domain within a corporate intranet or on the internet) accesses a service (at a portal or a basic web site/point of contact). Since access to these services are protected, the user is asked to provide a claimed identity and proof of that identity (authenticate). There are several ways for this to be accomplished. A protocol may be supported by the service application (GSS/Kerberos/PKI) or the transport (SSL) may support an authentication protocol (BasicAuth). A previously acquired token could be presented and evaluated (Kerberos,SAML, X509 Attribute Certificate) by either the service application or an intermediary (I). Based on the trust relationships that exist between the mobile domain/ internet provider and the portal, the user may be authenticated differently than when they access a service via the corporate intranet and may be presented with a set of services for them (authorized) and tailored to the device/public location from which the access originated. At this original point of contact the "issuing party" (IP1) is the entity asserting the authentication information and the POC service receiving the authentication information is the "relying party" (RP1).

To complicate the flow, the initial point of contact may be an actual service provider (SP1) or an intermediary (I) providing some additional value/protection to the service endpoint. Based on the trust and business relationships that exist between the initial issuing party and the service or intermediary, the end user request may be re-directed or automatically routed to another relying party (RP2) or additional contact with the end user may be required (challenge/response for non-repudiation).

If the request has been automatically routed (there may be additional headers wrapping the original request) the service may need to not only validate the claims of the original issuing party but they may also need to validate "I" which is acting as an agent for the end user. In some cases, the service doesn't need to know about the original end user, but only relies on the request coming from an intermediary it trusts.

5.11.2.2.2 Service Provider

The initial service provider (SP1) may itself be a web service consumer….be part of a workflow or business process transaction. The SP(SP1) then may take the original request and initiate an action passing the original message request to another service provider (SP2) who may be a 3rd party in another trust domain. The "relying party" (SP2) may authenticate the portal/provider (SP1) before accepting the request on behalf of the user. The "relying party" may require additional information (i.e, for personalization) about the user or the "issuing party" of the user or intermediary and additional authenticated/secured message exchanges may be required. Continuing the initial service request may require protected exchanges with the original user or the user may be informed that he/she needs to be enrolled with an additional provider in order for the request to be processed.

The set of services presented to the end user may change each time the user access the service due to changes in service providers or due to the way in which the end user has accessed the service. The establishment and maintenance of trust must support dynamic reconfiguration of the business relationships.

5.11.2.3 Alternative Flow

5.11.2.3.1 Administrator

The administrator of web services needs to identify all parties in these transactions. Audit trails need to report on assigning identities, mapping identities, validating the identity proof, validating attributes, validating the association of identity and attributes.

Identity management includes enrollment, authentication, entitlements, privacy, assigning identity, , deriving authorization from identity, providing pseudonyms, providing attributes, identifying decision points and the scope of decision making attributed to each of the decision points (user, at the intermediary, at the app). Different roles can be played by the actors at each exchange. For example, the user can sometimes maintain the identity proof themselves (maintain a private key). Sometimes the “issuing party” will maintain the proof (provide an assertion of an authentication event).

5.11.2.3.2 Deployment

The deployment of web services needs to allow individual web services to support various forms of authentication, authorization, privacy, integrity and confidentiality. Some subset of this information also needs to be made available to potential requesters of the service (policies).

Assertions regarding trust policies must be securely communicated between the parties involved in establishing a business relationship. These policies need to be flexible and allow for the brokering of trust by a trusted third party when two individuals do not themselves have a trust relationship.

5.11.2.4 Actors

- User –
    - Employees
        - On a mobile device
        - On a terminal within corporate intranet
    - Retirees (on public internet)
    - Beneficiaries (recipients of payouts but not participants in a plan)
- Providers of Content
    - Human Resources
    - Sub-Contractor Service Providers
        - 401K provider
        - Health Insurance Provider
        - Life Insurance Provider
- Intermediaries
- Administrators/deployers of web services

  - ID Management
  - Portal Development

5.11.2.5 Roles

Relying Party

Issuing Party

Trust Agents

Intermediaries

Initial Point of Contact Services

5.11.2.6 Pre-conditions

- We already have means to authenticate current employees; but we now must build identification/authentication capabilities for up to 100,000+ retirees and perhaps another 100,000+ beneficiaries.
- Trust relationships have been established between HR and sub-contractor providers of content.
- User has created an account with a 401K provider, Health Insurance provider, and a Life insurance provider
- User has an account with the Human Resources Department.
- Human resources provider has made necessary arrangements (business and technical) with 401K, Health and Life Insurer provider to use single sign on provided by Human Resources Department.

5.11.2.7 Post-conditions

- A user has access to his/her information at each provider site.
- Information is protected from unauthorized access.

5.11.2.8 Operational and Quality of Experience Requirements

- **Privacy protection.** Single sign on technology must protect user's privacy, and not reveal any more personal data to each service provider than is needed to provide the service, and user has given his consent to.
- **Multiple Devices**. The service intends to support 80 year old retirees accessing their benefits packages from PCs at public libraries. This means we cannot require any client-side software beyond a standard browser, nor can we require any special hardware (e.g., we cannot require smart cards and card readers). We may not be able to afford one-time-password tokens. We may be stuck with userids & passwords to authenticate this population.
- **Performance.** Single sign on must have high enough performance so that it does not deteriorate user experience.
- **Trust-** Federation/Single Sign On is based on the assumption that clear expressions of trust can be established/exchanged between the issuing party and the relying party.
- **Secure Message Exchange-** Often a "request" by a user, translates into several message exchanges and it is important that the information contained in the request be adequately protected and that it arrive at its intended destination.

5.11.3 Technical Analysis

Access to Web Services is divided into several areas.

- **User authentication** including (in some cases) SSO
- **User authorization extending identity management**
- ***Content selection*** allows user to browse available content and make a selection.

- With ***Content download*** Human Resource service provider can reliably deliver content to a terminal.
- Secure Information Exchange allows non-browser environments to present information to the requester
- Secure Identity Management

5.11.3.1 Mapping to Available Technologies

[WS-Security] "Web Services Security Language", IBM, Microsoft, VeriSign, April 2002.

"WS-Security Addendum", IBM, Microsoft, VeriSign, August 2002. "WS-Security XML Tokens", IBM, Microsoft, VeriSign, August 2002

[WS-Security Minimalist Profile]

[WS-Policy] "Web Services Policy Framework", BEA, IBM, Microsoft, SAP, December 2002

[WS-Trust] "Web Services Trust", http://www-106.ibm.com/developerworks/library/ws-trust/, December 2002

[WS-PolicyAttachment] "Web Services Policy Attachment Language", BEA, IBM, Microsoft, SAP, December 2002

5.11.3.1.1 User authentication

WS-Security- Kerberos, PKI, SAML credential tokens.

5.11.3.1.2 Integrity/Confidentiality

WS-Security

5.11.3.1.3 Portals

WS-RP

5.11.3.2 Gap and Overlap Analysis

Single sign on is one aspect of security for web services that will be needed if mobile web services are to be successful. OMA currently does not have a single sign on technology. In the market place there are several single sign on vendors – most of which are not based on open standards, and thus should not be endorsed by OMA.

Single sign on is only ONE aspect of Identity Management. IM is also central to B2B web services. If OMA is to provide continuity and participate in end to end scenarios, it needs to have a solution which addresses this broader definition of web services and identity management.

6. Requirements (Normative)

6.1 High-Level General Requirements

6.1.1 General Requirements

General requirements applicable to Identity Management are:

1. Identity Management mechanisms specified by OMA MWS MUST be independent of the client device that the Principal uses to access a Provider.
2. Identity Management mechanisms specified by OMA MWS MUST work on existing network infrastructures, implying that such mechanisms MUST NOT require new network infrastructures.

6.1.2 Security Requirements

Security requirements applicable to Identity Management are:

1. Identity Management mechanisms specified by OMA MWS MUST take into consideration potential security threats, including Denial-of-Service attacks.
2. Identity Management mechanisms specified by OMA MWS MUST provide the ability for communicating Providers to authenticate each other.
3. Identity Management mechanisms specified by OMA MWS MUST support confidential communication between Providers.
4. Identity Management mechanisms specified by OMA MWS MUST support integrity protection in communication between Providers.
5. In identity Management mechanisms specified by OMA MWS, additional security MAY be performed by intermediaries.

6.1.3 Privacy Requirements

Privacy requirements applicable to Identity Management are:

1. Identity Management mechanisms specified by OMA MWS MUST support the ability for a Principal to use a pseudonym as an identity.
2. Mechanism for the federation of two identities between two Providers where the Principal's identity at one provider may be different from that at the other.
3. Mechanism for identity federation between two Providers such that the integrity of the Provider's identity management is preserved.
4. Provider1 which has federated the Principal's identity (P1) with Principal's identity (P2) at an Identity Provider (IdP1), and Provider2 which has federated the Principal's identity (P3) with Principal's identity (P2) at the same Identity Provider (IdP1), should not be able to collude to determine that the Principal's identities (P1 and P3) at these Providers belong to the same Principal.

6.2 Overall System Requirements

The overall system requirements have been categorized into two functional categories:

- Identity Federation and Management: This includes aspects of identity federation, de-federation, Single Sign-On (SSO) and Single Logout. Authentication context during SSO, delegation of federation, federation to an affiliation, authentication brokering, as well as privacy aspects regarding identity federation and management fall under this category.

- Attribute Sharing: This includes aspects of attribute transfer. Basic attribute transfer, anonymous attribute transfer, permission-based attribute transfer, discovery service, attribute brokering, Principal interaction as well as privacy requirements regarding attribute transfer fall under this category.

Some of the requirements in the Identity Federation and Management category are also applicable for achieving Attribute Sharing. For instance, attribute sharing may also utilize identity federation. The classification above is not intended to mean that Requirements that fall within the 'Identity Federation and Management' category are all not applicable for Attribute Sharing.

6.2.1 Identity Federation and Management Requirements

The Identity Federation and Management requirements include aspects of identity federation, de-federation, Single Sign-On (SSO) and Single Logout. Authentication context during SSO, delegation of federation, federation to an affiliation, authentication brokering, as well as privacy aspects regarding identity federation and management fall under this category. The requirements are:

1. Providers MAY establish a Circle of Trust.

2. (a) Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Service Provider to discover one or more Identity Providers that the Principal has an identity at and which the Principal is currently authenticated by, prior to federation of the Principal's identity at the Identity Provider with the Principal's identity at the Service Provider.

   (b) Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Service Provider to discover one or more Identity Providers that the Principal has an identity at and which the Principal is currently authenticated by, subsequent to federation of the Principal's identity at the Identity Provider with the Principal's identity at the Service Provider.

3. Identity Management mechanisms specified by OMA MWS MUST support a mechanism to federate Principal's identity at one Provider with Principal's identity at another Provider.

4. (a) A Provider MUST be able to obtain and store consent of the Principal to federate identities.

   (b) A Principal MAY delegate consent to federate its identity, in which case the Provider must store that the federation occurred because of the delegated consent.

5. Upon request, a Provider MUST be able to produce a record of the Principal's consent or delegated consent for identity federation.

6. A Provider MAY be required to maintain evidence to support a claim of non-repudiation for either the Principal consent or the delegated consent, if the terms of the trust relationship between the Principal and the Provider requires it.

7. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Provider to prompt the Principal for consent to federate that Principal's identity at one Provider with the Principal's identity at another Provider.

8. Identity Management mechanisms specified by OMA MWS MUST support a:

   (a) Mechanism for a Principal to supply information in a message to a Service Provider which indicates Principal's consent to allow the Service Provider to federate their identity at the Service Provider with their identity at an Identity Provider.

   (b) Mechanism for a Principal to store consent to federate their identity in a profile/configuration on a terminal.

(c) Mechanism for a Principal to store consent to delegate the ability to federate their identity in a profile/configuration file on a terminal.

9. Identity Management mechanisms specified by OMA MWS MUST support:

   (a) Mechanism to de-federate Principal's identity at one Provider with Principal's identity at another Provider.

   (b) Ability for a Principal to initiate a de-federation.

   (c) Ability for a Principal to delegate the authority to de-federate its identity.

   (d) Ability for a Provider to initiate a de-federation.

10. When the terms of business relationship require it, Provider MUST notify another of one or more de-federation requests.

11. When de-federation occurs, a Provider that has collected any information about federating the Principal's identity MUST delete the information that was created at the time of federation.

12. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for one Provider to notify another Provider of one or more de-federation requests.

13. The types of authentication mechanisms SHOULD be able to be constrained by the business agreements between two Providers.

14. (a) Identity Management mechanisms MUST NOT be limited to (i.e. constrained by) one or more authentication mechanisms.

    (b) Identity Management mechanisms MUST permit Providers to change acceptable authentication mechanisms.

15. Identity Management mechanisms specified by OMA MWS MUST support a:

    (a) Mechanism for a Service Provider to request an Identity Provider for an authentication assertion corresponding to a Principal.

    (b) Mechanism that allows the request in (a) to be redirected through a Principal.

16. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for an Identity Provider to respond to a Service Provider with an authentication assertion corresponding to a Principal.

17. Identity Management mechanisms specified by OMA MWS MUST support a means for a Service Provider to indicate to an Identity Provider the acceptable type(s) of authentication mechanism(s) that the Identity Provider may use to authenticate the Principal.

18. Identity Management mechanisms specified by OMA MWS MUST support

    (a) A means for an Identity Provider to indicate to a requesting Provider that the requested authentication mechanism(s) is not supported by it.

    (b) A means for an Identity Provider to indicate to a requesting Provider the specific type(s) of authentication mechanism(s) supported by the Identity Provider.

19. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for the Identity Provider to convey to other Providers the authentication method(s) that was used to authenticate the Principal.

20. Identity Management mechanisms specified by OMA MWS MUST support

    (a) A mechanism for the Identity Provider to convey to other Providers the authentication method(s) that was used to authenticate the Principal.

(b) A mechanism for a Provider to request re-authentication of the Principal by the Identity Provider.

(c) Mechanism that permits a Provider to re-authenticate a Principal.

21. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a single sign-out.

22. The initial point of contact for a service MAY be a service provider.

23. The service agreement between the Principal and the Attribute Provider, the Identity Provider and the Service Provider SHOULD govern aspects such as when or how and under what conditions actions by the Principal or the Principal's delegate may be permitted.

24. Business agreements and potentially trust relationships MAY be needed between the entities belonging to an affiliation.

25. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Service Provider that is a member of an affiliation to request federation of a Principal's identity at an Identity Provider with the affiliation.

26. Identity Management mechanisms specified by OMA MWS MUST support

    (a) Mechanism for a Provider to request another Provider for a list of members in an affiliation.

    (b) Mechanism for the list of members of an affiliation to be protected from unauthorized modification during exchange.

    (c) Verification of identities of the providers according to the business and trust policies that define participation in the affiliation.

27. Identity Management mechanisms specified by OMA MWS MUST support a

    (a) Mechanism for a Provider to convey in a request that it is acting on behalf of an affiliation.

    (b) Mechanism for a Provider to optionally present the appropriate proof of the delegated authority it claims to have.

28. Identity Management mechanisms specified by OMA MWS MUST support a mechanism and guidelines for a Provider to verify that another Provider is a member of an affiliation.

29. Identity Management mechanisms specified by OMA MWS MUST support a

    (a) Mechanism for a Provider to introduce two other Providers to each other within the same Circle of Trust.

    (b) Mechanism for a Provider to introduce two other Providers to each other within different Circles of Trust.

    (c) Mechanism for a Provider to act as a broker of trust.

    (d) Mechanism for a Provider to securely convey the address of another Provider in a response message.

30. Business agreements established between Providers MAY govern whether a Provider can introduce two Providers to each other.

31. Provider MUST be able to convey to another Provider that it has terminated its business relationship with another Provider.

32. When the terms of business relationship require it, Provider MUST convey to another Provider that it has terminated its business relationship with another provider.

33. Identity Management mechanisms specified by OMA MWS MUST support the ability and provide guidelines for a Provider to determine that it had previously introduced two other Providers to each other across Circles of Trust.

34. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Provider to convey a chain of authentication assertions in its response to another Provider.

35. When chains of authentication assertions are sent, they MUST be protected from unauthorized modification (insertion, deletion etc.) of other authentication assertions.

36. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Provider to differentiate between a single authentication assertion and a chain of authentication assertions.

37. Different trust models MAY exist for single authentication assertions and “chains” of authentication assertions.

38. Identity Management mechanisms specified by OMA MWS MUST support a mechanism and provide guidelines for two Providers belonging to different Circles of Trust to securely obtain information about each other.

39. Audit trails MAY need to collect/report on the assignment of identities, the linking of identities, the validating of identities and the association of an identity with attributes.

6.2.2 Attribute Sharing Requirements

Attribute sharing requirements include aspects of attribute transfer. Basic attribute transfer, anonymous attribute transfer, permission-based attribute transfer, discovery service, attribute brokering, Principal interaction as well as privacy requirements regarding attribute transfer fall under this category. The requirements are:

1. Different attributes of the same Principal MAY be stored on different Attribute Providers.

2. Identity Management mechanisms specified by OMA MWS MUST support:

   (a) Ability for a Principal or Principal’s delegate to store, modify or delete Principal’s attributes at an Attribute Provider.

   (b) Subject to Principal’s consent, ability for the Provider to identify context, including context surrounding Principal’s attributes. (needs clarification on text)

3. Identity Management mechanisms specified by OMA MWS MUST support

   (a) Ability of Principal to set permissions for the release of Principal’s attributes stored at an attribute provider.

   (b) Ability of an Attribute Provider to indicate its policy for attribute release to Principals.

   (c) Guidelines for an Attribute Provider to check permissions prior to attribute release.

4. Identity Management mechanisms specified by OMA MWS MUST support a mechanism that allows a Service Provider to query an attribute provider or attribute broker for an attribute class.

5. Identity Management mechanisms specified by OMA MWS MUST support the ability for a Principal to be able to set the permissions associated with the release of Principal’s attributes including indicating whether or not they allow brokers to aggregate their attributes.

6. (a) Attribute query by a Service Provider to an Attribute Broker MUST be identical to an attribute query by a Service Provider to an Attribute Provider.

(b) Identity Management mechanisms specified by OMA MWS MUST support the ability for a Service Provider not to know whether the entity that it is querying is an Attribute Broker or an Attribute Provider.

7. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for an Attribute Broker to obtain attributes from different Attribute Providers and aggregate them.
8. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Service Provider to query an Attribute Provider or Attribute Broker for multiple attribute classes in a single request.
9. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for an Attribute Provider or Attribute Broker to convey multiple attribute classes in a single response.
10. Identity Management mechanisms specified by OMA MWS MUST support asynchronous attribute responses.
11. Identity Management mechanisms specified by OMA MWS MUST support a mechanism that allows a Service Provider to query for a Principal’s attributes without associating the identifier used in the query with the identity of the Principal.
12. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Service Provider to deny a request for a service and the ability to convey denial reason if appropriate.
13. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Provider that receives a request to respond with partial information.
14. Identity Management mechanisms specified by OMA MWS MUST support the ability for a Provider to indicate and provide proof that the contents of the message being sent are under a business agreement.
15. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for a Service Provider to associate usage directives with the corresponding attributes that are being requested.
16. Identity Management mechanisms specified by OMA MWS MUST support a mechanism for an Attribute Provider to associate usage directives with the corresponding attributes that are being included.
17. When the usage directive in the attribute request does not satisfy the permissions set by the Principal for release of the attribute class, Identity Management mechanisms specified by OMA MWS MUST support a mechanism for the Attribute Provider or Attribute Broker to deny the request and optionally include a list of acceptable usage directives for release of the attribute class.
18. Identity Management mechanisms specified by OMA MWS MUST providegGuidelines for an Attribute Provider to determine whether a certain usage directive is privacy-stricter than another.
19. Identity Management mechanisms specified by OMA MWS MUST support a
    (a) Mechanism that allows an attribute provider or attribute broker to register at a discovery service.
    (b) Mechanism that allows an attribute provider or attribute broker to include the attribute classes that it supports, in the registration performed in (a).
    (c) Mechanism that allows a Service Provider to query a Discovery Service for the Attribute Provider(s) or Attribute Broker(s) that hosts the Principal’s attribute class(es).
20. When a Provider or Broker registers at a Discovery Service, Identity Management mechanisms specified by OMA MWS MUST support the ability by the Discovery Service to verify authorization of such a registration.
21. When a Service Provider queries an Attribute Provider or Attribute Broker for one or more attribute classes of a Principal, Identity Management mechanisms specified by OMA MWS MUST support the
    (a) ability by the Attribute Provider or Attribute Broker to query the Principal directly

(b) ability by the Service Provider to redirect the Principal to the Attribute Provider or Attribute Broker, so that the Attribute Provider or Attribute Broker may query the Principal

(c) ability by the Service Provider to query the Principal and pass the result to the Attribute Provider or Attribute Broker.

22. When a Service Provider queries an Attribute Provider or Attribute Broker for one or more attribute classes of a Principal, there MUST be a trust relationship between the entities involved in the request. Such a trust relationship includes direct trust as well as brokered trust.

23. Identity Management mechanisms specified by OMA MWS MUST support a mechanism that allows an attribute provider or attribute broker to register and de-register at a discovery service any previously supported attribute classes of a Principal.

Appendix A. Change History (Informative)

Version Name	Date	Section	Description
	August 4, 2003		Initial Version taken from MWS
	November 18, 2003		Comments from Requirements group incorporated
OMA-RD_MWS_NI-V1_0-20031120-A	November 20, 2003		Version changed to 1_0