Identity Management Framework Requirements

Candidate Version 1.0 – 02 Feb 2005

Open Mobile Alliance

OMA-RD-Identity_Management_Framework-V1_0-20050202-C

Contents

Figures

Tables

1. Scope (Informative)

The intention of this Requirements Document is to tie together all existing efforts relating to Identity within the OMA in order to create a single Identity Management (IdM) enabler to be used by all OMA enablers. This document sets requirements for all technical working groups of OMA, and all Identity Management related functions should be satisfied according to the resulting enabler. The benefits of a single Identity Management enabler for all OMA enablers are:

- Management and use of Identity or personal information is easier for all stakeholders: End Users, mobile operators, enterprises and Service Providers;
- End Users do not have the burden of having to understand different service-specific Identity solutions;
- The same Identities and personal information can be utilised by multiple services;
- Privacy protection can be enabled more easily using a common Identity Management enabler;
- The OMA will not be seen to publish specifications with disparate, conflicting Identity Management solutions;
- Identity needs are the same (or very similar) for all enablers and so, by creating a single Identity Management enabler, duplication of work is kept to a minimum;
- New enablers with Identity requirements will be able to benefit from the existing Identity Management enabler;
- Greater interoperability between enablers;
- Improved time to market for those enablers that use the Identity Management enabler.

There are also additional benefits if existing, standardised Authentication / Authorisation methods can be re-used in an Identity Management enabler. One such example is mobile operator subscription-based Identity:

- Mobile operators already have an excellent trust relationship with millions of End Users due to their high level of security;
- Mobile operators can offer services of their own, or third party services, with improved Authentication and privacy protection by using IDP and Identity Broker models;
- Mobile operators can offer content Service Providers simple, event-based billing services suitable for low-value transactions.

Therefore a key overall requirement for the OMA Identity Management enabler is to enable (at least) the use of existing mobile operator Identity solutions for Authentication and End User Authorisation (e.g. the use of SIM Smart Cards, R-UIM Smart Cards and IS41 software solutions, depending on prioritisation).

This Requirements Document includes in its scope the following types of Identities:

- **End User Identity**: relating to the provisioning of and access to End User Identity information and related Attributes in the mobile operator, Service Provider, enterprise infrastructures and in the Device. This includes the management (e.g. conflict resolution) of several simultaneous Identities (for one End User) that enable multiple End User profiles, such as employee and a private customer profiles. Delegation and sharing of authority is also included in scope in order to enable the role of an intermediary Agent (e.g. for some enterprise situations).
- **Provider Identity**: for Authentication and to support delegation of authority.
- **Device Identity**: to enable topics such as digital rights management, for example.
- **Application / Service Identity**: to identify enterprise applications, for example, or enable the use of Identity Containers.

It should be noted that all OMA work is contribution driven, so it is always necessary to prioritise topics in terms of which are specified within the initial phase of work, and which are listed as requirements for a future specification phase.

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

[MWS NI RD] "MWS Network Identity Requirements", Open Mobile Alliance™
OMA-RD_MWS_NI-V1_0, http://www.openmobilealliance.org/

[OWSER 1.0 NI] "OMA Web Services Enabler (OWSER): Network Identity Specifications", Open Mobile Alliance™
OMA-OWSER-Network_Identity-Specification-V1_0, http://www.openmobilealliance.org/

2.2 Informative References

[DM-Charter] OMA Device Management Working Group Charter, Nov. 12, 2002
http://member.openmobilealliance.org/ftp/Public_documents/DM/charter/OMA-TP-2002-0128-DM-Charter.doc

[Lib-Arch] "Liberty ID-FF Architecture Overview", Version 1.2
http://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf

[RFC2828] "Internet Security Glossary", R. Shirley, IETF RFC 2828, May 2000
http://www.ietf.org/rfc/rfc2828.txt

[RFC3060] "Policy Core Information Model -- Version 1 Specification", B. Moore, E. Ellesson, J. Strassner, A. Westerinen, IETF RFC 3060, February 2001
http://www.ietf.org/rfc/rfc3060.txt

[RFC3198] "Terminology for Policy-Based Management", A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry, S. Waldbusser, IETF RFC 3198, November 2001
http://www.ietf.org/rfc/rfc3198.txt

[RFC3460] "Policy Core Information Model (PCIM) Extensions", B. Moore, Ed., IETF RFC 3460, January 2003
http://www.ietf.org/rfc/rfc3460.txt

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

Access Control	The process of restricting access to the resources of a system only to appropriately authorised Entities that have been previously authenticated (at an appropriate level).
Access Control Policy	A Policy that is enforced in the Access Control process.
Access Network	A network, with which Devices interact in order to get access to services.
Account	A formal business agreement between a Principal and a Provider, which allows for service consumption.
Address	A unique Identifier of an Entity in a network, used by another Entity for the purpose of communicating with it.
Affiliation	See Alliance
Agent	An Entity with the proper Authorisation to act autonomously on behalf of other Entities.
Alliance	An agreement between two or more independent Entities that defines how they will relate to each other and how they jointly conduct activities.
Assertion	A collection of one or more statements about a Principal (e.g. Authentication statement or Authorisation statement).
Attribute	An Attribute is a characteristic that describes a Principal.
Attribute Class	A pre-defined set of Attributes (e.g. the constituents of the Principal’s name, such as prefix, first name, last name, suffix). An Attribute Class could be defined either in an IdM specification or by business agreements.
Attribute Provider	A special type of Service Provider, whose service is to provide Attributes about a Principal.
Attribute Transfer	Transmission of a Principal’s Attribute from an Entity (i.e. an Attribute Provider) that manages it, on behalf of the Principal, to an Entity that requests it (e.g. a Service Provider).
Authentication	The process of verifying an Identity claimed by (or for) a Principal.
Authentication Assertion	An Assertion that can be sent from one Identity Provider (or an Identity Broker) to another Provider, which describes a successful Authentication of a Principal. An Authentication Assertion may also contain information such as for how long the Assertion is valid. An Authentication Assertion will also often include an Authentication Context, to notify the Provider what form of Authentication was used.
Authentication Context	The set of parameters (time, location, transaction value, etc.) within which a specific Authentication instance is acceptable, emphasising that a single Authentication instance may need to be re-established, perhaps with different mechanisms or classes of mechanisms, when some parameter changes.
Authentication Domain	Two or more Service Providers, one of which must be an Identity Provider, that have business relationships and operational agreements, and with whom Principals can interact in a secure and apparently seamless way. An Authentication Domain can only have one Identity Provider, but can have multiple Principals and multiple Service Providers. If two Identity Providers are involved, then this would be an example of two Authentication Domains. If the two Identity Providers also have business relationships and operational agreements, then these two Authentication Domains would, together, be called a Circle of Trust.
Authorisation	A right or permission that is granted to a system Entity to access a system resource, or the process of granting the right or permission [RFC 2828].
Circle of Trust	Two or more Authentication Domains, where the Identity Providers involved also have business

	relationships and operational agreements with each other.
Container	See Identity Container
Credential	See Identity Credential
De-Federation	A reversal of the process of Federation of two Accounts (belonging to the same Principal), or termination of the state of Identity Federation. De-Federation usually involves an exchange of messages among the systems which established the Identity Federation.
Device	A Device is a voice and/or data terminal that uses a wireless bearer for data transfer. Device types may include (but are not limited to): mobile phones (GSM, CDMA, 3GSM, etc.), data-only terminals, PDAs, laptop computers, PCMCIA cards for data communication, unattended data-only Devices (e.g. vending machines), and, when in a suitable terminal, Smart Cards (e.g. GSM SIM Smart Cards).
Device Management	The mechanisms and processes for managing Devices, including setting initial configuration information in Devices, subsequent updates of persistent information in Devices, retrieval of management information from Devices, and processing events and alarms generated by Devices. [DM-Charter]
Device Management Server	A computer or Device on a network which performs Device Management.
Device Management Tree	A data tree used for containing Device Management objects (information settings) on a Device.
Discovery Service	A service that allows requestors to discover resources and how to access those resources.
End User	An End User is a (human) user of a service. An End User is therefore a subset of the term Principal.
Entity	A thing with distinct existence. In this document the term Principal is regularly used as a subset of Entity, more specific to the Entities involved in an Identity Management enabler.
Event Token	An Event Token is a token that can be used: to allow access to an event; as a reference to an End User's Account; to enable the processing of payment for an End User's outstanding Account balance (for example, at a ticketing gate to access a theatre, or for drink purchase).
Federation	The binding of two or more Accounts (within an Authentication Domain or a Circle of Trust, where one of the Accounts is at an IDP) for a given Principal. Federation does not imply that Identity Attributes are being shared – it is simply a joining of two or more Accounts (e.g. for Single Sign On), after which Attributes could then be shared.
Group	An identifiable list of contacts (e.g. a list of URIs).
Identifier	A reference that uniquely maps to an Identity. One or more Identifiers are among the characteristics that define an Identity.
Identity	The characteristics by which an Entity or person is recognised or known.
Identity Broker	A special type of Identity Provider that receives requests for Identity information from a Service Provider and subsequently requests that information from other Provider(s). The Identity Broker aggregates the data and responds to the originating Service Provider.
Identity Container	An Entity that can be used to store, transport, process, dispose of, or otherwise handle Identity information.
Identity Credential	Data that is transferred or presented in order to attest to, or establish, the claimed Identity of a Principal, or the claimed Authorisation permissions of that Principal.
Identity Management	The management of Identity information, both internally and when it is passed from one Entity to another.
Identity Provider	A special type of Service Provider role that creates, maintains, and manages Identity information for Principals, and can provide an Authentication Assertion to other Service Providers within an Authentication Domain (or even a Circle of Trust).
Non-repudiation	Non-repudiation is the prevention of an End User wrongly denying having performed an action, in particular: - Accountability: The property of a system (including all of its system resources) that ensures that the actions of a system Entity may be traced uniquely to that Entity, which can be held responsible for its actions; - Proof of Origin: Presentation of evidence of having sent a message;

	- Proof of Delivery: Presentation of evidence of having delivered a message; - Proof of Receipt: Presentation of evidence of having received a message.
Payment Service Provider	A Service Provider whose service is to authorise and bill for financial transactions and then provide clearing services.
Policy	An ordered combination of Policy Rules that defines how to administer, manage, and control access to resources. (Derived from [RFC3060], [RFC3198] and [RFC3460])
Policy Rule	A combination of a condition and an action to be performed if the condition is true.
Principal	An Entity that has an Identity, that is capable of providing consent and other data, and to which authenticated actions are done on its behalf. Examples of Principals include an individual End User, a Group of End Users, a corporation, service enablers / applications, system Entities and other legal Entities.
Principal Agent	An IdM role that represents Principals in Identity Management interactions. Examples of Principal Agents are user interfaces in Devices, Devices themselves, SIM Smart Cards, the business support system of a mobile operator, etc. A Principal Agent can be thought of as a delegated source of Identity information.
Privacy Settings	Privacy Settings describe the rights and limitations of access to and processing of personal data (of an End User). Privacy Settings may be expressed in terms of access rules that determine a Policy with respect to the privacy protection of personal data of an End User towards requestors.
Provider	An Entity that performs one or more of the roles in an Identity Management enabler, for example an Attribute Provider, Service Provider or Identity Provider.
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.
Rights Object	A collection of permissions, constraints and other Attributes, which define under what circumstances access is granted to, and what usage is allowed for, DRM Content.
Service Provider	An Entity that provides services and/or goods to Principals.
Session	An active connection between two or more Entities for the purpose of communicating and transferring information.
Single Log Out	The ability for End Users to properly terminate all open connections, active services or relationships associated with a Single Sign On (SSO) Session, with one logout process.
Single Sign On	The ability to use an Authentication Assertion from one Provider (an Identity Provider or an Identity Broker) at another Provider, in order to ease the burden (for a Principal) of having to authenticate to each Provider separately within a single Session.
Smart Card	A secure, removable Device, used to store, process and transmit information, such as Identifiers and Identity Attributes. Subscriber Identity Module (SIM) Smart Cards and Removable User Identity Module (R-UIM) Smart Cards are examples.
Usage Directive	A set of instructions or rules describing how a particular Attribute would / can subsequently be used by the Service Provider once the Attribute has been released to it.

3.3 Abbreviations

AD	Authentication Domain
AP	Attribute Provider
DRM	Digital Rights Management
GUP	Generic User Profile
IdM	Identity Management
IDP	IDentity Provider
IM	Instant Messaging
IMSI	International Mobile Subscriber Identity

ISP	Internet Service Provider
MDN	Mobile Directory Number
MIN	Mobile Identification Number
MSISDN	Mobile Station Integrated Services Digital Network (End User phone number in GSM networks)
MTSP	Movie Ticket Service Provider
MWS	Mobile Web Services
MWS NI RD	Mobile Web Services Network Identity Requirements Document
OMA	Open Mobile Alliance
OWSER	OMA Web Services Enabler Release
P2P	Person 2 Person
PEEM	Policy Evaluation, Enforcement and Management
PoC	Push-to-talk over Cellular
SIM	Subscriber Identity Module
SLO	Single Log Out
SSO	Single Sign On

4. Introduction (Informative)

Identity or personal information is needed in most mobile services (implemented using enablers and applications) for: identifying the communicating Entities; controlling access to services; personalisation; charging or billing. Communication can happen between an End User and a service, between two or more End Users, or between two or more services. In all cases the questions to be answered are:

- How can Identities or personal information about other parties be *discovered*?
- How can Identities or personal information be *transferred* from one party to another?
- How can the owner of the information control the availability, visibility, and use of their Identity or personal information?

Various proprietary and standardised Identity solutions are used today. However, as mentioned above, there are several benefits if all services use a single Identity Management enabler. The high level objective of this Requirements Document, therefore, is to capture the requirements for an Identity Management enabler suitable for all OMA enablers, covering Identity discovery (i.e. what Attributes are available) and transfer, and management of Identity information availability.

The first step in defining the requirements for the Identity Management enabler is to identify the key Entities, roles within those Entities, and relationships between those roles.

4.1 Strategy and Approach

The task of creating the right set of requirements for an Identity Management enabler is faced with the typical trade-off between completeness and consistency on one side, versus resource and time-to-market on the other side. Furthermore, the development of requirements in the OMA must also deal with the reality of the input contribution driven process. As a consequence of these realities the creation of these requirements was achieved through an iterative process, approaching the total applicable scope as a continuum and addressing it in steps governed by the above-mentioned realities. In order to manage these steps the end points for the work must be defined.

4.1.1 End Points

At one end point (the start) of the total applicable scope for an Identity Management enabler it is necessary to define the Identity ecosystem. This definition must include all information required to ensure that all Working Groups of the OMA (and ideally the whole mobile industry) have a consistent understanding of Identity Management. The definition must therefore include (at least):

- All roles of the ecosystem;
- The relationships between the roles of the ecosystem;
- A definition of all Identity-related interactions between the roles.

At the other end point (the end) of the total applicable scope is a complete and consistent specification, driven by a consistent set of requirements, which addresses all interactions defined by the first endpoint.

4.1.2 Co-ordination

In reality the process of creating an Identity Management enabler was started before this strategy was in place, but all work completed prior to the creation of this strategy is consistent and supportive of it.

Before the creation of this strategy the OMA MWS Working Group identified an immediate need to address certain aspects of Identity Management (Single Sign On, Single Log Out, Federation of Accounts, Identity Attribute Sharing) in the context of Mobile Web Services. Therefore the MWS Working Group produced a set of ‘Network Identity’ requirements [MWS NI RD] to address this need. These requirements were approved by the OMA TP in November 2003.

The MWS Working Group also developed a specification, as part of the OWSER 1.0 MWS [OWSER 1.0 NI] candidate enabler, to address the first half of the MWS NI Requirements (those requirements relating to Single Sign On, Single Log Out and Federation of Accounts).

Due to the success of the MWS Working Group in creating a specification to address the first half of the requirements in a timely and efficient way the OMA Requirements Identity Management Breakout Group recommended that the MWS Working Group should create a specification to address the remaining, TP-approved Network Identity requirements. This work was progressed in parallel to the REQ IdM breakout requirement development work. Therefore, in order to ensure alignment between the MWS NI specification work and the Requirements IdM work, joint meetings were held to discuss and agree how the existing MWS NI requirements would be adopted in the OMA IdM RD.

The vision of the IdM Breakout Group is that the evolution of the specifications should be as follows:

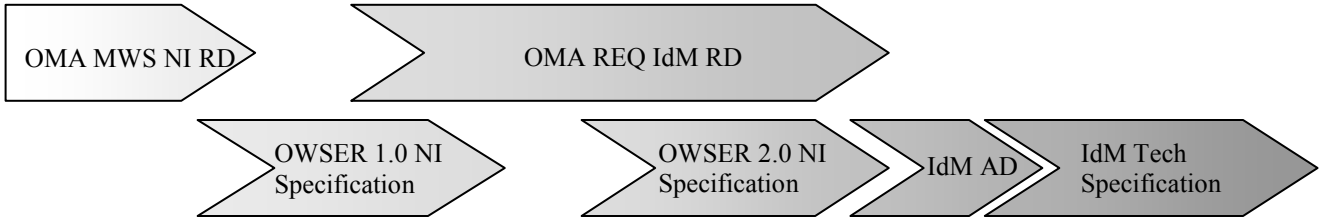

Figure 1: Vision for Evolution of Identity Management Specifications in the OMA

The IdM vision is to ensure that the Requirements Documents and the Specifications all build upon each other, in order to ensure backwards compatibility. It is also intended for the IdM RD to supersede the MWS NI RD, and likewise for the IdM AD and Technical Specification to build on and supersede the OWSER NI Specifications. After completion of the IdM specification, all future development of Identity related topics should be carried out within the development of future phases of the Identity Management enabler.

4.1.3 Topics included in the Identity Management Enabler

The following topics were discussed regarding their possible inclusion in the IdM analysis work. The discussion led to the selection of those topics shown as high priority for analysis within the scope of IdM.

High Priority	Medium Priority	Low Priority
Location	Data Synchronisation	Broadcast (covered in Download)
Download and DRM	WAP Push	OMA Service Provider Environment (covered in EPEM)
Device Management	Browsing	Integrated Messaging
Push to talk over Cellular		MMS
Presence		Creating a business agreement on the fly
Execution Policy Enforcement Management		Standard Transcoding Interface
Mobile Web Services		Multi-Modal
Enterprise		Proxy-based redirect
Charging		
Privacy		
Group Management		
User Agent Profile		
M-Commerce		
Content Screening		
IMS		
Instant Messaging		
Gaming		

Table 1: Topic Priorities for Inclusion in the OMA REQ Identity Management RD

Having selected the high priority topics to be covered within the Identity Management enabler, these choices were socialised with the wider OMA Requirements community.

Note that if the Identity needs of OMA change in the future (as new Enablers are introduced, or as Enablers develop), then a new version of the IdM RD could be developed, in order to address the new needs.

4.1.4 Process

The existing, TP-approved Network Identity requirements from the MWS Working Group provided an important building block in the set of requirements for the Identity Management enabler. In order to build on this work to the fullest extent, the Requirements IdM Breakout approach was to take the MWS NI requirements as a base line and, where appropriate, add more requirements to address the requirements of all OMA enablers. These requirements were derived from two sources, as follows:

- Exploration and analysis, from an Identity perspective, of existing use cases and Requirements Documents available from other OMA Working Groups;
- Exploration and analysis, from an Identity perspective, of new use cases and potential requirements submitted to the REQ IdM Breakout Group by member companies.

The actual process for extracting additional requirements (to the existing MWS NI requirements) was as follows:

1. For every use case submitted, the potential relevance to an Identity Management enabler was highlighted.
2. For those use cases deemed relevant to an Identity Management enabler an analysis was conducted in order to:
   - Determine whether the issue *contradicted* existing MWS NI requirements;
   - Capture any new requirements not covered by the MWS NI requirements.

   Had there been any contradictory requirements, then a decision would have had to be made whether to change the existing MWS NI requirements. However, this was not the case.
3. Review by the IdM Breakout Group to determine whether the proposed new requirements should be added to the IdM requirements.

Using this process it was possible to develop the existing MWS NI Requirements Document to include the Identity needs of all the (high priority) OMA enablers.

4.1.5 Identity Management Enabler Requirements Document

This Requirements Document is a single, complete set of requirements for an Identity Management enabler, and the REQ IdM Breakout Group proposes that OMA MWS and Architecture Working Groups (as well as all other OMA enabler working groups) should use this document (or future releases of it) for all Identity needs within the OMA, including any future specification work. All existing MWS NI requirements are included in this document (although the wording has been updated to ensure consistency, and some duplication was removed).

It is not thought that the current set of requirements will completely address all feasible Identity related aspects of a particular set of relationships between roles of the ecosystem. This is due to the nature of the realities described above (input contribution approach), and the desire of the IdM Breakout Group to release a set of market-driven requirements in a timely manner.

All of the requirements in this Requirements Document are owned by, and the responsibility of, the OMA Requirements Group.

4.2 Identity Management ecosystem

The Identity Management ecosystem is described in three steps. The first step is a set of two diagrams that shows how the different actors involved in Identity Management interact both today and according to the IdM vision. The second step describes a set of simplified Identity Management roles that the different actors in the ecosystem can implement and the interactions that would happen between them. The third step describes the relationship between the Identity Management

enabler and the OMA Policy enforcement infrastructure. The purpose of the ecosystem is to clarify the scope covered by the IdM RD, and to introduce some terminology that is used in this document.

4.2.1 Identity Management interactions, today and according to the IdM Vision

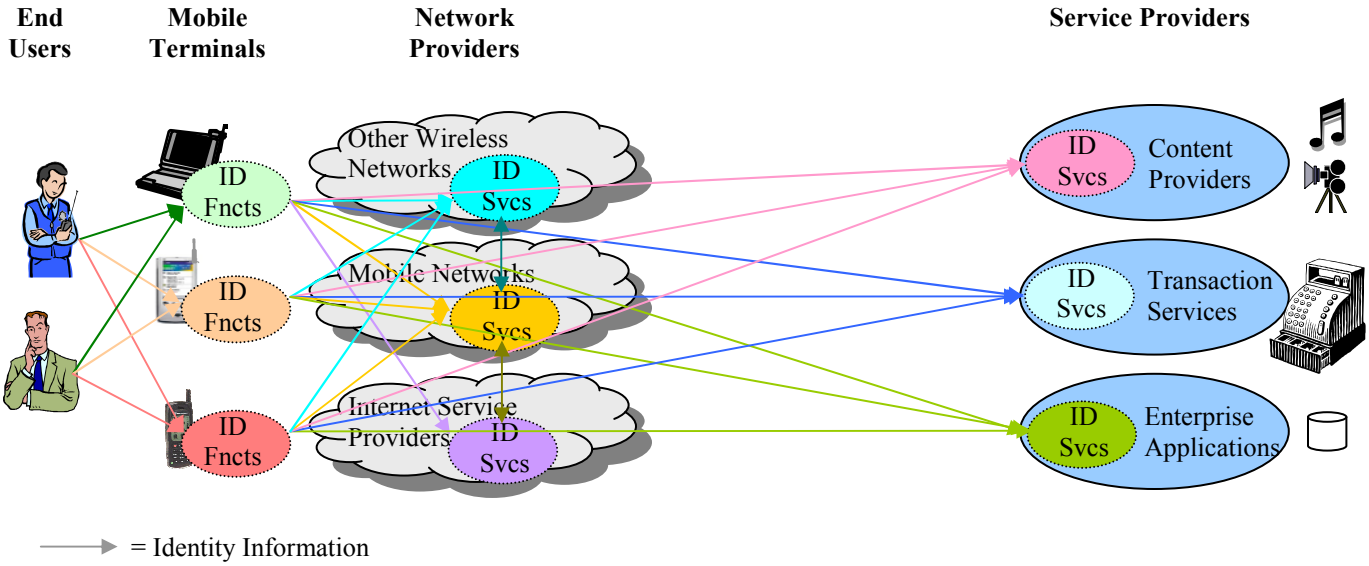

Figure 2: Identity Management ecosystem today

As can be seen in Figure 2, each different actor / role in the ecosystem has its own implementation of Identity Management (represented by the different colours) so there are many different vertical, Identity 'silos'. The IdM ecosystem vision, shown in Figure 3, shows that the actors / roles in the ecosystem can re-use other Identity functions in the ecosystem, using the Identity Management enabler to mediate between them.

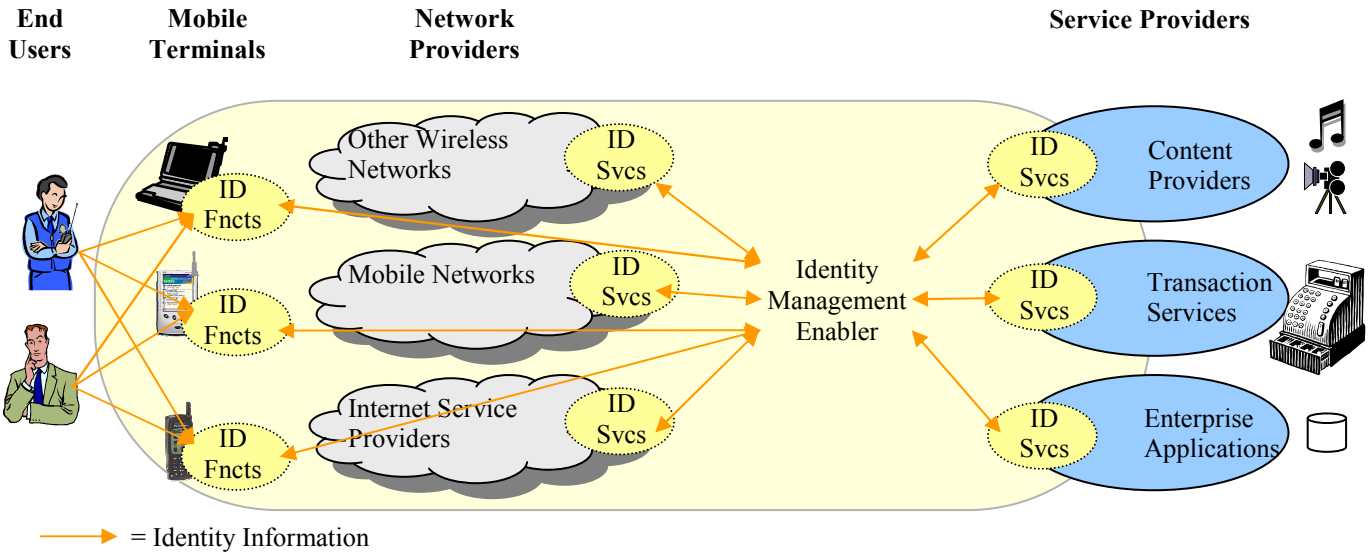

Figure 3: IdM vision for the future Identity Management ecosystem

4.2.2 Roles and Interactions in the IdM ecosystem

The IdM enabler provides the mechanisms by which the actors in the IdM ecosystem can interact to exchange Identity information. These mechanisms comprise:

1. The ability to discover Identity information;
2. How Identity information can be transferred from one Entity to another;
3. The ability to control the availability, visibility, and use of Identity information (and the associated provisioning aspects relating to this).

These are the roles that the different actors of the Identity Management ecosystem can implement and utilise:

- **Principal Agent**

  A Principal is an Entity that has an Identity, and owns all Identity information about itself. Examples of Principals include human beings (End Users), a Group of End Users, a corporation, service enablers / applications, system Entities and other legal Entities.

  A Principal Agent is an IdM role that represents 'real world domain' Principals in the electronic domain for the purposes of Identity Management interactions. Examples of Principal Agents are user interfaces in Devices, Devices themselves, SIM Smart Cards, the business support system of a mobile operator or enterprise, etc. A Principal Agent can be thought of as a delegated source of Identity information (i.e. delegated by the 'real world domain' Principal).

- **Identity-based Service Consumer**

  An Identity-based Service Consumer is an IdM role that, in order to perform its functions, requires some Identity information about a Principal. An Identity-based Service Consumer would use some form of Identifier in order to access other Identity information or Identity services about a Principal. Most services and applications will include functions that are acting as Identity-based Service Consumers.

  An example of an Identity-based Service Consumer could be a Provider that implements a weather forecast service. The Provider might wish to request location information (from an Identity-based Service Provider) about a certain End User in order to provide a local weather report to that End User.

- **Identity-based Service Provider**

  An Identity-based Service Provider is an IdM role that provides Identity information or Identity services for / about a Principal. The role of an Identity-based Service Provider includes acting upon some resource in order to either retrieve information about an Identity, update information about an Identity, or perform some action for the benefit of some Identity.

  An Attribute Provider is a special type of Identity-based Service Provider, whose function is to provide Identity Attributes about a specified Principal. Therefore an Attribute Provider would create, read, update, or delete Attributes of a Principal. Examples of Attributes that an Attribute Provider may store on behalf of a Principal include location, presence, personal information, Principal Agent configuration, etc. (note that this is not an exhaustive list).

- **Identity Provider (IDP)**

  An Identity Provider is an IdM role that offers key, core Identity functions that are required in order for other Identity services to be possible. For example, an Identity Provider would authenticate Principals and obtain Authorisation from them in order to provide the level of trust required for Identity-based Service Consumers and Identity-based Service Providers to interact. It is likely that an IDP would also take on a Discovery Service role.

- **Discovery Service Provider**

  A Discovery Service Provider is an IdM role that knows what Attributes are available for a particular Principal and how to gain access to those Attributes. Note that a Discovery Service Provider would not actually know the value of a particular Attribute, but just the Address of an appropriate Identity-based Service Provider. The service offered by a Discovery Provider is considered a core Identity Service because it is used by other IdM roles to enable Identity Management interactions between them.

Figure 4 represents a model of the possible relationships between the roles of the IdM enabler. Descriptions of the types of interactions between the different roles are listed below.

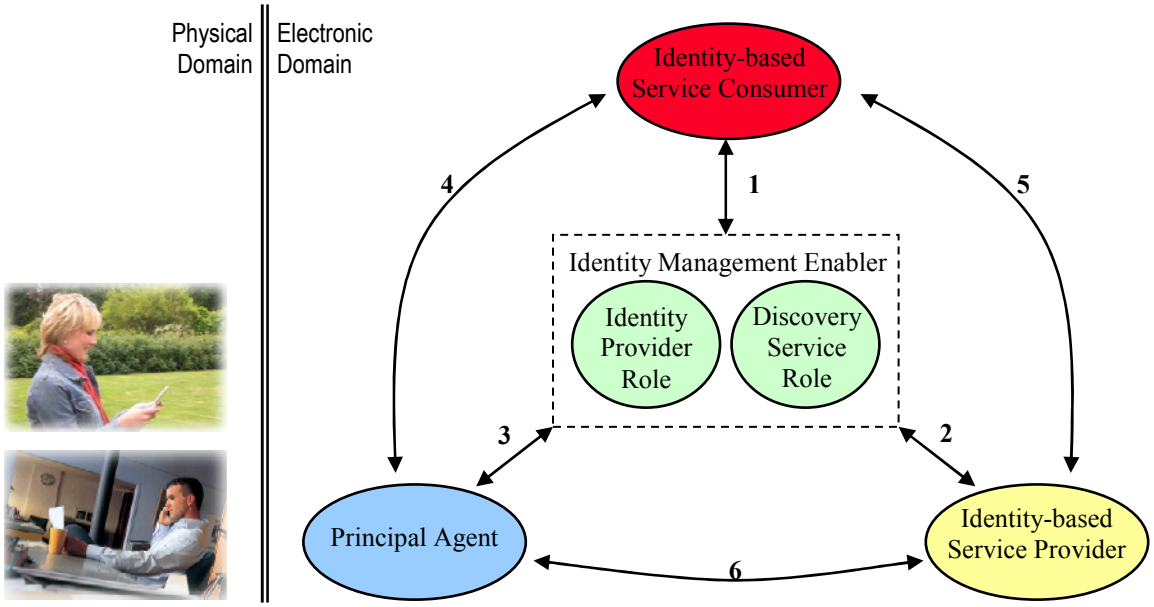

Figure 4: Model of relationships between the roles of the IdM ecosystem

Relationship 1: Identity-based Service Consumers interact with the IdM enabler:

- To discover what Identity-based services exist for a particular Principal, and to retrieve the necessary information in order to invoke the Identity-based services (e.g. Authentication Assertions used to enable Single Sign On, or an appropriate Identifier to use at a particular Identity-based Service Provider);
- To manage the Federation (linking) of a Principal's Identities at different Providers.

Relationship 2: Identity-based Service Providers interact with the IdM enabler:

- To register the Identity-based services that are offered by the Identity-based Service Provider for a particular Principal;
- To manage the Federation (linking) of a Principal's Identities at different Providers;
- To facilitate the request of missing Identity information directly from the Principal, along with explicit access permissions for that Identity information;
- To communicate to Identity-based Service Providers the means by which a Principal was authenticated.

Relationship 3: Principal Agents interact with the IdM enabler:

- To allow Principals to create Accounts and to manage their Identity information (e.g. initiate Federations, delegate Authorisations, etc.);
- To allow the IdM enabler to authenticate the Principal Agent (and, in many cases, the Principal as well). The IdM enabler does not specify one particular Authentication mechanism but must enable the communication to Identity-based Service Providers of the means by which a Principal was authenticated.

Relationship 4: Principal Agents interact with Identity-based Service Consumers:

- To create Accounts, subscribe to services, and to allow Principals to manage Federation of their various Accounts;
- To allow the Identity-based Service Consumer to authenticate the Principal Agent (and, in many cases, the Principal as well) until Federation has occurred and Single Sign On can be used;
- To invoke services.

Relationship 5: Identity-based Service Consumers interact with Identity-based Service Providers:

- To gain access to a Principal's Attributes or other Identity-based services, using an Identifier for the Principal provided by the Identity Provider. The definition of these interactions by the Identity Management enabler specification will enable homogeneous access to Identity-based services.

Relationship 6: Principal Agents interact with Identity-based Service Providers:

- To supply, modify or delete Identity Attributes;
- For a Principal to approve or reject changes to its Attributes (although this may require interaction via the IdM enabler);
- To allow the Identity-based Service Provider to authenticate the Principal Agent (and, in many cases, the Principal as well) until Federation has occurred and Single Sign On can be used;
- For a Principal to manage the permissions relating to who may access its Attributes or Identity-based services. Although this RD introduces requirements for these interactions, these will need socialisation with the developers of the Policy evaluation enabler, as they fall naturally under its scope.

4.2.3 Relationship between IdM and the Policy enforcement infrastructure

Note that in order to carry out their duties, the roles of the IdM ecosystem may need to make Authorisation decisions and evaluate other Policies (i.e. they may have to perform functions that belong to a Policy evaluation and enforcement enabler). In that respect, the IdM enabler RD might constitute a source of requirements for the interfaces of such a Policy evaluation and enforcement enabler.

The PEEM (Policy Evaluation, Enforcement and Management) Requirements Document (not yet approved at the time of developing this RD) includes requirements with respect to enforcement of OMA Policies (enforcement is perceived as a two-step process, namely evaluation and execution). As such, the PEEM enabler (which will be specified according to the PEEM Requirements Document) will be the OMA enabler that handles Policy enforcement.

That said it is possible that Policy enforcement will be handled via delegation of certain PEEM functions to those other enablers that specialise in the particular functions. Given that PEEM and IdM are both currently in the requirements phase, it is appropriate to include any IdM-specific Policy enforcement requirements in the IdM RD (this document), while at the same time making those same requirements available to the PEEM breakout team.

Furthermore, any IdM (Policy enforcement) requirements that are "local" to IdM (in the sense that they are only related to internal resources and may never be exposed to an external PEEM enabler) shall definitely be part of the IdM Requirements Document.

After completion of the IdM enabler RD it is recommended that the IdM enabler should use the PEEM Architecture Document and Technical Specification for all applicable Policy enforcement (unless the PEEM enabler is not yet specified, or does not cover all of the needs of the IdM enabler). This would then ensure IdM compliance with the specific subset of the OSE architectural requirements and guidelines that deals with the interface between applications and enablers using the Policy enforcement paradigm.

4.3 Informative Business Requirements

These requirements are included for context / consistency, but they do not have to be addressed by subsequent AD and technical specification development. For this reason they are included here in section 4 rather than the (formative) section 6.

BR-A When a Service Provider queries an Attribute Provider for one or more Attribute Classes of a Principal, there SHALL be a trust relationship between the Entities involved in the request. Such a trust relationship includes direct trust as well as brokered trust.

BR-B Business agreements and potentially trust relationships MAY be needed between the Service Providers belonging to an Affiliation.

BR-C Business agreements established between Providers MAY govern whether an Identity Broker may be used to allow Federation of Principal Accounts at an Identity Provider and a Service Provider.

BR-D When the terms of a business relationship require it, a Provider SHALL notify another Provider of one or more De-Federation requests.

BR-E When De-Federation occurs, a Provider that has collected any information about the Federation of the Principal's Identity SHALL delete the information that was created at the time of Federation.

5. Use Cases (Informative)

Before highlighting use cases that each define a small part of an Identity Management enabler, a scenario is included here to show an example of a complete service offering that could be built using the various Identity Management enabler concepts. It highlights that an Identity Management enabler must offer the same security and Identity functions for both B2B and B2C services, and that any Identity Management enabler solution must be both extensible and scalable.

A large corporate company, CompanyX, provides a corporate web portal for its 100,000 employees, 40,000 retirees and 150,000 beneficiaries. This portal includes a wide range of content both from CompanyX itself and from CompanyX's partner companies such as SafeInvestmentAdvice, SOSHealthcare, and CompanyCarCo. The portal service offers its End Users a variety of Identity Management services. One key Identity service is Single Sign On, which allows an End User to browse from one site to the next without having to remember multiple different usernames/passwords and explicitly login to every site. Another key Identity service is seamless Attribute Transfer, which allows an End User to avoid having to enter the same personal information multiple times at the different partner company sites. CompanyX currently uses a username/password combination for initial Authentication of its End Users, but it may migrate to a different Authentication solution in the future (such as Smart Card based Authentication) so the corporate web portal service Identity Management solution must allow for this migration.

Although some End Users of the system (retirees and beneficiaries) can browse the partner company web sites directly (only using the Single Sign On service of CompanyX), CompanyX employees access all the information on the corporate web portal itself. (This ensures that employees experience the same corporate look and feel for all of the different services.) Therefore the portal securely pulls in content from the partner companies (using Attribute Transfer) based on the employee permissions and preferences (managed by CompanyX's HR department). While retirees and beneficiaries typically access these services via the Internet, using their own computers or public computers at a library, employees can access the services using either their CompanyX computer, a CompanyX provided mobile Device or, in some cases, their personal computer or personal mobile Device.

In order to comply with CompanyX Policies (which are driven by Government regulations, the CompanyX HR Department, the CompanyX IT Department, and by the business agreements that CompanyX has with its partner companies) the corporate web portal must be able to modify what content is available to End Users in different circumstances. For example, when an employee accesses the portal using their CompanyX provided mobile Device all information is available for viewing, but only some information can be edited. However, when an employee accesses the portal using their personal mobile Device, they can only access some information, and only very limited updates can be made to the information. The CompanyX corporate web portal also allows End Users themselves to select which content they wish to view in different circumstances (provided these choices to not contravene CompanyX Policies).

The use of a personal mobile Device for accessing (employee) CompanyX services poses some interesting challenges:

- One challenge relates to the management of which parties have the authority to provision / access / manage different Identity information stored on the Device. For example, only CompanyX should be able to provision and manage information relating to CompanyX and partner companies, whilst only the employee's mobile operator should be able to provision and manage information relating to mobile network access. However, there may be other Identity information stored on the Device for which the management is delegated (e.g. from CompanyX to the mobile operator or vice versa). Furthermore the employee may wish to provision and manage some personal Identity information on the Device, and not allow access either to the mobile operator or to CompanyX.
- A second challenge relates to Single Sign On (SSO) and Attribute Transfer. As stated earlier CompanyX offers SSO and Attribute Transfer services to its employees. However, the employee's mobile operator also offers its own SSO and Attribute Transfer services. An employee, who is using their personal mobile Device to access the CompanyX corporate web portal, should be able to use the SSO and Attribute Transfer services of both CompanyX and the mobile operator at the same time without one causing the other to malfunction. It may also be that CompanyX and the mobile operator wish to extend their services to complement each other so that SSO and Attribute Transfer work seamlessly across both domains.
- A third challenge relates to the re-use of Devices (CompanyX or personal). There are instances where a Device may be lent temporarily to another End User or where a Device is assigned to a new End User. Furthermore, an End User may start to work for a different company, or CompanyX may change the mobile operator they use for their (company) Devices. In all of these scenarios a new End User (or mobile operator / company) must not be able to discover the

Identity information relating to the previous End User / mobile operator / company except with explicit permission from the previous End User / mobile operator / company.

Therefore, for all Identity information stored on a Device, it must be possible to also store which parties have the authority to provision the information, access the information, and manage the information in order to meet the Policies of all involved parties.

Each year CompanyX negotiates new contracts with new partner companies and ends contracts with some existing partner companies. Employee status can also change (e.g. they retire) and new employees are hired and fired regularly. CompanyX may also decide to outsource some of its Identity Management systems (the Authentication system for its beneficiaries, for example) to a third party company. CompanyX's Identity Management solution must allow for all of these possibilities.

One service that is popular with CompanyX employees and retirees is the *Keep Fit Programme*, which is sponsored by SOSHealthcare. The *Keep Fit Programme* is a benefit that employees and retirees can take advantage of, but not beneficiaries. The *Keep Fit Programme* allows End Users to buy 'electronic entry vouchers' for any SOSHealthclub at extremely preferential rates. The End Users must buy these vouchers on the corporate web portal using their credit cards, after which the 'electronic entry vouchers' are issued either to their CompanyX provided mobile Device, or their personal mobile Device. At the SOSHealthclub the 'electronic entry voucher' is verified automatically at the entrance, and a photograph of the End User appears on the health club access gate so that a health club employee can see that it is the correct End User. The CompanyX corporate web portal also allows *Keep Fit Programme* End Users to use their mobile Devices to find the nearest SOSHealthclub (both at home and when travelling).

Whilst on honeymoon (before going scuba diving), a CompanyX employee wishes to change the beneficiary on her life insurance policy from her parents to her new husband. She is able to do this by accessing the CompanyX corporate web portal using her personal mobile Device, which she has taken abroad with her.

CompanyX's Identity Management system must manage all Identity information and preferences for these services, along with very many other services that CompanyX offers to its employees, retirees and beneficiaries. Furthermore, the system must be capable of keeping complete audit trails relating to all transactions involving End User Identity information, and it must also be capable of identifying all parties involved in these transactions.

5.1 Use Case 1, Single Sign On and Authentication Contexts

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X		X	X	
Additional Keywords					

Table 2: Affected Areas for Single Sign On and Authentication Contexts

5.1.1 Short Description

The purpose of this use case is to illustrate how Single Sign On (SSO) technology can increase security and simplify an End User's experience of using Internet-based services using their mobile Device.

When accessing Internet-based services today, an End User typically has to authenticate herself to each different Service Provider (SP) using a combination of a username and a password (specific to the particular SP). This solution has the following drawbacks:

- The End User has to remember multiple different username / password combinations, which is both tedious and almost inevitably leads to one of the following:
  - The End User re-uses the same username / password combination for multiple different SPs (which has obvious security flaws since knowing the combination at one allows access to all others);
  - The End User stores their various username / password combinations in insecure repositories on their Devices;
- Username / password solutions only offer a 1-Factor[1] Authentication solution;
- Entering usernames and passwords on Devices with only a numeric keypad is tiresome for End Users.

Single Sign On improves the End User experience by reducing the number of username / password combinations that the End User must remember, and by reducing the number of keystrokes required on the Device. Single Sign On can also improve security because it is more likely that an Identity Provider would use a more secure, 2 or 3-Factor Authentication solution than a Service Provider would (e.g. a SIM Smart Card in combination with an End User PIN).

In this Use Case, an End User uses her Device to access the services of a Movie Ticket Service Provider (MTSP) and a Restaurant Locator Service Provider (RLSP). First she must authenticate herself to the MTSP site, then she selects a movie that she wishes to see, and finally authorises a transaction to purchase a movie ticket (initiating payment and the download of an electronic ticket to her Device – see Use Case 6 for more details). The End User then browses to the Restaurant Locator Service Provider and experiences the benefits of Single Sign On (she doesn't have to authenticate herself to the RLSP separately). The focus of this use case is the Single Sign On feature and Authentication Contexts.

When authenticating herself to the MTSP and RLSP sites the End User does not have to remember MTSP and RLSP-specific usernames and passwords because the MTSP and the RLSP use the services of an external Identity Provider (IDP) to authenticate her. The MTSP and RLSP simply request the IDP to verify whether the End User has been authenticated and, provided the IDP has previously authenticated the End User, the IDP simply sends a message (an Authentication Assertion) back to both the MTSP and the RLSP, stating that the End User has been authenticated successfully. Thus less input (i.e. keystrokes) is required from the End User before using the services of the MTSP and the RLSP. In this use case it is assumed that the Movie Ticket Service Provider service and the Restaurant Locator Service Provider service require End Users to have an Account and authenticate themselves before using the service (in order to provide a customised service).

---

[1] *It is generally accepted that an Authentication method can use up to 3 Factors: something you have, something you know, or something you are. Username / password is an example of something you know, so 1-Factor. A bankcard with a PIN, for example, provides 2-Factor Authentication since the End User must both have the card and know the PIN.*

Authentication Contexts

In many cases a Service Provider may not be content with any form of Authentication that the IDP uses to authenticate the End User, but may request a specific form of Authentication to be used, or at least a specific *class* of Authentication (i.e. level of security) to be used. The SP may also request the IDP to re-authenticate the End User regardless of whether the IDP had previously authenticated the End User or not. Such context surrounding the Authentication of the End User by the IDP is collectively referred to as the Authentication Context. Hence an Authentication Context captures such concepts as:

- The ability of a SP to request an IDP to authenticate the End User using a specific Authentication mechanism;
- The ability of a SP to request an IDP to authenticate the End User using a certain *class* of Authentication mechanism;
- The ability of an SP to request an IDP to re-authenticate the End User even if the End User has already been authenticated by the IDP;
- The ability of an SP to request an IDP to re-authenticate the End User if the End User was previously authenticated more than a certain time interval (e.g. 30 minutes) previously;
- The ability of an IDP to inform the SP about what form of Authentication was used to authenticate an End User.

Extending the example above (with the End User, the MTSP, the RLSP and the IDP), consider the case where the End User's IDP is her GSM mobile operator. The End User's mobile Device has previously been authenticated by the mobile operator (using her GSM SIM Smart Card) in order to register onto the mobile network. When the MTSP and the RLSP request an Authentication Assertion from the mobile operator to allow the End User to browse their web sites, GSM SIM Authentication is acceptable for the MTSP and the RLSP (according to the Authentication Contexts that they send to the mobile operator with the requests), so the mobile operator responds immediately with an Authentication Assertion (a separate Authentication Assertion for each SP). However, in the case of the MTSP, when the End User wishes to make a purchase, the level of Authentication required to authorise the purchase is higher. Therefore the MTSP requests an Authentication Assertion from the mobile operator and uses an Authentication Context to request re-Authentication of the End User, this time using a more secure form of Authentication that verifies that the correct End User is using the Device. The mobile operator re-authenticates the End User, this time using both GSM SIM Authentication and End User PIN entry, before sending an appropriate Authentication Assertion back to the MTSP.

5.1.2 Actors

- End User – using a mobile Device
- Identity Provider – a mobile operator (or another Service Provider) that offers Single Sign On Identity services
- Movie Ticket Service Provider – a Service Provider providing downloadable movie tickets
- Restaurant Locator Service Provider – a Service Provider providing a free restaurant locator service to RLSP Account holders

5.1.2.1 Actor Specific Issues

5.1.2.2 Actor Specific Benefits

5.1.3 Pre-conditions

- The End User has an Account with the Identity Provider
- The End User has an Account with the Movie Ticket Service Provider
- The End User has an Account with the Restaurant Locator Service Provider

- The Movie Ticket Service Provider has made the necessary arrangements (business and technical) with the Identity Provider in order to use the Single Sign On service offered by the Identity Provider
- The Restaurant Locator Service Provider has made the necessary arrangements (business and technical) with the Identity Provider in order to use the Single Sign On service offered by the Identity Provider
- The End User has federated (linked) her Account at the Movie Ticket Service Provider to her Account at the Identity Provider in order to make use of the Single Sign On service (see Use Case 2)
- The End User has federated her Account at the Restaurant Locator Service Provider to her Account at the Identity Provider in order to make use of the Single Sign On service
- The Identity Provider has previously authenticated the End User using GSM SIM Authentication

5.1.4 Post-conditions

- The End User has authorised the purchase of a movie ticket from the Movie Ticket Service Provider
- The End User has located a restaurant using the services of the Restaurant Locator Service Provider

5.1.5 Normal Flow

1. The End User accesses the Movie Ticket Service Provider's service using a browser on her Device. The End User must be authenticated before being granted access to her personalised site.

2. The MTSP sends a request to the IDP for an Authentication Assertion for the End User, and requests (using an Authentication Context) that the End User is authenticated using either username / password or GSM SIM Authentication.

3. The IDP sends back an Authentication Assertion to the MTSP (without re-authenticating the End User, since she was already authenticated using SIM Authentication), which contains information about how the End User was authenticated.

4. The End User is granted seamless access to the MTSP site and finds a movie that she is interested in.

5. The End User selects a movie theatre and time that are suitable and indicates to the MTSP that she wishes to purchase a ticket.

6. The MTSP requires End User re-Authentication, using GSM SIM Authentication and End User PIN entry, in order to authorise the purchase so the MTSP contacts the IDP to request a further Authentication Assertion. The MTSP also sends an Authentication Context, requesting both that the End User is re-authenticated and that the Authentication should use GSM SIM Authentication *and* End User PIN entry.

7. The IDP carries out the Authentication directly with the End User, asking her to enter her user PIN.

8. Upon successful Authentication, the IDP sends a further Authentication Assertion to the MTSP, containing information about how the End User was authenticated.

9. The MTSP acknowledges that the End User has authorised the movie ticket purchase.

10. The End User now accesses the Restaurant Locator Service Provider's service using the browser on her Device. The End User must be authenticated before being granted access to her personalised site.

11. The RLSP sends a request to the IDP for an Authentication Assertion for the End User, and requests (using an Authentication Context) that the End User is authenticated using either username / password or GSM SIM Authentication.

12. The IDP sends back an Authentication Assertion to the RLSP (without re-authenticating the End User, since she was already authenticated using SIM Authentication and PIN entry) and includes information about how the End User was authenticated.

13. The End User is granted seamless access to the RLSP site and finds a restaurant that she would like to eat in.

5.1.6 Alternative Flow

5.1.7 Operational and Quality of Experience Requirements

- Single Sign On solutions must protect the End User's privacy and must not reveal any more personal data to the MTSP than is required to provide the service. Any personal data sent to the MTSP must also be given only with the consent of the End User (in the form of End User preferences or direct End User permission). For example, one of the primary requirements relating to this is that two different Service Providers should not be able to collude and determine that it is the same End User that visited their sites. The name Identifier associated with the same End User at two different Service Providers should therefore be different.
- Single Sign On should not be dependent on any Device-stored state (e.g. a cookie), in order to ensure that SSO services can be used from multiple Devices – even if the Device is being used for the very first time.
- Single Sign On solutions must have a high enough performance to ensure that the End User experience is not deteriorated.
- The initial set-up of the Single Sign On mechanism and the control of Privacy Settings must be simple enough for End Users to find the services an attractive proposition.

5.2 Use Case 2, Federation, Single Log Out, and De-Federation

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X		X	X	
Additional Keywords					

Table 3: Affected Areas for Federation, Single Log Out, and De-Federation

5.2.1 Short Description

The benefits of Single Sign On were highlighted in Use Case 1. Using SSO, an End User authenticated by an Identity Provider is able to obtain seamless access to the services of every Service Provider that the End User has linked (or *federated*) her IDP Account to. This use case describes some of the background processes that enable SSO. Specifically, this use case discusses:

- Federation of an End User's Account at an IDP with her Account at an SP;
- De-Federation of an existing Federation;
- Single Log Out (SLO) of an End User.

Consider a scenario where an End User has an Account with a mobile operator (acting as an Identity Provider) and the operator has already authenticated the End User. The mobile operator has entered into business agreements with several Service Providers so that the End User's Account at the operator may potentially be linked (or *federated*) with the End User's Account at each Service Provider, if the End 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. The Movie Ticket Service Provider and the Restaurant Locator Service Provider, mentioned already in Use Case 1, are examples of such Service Providers in the same Authentication Domain as the mobile operator. Remember that the MTSP and RLSP require End User Authentication prior to the End User being able to browse her personalised MTSP and RLSP web sites.

Federation of End User Accounts

(Note that this same process would happen separately for the MTSP and the RLSP. The MTSP is used for this example.)

When the End User sets up an Account with the MTSP, the MTSP determines that the End User has an Account with the operator (perhaps by displaying a list of supported Identity Providers that the End User can choose from). The MTSP then prompts the End User to ask if she would like to simplify her Authentication process in the future by federating her Account at the MTSP with her Account at the operator. Since the End User would like to obtain the benefits of Single Sign On, she consents to such a Federation being made. The MTSP sets up the Federation with the operator (see Normal Flow, below). The next time the End User visits the MTSP web site, she is able to click on an icon representing her operator (for example) and then enter her Identifier at the operator to take advantage of SSO.

Single Log Out (SLO) of federated Accounts

The End User is currently authenticated by the operator and has also federated her Account at the operator with her Account at the MTSP and her Account at the RLSP. The End User may or may not be authenticated by the MTSP and the RLSP (either directly or via SSO). The End User then sends a Single Log Out request message to the operator, requesting that she is logged out both at the operator and at any SP site within the operator's Authentication Domain that the End User is currently logged into (e.g. the MTSP and the RLSP). The operator carries out the Single Log Out instruction (see Normal Flow, below) then sends a response message to the End User confirming successful Log Out at all Providers within the Authentication Domain.

De-Federation of federated Accounts

After the End User has federated her Account at the operator with her Account at the MTSP (or the RLSP), at some future point in time, the End User decides to de-federate these Accounts i.e. the End User does not want these two Accounts to be linked any longer. This could be because the End User plans to change operator, or because the End User no longer wishes to use the services of the MTSP (or the RLSP). This form of De-Federation is termed *user-initiated De-Federation* (see Use Case 3 for more information on *network-initiated De-Federation*).

For user-initiated De-Federation to occur the End User must currently be authenticated by the operator. The End User then explicitly requests the operator to de-federate her Account with the MTSP (or the RLSP) with her Account at the operator. The operator then completes the De-Federation (see Normal Flow, below) and sends an acknowledgement to the End User confirming successful De-Federation of the End User's Account at the operator with the End User's Account at the MTSP (or RLSP).

5.2.2 Actors

- End User – using a mobile Device
- Identity Provider – a mobile operator (or another Service Provider) that offers Single Sign On Identity services
- Movie Ticket Service Provider – a Service Provider providing downloadable movie tickets
- Restaurant Locator Service Provider – a Service Provider providing a free restaurant locator service to RLSP Account holders

5.2.2.1 Actor Specific Issues

5.2.2.2 Actor Specific Benefits

5.2.3 Pre-conditions

- The End User has an Account with the Identity Provider
- The End User has an Account with the Movie Ticket Service Provider
- The End User has an Account with the Restaurant Locator Service Provider
- The Movie Ticket Service Provider has made the necessary arrangements (business and technical) with the Identity Provider in order to use the Single Sign On service offered by the Identity Provider
- The Restaurant Locator Service Provider has made the necessary arrangements (business and technical) with the Identity Provider in order to use the Single Sign On service offered by the Identity Provider
- The Identity Provider has previously authenticated the End User

There are additional pre-conditions for the Single Log Out and De-Federation cases, as follows:

- The End User's Account at the Identity Provider is federated with the End User's Account at the Movie Ticket Service Provider
- The End User's Account at the Identity Provider is federated with the End User's Account at the Restaurant Locator Service Provider

5.2.4 Post-conditions

Federation of End User Accounts

- The End User's Account at the operator is federated with the End User's Account at the MTSP (or the RLSP). This allows the End User to make use of the SSO services mentioned in Use Case 1

Single Log Out (SLO) of federated Accounts

- The End User has been successfully logged out at the operator and at the MTSP and RLSP sites (and all other sites in the Authentication Domain that she was logged into)

De-Federation of federated Accounts

- The End User's Account at the operator has been de-federated with the End User's Account at the MTSP (or the RLSP). The End User can no longer make use of SSO services

5.2.5 Normal Flow

Federation of End User Accounts

(Note that this same process would happen separately for the MTSP and the RLSP. The MTSP is used for this example.)

The normal flow for Federation of the End User's Account at the operator with her Account at the MTSP is as follows:

1. The End User accesses the MTSP web site and decides to set up a user Account at the MTSP. The MTSP determines that the End User has an Account with the operator (perhaps by displaying a list of supported Identity Providers that the End User can choose from).

2. The MTSP prompts the End User to ask if she would like to simplify her Authentication process in the future by federating her Account at the MTSP with her Account at the mobile operator. The End User would like to obtain the benefits of Single Sign On, so she consents to such a Federation being made.

3. The MTSP contacts the operator to request the Federation of the End User's Account at the MTSP with the End User's Account at the operator. The MTSP includes an optional name Identifier (e.g. Sarah980) that it would like the operator to refer to the End User as when the operator subsequently contacts the MTSP about that particular End User. Note that the End User may be known by a different Identifier (e.g. smiller1708@operator.com) at the operator.

4. Upon receiving the Federation request from the MTSP the operator prompts the End User to identify herself (alternatively her mobile Device and GSM SIM could handle this, for example) and then the operator authenticates her and verifies that she would like to federate her Account at the operator with her Account at the MTSP.

5. Having obtained the End User's consent the operator federates her Accounts. The operator then sends a Federation response message back to the MTSP indicating successful Federation. (Had the MTSP not included the optional name Identifier (Sarah980) for the End User in the Federation request message, the operator would have generated a random name Identifier (e.g. abxy35mn) to use as a Pseudonym for the End User, and sent this Pseudonym back to the MTSP in the successful Federation response.)

6. The End User's Account at the operator has now been federated with her Account at the MTSP and the MTSP notifies the End User that this is the case. The next time the End User visits the MTSP web site she is able to click on an icon representing her operator (for example) and then enter her Identifier at the operator to take advantage of SSO.

Note that when the same End User subsequently federates her Account at the operator with her Account at another Service Provider, a completely different Pseudonym will be used as a name Identifier for the End User. The advantage of this is that different Service Providers cannot then collude to determine the service usage patterns of the End User.

Single Log Out of federated End User Accounts

The normal flow for Single Log Out of federated End User Accounts is as follows:

1. The End User is currently authenticated at the operator. She requests the operator to log her out at all Providers in the same Authentication Domain as the operator. Note that the End User may or may not currently be logged in (i.e. authenticatced) at the MTSP web site and the RLSP web site.

2. The operator sends a request message to every SP in that Authentication Domain, including the MTSP and the RLSP, requesting that the End User be logged out.

3. If the End User is currently authenticated at the MTSP or the RLSP (either directly or via SSO), the MTSP and the RLSP log her out and send a response to the operator confirming the logout. This is also the case for all other SPs within the same Authentication Domain as the operator.

4. The operator logs the End User out at the operator.

5. The Operator sends a confirmation message to the End User, confirming that she has been successfully logged out of all Providers within the same Authentication Domain as the operator.

User-Initiated De-Federation of End User's federated Accounts

(Note that this same process would happen separately for the MTSP and the RLSP. The MTSP is used for this example.)

The normal flow for user-initiated De-Federation of an End User's Account at the operator that is federated with her Account at the MTSP is as follows:

1. The End User, who is currently authenticated by the operator, requests the operator to de-federate her Account at the operator with her Account at the MTSP.

2. The operator sends a de-federate request message to the MTSP, requesting De-Federation of the End User's Account at the operator with the End User's Account at the MTSP (e.g. using the Pseudonym Sarah980 to identify the End User).

3. Having taken the necessary steps to tear down the Federation, the MTSP responds to the operator confirming the De-Federation.

4. The operator then de-federates the End User's Accounts in the operator's own Identity systems.

5. The operator sends a confirmation back to the End User, confirming that her Account at the operator has been de-federated with her Account at the MTSP.

Note that the End User could either ask the operator *or the MTSP* to initiate the De-Federation on her behalf.

5.2.6 Alternative Flow

5.2.7 Operational and Quality of Experience Requirements

5.3 Use Case 3, Delegation of Authority to Federate Identities, Bulk Federations and De-Federations

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X		X	X	
Additional Keywords	For Delegation of Authority				

Table 4: Affected Areas for Delegation of Authority to Federate Identities, Bulk Federations and De-Federations

5.3.1 Short Description

There are many cases where an End User may wish to delegate authority to federate her Identity Provider Account with her (new or existing) Accounts at other Service Providers to the Identity Provider itself, so that the IDP may federate her Accounts on her behalf. Using this delegated authority, the IDP can federate the End User's IDP Account with (new or existing) End User Accounts at SPs without the End User having to be logged in (i.e. authenticated) at the time. Such scenarios are typically found in the enterprise or B2B area:

- Employees (as End Users) in an enterprise delegate authority to the employer (IT department) to federate their Accounts on their behalf (such delegation of authority would typically be part of an employment contract). This allows the enterprise to carry out bulk Federations of employee IT Accounts at the enterprise with their Accounts at, for example, SafeInvestmentAdvice, SOSHealthcare, and CompanyCarCo. The employee can then take advantage of Single Sign On and, once logged in to the corporate IT network, can enjoy seamless access to the SafeInvestmentAdvice, SOSHealthcare, and CompanyCarCo sites. In this scenario the enterprise is acting as the IDP and SafeInvestmentAdvice, SOSHealthcare, and CompanyCarCo are all acting as SPs.
- In a B2B scenario, a mobile operator connects Service Providers to End Users. Each of the End Users has an Account with the mobile operator, which is acting as the Identity Provider. At the time of mobile operator Account creation, the End User may wish to delegate authority to federate her operator Account with (probably new) Accounts at operator partner Service Providers (such as a Game Service Provider). With such delegation of authority, as the operator signs agreements with new partner Service Providers, or ends existing agreements, the End User does not have to explicitly federate and de-federate her Accounts, as the operator can do this instead (probably in bulk Federations and De-Federations). This provides a seamless user experience to the End User. Note that when the operator (as opposed to the End User) initiates De-Federation, this is termed *network-initiated De-Federation*.

The purpose of presenting this use case is to illustrate the benefits of an End User delegating authority (to her IDP) for Federation of her IDP Account with other SP Accounts. The use case includes four scenarios:

- An End User creates a new Account at a mobile operator, who has business agreements with partner Service Providers (in this case GameProvider1 and GameProvider2). The operator automatically federates the new End User's Account with new Accounts at all its partner Service Providers;
- The mobile operator quits its business agreement with GameProvider2 (and therefore de-federates all of its End Users' Accounts with their respective Accounts at GameProvider2);
- The mobile operator creates a new business agreement with GameProvider3 (and therefore federates all of its End Users' Accounts with new Accounts at GameProvider3);
- The End User quits her Account at the mobile operator (so the operator de-federates her operator Account with her Accounts at GameProvider1 and GameProvider3).

5.3.2 Actors

- End User(s) – (each) using a mobile Device
- Identity Provider – a mobile operator (or another Service Provider) that offers Single Sign On Identity services
- GameProvider1 – a Service Provider who provides a game service to authorised End Users
- GameProvider2 – a Service Provider who provides a game service to authorised End Users
- GameProvider3 – a Service Provider who provides a game service to authorised End Users

5.3.2.1 Actor Specific Issues

5.3.2.2 Actor Specific Benefits

5.3.3 Pre-conditions

New End User creates an Account at the mobile operator

- A new End User has just set up a new Account with the mobile operator
- GameProvider1 and GameProvider2 have made the necessary arrangements (business and technical) with the mobile operator in order to use the Single Sign On service offered by the operator
- The End User has delegated authority (in her operator contract) to the operator to federate her operator Account with (new) End User Accounts at all of the operator's partner Service Providers (in this case, with new Accounts at GameProvider1 and GameProvider2)

Mobile operator quits business relationship with GameProvider2

- GameProvider2 has made the necessary arrangements (business and technical) with the operator in order to use the Single Sign On service offered by the operator
- Many End Users have Accounts with the operator
- All the operator's End Users also have Accounts at GameProvider2, and these Accounts are federated with the appropriate End User Accounts at the operator
- Each of the operator's End Users have delegated authority to the operator to federate and de-federate their operator Accounts with their Accounts at the operator partner Service Providers
- The operator End Users are not currently authenticated at the Operator

Mobile operator creates business relationship with GameProvider3

- GameProvider3 has just made the necessary arrangements (business and technical) with the operator in order to use the Single Sign On service offered by the operator
- Many End Users have Accounts with the operator
- The mobile operator's End Users do not have Accounts at GameProvider3
- Each of the operator's End Users have delegated authority to the operator to federate and de-federate their operator Accounts with (their) Accounts at the operator partner Service Providers
- The operator End Users are not currently authenticated at the Operator

End User quits her Account at the mobile operator

- GameProvider1 and GameProvider3 have made the necessary arrangements (business and technical) with the operator in order to use the Single Sign On service offered by the operator

- The End User has an Account at the operator, and an Account at each of the operator's partner Service Providers (i.e. GameProvider1 and GameProvider3)
- The End User has delegated authority to the operator to federate and de-federate her operator Account with her Accounts at the operator partner Service Providers
- The End User is not currently authenticated at the Operator

5.3.4 Post-conditions

New End User creates an Account at the mobile operator

- The new End User's Account at the operator is federated with a new End User Account at each of the operator's partner Service Providers (GameProvider1 and GameProvider2 in this case). This ensures that the End User can seamlessly access any game offered by either GameProvider1 or GameProvider2 without having to initiate Account Federation herself

Mobile operator quits business relationship with GameProvider2

- All of the (many) End Users' Accounts at the operator have been de-federated with their respective Accounts at GameProvider2. The operator's End Users can no longer seamlessly access the games offered by GameProvider2

Mobile operator creates business relationship with GameProvider3

- All of the operator's (many) End Users have Accounts at GameProvider3, and their operator Accounts are federated with their (new) GameProvider3 Accounts. All of the operator's End Users can seamlessly access the games offered by GameProvider3

End User quits her Account at the mobile operator

- The End User's Account at the Operator has been de-federated with her Accounts at each GameProvider, so that she is no longer able to have seamless access to the games offered by GameProvider1 and GameProvider3

5.3.5 Normal Flow

New End User creates an Account at the mobile operator

(Note that this will happen twice over – once for GameProvider1 and once for GameProvider2.)

1. The Operator sends a Federation request message to the GameProvider, including a (unique) Pseudonym to use to refer to the End User in future communications.

2. The GameProvider creates a new End User Account and federates this newly created Account with the Account of the End User at the operator (refer back to Use Case 2 for more details).

3. The GameProvider responds to the operator to state that the Federation has been completed.

4. When the End User first registers (authenticates) onto the operator's network, she is already able to seamlessly access games at the GameProvider.

Mobile operator quits business relationship with GameProvider2

1. The operator sends a bulk De-Federation request to GameProvider2, requesting that every operator End User Account is de-federated from the appropriate End User Account at GameProvider2.

2. GameProvider2 de-federates all of the End User Accounts at the operator with the appropriate GameProvider2 End User Accounts.

3. GameProvider2 responds to the operator to state that the bulk De-Federation has been completed.

4. None of the operator's End Users will be able to seamlessly access games offered by GameProvider2 any longer.

Mobile operator creates business relationship with GameProvider3

1. The operator sends a bulk Federation request to GameProvider3 requesting Federation of every operator End User Account with End User Accounts at GameProvider3.

2. GameProvider3 creates new End User Accounts for every operator End User and then federates these new Accounts with the appropriate operator End User Accounts.

3. GameProvider3 responds to the operator to state that the bulk Federation has been completed.

4. All of the operator's End Users will be able to seamlessly access games offered by GameProvider3 when they next authenticate with the operator.

End User quits her Account at the mobile operator

(Note that in this example this will happen twice over – once for GameProvider1 and once for GameProvider3)

1. The operator sends a de-federate request to each of its partner Service Providers (in this case GameProvider1 and GameProvider3) requesting De-Federation of the End User's Account at the operator with the End User's Account at the Service Provider.

2. The GameProvider de-federates the End User's Account at the operator with the End User's Account at the GameProvider.

3. The GameProvider responds to the operator to state that the De-Federation has been completed.

4. The End User will no longer be able to seamlessly access the games offered by the GameProvider.

5.3.6 Alternative Flow

One alternative flow should be noted, relating to the scenario above called 'Mobile operator creates business relationship with GameProvider3'. Imagine instead a scenario where an enterprise is acting as an Identity Provider (using its IT network), and it wishes to federate all of its employees' Accounts with its employees' Accounts at SafeInvestmentInc.

Whereas GameProvider3 created new Accounts for all of the operator's End Users (in order to then federate the Accounts), it may be that the enterprise's employees already have existing Accounts at SafeInvestmentInc. Furthermore, it may be that despite the End Users not currently being authenticated by both the enterprise IT network and SafeInvestmentInc (as would have to be the case in Use Case 2 for Federation of two existing Accounts to occur) the enterprise and SafeInvestmentInc know enough information about each other's End User Accounts to be able to federate them without the End Users' (employees) presence.

5.3.7 Operational and Quality of Experience Requirements

5.4 Use Case 4, Seamless Attribute Transfer and Usage Directives

	Affected Areas				
	Device	**Connectivity**	**Enabling Services**	**Applications**	**Content**
Tickmarks (X)	X		X	X	
Additional Keywords	For location, or for storing End User preferences				

Table 5: Affected Areas for Seamless Attribute Transfer and Usage Directives

5.4.1 Short Description

The purpose of this use case is to illustrate how an Identity Management enabler can further simplify an End User's service experience by offering seamless Attribute Transfer as well as Single Sign On. Typically, an End User has to enter her personal profile information (her Identity *Attributes*) many times when using on-line services. For instance:

- When setting up a new End User Account at a Service Provider she could have to enter her name, her Address, her land line telephone number, her mobile telephone number, her e-mail Address etc.;
- When making a credit card payment she would have to enter (at least) her credit card number and expiry date, the credit card Account name, and her billing Address.

This is tedious for the End User because she has to remember the information and also type it in repeatedly (which is especially tedious when using a numeric keypad). By offering seamless Attribute Transfer an Identity Management enabler can relieve the End User of this tiresome task.

Furthermore, End User Attributes could change dynamically. Example of this are End User location or End User presence, for which the End User would not wish to update her Attributes manually every time an update was needed.

This use case also illustrates the concept of Service Providers including *Usage Directives* when requesting End User Attributes from *Attribute Providers*. By Usage Directives we mean a set of directives regarding how a particular Attribute would be used by the Service Provider once the Attribute has been released to it. By Attribute Provider we mean a Service Provider whose service is to store and manage End Users' Attributes on their behalf.

When the Service Provider requests a particular End User Attribute from the Attribute Provider (and includes a Usage Directive in the request), the Attribute Provider only then releases the Attribute to the requesting Service Provider if:

- The specified Usage Directive in the request complies with the Usage Directive Policy that the End User has established for that particular Attribute (based on the End User's preference and permissions settings);
- The End User's *Access Control Policy* allows it to do so for that particular Service Provider. (An Access Control Policy is stored at the Attribute Provider, and is used to determine whether a particular Service Provider can gain access to an End User's Attributes, based on End User preference and permissions settings.)

In the use case described here, a location Attribute Provider knows the current location information of the (mobile) End User and the Movie Ticket Service Provider wishes to obtain the location information of the End User in order to personalise its service for the End User.

5.4.2 Actors

- End User – using a mobile Device
- Identity Provider – a mobile operator (or another Service Provider) that offers Single Sign On and Identity Attribute Discovery Service Identity services
- Movie Ticket Service Provider – a Service Provider providing downloadable movie tickets
- Attribute Provider – a Service Provider who knows and manages the location information of the End User and (when appropriate) provides it to authorised requesting Service Providers

5.4.2.1 Actor Specific Issues

5.4.2.2 Actor Specific Benefits

By storing such End User Attributes at an Attribute Provider the End User need not be prompted for these Attributes every time they are required for a service. Instead, the requesting Service Provider could seamlessly obtain them from the Attribute Provider (provided the End User's preferences and permissions are satisfied). This makes the End User experience better.

5.4.3 Pre-conditions

- The End User has an Account with the Identity Provider (the mobile operator)
- The End User has an Account with the Movie Ticket Service Provider
- The End User has an Account with the location Attribute Provider (AP)
- The MTSP has made the necessary arrangements (business and technical) with the Identity Provider to use Single Sign On services and Identity Attribute Discovery Service services provided by Identity Provider
- The Attribute Provider has made the necessary arrangements (business and technical) with the Identity Provider to use Single Sign On services and Identity Attribute Discovery Service services provided by the Identity Provider
- The End User has federated her MSTP Account with her IDP Account, so that the MTSP can receive Authentication Assertions from the IDP
- The End User has federated her Account at the location Attribute Provider with her IDP Account so that the Identity Provider may provide an Identity Attribute Discovery Service (to authorised requesting Service Providers) on behalf of the location Attribute Provider
- The IDP has already authenticated the End User using a mechanism that is acceptable for the MTSP
- The location Attribute Provider knows the current location information of the End User
- The End User has set permissions (including Access Control Policy preferences and Usage Directive preferences) for the release of her location information to authorised requesting Service Providers. (Note that the End User may not use her mobile Device (with limited input capabilities) to set up these policies and preferences, but may instead use a personal computer or some other input-friendly Device)

5.4.4 Post-conditions

- The End User's location information has been obtained by the MTSP from the location AP
- The MTSP can provide the End User with a customised view based on her current location

5.4.5 Normal Flow

1. The End User accesses the Movie Ticket Service Provider's service using a browser on her Device. The End User must be authenticated before being granted access to her personalised site.

2. The MTSP sends a request to the IDP for an Authentication Assertion for the End User (including an Authentication Context). The IDP sends back an Authentication Assertion to the MTSP. The End User is granted seamless access to the MTSP site (see Use Case 1, steps 1-4 for more details).

3. The MTSP wishes to obtain the current location information of the End User so it requests the IDP (more specifically the Identity Attribute Discovery Service of the IDP) for the Address of the location AP associated with the End User. (Note that this request could also happen in conjunction with the request for an Authentication Assertion.)

4. Upon receiving the Address of the location AP from the IDP, the MTSP requests the location AP for the current location of the End User. The MTSP includes a Usage Directive for the requested Attribute, and also appropriate information (provided by the IDP) for the location AP not to have to ask the End User to identify herself.

5. The location AP checks the permissions set by the End User and compares the Usage Directive received from the MTSP with the Usage Directive Policy specified by the End User for the location Attribute stored at the location AP.

6. Upon determining that the MTSP is authorised to obtain the End User's location information, the location AP responds to the MTSP and includes the End User's location Attribute.

7. The MTSP uses the End User's location Attribute to provide a customised service to the End User.

5.4.6 Alternative Flows

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

Alternative Flow 1: Missing Attribute Value, AP contacts End User

In this alternative flow the desired Attribute value (current location information) is not present at the location AP. Consequently the MTSP redirects the End User's Device browser directly to the location Attribute Provider so that the End User (if they know their current location in a suitable format) can notify the location AP of their current location. The location Attribute Provider would then redirect the End User's Device browser back to the MTSP site.

Steps 1 to 5 are identical to Normal Flow, after which we have:

6. Upon determining that the MTSP is authorised to obtain the End User's location information, the location AP determines that the End User's location Attribute was last updated too long ago for the Attribute to be of use to the MTSP.

7. The location AP responds to the MTSP with the location information available, but indicates to the MTSP that it does not have the current location information of the End User (updated within the MTSP's desired time window).

8. The MTSP seamlessly redirects the End User's browser to the location AP, which requests the End User to enter her current (e.g. GPS) location. The End User can obtain her location information from her mobile Device and so she submits her location information to the location AP.

9. The location AP sends the End User's (now current) location Attribute to the MTSP.

10. The location AP seamlessly redirects the End User's browser back to the MTSP.

11. The MTSP uses the End User's location Attribute to provide a customised service to the End User.

Alternative Flow 2: Missing Attribute Value, SP contacts End User

This alternative flow is similar to Alternative Flow 1, in that the desired Attribute value is not present at the location AP. However, rather than redirect the End User to the location AP, the MTSP itself obtains the current location information from the End User, and then updates the location AP with this up-to-date information. This alternative flow may be desirable for a Service Provider that does not wish to hand over the End User to another Entity (in this case the location AP).

Steps 1 to 5 are identical to Normal Flow, after which we have:

6. Upon determining that the MTSP is authorised to obtain the End User's location information, the location AP determines that the End User's location Attribute was last updated too long ago for the Attribute to be of use to the MTSP.

7. The location AP responds to the MTSP with the location information available, but indicates to the MTSP that it does not have the current location information of the End User (updated within the MTSP's desired time window).

8. The MTSP prompts the End User to enter her current location so that the service can be personalised. The End User can obtain her location information from her mobile Device and so she submits her location information to the MTSP.

9. The MTSP requests the location AP to update the location Attribute for the End User to the value given in the request. The location Attribute Provider updates the End User's location Attribute.

10. The MTSP uses the End User's location Attribute to provide a customised service to the End User.

Alternative Flow 3: Usage Directive Policy (or Access Control Policy) Not Satisfied, Request Denied

Steps 1 to 5 are identical to Normal Flow, after which we have:

6. The location AP concludes that the Usage Directive received from the MTSP does not match the Usage Directive (or the Access Control Policy) set by the End User.

7. The location AP responds to the MTSP to state either that:

- The Usage Directive does not satisfy the Usage Directive Policy specified by the End User;
- The MTSP falls outside the Access Control Policy of the End User.

8. The MTSP is unable to provide a customised service to the End User based on location.

Alternative Flow 4: Usage Directive Policy Not Satisfied, Request Denied, Allowed Usage Directives Specified

Steps 1 to 5 are identical to Normal Flow, after which we have:

6. The location AP concludes that the Usage Directive received from the MTSP does not match the Usage Directive set by the End User.

7. The location AP responds to the MTSP to state that the Usage Directive does not satisfy the Usage Directive Policy specified by the End User. The location AP also includes a list of Usage Directives that would be acceptable.

8. The MTSP sends a new request for the End User's location Attribute to the location AP, and includes a modified Usage Directive based on the list of acceptable Usage Directives.

9. The location AP checks the permissions set by the End User and compares the Usage Directive received from the MTSP with the Usage Directive Policy specified by the End User for the location Attribute stored at the location AP.

10. Upon determining that the MTSP is authorised to obtain the End User's location information, the location AP responds to the MTSP and includes the End User's location Attribute.

11. The MTSP uses the End User's location Attribute to provide a customised service to the End User.

Alternative Flow 5: Unknown Permission, AP contacts End User

In this alternative flow the location AP is unable to determine whether the End User has authorised it to release the End User's location Attribute to the requesting MTSP or not. Consequently it requests the MTSP to seamlessly re-direct the End User's Device browser to the location AP so that the location AP can ask for the End User's permission directly.

Steps 1 to 5 are identical to Normal Flow, after which we have:

6. The location AP concludes that it is unable to determine (from the Usage Directives) whether the End User has authorised it to release the End User's location Attribute to the requesting MTSP.

7. The location AP responds to the MTSP to say that it is unsure, and to request the MTSP to re-direct the End User's browser to the location AP site.

8. The MTSP seamlessly re-directs the End User's browser to the location AP's site, which asks the End User directly whether she would like her location Attribute to be given to the MTSP (parts of the MTSP's Usage Directive may also be displayed to the End User in an appropriate format).

9. The End User decides that she does want to give her location Attribute to the MTSP, and so she submits this preference to the location AP.

10. The location AP responds to the MTSP and includes the End User's location Attribute.

11. The location AP seamlessly re-directs the End User's browser back to the MTSP site.

12. The MTSP uses the End User's location Attribute to provide a customised service to the End User.

Alternative Flow 6: Unknown Permission, SP contacts End User

This alternative flow is similar to that of Alternative Flow 5, in that the location AP is unable to determine whether the End User has authorised it to release the End User's location Attribute to the requesting MTSP or not. The difference is that in this alternative flow it is the MTSP that contacts the End User to determine her permissions.

Steps 1 to 5 are identical to Normal Flow, after which we have:

6. The location AP concludes that it is unable to determine whether the End User has authorised it to release the End User's location Attribute to the requesting MTSP.

7. The location AP responds to the MTSP to say that it is unsure, and to request the MTSP to ask the End User directly whether she would like her location Attribute to be given to the MTSP.

8. The MTSP asks the End User directly whether she would like her location Attribute to be given out to the MTSP. The End User decides that she would like her location Attribute to be given out.

9. The MTSP forwards proof of the End User's affirmative preference to the location AP.

10. Upon determining that the MTSP is authorised to obtain the End User's location information, the location AP responds to the MTSP and includes the End User's location Attribute.

11. The MTSP uses the End User's location Attribute to provide a customised service to the End User.

5.4.7 Operational and Quality of Experience Requirements

5.5 Use Case 5, Anonymous Attribute Transfer

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X		X	X	
Additional Keywords					

Table 6: Affected Areas for Anonymous Attribute Transfer

5.5.1 Short Description

There are many scenarios where a Service Provider may wish to access certain Attributes associated with an End User without actually knowing the Identity of the End User. For instance a Service Provider may require the zip code of an End User in order to greet the End User appropriately (e.g. 'Good Morning' or 'Good Evening'), or the date of birth of an End User in order to provide an appropriate horoscope service. In both of these examples there is no need for the End User to have an Account with the Service Provider since the SP never needs to know the Identity of the End User. The Service Provider simply requires anonymous transfer of the End User's Attributes.

Consider the case where an End User has an Account with:

- A mobile operator (acting as an Identity Provider and a Discovery Service Provider);
- An Attribute Provider (AP1), where she stores her *preferred language* preference and her *home zip code*;
- A location Attribute Provider (location AP), where her *current location* is stored.

The End User has also federated her Accounts at all of these Providers so that she can enjoy the benefits of Identity-based services. The End User now browses to CustomisedWeather.com, which is a customised weather Service Provider. CustomisedWeather.com requires the End User's *home zip code*, *preferred language*, and *current location* Attributes in order to offer a customised weather service. However, the End User does not have an Account at CustomisedWeather.com, and CustomisedWeather.com has no interest in the End User's Identity.

5.5.2 Actors

- End User – using a mobile Device
- Identity Provider – a mobile operator (or another Service Provider) that offers Single Sign On and Identity Attribute Discovery Service Identity services
- CustomisedWeather.com – a Service Provider providing customised weather information
- AP1 – an Attribute Provider that knows and manages the End User's *home zip code* and *preferred language* information and, when appropriate, provides this information to authorised requesting Service Providers
- Location AP – an Attribute Provider that knows and manages the End User's *current location* information and, when appropriate, provides this information to authorised requesting Service Providers

5.5.2.1 Actor Specific Issues

5.5.2.2 Actor Specific Benefits

Using anonymous Attribute Transfer the End User is relieved from the tedious task of filling in her own Identity information at Service Providers with whom she does not have an Account.

5.5.3 Pre-conditions

- The End User has an Account with the Identity Provider (mobile operator, who is fulfilling the role of Identity Provider and Discovery Service Provider)
- The End User does not have an Account with CustomisedWeather.com (although she could have)
- The End User has an Account with AP1
- AP1 knows the End User's *home zip code* and *preferred language* Attributes
- The End User has an Account with the location Attribute Provider
- Location AP knows the End User's current location
- AP1 and location Attribute Provider have made the necessary arrangements (business and technical) with the Identity Provider to use Single Sign On and Discovery Service services provided by Identity Provider
- The End User has federated her AP1 and location AP Accounts with her IDP Account so that she can take advantage of SSO services and Discovery Service services
- The End User has set the appropriate permissions for the release and usage of her Attributes stored at AP1 and location AP
- The IDP (mobile operator) has already authenticated the End User using GSM (SIM Smart Card based) Authentication. This form of Authentication is easily secure enough to be acceptable for AP1 and the location AP

5.5.4 Post-conditions

- CustomisedWeather.com has obtained the End User's *home zip code* and *preferred language* Attributes from AP1
- CustomisedWeather.com has obtained the End User's *current location* Attribute from location AP
- CustomisedWeather.com provides a customised view of the End User's weather - both at the End User's current location as well as at their home location - using the End User's preferred language

5.5.5 Normal Flow

1. End User accesses CustomisedWeather.com service using the browser on her Device.

2. CustomisedWeather.com requires the End User's *home zip code*, *preferred language*, and *current location* Attributes, and so it contacts the mobile operator to discover which Attribute Providers it should contact for the Attribute information it requires.

3. The operator checks whether the End User has been authenticated. (This could be done in one of two ways: either the operator could display a dialogue requesting the End User to enter her operator Identifier, or the End User's Device could interrogate the End User's SIM Smart Card to obtain a suitable operator Identifier.) The operator determines that the End User has already been authenticated.

4. The operator checks the End User's preferences to verify that the End User has not asked the operator to 'black list' CustomisedWeather.com.

5. The operator determines that it is allowed to give the Addresses of the End User's Attribute Providers to CustomisedWeather.com, and so responds to CustomisedWeather.com with the Addresses of AP1 and location AP. The operator also passes CustomisedWeather.com suitable Identity Credential information to pass to the Attribute Providers so that the APs will know the Identity of the End User without requiring End User interaction. (Note that CustomisedWeather.com will not be able to determine the End User's Identity from this Credential information. Note also that the Credential information to be used at AP1 will be different from the Credential information to be used at the location AP.)

6. CustomisedWeather.com requests the End User's *home zip code* and *preferred language* information from AP1, and her *current location* information from the location AP.

7. Having checked that the End User's permissions allow the release of the Attribute information, AP1 releases the *home zip code* and *preferred language* information to CustomisedWeather.com.

8. Having checked that the End User's permissions allow the release of the Attribute information, AP2 releases the *current location* information to CustomisedWeather.com.

9. CustomisedWeather.com provides a customised view based on the zip code and language preference of the End User.

Note that CustomisedWeather.com has not received or been able to deduce the Identity of the End User at any time during this flow. This means that if the same End User revisited CustomisedWeather.com there is no way for CustomisedWeather.com to identify that it is the same End User browsing its site (unless cookies are stored).

5.5.6 Alternative Flow

5.5.7 Operational and Quality of Experience Requirements

5.6 Use Case 6, Transactions and Event Tokens

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X	X	X	X	X
Additional Keywords					

Table 7: Affected Areas for Transactions

5.6.1 Short Description

This use case describes the Identity aspects of how an End User can make purchases of goods and services using mobile Device enabled payment processes, where the merchant selling the goods and / or services could be a retail establishment or an online vendor. (Note that this use case describes the case of a physical shop, but it could easily also apply to an online merchant.)

In this use case an End User makes several purchases - she purchases a CD, an electronic concert ticket, and some digital content. Both the electronic concert ticket and the digital content (a ring tone) are then stored locally on her mobile Device or on a different Principal Agent for subsequent use.

The End User is a great fan of a new band called Mopaybius. While wandering around a (physical) CD shop she sees a poster that advertises a special promotion. The promotion is for a discounted package that includes the latest Mopaybius CD and a ticket to an upcoming Mopaybius concert. The End User wishes to purchase this promotional package, and so takes a copy of the CD to the shop's point of sale. Whilst waiting in the queue she notices a further poster, advertising that anyone that uses a special mobile payment service, called Paymate, to buy a CD will also be given a free ring tone download for use on their mobile Device.

The End User has a Paymate Account and so she decides to use Paymate to pay for her Mopaybius package. She tells the shop assistant that she would like to use Paymate, and then she presses a button on her mobile Device and holds it near to the point of sale terminal. A message appears on her Device screen asking her to enter her PIN code to authorise a transaction of amount X to Shop. She does this, and then a few seconds later her transaction is shown as authorised on the point of sale terminal. A further message appears on the End User's Device screen to inform her that an electronic Event Token for a Mopaybius concert and a Mopaybius ring tone have been received (by her Principal Agent). The End User is able to start using the ring tone immediately.

On the evening of the Mopaybius concert, the End User selects the electronic Event Token from a list (of tokens that she has previously bought) displayed on her mobile Device screen. She then presses a button and holds her Device near the turn-style that will allow her access into the concert arena.

The key to this use case is the trust between all of the parties involved:

- The End User trusts that her Identity information will be kept secure during the transaction, and that she will receive all of the products and services that she purchases;
- The Shop trusts that it will be paid by the Payment Service Provider ('Paymate') for the products that it sells;
- The Payment Service Provider ('Paymate') trusts that the End User authorised the transactions that it bills to her Account, and that she will pay her bill at the end of the month;
- The Identity Provider (the mobile operator) trusts that the Authentication Assertions that it provides to 'Paymate' will be kept securely, and that it will be paid for the Identity services that it provides;
- The Concert Promoter trusts that it will be paid for the electronic ticket Event Tokens, and that the electronic Event Token distribution process will be secure and auditable.

The key element required to support all of these trust relationships is the Identity process that ensures that all participants are who they say they are. The rest of this use case describes how an Identity Management enabler can be used to support this scenario.

5.6.2 Actors

- End User – using a mobile Device
- Identity Provider – a mobile operator, that provides Identity Authentication Assertions for transaction Authorisation
- Payment Service Provider – called 'Paymate', that provides transaction Authorisation, billing and clearing services. 'Paymate' has agreements with several mobile operators, allowing End Users to use their mobile Devices to authorise transactions and, in some cases, use their mobile operator Accounts to pay for the transactions
- Shop – a merchant retail facility that sells goods or services and supports the mobile payment mechanism offered by 'Paymate' for purchase of merchandise and/or services. The Shop also has an online buying site
- Concert Promoter – a merchant that organises pop concerts and uses other merchants (such as Shop) to sell tickets for the concerts. Concert Promoter uses electronic Event Token tickets as well as physical tickets

5.6.2.1 Actor Specific Issues

- The End User must be assured that she will not be billed for transactions that she did not authorise
- The Identity Provider must be assured that Identity information and Authentication Assertions that it provides will only be used for authorised purposes
- The Payment Service Provider must be assured that transactions that it processes were authorised by the End User (and, as an aside, that the End User will pay for them)
- The merchants must be assured that they will be paid for the goods and services that they sell to the End User

5.6.2.2 Actor Specific Benefits

- The End User has a convenient and secure way to purchase goods and services
- The Identity Provider (mobile operator) has an additional source of revenue for the Authentication Assertion services offered to 'Paymate'
- 'Paymate' reduces its transaction risk by using reliable Authentication for transactions (including for low value transactions)
- The merchants are able to attract customers by offering a convenient payment option that also allows for new service packages to be created. The merchants also benefit from the security of 'Paymate's secure End User Authorisation mechanisms

5.6.3 Pre-conditions

- The End User has an Account with the Identity Provider (the mobile operator)
- The End User has an Account with the Payment Service Provider ('Paymate'), and her 'Paymate' Account details are stored in her GSM SIM Smart Card inside her Device
- The merchant has made the necessary arrangements (business and technical) in order to use the services of 'Paymate'

- 'Paymate' has made the necessary arrangements (business and technical) with the mobile operator, in order for End Users to use their Devices to authorise transactions at points of sale (physical and online)
- The End User has federated her Accounts at the Identity Provider and 'Paymate'
- The Concert Promoter has made the necessary arrangements (business and technical) with the merchant to allow electronic Event Tokens to be sold by the merchant and stored locally on End Users' Devices (e.g. on the End Users' GSM SIM Smart Cards) until time of the concert
- The merchant has made the necessary arrangements (business and technical) with the mobile operator to use their 'Digital Content Secured' service
- The Concert Promoter has made the necessary arrangements (business and technical) with the mobile operator to use the operator 'Event Tokens Secured' service

5.6.4 Post-conditions

- The End User has purchased goods or services from the merchants and she has authorised the Shop to process a payment request to her Payment Service Provider ('Paymate')
- The Shop has processed a payment request to the End User's Payment Service Provider, and has collected payment

5.6.5 Normal Flow

Initial Transaction

1. The End User decides to purchase goods from the Shop. She tells the Shop assistant that she would like to use 'Paymate' to pay for the transaction.

2. The Merchant creates a transaction for the goods in a point of sale terminal and asks the End User to send her 'Paymate' details (e.g. her name and 'Paymate' Account details) to the point of sale terminal.

3. The End User presses a button on her mobile Device and holds it near to the point of sale terminal. Her Device accesses her 'Paymate' information (e.g. from her GSM SIM Smart Card inside the Device), and then transmits it wirelessly to the point of sale terminal, using some type of local link radio technology.

4. The Shop point of sale terminal contacts 'Paymate' to request transaction Authorisation. For low value transactions (such as buying a can of drink) 'Paymate' may allow End Users to not have to enter a PIN to authorise the transaction (Device Authentication would be sufficient, without having to bother the End User). However, to authorise the purchase of a CD the End User must first be authenticated (including PIN entry) to give Authorisation for the purchase.

5. 'Paymate' already has the name of the End User's mobile operator stored in her 'Paymate' Account, and so contacts her mobile operator, requesting the mobile operator to authenticate the End User in order to prove her Authorisation.

6. The mobile operator sends an End User Authentication request to her Device (e.g. by sending a message to her GSM SIM Smart Card), and a message appears in her Device screen, asking her to enter her PIN if she wishes to pay an amount X to Shop.

7. The End User enters her PIN and presses OK. The mobile operator (e.g. by using her GSM SIM Smart Card) verifies the End User's PIN and Device Identity.

8. Assuming the Authentication is successful then the mobile operator sends an affirmative message back to 'Paymate', including a transaction number.

9. 'Paymate' determines whether the End User has adequate credit capability to process the transaction and, assuming she has adequate credit, sends a message, which includes the mobile operator transaction number, back to the Shop authorising the transaction.

10. Upon receiving the transaction Authorisation from 'Paymate', the Shop's point of sale terminal completes the transaction and sends a transaction completed and payment request message to 'Paymate' and the initial transaction is complete.

Delivering the Digital Content

11. The merchant sends a request to the mobile operator requesting the use of the mobile operator 'Digital Content Secured' service, and includes the digital content (the ring tone) to be secured, and the transaction number that was used in the initial transaction.

12. The mobile operator secures the content (by encrypting it for the correct End User's Principal Agent) and delivers it to the Device of the End User. The mobile operator also sends the Rights Object for the digital content to the End User's Principal Agent (e.g. her GSM SIM Smart Card. If the End User subsequently gets a new Device, then if she moves her GSM SIM Smart Card to the new Device, she will keep her Rights Object for the digital content).

Delivering the electronic Event Token

13. The Shop sends a message to the Concert Promoter, to say that an End User has purchased a ticket for the Mopaybius concert. The message includes the transaction number that was created by the mobile operator.

14. The merchant sends a request to the mobile operator requesting the use of the mobile operator 'Event Tokens Secured' service, and includes the Event Token (the Mopaybius ticket) to be secured, and the transaction number that was used in the initial transaction.

15. The mobile operator secures the content (by encrypting it for the correct End User's Principal Agent) and delivers it to the Device of the End User (e.g. to her GSM SIM Smart Card, as it is a removable Device. If the End User subsequently gets a new Device, then if she moves her GSM SIM Smart Card to the new Device, she will be able to keep her electronic Event Token).

16. On the day of the concert, when the End User gets to the turn-style, she selects the Mopaybius ticket Event Token from a list that is displayed by her Device. She then presses a button and holds her Device near the turn style (which is operated by the Concert Promoter).

17. The End User's Device sends the secured content (the Event Token) wirelessly to the turn style, and includes an encrypted Identifier for itself (or its Principal Agent), and the Address of the End User's Identity Provider.

18. The Concert Promoter sends this information to the mobile operator for verification. The mobile operator verifies that the digital content (Event Token) came from the correct Principal Agent, and then responds to the Concert Promoter.

19. The End User is allowed to pass through the turn style and enjoy the Mopaybius concert.

Payment

20. The Payment Service Provider ('Paymate') bills the End User for all the charges incurred during a billing period, and then distributes the money appropriately.

5.6.6 Alternative Flow

5.6.7 Operational and Quality of Experience Requirements

5.7 Use Case 7, Authentication Domains, Identity Brokers and Circles of Trust

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X	X	X	X	
Additional Keywords					

Table 8: Affected Areas for Authentication Domains, Identity Brokers and Circles of Trust

5.7.1 Short Description

The relevance of Single Sign On to OMA was discussed in Use Case 1. One of the pre-conditions there was that the Service Providers (Movie Ticket Service Provider and Restaurant Locator Service Provider) and the Identity Provider (mobile operator) had made the necessary arrangements (both technical and business) in order to federate an End User's Accounts. In a deployment scenario where several Identity Providers and Service Providers exist though, it is highly likely that each Identity Provider will have business agreements with several Service Providers. Furthermore, a Service Provider may have to enter into a business agreement with many Identity Providers in order to cover a large customer base, which is not desirable from a Service Provider's point of view. In order to address these points the notion of Authentication Domains, Identity Brokers and Circles of Trust are introduced.

An Authentication Domain consists of one Identity Provider and all the Service Providers (and End Users) that have the necessary technical and business arrangements in place with the Identity Provider in order to be able to offer (or use) SSO services. The Service Providers (and End Users) in an Authentication Domain need not have business relationships amongst themselves since they can use the Identity Provider to provide the level of trust required to co-operate. Therefore two Authentication Domains (that each consist of an IDP, six SPs and six End Users) could be drawn as follows:

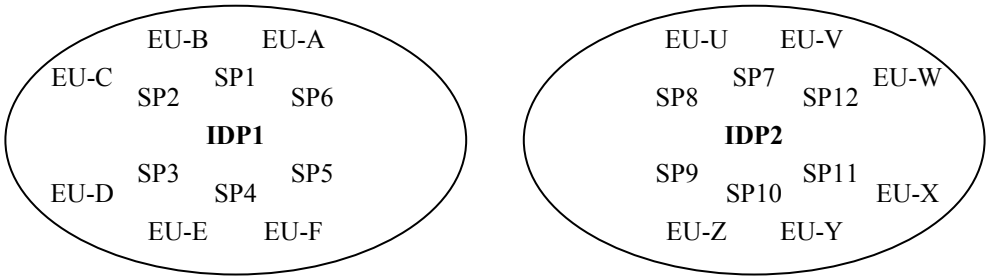

Figure 5: Two separate Authentication Domains

Let's say now that IDP1 and IDP2 create a business agreement that allows them to act as *Identity Brokers* for each other. We have two Authentication Domains still, but IDP1 and IDP2 can act as Identity Brokers in order to introduce Service Providers in one Authentication Domain to an Identity Provider (and hence End Users) in another Authentication Domain. Now the diagram would be updated as follows:

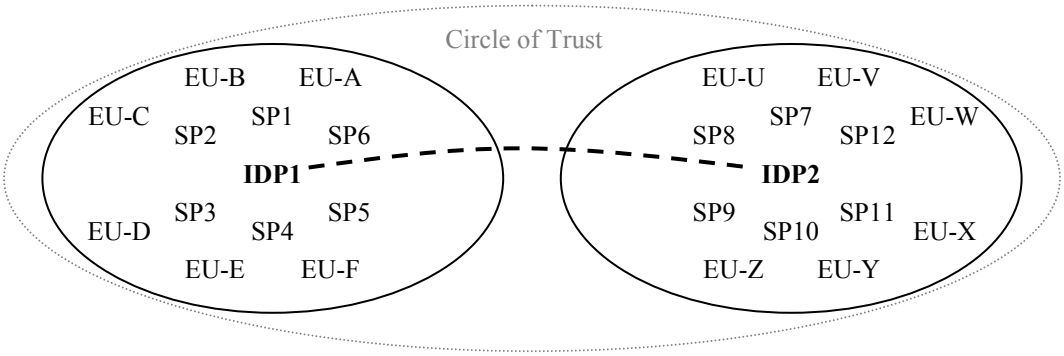

Figure 6: Two separate Authentication Domains, with a business relationship between IDP1 and IDP2 that creates a Circle of Trust

To introduce the final term, Circle of Trust, a Circle of Trust means that there is a potential trusted link between every End User and every Service Provider in the Circle of Trust. For example, in Figure 6, End User W could communicate with SP2 using IDP2 and IDP1 to provide the level of trust required (because End User W has a business agreement with IDP2, IDP2 has a business agreement with IDP1, and IDP1 has a business agreement with SP2).

A Circle of Trust could, itself, be a part of a bigger Circle of Trust, to the extent that if every IDP acts as an Identity Broker for at least one or two other IDPs then it would be easily possible to create an almost global Circle of Trust[2]. To complete the description of Circles of Trust, Figure 7 shows an extension of the Circle of Trust shown above, where more Authentication Domains are involved. (Note that a solid oval represents an Authentication Domain, whilst a dotted oval represents a Circle of Trust.) An End User in IDP5's Authentication Domain could use the services of a Service Provider in IDP1's Authentication Domain, using IDP5, IDP3, IDP2 and IDP1 to broker the trust required for them to communicate.

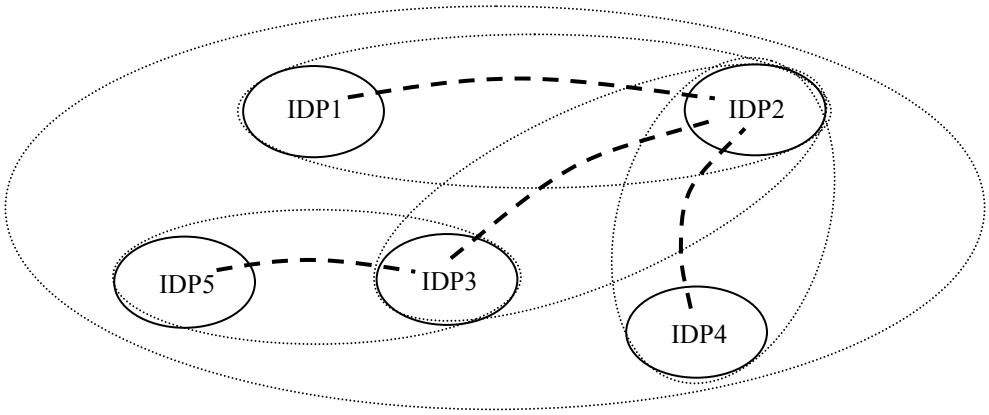

Figure 7: Multiple Authentication Domains, all part of one Circle of Trust due to Identity Brokering agreements

Note that an Identity Broker need not necessarily be an Identity Provider, but could be a Service Provider that creates the necessary technical and business agreements with several Service Providers and several Identity Providers in order to fulfil the role of Identity Broker. Note that in this case the Identity Broker would not need to have a direct (business) relationship with End Users, but just with Service Providers.

To see how an Identity Broker would actually be used, let's say that End User A (EU-A, in IDP1's Authentication Domain) wishes to use the services of SP7 (in IDP2's Authentication Domain), and also enjoy the benefits of Single Sign On and Seamless Attribute Transfer. End User A does not have a business relationship with IDP2, and neither does SP7 have a

[2] *As an aside, there is a saying that everyone in the world knows everyone else in the world using only 6 'connections' to introduce them. E.g. Anna knows Bob, Bob knows Charlotte, Charlotte knows Dave, Dave knows Emma, Emma knows Frank, and Frank knows Gary, so Anna could be introduced to Gary using only 5 'intermediaries'. Extending this to the concept of Circles of Trust would imply that for any Service Provider to communicate in a trusted manner with any End User would only take a maximum of 5 Identity Broker 'introductions'. Of course this is pure surmise, based on no fact, but it may help to clarify the concept of Identity Brokers and Circles of Trust. In reality it is possible, or even likely, to take much fewer than 5 intermediaries.*

business relationship with IDP1. However, End User A and SP7 can make use of IDP1 and IDP2 to broker the trust required to support:

- Single Sign On;
- A Discovery Service for End User A's available Identity Attributes;
- Attribute Transfer.

Each of these requires Federation of End User A's Account with IDP1 with End User A's Account at SP7. Therefore the first part of this use case addresses how Federation can take place using an Identity Broker. Subsequent to the Federation, SSO and Seamless Attribute Transfer are discussed briefly.

In order to support the Normal Flow of this use case, Figure 7 is updated to include End User A and SP7. Remember that IDP2 is acting as an Identity Broker henceforth in this use case.

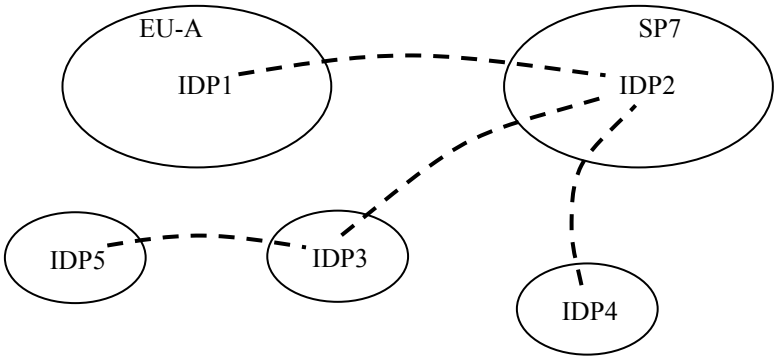

Figure 8: IDP2 acts as an Identity Broker for SP7, and End User A wishes to use SP7 services

5.7.2 Actors

- End User A – using a mobile Device
- IDP1 – a mobile operator that offers Identity services
- IDP2 and IDP 3 – two Identity Providers that are acting as Identity Brokers
- IDP4 and IDP 5 – two further Identity Providers
- SP7 – A Movie Ticket Service Provider (referred to as MTSP) that provides downloadable movie tickets

5.7.2.1 Actor Specific Issues

5.7.2.2 Actor Specific Benefits

5.7.3 Pre-conditions

Federation

- End User A has an Account with the mobile operator (IDP1)
- End User A does not have an Account with IDP2, IDP3, IDP4 or IDP5
- End User A has an Account with the Movie Ticket Service Provider (SP7)
- The Movie Ticket Service Provider has made the necessary arrangements (business and technical) with IDP2 (who is acting as an Identity Broker) to use the Identity Services offered by IDP2

- IDP2 has made the necessary arrangements (business and technical) with the mobile operator (IDP1), IDP3 and IDP4 in order to act as an Identity Broker between them and the MTSP
- IDP3 has notified IDP2 of all the names of the Identity Providers for which it can act as a Broker (i.e. the name of IDP5)
- IDP2 has notified the Movie Ticket Service Provider of all the names of the Identity Providers for which it can act as an Identity Broker (i.e. the names of the mobile operator (IDP1), IDP3, IDP4 and IDP5)

Single Sign On

- End User A's Account at the mobile operator (IDP1) has been federated with her Account at the MTSP
- The mobile operator has previously authenticated End User A, by authenticating the GSM SIM Smart Card inside her Device

5.7.4 Post-conditions

Federation

- End User A's Account at the mobile operator (IDP1) has been federated with her Account at the MTSP, using IDP2 to provide the level of trust required for this to happen

Single Sign On

- End User A has seamlessly signed in to the MTSP's web site

5.7.5 Normal Flow

Federation

1. End User A accesses the MTSP web site, where she has an Account. The MTSP advertises a feature called Single Sign On, which End User A decides to try out. The MTSP web site explains the concept of SSO, and also tells End User A that her mobile operator is likely to be an Identity Provider that she could use for SSO at the MTSP site.

2. The MTSP displays a list of all the possible Identity Providers that could be used for SSO at the MTSP web site, which includes the mobile operator's name (the MTSP was notified by IDP2 of all the possible Identity Providers that can be used).

3. End User A selects the mobile operator's name and consents to the MTSP federating her Account at the MTSP with her Account at the mobile operator.

4. Since the MTSP does not have a direct business relationship with the mobile operator, but knows that IDP2 can broker a relationship with the mobile operator, the MTSP contacts IDP2 to request the Federation of End User A's Account at the MTSP with End User A's Account at IDP2. The MTSP includes an optional name Identifier (e.g.x9rr56y) that it would like IDP2 to refer to End User A as when the MTSP subsequently contacts IDP2 about that individual End User. The MTSP also notifies IDP2 which Identity Provider (i.e. the mobile operator) End User A selected.

5. IDP2 (if this was not already done when the brokering agreement was set up with IDP1 – the mobile operator) creates an Account for End User A, and gives it an Identifier of 'x9rr56y'.

6. IDP2 contacts the appropriate Identity Provider (the mobile operator) to request the Federation of End User A's Account at IDP2 with End User A's Account at the operator. IDP2 includes an optional name Identifier (e.g. 124xyz) that it will use as an Identifier for End User A subsequently. Note that End User A may be known by a different Identifier internally at the operator. IDP2 also includes the name of the MTSP, as it is End User A's Account at the MTSP that End User A wishes to federate with her Account at the mobile operator.

7. Upon receiving the Federation request from IDP2 the mobile operator prompts End User A to identify herself (alternatively her Device and GSM SIM could handle this, for example). The mobile operator then authenticates End User A

and verifies that she would like to federate her Account at the mobile operator with her Account at the MTSP (IDP2 had passed the name of the MTSP to the mobile operator in the previous step).

8. Having obtained End User A's consent the operator federates her Account at the mobile operator with her Account at IDP2. The operator then sends a Federation response message back to IDP2 indicating successful Federation.

9. Once End User A's Accounts at the mobile operator and IDP2 have been federated, IDP2 then federates her Account at IDP2 with her Account at the MTSP, and then sends a Federation response message back to the MTSP indicating successful Federation. The MTSP notifies End User A that her Accounts have been federated successfully.

10. End User A's Account at the mobile operator has now been federated with her Account at the MTSP, using an Account for End User A at IDP2 to mediate the trust required for the Federation to occur. The next time that End User A visits the MTSP web site, she is able to click on an icon representing her operator (for example) and then enter her Identifier at the operator to take advantage of SSO.

Single Sign On

1. End User A visits the MTSP site using her Device and wishes to authenticate herself to the MTSP using Single Sign On. The MTSP displays a list of possible Identity Providers that it can make use of for SSO services.

2. End User A selects the name of her mobile operator from the list, and clicks on a 'Log In' button (the service could alternatively request End User A's GSM SIM Smart Card to obtain the name of her preferred Identity Provider, thereby simplifying the End User experience further).

3. The MTSP contacts IDP2, requesting SSO for whomever is currently accessing the MTSP using the browser on their Device. The MTSP also passes the name of the IDP that End User A selected (i.e. the mobile operator).

4. IDP2 contacts IDP1 (the mobile operator) and requests the mobile operator to authenticate whomever is currently accessing the MTSP using the browser on their Device.

5. The mobile operator requests the End User to identify herself (note that the mobile operator could alternatively interrogate End User A's GSM SIM Smart Card for an Identifier for End User A). The mobile operator does not need to authenticate End User A because she was previously authenticated by the mobile operator when she powered up her Device.

6. The mobile operator sends an Authentication Assertion to IDP2, using the Pseudonym Identifier that was created during Federation to identify End User A (i.e. 124xyz).

7. IDP2 can use the Pseudonym Identifier 124xyz to determine who the End User is.

8. IDP2 sends an Authentication Assertion to the MTSP, using the Pseudonym Identifier that was created during Federation to identify End User A (i.e. x9rr56y). Note that when IDP2 forwards the Authentication Assertion on to the MTSP it could potentially make modifications such as adding its own signature, adding its own Authentication Assertion, etc.

9. The MTSP can use the Pseudonym Identifier 124xyz to determine who the End User is, and therefore allows End User A to access her Account seamlessly.

(Seamless Attribute Transfer)

Note that once Federation and SSO have taken place, then Seamless Attribute Transfer could also occur. Note that all messaging between a Service Provider (the MTSP in this case) and an End User's Identity Provider (the mobile operator in this case) would be directed via the Identity Broker (IDP2 in this case).

5.7.6 Alternative Flow

5.7.7 Operational and Quality of Experience Requirements

5.8 Use Case 8, Service Provider Alliances

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X		X	X	
Additional Keywords					

Table 9: Affected Areas for Affiliations of Service Providers

5.8.1 Short Description

There are many cases where several Service Providers decide to work together to form an Alliance so 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 Alliance has to offer as a collective unit. Consider the following Alliances:

- Alliance among airline carriers (e.g. the Star Alliance, consisting of United Airlines, Lufthansa and several other airline carriers, or the One World Alliance, consisting of American Airlines, British Airways, Finnair and several other airline carriers);
- 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, an investment advice Provider and a company car Provider, which appear as one Alliance on a company's web portal.

Use Cases 1 and 4 described cases where the End User experience is enhanced by the use of SSO and Seamless Attribute Transfer between a (Attribute) Service Provider and an Identity Provider. 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.

The purpose of presenting this use case is to illustrate that there are benefits if an End User federates her Account at an IDP with not just a single Service Provider, but with an Alliance of Service Providers instead, and benefits if Seamless Attribute Transfer is possible between an Attribute Provider and an Alliance of Service Providers as opposed to just one. Two advantages of this are:

- The End User does not need to have an individual Account at each member of the Alliance;
- The End User does not need to individually federate her Accounts at each member of the Alliance with her Account at the IDP.

This use case shows an End User using her Device to browse the site DiscountAirlineTickets.com for airline ticket prices and suitable travel itineraries.

5.8.2 Actors

- End User – using a mobile Device
- Identity Provider – a mobile operator that offers Identity services
- DiscountAirlineTickets.com – a Service Provider that sells airline tickets
- DiscountCarRentals.com – a Service Provider that makes car rental reservations
- DiscountHotels.com – a Service Provider that makes hotel reservations

- DiscountAlliance – an Alliance service that includes three Service Providers: DiscountAirlineTickets.com, DiscountCarRentals.com and DiscountHotels.com
- Attribute Provider – a Service Provider who knows and manages the End User's residential Address, and is able to store other End User preferences, such as hotel and hotel room preferences

5.8.2.1 Actor Specific Issues

5.8.2.2 Actor Specific Benefits

5.8.3 Pre-conditions

- The End User has an Account with the Identity Provider (the mobile operator)
- The End User has been authenticated by the mobile operator, using the SIM Smart Card in her Device
- The End User has an Account with the Alliance DiscountAlliance
- The Alliance DiscountAlliance has made the necessary arrangements (business and technical) with the Identity Provider to use Single Sign On services and Identity Attribute Discovery Services provided by the Identity Provider
- The End User has stored her residential Address, and her hotel and hotel room preferences at the Attribute Provider. The End User has also set her permissions appropriately to allow the DiscountAlliance to obtain these Attributes from the Attribute Provider
- The Attribute Provider has made the necessary arrangements (business and technical) with the Identity Provider to use the Identity Attribute Discovery Services offered by the Identity Provider

Single Sign On and Seamless Attribute Transfer

- The End User has federated her Account at Discount Alliance (via one of the DiscountAlliance Service Providers) with her Account at the IDP

5.8.4 Post-conditions

Federation

- The End User's Account at the IDP (the mobile operator) is federated with the Alliance DiscountAlliance. This ensures that the End User can seamlessly browse any site that is a member of the Alliance DiscountAlliance

Single Sign On

- The End User can seamlessly access any of the sites (e.g. DiscountCarRentals.com) that is a member of the Alliance DiscountAlliance

Seamless Attribute Transfer

- The End User's residential Address information (stored at the Attribute Provider) is seamlessly provided to DiscountHotels.com, on the basis that DiscountHotels.com is a member of the DiscountAlliance

5.8.5 Normal Flow

Federation of an IDP Account with an Alliance

1. The End User browses the site discountAirlinesTickets.com (which required the End User to authenticate herself to the site).

2. The site DiscountAirlineTickets.com realises that the End User experience can be simplified if her Account at DiscountAirlineTickets.com is federated with her Account at an Identity Provider. The site DiscountAirlineTickets.com also realises that since it is a member of the Alliance DiscountAlliance, the End User experience can be further enhanced if the Federation is done not just to DiscountAirlineTickets.com but to the Alliance as a whole. Therefore DiscountAirlinesTickets.com prompts the End User, asking whether she would like to federate her Account at an Identity Provider with the Alliance DiscountAlliance (which DisountAirlineTickets.com is a member of). The End User decides that she would like to do this.

3. DiscountAirlineTickets.com displays a list of all the possible Identity Providers that could be used for SSO at the DiscountAirlineTickets.com, which includes the End User's mobile operator's name. The End User selects the mobile operator's name and consents to DiscountAirlineTickets.com federating her Account at the mobile operator with the Alliance DiscountAlliance.

4. DiscountAirlineTickets.com requests Federation with the IDP in the normal way (see Use Case 2 for more details).

5. Furthermore, DiscountAirlineTickets.com is able to create Federation requests on behalf of all the other Providers in DiscountAlliance (using a bulk Federation (see Use Case 3 for more details)), before passing the appropriate Federation information on to each of the other members of the DiscountAlliance.

SSO with an Alliance

Since the End User's Account at each of the Providers in DiscountAlliance has been federated with her Account at the mobile operator, SSO is possible in the usual way (see use case 1 for more details).

Seamless Attribute Transfer

Since the End User's Account at each of the Providers in DiscountAlliance has been federated with her Account at the mobile operator, Seamless Attribute Transfer is possible in the usual way (see use case 4 for more details).

5.8.6 Alternative Flow

5.8.7 Operational and Quality of Experience Requirements

5.9 Use Case 9, Instant Messaging, Presence, Group Management and PoC

	Affected Areas				
	Device	Connectivity	Enabling Services	Applications	Content
Tickmarks (X)	X		X	X	X
Additional Keywords					

Table 10: Affected Areas for Instant Messaging, Presence, Group Management and PoC

5.9.1 Short Description

As mobile operators broaden the range of P2P communication services they offer, instant communication tools such as IM or Push-to-Talk services are expected to appeal to an increasingly important portion of their customer base, such as corporate customers or young End Users. A central element in this service architecture, the Group Management enabler, is responsible for creating and maintaining lists of contacts / buddies – potentially in an ad hoc manner.

A typical use case could involve three End Users: Alan, Sarah and Sam. Alan is a customer of mobile operator 1 and has subscribed to the instant communication service of Instant Communication Service Provider 1, ICSP1 (a partner of mobile operator 1), which he accesses using his mobile Device. Sarah, a friend of Alan's, is a customer of mobile operator 2 and uses the instant communication service of ICSP2 (a partner of mobile operator 2), which inter-works with ICSP1's service. Sam, another friend of Alan's, is also a customer of mobile operator 2 and also uses the instant communication services of ICSP2. Presence AP is a partner of mobile operator 2, and is a presence Attribute Provider for all customers of mobile operator 2.

Mobile operator 1 offers a 'buddy list' service that allows Alan to create and maintain a list of his buddies. These buddies could potentially be serviced by other mobile operators or SPs (with whom mobile operator 1 has inter-working agreements). For each buddy (referred to by a nickname chosen by Alan) a set of Attributes can also be specified (e.g. preferred methods of communication (text messaging, PoC, etc.), preferred timing, etc.). Note that Alan has already added Sam to his buddy list, but has not yet added Sarah to his buddy list.

Alan can use ICSP1 to obtain the presence status of each of his buddies (e.g. 'available', 'present but not available', 'not present' etc.) so that he knows how and when to contact them. When Alan turns on his instant communication application on his Device, it sends a request to ICSP1 asking ICSP1 to obtain the presence information of all of Alan's buddies. This could be done:

- using a single request that would indicate the Identity of Alan's buddy list (Identity of a Group), thus letting ICSP1 interrogate mobile operator 1's Group Management 'buddy list' enabler in order to get the Identities of each buddy;
- using separate requests for each of the individual Identities in the buddy list (the Device itself would have to know / find out the Identities of Alan's buddies in this case).

In either case, ICSP1 would then use the Identities of all of Alan's buddies to obtain their presence information. This presence and availability information could be maintained by Attribute SPs in the same Authentication Domain as ICSP1, or in different Authentication Domains. In the case where an End User's presence information is stored in a different Authentication Domain, ICSP1 may contact the IDP of the Authentication Domain to discover how to obtain the presence information itself, or ICSP1 may use another ICSP (e.g. ICSP2) as a proxy to obtain the End User's presence information. In this use case, ICSP2 is used as a proxy to obtain the presence information. The buddies' presence and availability Attribute Provider(s) (i.e. Presence AP in the case of Sarah and Sam) would then decide what information to release, based on the preferences and permissions set by each buddy.

As previously stated, Sarah is not yet in Alan's buddy list. Alan decides to add Sarah to his buddy list and chooses a nickname for her (e.g. Sar01). Alan also indicates the Identity of mobile operator 2 (that provides service to Sarah) as well as an Identifier that would allow mobile operator 1 and mobile operator 2 to recognise / resolve Sarah's Identity (e.g. a telephone number or an e-mail Address). Alan and Sarah then start an instant communication (either using PoC or an IM

exchange), and decide to create a temporary chat room (which they call OurChat). The chat room may be private or public, but in this case it is public.

They then choose to invite a third person – Sam, who is another of Alan's buddies – to OurChat in order to begin a conversation. (Note that an alternate scenario would be for Sam to decide to join OurChat without specifically receiving an invitation from Alan, either using his real Identity or using a Pseudonym (i.e. anonymously – possible because OurChat is a public chat room).)

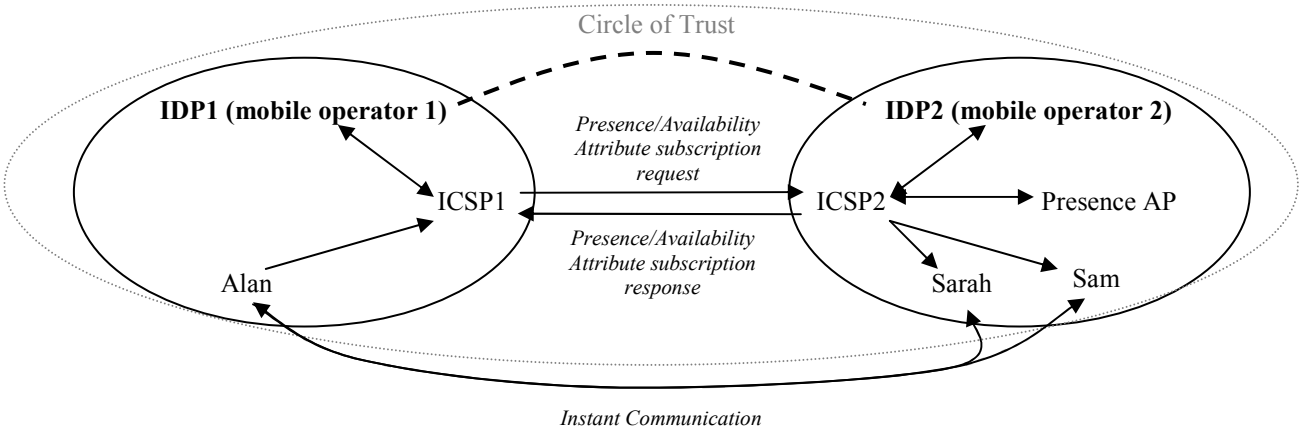

Figure 9: Roles involved in offering an Instant Communication service between three End Users who use two different mobile operators and Instant Communication Service Providers

5.9.2 Actors

- End User 1 – Alan, using a mobile Device
- End User 2 – Sarah, who is a friend of Alan's, using a Device
- End User 3 – Sam, who is a friend of Alan's, using a Device
- Identity Provider 1 – mobile operator 1, that offers Single Sign On and 'buddy list' Identity services
- Identity Provider 2 – mobile operator 2, that offers Single Sign On and Discovery Service Identity services
- Instant Communication Service Provider 1 (ICSP1) – a Service Provider that provides an Instant Communication service (PoC, IM, …) in partnership with mobile operator 1
- Instant Communication Service Provider 2 (ICSP2) – a Service Provider that provides an Instant Communication service (PoC, IM, …) in partnership with mobile operator 2
- Presence Attribute Provider (Presence AP) – an Attribute Service Provider that manages presence information for End Users

5.9.2.1 Actor Specific Issues

5.9.2.2 Actor Specific Benefits

5.9.3 Pre-conditions

- ICSP1 has made the necessary arrangements (business and technical) with mobile operator 1 in order to use the Single Sign On service and 'buddy list' service offered by mobile operator 1
- ICSP2 has made the necessary arrangements (business and technical) with mobile operator 2 in order to use the Single Sign On service and Discovery Service offered by mobile operator 2
- Presence AP has made the necessary arrangements (business and technical) with mobile operator 2 in order to use the Single Sign On service and Discovery Service offered by mobile operator 2
- ICSP1 and ICSP2 have an inter-working agreement with each other
- Alan has an Account with mobile operator 1 and an Account with ICSP1
- Alan has previously been authenticated by mobile operator 1
- Alan's Account at mobile operator 1 has been federated with his Account at ICSP1
- Alan uses the mobile operator 1 'buddy list' service to maintain a list of his buddies
- Sarah and Sam both have Accounts with mobile operator 2, Accounts with ICSP2, and Accounts with Presence AP
- Sarah and Sam have both previously been authenticated by mobile operator 2
- Sarah's Account at mobile operator 2 has been federated with her Account at ICSP2
- Sarah's Account at mobile operator 2 has been federated with her Account at Presence AP
- Sam's Account at mobile operator 2 has been federated with his Account at ICSP2
- Sam's Account at mobile operator 2 has been federated with his Account at Presence AP
- Sarah and Sam's preferences at Presence AP allow Presence AP to give out their presence information to ICSP2, even if ICSP2 is acting as a proxy for other Instant Communication Service Providers

5.9.4 Post-conditions

Registration of a new buddy

- Sarah becomes one of Alan's buddies that mobile operator 1 maintains in Alan's 'buddy list'

Subscription to presence information and Instant Communication

- ICSP1 is subscribed to Sarah's and Sam's presence / availability information
- Alan and Sarah start an Instant Communication through the preferred media (PoC, IM, etc…)

Chat Room Creation

- A public chat room, OurChat is created, which other people that use an Instant Communication Service Provider can join
- Sam joins OurChat

5.9.5 Normal Flow

Registration of a new buddy

1. Alan chooses a nickname for Sarah (Sar01) and indicates Sarah's Identity to mobile operator 1 using an Identifier for her that allows recognition / resolution of the Identifier both at mobile operator 1 and mobile operator 2. Alan would also indicate to mobile operator 1 an Identifier for mobile operator 2 and an Identifier for Sarah's preferred Instant Communication Service Provider (ICSP2 in this case).

2. Alan indicates the "buddy list" (colleagues, friends, family, etc…) to which he wants to add Sarah's nickname.

3. Mobile operator 1 adds Sarah to Alan's buddy list.

Subscription to presence information and Instant Communication

1. Alan activates his instant communication application on his mobile Device.

2. The instant communication application requests ICSP1 to find out the presence information for all of Alan's buddies. The application also passes an Identifier for Alan's buddy list 'Group', and an Identifier for mobile operator 1, who maintains Alan's buddy list on his behalf.

3. ICSP1 contacts mobile operator 1 and requests the Identities of all of the members of 'Alan's Buddy List' Group.

4. Mobile operator 1 responds to ICSP1 with the Identities and preferred Instant Communication Service Providers of Alan's buddies.

5. For each of Alan's buddies, ICSP1 makes requests to the relevant ICSPs (in the case of Sarah and Sam, ICSP2) for the presence information of Alan's buddies.

6. ICSP2 contacts mobile operator 2, passing the Identifiers for Sarah and Sam (e.g. phone numbers or e-mail Addresses), to discover how to obtain Sarah and Sam's presence information.

7. Mobile operator 2 uses the Identifiers to determine which Attribute Providers have the relevant presence information for Sarah and Sam (in this case Presence AP is used for both Sarah and Sam), and passes the AP information back to ICSP2.

8.ICSP2 contacts Presence AP to obtain the presence Attributes of Sarah and Sam.

9. Since Sarah and Sam's preferences allow their presence Attributes to be given out in this situation, Presence AP responds to ICSP2 with the information, which ICSP2 then passes back to ICSP1.

10. ICSP1 informs Alan of his buddies' whereabouts.

11. Alan wishes to start an Instant Communication (PoC, IM etc…) with Sarah and clicks on a "Start a communication using PoC" icon.

12. ICSP1 sends a request to ICSP2 requesting Instant Communication with Sarah.

13. ICSP2 asks for Sarah's approval to start the communication.

14. Sarah approves the request, and Alan and Sarah start to communicate.

Chat Room Creation

1. Alan and Sarah decide to start a temporary chat room in order to include other buddies in their conversation (PoC or text) and name it OurChat.

2. OurChat may be private or public, and may be restricted to specific buddies (aged under 25 only, etc…).

3. Sam, one of Alan's other buddies, who was also available, is invited to OurChat by Alan, who clicks on the 'invite a buddy' icon.

4. Sam approves the invitation and takes part in Alan and Sarah's conversation.

5.9.6 Alternative Flow

5.9.7 Operational and Quality of Experience Requirements

5.10 Open Issues

6. Requirements (Normative)

The following requirements were derived both from the Use Cases described in section 5 of this RD and, in some cases, from additional analysis of the topic:

6.1 High-Level Functional Requirements

HLF-1 The IdM enabler SHALL be able to distinguish between different types of Identities (e.g. Devices, Providers, End Users).

HLF-2 The IdM enabler SHOULD support a mechanism to map a Rights Object to a combination of Device Identities and other Principal Identities.

HLF-3 The IdM enabler SHALL support the use of removable or embedded secure storage (e.g. an operator SIM Smart Card or a built-in hardware module in a Device) as a secure Container for a Principal's Identity information.

HLF-4 In the IdM enabler:

(a) A Group SHALL be handled as a type of Principal, with its own Identity;

(b) Identity Attributes directly relevant to a Group's Identity (including a Group Identifier) SHALL be supported as Attributes of that Group (e.g. Group member Identifiers, Group 'active status', etc.).

HLF-5 If a Group publishes a list of the Principals in that Group (according to the Access Control Policies of those Principals), then the IdM enabler SHALL allow any (other) Principals (that have access to the information in the published list) to make use of any Identity services that relate to the Principals in the Group.

HLF-6 The IdM enabler SHALL allow a Device to act as a Principal Agent for an Attribute Provider or Identity Provider.

HLF-7 It SHALL be possible for a Principal to delegate the management of its Identity information to another Principal.

HLF-8 The IdM enabler SHALL include a mechanism for a Principal to specify the validity conditions (time, at least, SHALL be supported as one of these conditions) for an Attribute stored by an Attribute Provider. This mechanism SHALL specify what action is to take place if the validity conditions are not met.

HLF-9 A Principal SHALL be able to authorise who may receive their Attribute (e.g. location) information. This could be done using their Device, or using some other mechanism.

HLF-10 It SHALL be possible for End Users to have multiple Identities, and it SHALL be possible to segregate one Identity from another (e.g. for private use and business use).

HLF-11 The IdM enabler SHALL allow multiple Device Identities to be associated with one End User Identity (a Device is assumed to have only one Device Identity). It SHALL be possible to:

(a) Allow one End User (Identity) to use multiple Device Identities simultaneously;

(b) Limit the End User (Identity) to using only one Device Identity at a given time or for a particular service.

HLF-12 It SHALL be possible for multiple End User Identities to be associated with a single Device Identity.

HLF-13 It SHALL be possible to exchange Identity Attributes (e.g. presence info) across Authentication Domains (within Circles Of Trust).

HLF-14 The IdM enabler SHALL include a standard way for an Identity Provider to send an Assertion (that something occurred - e.g. an Authentication, or an Authorisation) to another Provider. It is assumed that the End User would authorise the sending of the Assertion (either directly or indirectly). Sending of Assertions will be subject to Identity Provider Policies. (Note that the Identity Provider could be the End User acting on his/her own behalf.)

HLF-15 The IdM enabler SHALL allow a Principal to:

(a) Use multiple unique Identities, where each Identity has its own Identifier;

(b) Have multiple Identifiers for a single Identity.

HLF-16 The IdM enabler SHOULD make use of existing, unique End User Identifiers for addressing End Users (e.g. MSISDN/IMSI, MDN/MIN, e-mail Address).

HLF-17 Where a Device is used to make a service request, the IdM enabler SHALL include a mechanism by which a Provider can ensure that responses (e.g. content that has been purchased) can only be returned to that same Device.

HLF-18 It SHALL be possible for a service acting on behalf of End User A to invoke an Identity service relating to End User B (within the constraints set by End User B). This SHALL be possible when:

- End User A and End User B use either the same or different IDPs;
- The SP that provides a service for End User A is in either the same or a different Authentication Domain from the SP that provides a service for End User B.

(e.g. this could be used to enable a friend finder service to get the current location of another user, or to enable a buddy list to access the presence of another user).

HLF-19 The IdM enabler SHALL be independent of the Device that the Principal uses to access a Provider.

HLF-20 The IdM enabler SHALL be agnostic to underlying network technologies (please see OMA Architecture Principles, section 5.1.1).

HLF-21 The IdM enabler SHALL support the ability of a Principal to use a Pseudonym as an Identifier for an Identity.

HLF-22 The IdM enabler SHALL enable (at least) the use of existing mobile operator Identity solutions for Authentication and End User Authorisation (e.g. the use of SIM Smart Cards, R-UIM Smart Cards and IS41 software solutions, depending on prioritisation).

6.1.1 Security

SEC-1 It SHALL be possible to authenticate the source of protected content.

SEC-2 The IdM enabler SHOULD support dynamic establishment of trust between two Providers (e.g. IDP/IDP or SP/IDP). This MAY require a mutually trusted 3rd party to introduce the IDP/IDP or SP/IDP.

SEC-3 It SHALL be possible for a Service Provider to belong to more than one Circle of Trust.

SEC-4 It SHALL be possible for any two communicating Principals to mutually authenticate, through the exchange of Authentication Assertions.

SEC-5 Where a Principal contacts a Device, the Device SHALL be able to authenticate the Principal and therefore obtain an Identifier for that Principal.

SEC-6 It SHALL be possible for applications on Devices to have authorised access to End User Identity information.

SEC-7 It SHALL be possible for an Identity Provider to authenticate an End User, independent of the type of Access Network involved (e.g. in the case where an End User roams between mobile operators, or in the case where an Identity Provider is not also an Access Network Provider).

SEC-8 It SHALL be possible to authenticate a Device (i.e. to determine whether the Device has at least one, unique, persistent, secured Identity).

SEC-9 The IdM enabler SHALL protect against potential security threats, including denial-of-service attacks and

Identity theft (e.g. when an Identity is reported stolen, notification could be sent from the Identity Provider to all Providers within the Authentication Domain).

SEC-10 The IdM enabler SHALL support confidential communication between Principals.

SEC-11 The IdM enabler SHALL support integrity protection in communication between Principals.

SEC-12 In Identity Management mechanisms specified by OMA, additional security MAY be performed by intermediaries.

6.1.2 Charging

CHRG-1 An IMF SHALL support a mechanism for Providers to capture charging/billing information when Identity services are provided.

6.1.3 Administration and Configuration

ADM-1 It SHALL be possible for multiple Principals to access / modify / monitor Identity information (within its scope of management control) on the Device and/or in the network. (Note that business agreements could create a hierarchy of management control scopes.)

ADM-2 The Principal that controls certain Identity information on a Device and/or in the network SHALL be able to authorise other Principals to access and/or change that Identity information in the in the Device and/or in the network on their behalf.

ADM-3 The IdM enabler SHALL include a mechanism for:

(a) The Principal (or the Principal's authorised delegate) that controls certain Identity information in a Device and/or in the network to be able to set/change permissions for how that Identity information in that Device and /or in the network may be changed. (e.g. Identity information could be Device Management Server information, End User Identity information, Device Identity information.);

(b) A provisioning function to be able to determine what information/settings in a Device and/or in the network may be provisioned, and the permissions associated with it;

(c) A provisioning function to set/change Identity information in a Device and/or in the network (according to the controlling Principal's permissions).

ADM-4 The Principal in control of certain Identity information in a Device and/or in the network SHALL be able to permanently transfer control of that Identity information in the a Device and/or in the network to a different Principal.

ADM-5 The IdM enabler SHALL support a mechanism for a Provider to obtain End User Access Control permissions (relating to Identity information in their Device and/or in the network) regardless of where the permissions are stored.

ADM-6 The IdM enabler SHALL support the ability of a Provider (e.g. to support Device Management):

(a) To find presence and other Identity information (e.g. software version Attribute) about a specified Device;

(b) To authenticate a specified Device.

ADM-7 The IdM enabler SHALL support a mechanism where Identity information stored in one Identity Container takes precedence over the Identity information stored in other Identity Containers (if there are multiple Identity Containers that include different values for the same Identity information type).

Note that the precedence hierarchy would be governed by End User and Provider Policies.

ADM-8 (a) The IdM enabler SHALL support a notification service when a Principal's Identity Attributes change.

(b) A Principal (and an Attribute Provider) SHALL be able to set permissions to control which other Principals may be notified of changes in their Identity Attributes.

(c) The IdM enabler SHALL support a mechanism to allow an appropriately authenticated and authorised Principal (or its delegate) to subscribe to receive notifications when the Identity Attributes of another, specified Principal are modified.

ADM-9 The IdM enabler SHALL allow delegation of authority from one Principal to another Principal (e.g. from an operator to an enterprise, or vice versa).

ADM-10 It SHALL be possible to create, manage the lifecycle of, and share application-specific Identity Attributes. (A solution for this requirement SHOULD consider common data models.)

ADM-11 The IdM enabler SHALL support an Identity Attribute that defines the lifetime of that Identity.

ADM-12 The IdM enabler SHALL support an Attribute that describes the preferred Device that SHOULD be used for a particular service.

ADM-13 (a) It SHALL be possible for a Principal to register/modify/delete a Principal's Identity at an Identity Provider, subject to Access Control Policies. This could be for itself, or for another (potentially new) Principal.

(b) It SHALL be possible for a Principal to register/modify/delete a Pseudonym as an Identifier for itself (or another Principal) at an IDP.

(c) It SHALL be possible for a Principal to register/modify/delete Pseudonyms (that the Principal uses at different Groups, for example) as Attributes of its Identity at an IDP.

ADM-14 In the case where the Access Network Service Provider (e.g. mobile operator, ISP, enterprise IT department) is also acting as an Identity Provider, it SHALL be possible for the Access Network Service Provider to have their IDP settings used by default.

6.1.4 Usability

US-1 There SHALL be no impact to the quality of experience when using supported IdM services (e.g. performance, behaviour) due to a Principal roaming across mobile networks (roaming in the traditional cellular sense).

US-2 (a) Where an End User's Identity information is transferred from their existing Device to another Device it SHALL be possible for the End User to control what data can be transferred.

(b) It SHALL be possible for the End User to authorise the transfer of their Identity information by providing input either on their own Device, or on the receiving Device (e.g. Point of Sale terminal).

US-3 An IDP SHALL be able to obtain End User Authorisation for a transaction (e.g. End User Authorisation for a text string reading "I would like to pay shop.com 20 USD").

US-4 An IDP SHALL be able to obtain End User Authorisation to consume a service. This Authorisation could then be passed on to the Service Provider offering the service.

6.1.5 Interoperability

IOP-1 Interfaces exposed by the IdM enabler to applications, other enablers and/or other network resources SHALL be compliant with OMA Service Environment architectural requirements.

IOP-2 Where standardised interfaces exist for obtaining data pertinent to the IdM enabler (e.g. an IdM Attribute Provider server obtaining Attributes from lower level network servers), then the IdM enabler specification SHOULD not duplicate the functionality of these existing interfaces. It is recommended that the existing standardised interface protocols SHOULD be used.

Furthermore, if other standards allow complex Attributes to be built up of lower level data from different sources transparently, then the IdM enabler SHOULD not duplicate these standardised functions.

An example of such a standardised interface is the 3GPP GUP specifications (TS 22.240 v6.3.0, TS23.240 v6.4.0, TS 29.240 v0.1.0).

IOP-3 The IdM specification SHALL support all Identity Attributes specified by other standards bodies, as deemed appropriate by the OMA IdM enabler. At the current time, the following standards bodies are deemed appropriate, and SHALL be complied with:

- 3GPP (e.g. GUP)
- 3GPP2 (if available at the time of IdM technical specification writing)

IOP-4 (a) If a Policy enforcement enabler is deployed by a Provider then the IdM enabler SHALL communicate with the Policy enforcement enabler in order for the enabler to carry out Policy enforcement.

(b) Where a Policy enforcement enabler delegates either the evaluation or execution steps to the IdM enabler, or no Policy enforcement enabler is deployed, then the IdM enabler SHALL be able to perform the Identity related Policy enforcement (the evaluation and/or execution) itself.

IOP-5 The IdM enabler specification SHALL document all Identity related information it may produce, including the conditions under which it would produce such information. This information could be used in order to create Policies, for example.

6.1.6 Privacy

PRV-1 It SHALL be possible for a provisioning function to erase a previous End User's Identity information from a Device without first being able to access the previous End User's Identity information.

PRV-2 In the case where an IDP has separately federated a Principal's Identity with two or more SPs, it SHALL not be possible for the SPs to use information given to them by the IDP in order to collude to determine that the Identities refer to the same Principal.

6.2 Overall System Requirements

6.2.1 Affiliation

AFF-1 The IdM enabler SHALL 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.

AFF-2 The IdM enabler SHALL support a mechanism for a Provider to request another Provider for a list of members in an Affiliation.

AFF-3 The IdM enabler SHALL support a:

(a) Mechanism for a Service Provider to convey in a request that it is acting on behalf of an Affiliation;

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

(as a member of an Affiliation).

AFF-4 The IdM enabler SHALL support a mechanism and guidelines for a Provider to verify that another Provider is a member of an Affiliation.

6.2.2 Discovery Service

DS-1 The IdM enabler SHALL support a:

(a) Mechanism that allows an Attribute Provider to register at a Discovery Service;

(b) Mechanism that allows an Attribute Provider 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 information necessary (e.g. Address, encrypted Identifier for the Principal that the AP will understand) to provide access to the Attribute Provider(s) that host the Principal's Attribute Class(es).

DS-2 The IdM enabler SHALL allow an Attribute Provider to register and de-register Attribute Classes of a Principal at a Discovery Service.

DS-3 When a Provider or Broker requests registration at a Discovery Service, the IdM enabler SHALL provide a mechanism for the Discovery Service to authorise that the registration is allowed.

DS-4 The IdM enabler SHALL support a mechanism for a Service Provider to query a Discovery Service for Attributes pertaining to a Principal other than the Principal initiating the request.

DS-5 The IdM enabler SHALL support dynamic registration and discovery of all *types* of Identity Credentials supported in order to access a registered Service.

DS-6 The IdM enabler SHALL support standard mechanisms for registration of changes in their request or response interface (e.g. to allow a Policy evaluation and enforcement enabler to discover such changes).

DS-7 It SHALL be possible for a Provider (i.e. an Identity Provider) to support SSO / SLO, and publish this capability in a standard way, so that it becomes discoverable.

6.2.3 Attribute Sharing

AS-1 The IdM enabler SHALL allow for different Attributes of the same Principal to be stored at different Attribute Providers.

AS-2 The IdM enabler SHALL support a mechanism that allows a Service Provider to query an Attribute Provider for an Attribute Class.

AS-3 The IdM enabler SHALL support a mechanism for a Service Provider to query an Attribute Provider for multiple Attribute Classes in a single request.

AS-4 The IdM enabler SHALL support a mechanism for an Attribute Provider to convey multiple Attribute Classes in a single response.

AS-5 The IdM enabler SHALL support asynchronous Attribute responses.

AS-6 The IdM enabler SHALL 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.

AS-7 The IdM enabler SHALL support a mechanism for a Service Provider to deny a request for a service and the ability to convey the reason for denial if appropriate.

AS-8 The IdM enabler SHALL support a mechanism for an Attribute Provider that receives a request to respond with partial information.

AS-9 The IdM enabler SHALL support the ability for a Provider to indicate and provide proof that the contents of the message being sent are under a business agreement.

AS-10 The IdM enabler SHALL support the ability for a Principal to be able to set permissions indicating whether or not they allow Identity Brokers to aggregate their Attributes.

AS-11 The IdM enabler SHOULD support anonymous transfer of a Principal's Attributes between an Attribute Provider and a Service Provider, including the case where the Principal does not have an Account with the Service Provider.

AS-12 The IdM enabler SHOULD support different permissions for different Principals regarding access to and usage of Identity Attributes (e.g. on a 'per Attribute' basis it SHOULD be possible for a Principal to specify which Attribute requestors may use an Attribute and which Attribute requestors may not. e.g. SP vs. IDP or administrator vs. employee vs. 3rd party).

AS-13 The IdM enabler SHALL include a mechanism:

(a) for a Service Provider to securely transfer an End User Identity Attribute, which is to be used as an Event Token, to the End User's Device;

(b) to securely store an End User Identity Attribute (that is to be used as an Event Token) on a Device;

(c) for an End User to initiate the secure transfer of an End User Identity Attribute (to be used as an Event Token) from the End User's Device to another (receiving) local Device, where the End User Identity Attribute could be:

- One or more single-use Event Token(s);
- A subscription Event Token that can be used to gain access to a service / content over a defined period of time.

(The Provider that owns the receiving local Device does not have to be federated with the End User's Identity Provider(s), but MAY have a relationship with the Event Token Issuer in order to check the validity of the Event Token.)

6.2.4 Attribute Modification

AM-1 The IdM enabler SHALL support the:

(a) Ability for a Principal or Principal's delegate to store, modify or delete the Principal's Attributes at an Attribute Provider;

(b) Ability (subject to a Principal's consent) of the Attribute Provider to provide a level of confidence regarding the accuracy of the Attribute stored.

6.2.5 Usage Directives

UD-1 The IdM enabler SHALL support a mechanism for a Service Provider to associate Usage Directives with the corresponding Attributes that are being requested.

UD-2 The IdM enabler SHALL support a mechanism for an Attribute Provider to associate Usage Directives with the corresponding Attributes that are being included.

UD-3 When the Usage Directive in the Attribute request does not satisfy the permissions set by the Principal for release of the Attribute Class, it SHALL be possible for the Attribute Provider to deny the request and optionally include

a list of acceptable Usage Directives for release of the Attribute Class.

UD-4 It SHALL be possible for an Attribute Provider to determine whether a certain Usage Directive is privacy-stricter than another.

6.2.6 Multiple Identity Providers

MIP-1 The IdM enabler SHALL support a mechanism for an Identity Broker:

(a) to allow Federation of Principal Accounts at an Identity Provider and a Service Provider in different Authentication Domains provided each has appropriate permissions from the Identity Broker;

(b) to convey the Address of an Identity Provider in a response message to a Service Provider.

MIP-2 The IdM enabler SHALL provide the following mechanism:

Where Federation was created through an Identity Broker, if there is a change in the Identity Broker's Policies with respect to the SP (or the IDP) then the Identity Broker SHALL be able to notify the IDP (or SP) that the change took place. (This is so that the IDP or SP know that they SHOULD tear down the Federation and, if an Authentication Session was open and was only possible because of that Federation, the Authentication.)

MIP-3 The IdM enabler SHALL include a mechanism for a Provider to be able to determine that it previously introduced two other Providers to each other across Authentication Domains.

MIP-4 The IdM enabler SHALL support a mechanism for a Provider to convey a chain of Authentication Assertions in its response to another Provider.

MIP-5 When (chains of) Authentication Assertions are sent, they SHALL be protected from unauthorised modification (e.g. insertion, deletion).

MIP-6 The IdM enabler SHALL support a mechanism for a Provider to differentiate between a single Authentication Assertion and a chain of Authentication Assertions.

6.2.7 Interaction Service

IS-1 The IdM enabler SHALL allow:

(a) A Principal to set permissions for the release of their Attributes stored at an Attribute Provider;

(b) An Attribute Provider to check a Principal's permissions prior to Attribute release;

(c) An Attribute Provider to indicate to Principals (e.g. End Users / Service Providers) its Policy for Attribute release.

IS-2 When a Service Provider queries an Attribute Provider (an IDP could also be an Attribute Provider in this case) for one or more Attribute Classes of a Principal, the IdM enabler SHALL allow:

(a) The Attribute Provider to query the Principal directly;

(b) The Attribute Provider to request the Service Provider to redirect the Principal to the Attribute Provider, so that the Attribute Provider may query the Principal directly;

(c) The Attribute Provider to request the Service Provider itself to query the Principal directly, and then pass the result back to the Attribute Provider.

6.2.8 Federation

FED-1 Providers MAY establish an Authentication Domain and a Circle Of Trust.

FED-2 The IdM enabler SHALL support a mechanism for a Service Provider to discover one or more Identity Providers with whom a Principal has both established an Identity and been authenticated by. This SHALL be possible:

(a) Prior to Federation of the Principal's SP Identity with the Principal's IDP Identity (i.e. the Principal must be currently authenticated by both the IDP and the SP before Identity Federation can occur);

(b) Subsequent to the Federation of the Principal's Identities at the IDP and the SP (e.g. so an SP can discover a suitable IDP for a particular service usage instance).

FED-3 (a) There SHALL be a mechanism to federate a Principal's Identity at one Provider (an Identity Provider) with a Principal's Identity at another Provider. (Note that this means one Principal, who may have two different Identities at two different Providers.)

(b) The mechanism mentioned in (a) SHALL ensure that each Provider SHALL NOT be able to determine Identity Attributes of the Principal stored by the other Provider.

FED-4 (a) A Provider SHALL be able to obtain Authorisation from the Principal to federate the Principal's Identities.

(b) A Principal MAY delegate authority to federate its Identity.

(c) There SHALL be a mechanism for a Provider to prove that Federation took place with Authorisation from the Principal.

(d) The IdM enabler SHALL support a Non-repudiation mechanism for either the Principal Authorisation or the delegated Authorisation.

FED-5 The IdM enabler SHALL support a mechanism for a Provider to prompt the Principal for Authorisation to federate that Principal's Identity at one Provider with that Principal's Identity at another Provider.

FED-6 The IdM enabler SHALL support a:

(a) Mechanism for a Principal to supply information in a message to a Service Provider that indicates the Principal's Authorisation 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 provision Authorisation to federate their Identity in a profile/configuration file;

(c) Mechanism for a Principal to provision Authorisation to delegate the ability to federate their Identity in a profile/configuration file.

FED-7 The IdM enabler SHALL support:

(a) A mechanism to de-federate a Principal's Identity at one Provider with the Principal's Identity at another Provider;

(b) The ability for a Principal to initiate a De-Federation;

(c) The ability for a Principal to delegate the authority to de-federate its Identity;

(d) The ability for a Provider to initiate a De-Federation.

FED-8 The IdM enabler SHALL support a mechanism for any one Provider to notify any other Provider of one or more De-Federations (i.e. De-Federation of one Principal's Identities, or bulk De-Federation of multiple Principals' Identities).

FED-9 The IdM enabler SHALL allow:

a) The use of multiple Authentication mechanisms;

b) The creation of / update of a set of Authentication mechanisms supported by the Identity Provider;

c) The provisioning of the Authentication mechanisms to be used based on criteria agreed between the Providers.

FED-10 The IdM enabler specification SHALL include a list of Authentication Contexts (groupings of Authentication mechanisms that Providers can use to categorise the security level of Authentication methods), which MAY be used by Providers.

FED-11 The IdM enabler SHALL support a:

(a) Mechanism for a Service Provider to request an Identity Provider for an Authentication Assertion corresponding to a specified Principal;

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

FED-12 The IdM enabler SHALL support a mechanism for an Identity Provider to respond to a Service Provider with an Authentication Assertion corresponding to a specified Principal.

FED-13 The IdM enabler SHALL 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.

FED-14 The IdM enabler SHALL support:

(a) A means for an Identity Provider to indicate to a requesting Provider that it does not support the requested Authentication mechanism(s);

(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.

FED-15 The IdM enabler SHALL support:

(a) A mechanism for an Identity Provider to convey to other Providers the Authentication method(s) that was(were) used to authenticate the Principal;

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

(c) A mechanism that permits an Identity Provider to re-authenticate a Principal.

FED-16 The IdM enabler SHALL support a mechanism for Single Log Out.

FED-17 The IdM enabler SHALL provide a mechanism to allow provisioning of conditions that govern aspects such as when, how, and under what conditions actions by the Principal or the Principal's delegate may be permitted.

FED-18 The IdM enabler SHALL include mechanisms for a Provider to be able to trace the assignment of Identities, the Federation of Identities, the validation of Identities, and the association of Attributes with a particular Identity.

FED-19 SSO / SLO SHALL work across Authentication Domains (e.g. to allow access to enterprise applications from outside an intranet).

FED-20 The IdM enabler SHALL support a mechanism for Single Sign On.

6.2.9 Business requirements

BR-1 The IdM enabler SHALL support a mechanism for a Provider to maintain evidence to support a claim of Non-repudiation for either the Principal Authorisation or the delegated Authorisation.

Appendix A. Change History (Informative)

A.1 Approved Version History

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

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD_Identity_Management_Framework-V1_0	17th Sep 2004	All	Sections, Use Cases and Requirements all compiled into one document First fully compiled draft
	18th Nov 2004	All	Final version of document ready for formal REQ review
	6th Jan 2005	All	Updated version that includes all handling of comments from formal REQ review
	7th Jan 2005	2.2 4.1.4	Removed all references to internal OMA documents
Candidate Version OMA-RD-Identity_Management_Framework-V1_0	2 Feb 2005	N/A	Status changed to Candidate by TP TP ref # OMA-TP-2005-0044-IMF-RD-Package-For-Approval