XML Document Management Requirements

Candidate Version 1.0 – 17 Mar 2005

Open Mobile Alliance

OMA-RD-XDM-V1_0-20050317-C

Contents

1. Scope (Informative)

This document describes use cases and requirements for the management of information (e.g., URI Lists) that are stored as documents using an extensible and platform-neutral format that could be used by other OMA service enablers. Therefore, the requirements contained in this document are limited to these aspects (i.e., the storage, management and re-use of such documents containing information by other applications).

The privacy of personal data, such as, principal identity is protected according to privacy regulations. However, mechanisms to obtain the permission of principal (e.g., before they are included in lists that are managed by the XDM enabler) are out of scope.

The XDM enabler provides mechanisms for principals to specify who can access the data they have stored.

In addition, the owner of a XDM enabler deployment has full access to this data (overriding any principal preferences) for purposes, such as, administration and maintenance. The application of those administrative rights in relation to principal preferences may be described in legal or contractual policies, and as such is out of scope for this enabler.

The XDM enabler is designed to support other OMA service enablers and applications. It is envisioned that there will be multiple enabler specifications to satisfy the requirements in this document.

2. References

2.1 Normative References

[RFC 2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997.
URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC 2396] "Uniform Resource Identifiers (URI): Generic Syntax", T. Berners-Lee et al, August 1998.
http://www.ietf.cnri.reston.va.us/rfc/rfc2396.txt?number=2396

[Privacy] "OMA Privacy Requirements for Mobile Services", Open Mobile Alliance™
http://www.openmobilealliance.org

[XDM_AD] "Group Management Architecture", Version 1.0, Open Mobile Alliance™, OMA-GM-AD-V1_0, URL: http://www.openmobilealliance.org/

2.2 Informative References

[OMA PoC RD 1.0] "OMA Push to Talk over Cellular Requirements, Open Mobile Alliance™, OMA-RD-PoC-V1_0, Version 1.0
http://www.openmobilealliance.org

[OMA Presence RD 1.0] "OMA Presence SIMPLE Requirements", Open Mobile Alliance™, OMA-RD-Presence_SIMPLE-V1_0, Version 1.0
http://www.openmobilealliance.org

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119].

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

3.2 Definitions

Access Control Policy A set of lists (e.g., access control lists, such as, accept/reject lists) and associated rules on how they apply to incoming requests.

Primary Principal The principal who has full access rights (e.g., read, write, delete) for a given document, including the right to delegate some of these rights to other principals.

Principal See OMA Dictionary.

Subscription Authorisation Policy An example of access control policy for Presence, which specifies whether a particular watcher (i.e. principal) is authorised to subscribe to a certain set of events.

URI List A collection of URIs put together for convenience.

3.3 Abbreviations

CS	Circuit Switched
GUI	Graphical User Interface
IM	Instant Messaging
MSISDN	Mobile Station ISDN number (as defined by the E.164 numbering plan).
MSISDN	Mobile Station Internation ISDN Number
OMA	Open Mobile Alliance
P2P	Peer to Peer
PoC	Push to Talk over Cellular
PSL	Presence Subscription List
RD	Requirements Document
RFC	Request For Comments
SIP	Session Initiation Protocol.
SMS	Short Messaging Service
UI	User Interface
URI	Uniform Resource Identifier.
VoIP	Voice Over IP
XDM	XML Document Management
XML	Extensible Markup Language.

4. Introduction (Informative)

Various OMA enablers such as, Presence, Push to Talk Over Cellular (PoC), Instant Messaging (IM), etc. need support for access to and manipulation of certain information that are needed by these enablers. Some examples of such information (whose semantics and syntax are outside the scope of the XDM enabler) include:

- *PoC Group*: the list of PoC participants who can take part in a PoC session as well as additional PoC-specific properties such as auto-answering incoming PoC call requests, etc.
- *PoC Accept/Reject List*: the lists of PoC callers who are allowed/not allowed to call a given user
- *Presence List*: a list of users who are potential presentities, so that this list can be used to collectively subscribe to the presence status of each member in that list
- *Subscription Authorisation Policy*: An example of an access control policy for Presence, which specifies whether a particular watcher (i.e., principal) is authorized to subscribe to a certain set of events.

Notice from these examples that such information is not always pure lists (of principals), but can be a combination of lists together with other properties that define an end-user's personalization of the service behaviour. The enablers specify the items that make up the documents representing the information in the examples above, including their semantics and usage. Over time, it is expected that other OMA enablers will define other types of documents needed for their operation.

To make such information accessible to the enablers that need them, the information is expected to be stored in the network where it can be located, accessed and manipulated (created, changed, deleted) by authorised principals. To this end, the OMA is expected to specify the use of an extensible and neutral format (e.g., XML) by which such information will be defined, as well as the common protocol for access and manipulation of such information, represented as XML documents, by authorized principals.

The XDM enabler specifies documents that can be shared by multiple enablers. One such case is a particular type of list, the URI List, which is a convenient way for a principal to group together a number of end users (e.g., "Friends" or "Family) or other resources, where such a list is expected to be reused for a number of different enablers. Such a list can be re-used wherever a principal has a need to collectively refer to a group of other end users or resources.

Thus, it is envisaged that the XDM RD would result in multiple specifications. One specification will define a protocol that could be used by any enabler or end-user to manipulate documents containing information pertaining to that enabler or end-user. Another specification would define certain types of shared information (e.g., URI lists) that can be stored, retrieved, and re-used by multiple enablers. It is expected that other enablers will define the document structure needed for their information as part of their enabler specification.

4.1 Requirements Fulfilled

Requirement ID/Number	Notes
6.1.1 – General bullet 5 item d	Visibility: This property determines which principals are able to find this document when performing a search.
6.1.1 – General bullet 5 item f	Permissions: This property identifies which principals have which rights to perform which operations on this document. Since delegation is not supported this is unnecessary.
6.1.2 - Delegation	
6.1.3 bullet 10	Permissions: This property identifies which principals have which rights to perform which operations on this document. Since delegation is not supported this is unnecessary.
6.1.3.3 - Copy	Copy is implemented using Retrieve and Rename. Future versions may implement this as a separate protocol operation.
6.1.3.5 - Suspend	
6.1.3.6 - Resume	
6.1.3.7 - Search	

Requirement ID/Number	Notes
6.1.3.9 - Administration and Configuration	This is only necessary if delegation is supported.
6.1.4.2 – Security / Common way	
6.1.5 - Charging	Charging: Not enough details known by now to implement charging functionality as required.
6.2.2 bullet 3	Charging: The detailed requirement is left for a later phase
6.3.1.1 bullet 4, item a)	Maximum number of URIs: This requirement is left for a later phase
6.3.2.1 bullet 7	Copy: This requirement is left for a later phase
6.3.3.2 bullet 2 and 3	Attribute List for all list members: Attribute List for some list members:

Table 1: RD requirements not met in this enabler release

5. Use Cases (Informative)

The use cases are separated into two parts to identify the generic and the service specific set of XDM functionality.

Functions like “Access Control, Addressing, Copy, Create, Delete, Management of Members and Modify Group Properties” need to be referenced by the use cases.

5.1 Generic Use Cases

The generic use cases define the behaviour, information elements and actors that are common for all services using XDM.

5.1.1 Use Case - URI List

5.1.1.1 Short Description

This use case will describe the general URI list for an end-user. The end-user can store URI information about other end-users to later initiate URI with them or to subscribe for their presence. A URI list is an essential basis for other OMA enabler (such as, PoC or messaging) as the addresses on the URI list are used to set up a session.

John has been on Summer Camp during two summers. The first year he made three new friends Lisa, Jeff and Toby. John wants to keep in URI with his new friends and need a place to store their URI information. The URI information must be accessible through different devices and be possible to use for initiating different types of communication.

The second year he met two new friends, Paula and Andy. John wants to group his URI list so the people from first Summer Camp year is in one list and the ones from year two is in another list.

5.1.1.2 Actors

John: Owner of the URI List

Lisa: Friend of John that he met during the first Summer Camp

Jeff: Friend of John that he met during the first Summer Camp

Toby: Friend of John that he met during the first Summer Camp

Paula: Friend of John that he met during the second Summer Camp

Andy: Friend of John that he met during the second Summer Camp

URI List Service: A service enabling storage and managing of URI Lists

URI List Client: A client on the device able to display and manage URI Lists

5.1.1.3 Actor Specific Issues

John: Needs a place to store contacts.

5.1.1.4 Actor Specific Benefits

John: Will have contact information for his friends stored in the network.

He will be able to access this list from different devices.

He can use this list to establish different types of communication with his friends.

5.1.1.5 Pre-conditions

John has a subscription that enables him to store URI list(s).

John knows the address to access for storing his URI lists.

5.1.1.6 Post-conditions

John has stored his friend communication contact information in the network;

The various URI lists that John creates are organised in a way that John wants it.

John will use the information stored in the URI list to initiate communication with his friends.

5.1.1.7 Normal Flow

- John turns on his device.
- John accesses his URI List service and creates a new URI list for the friends from the first Summer Camp year.
- John sets the name “summercamp97” on the list.
- John adds the URI address of Lisa, Jeff and Toby to this URI list.
- The URI list with the new entry is stored in the URI List service.
- The updated data in the URI list is now accessible to John from different devices.
- John accesses his URI List service and creates a new URI list for the friends from the second Summer Camp year.
- John sets the name “summercamp98” on the list.
- John adds the URI address of Paula and Andy to this URI list.
- The URI list with the new entry is stored in the URI List service.
- The updated data in the URI list is now accessible to John from different devices.
- John can view the various URI lists (“summercamp97”, “summercamp98”) that he has created on his device.

Later John uses one of the entries from his list of URI list to establish communication, such as, a PoC session, with the members of that list.

5.1.1.8 Alternative Flows

None.

5.1.1.9 Operational and Quality of Experience Requirements

- The access to the URI list should be secure so only John can access it
- The performance for accessing the URI list should be fast to give a good end-user experience
- The information in the URI list should be consistent if several devices are used to access the URI list.

5.1.2 Use Case - Subscribing for Presence of End-users in a URI List

5.1.2.1 Short Description

This use case will describe the how to use the URI list for subscribing of the presence status of end-users in that list.

John has been to Summer Camp during two summers and met a lot of new friends. They are soon to have a reunion and John is responsible for setting up the logistics. John has stored all his friends in URI list(s). Before contacting them he thinks it would be good to know if they are available or not before placing a call.

5.1.2.2 Actors

John: Owner of various URI lists.

URI List Service: A service enabling storage and managing of URI Lists.

Presence Service: A service enabling subscription and notifications of presence information.

5.1.2.3 Actor Specific Issues

John wants an easy way to view the presence of his friends in his URI list.

5.1.2.4 Actor Specific Benefits

John can add friends to his URI list and view their presence status. John starts receiving the presence status of his friends in a timely fashion, as he doesn't have to wait for individual subscriptions to be placed.

5.1.2.5 Pre-conditions

John has one or several URI lists.

John has a subscription for the presence service.

All the entries in any URI list that he uses for subscribing for presence are end-users.

5.1.2.6 Post-conditions

John has subscribed for presence of all the end-users in the URI list.

If authorised to access their presence information, he will be able to see the presence state of his friends.

5.1.2.7 Normal Flow

- John accesses his URI List Service using an appropriate application on his terminal and selects a particular URI list.
- This application sends a subscription request to the presence service, requesting to subscribe to that URI list.
- The presence service will communicate with the URI List Service to resolve the end-users of the URI List and place a subscription to each member of the URI list.
- The application begins receiving notifications from those subscriptions and appropriately displays the results to John.

How the presence subscription and authorization is done is outside the scope of this document.

5.1.2.8 Alternative Flows

None.

5.1.2.9 Operational and Quality of Experience Requirements

None.

5.1.3 Use Case – Groups

5.1.3.1 Short Description

Groups described here are used for communication sessions, such as, PoC sessions or immediate messaging sessions for chat rooms. The use case might be expanded to catch the full flavour of communication services, such as, PoC where the group has additional attributes than those identified in this use case.

John is the leader for a curling team. Jeff and Andy are the two members of that curling team. John creates a group called "Curling" to communicate with his team.

5.1.3.2 Actors

John: Owner of the group

Jeff: Member of the group

Andy: Member of the group

The Group Service: A service for storage and modification of a end-user's groups.

The Communication Service: A service (such as, PoC or messaging) that the end-users in the group use to communicate.

5.1.3.3 Actor Specific Issues

John wants to set up a group to enables communication. The group has properties (e.g., "open" or "restricted") that sets the rules for the communication

Jeff and Andy want to participate in group communications.

5.1.3.4 Actor Specific Benefits

John is able to set up a group for some specific purpose and is able to restrict its use if he wants.

5.1.3.5 Pre-conditions

John, Jeff and Andy have subscription and devices enabled for the Communication Service.

5.1.3.6 Post-conditions

A group communication service has been setup between John, Jeff and Andy.

5.1.3.7 Normal Flow

- John creates a group and sets the properties of the group to "restricted".
- John uses the group name "Curling" at the Communication Service to invite Jeff and Andy to participate in the group communication.
- Andy and Jeff accept the invitation to participate in the group communication.
- The group communication session is established.

5.1.3.8 Alternative Flows

None.

5.1.3.9 Operational and Quality of Experience Requirements

- The access to the Group should be secure so that only John can access it.
- The performance when manipulating the Group data should be fast to give a good end-user experience.
- The Group data should be kept consistent if several devices are used to access the data.

5.1.4 Use Case - P2P Using a Group List

5.1.4.1 Short Description

This scenario describes the creation and management of group of golf buddies. The use case describes the end-user's experience as a group administrator. It motivates several requirements related to usability, security, charging when managing groups.

5.1.4.2 Actors

John – an end-user who creates a group from a list of buddies who share an interest in golf.

Alan – a golfing buddy of Johns who is willing to help organise a golfing party.

Other end-users of mobile services, who regularly play golf with John and/or Alan.

The Service Provider.

5.1.4.3 Actor Specific Issues

Group members want to communicate with all or some of the other members before and during the course of the golf match

Group members want to communicate and view the presence state of all or some of the group members

John wants to be able to add or remove members from the group whenever necessary

The Service Provider wants to securely perform all management transactions

5.1.4.4 Actor Specific Benefits

All members of the group can communicate quickly and effectively using a group list

The Service Provider can offer its end-users a flexible way to communicate to groups

The Service Provider generates revenue

5.1.4.5 Pre-conditions

John and Alan have mobile service subscriptions with the same service provider

Some of the potential group members have service subscriptions with different service providers

John's service subscription allows him to create and manage groups to communicate with

5.1.4.6 Post-conditions

John and the rest of the "Weekend Golfing" group communicate their approval to play another round in a month's time, so John keeps the group set up in his URIs list.

5.1.4.7 Normal Flow

1. John wants to play golf at the weekend with some friends. He wants to communicate with the group before and during the course of the game, using Instant Messaging and voice calls, so he decides to set up a golfing group list of contacts. He knows his colleague, Alan regularly plays golf and Alan gives him details of some contacts who might like to play.
2. John uses his mobile device and establishes a session with his service provider to request that a group be created.
3. John is authorised by the service provider and is allowed access to group list data. He creates a "Weekend Golfing" group.

4. John adds the end-user identities of the names from his address book, plus Alan's friends. He also retrieves an existing buddy list and copies some names from that list into the "Weekend Golfing" group. John also selects "private" in the group properties field.

5. John finalises all his settings and confirms the group creation

6. A few minutes later, John sends a notification to all of the members in the "Weekend Golfing" group by SMS that they have been added as a member of this private group list set up by John.

7. Before the weekend, John sends a multimedia message with a location map of the golf course as an attachment to the group

8. On the golfing day, Alan asks John to add Bob, a latecomer to the group, so John contacts his Service Provider, (steps 2 and 3) and selects the "Weekend Golfing" group and "Modify" from the service options. John then adds Bob to the list. The Service Provider acknowledges and confirms the addition before ending the session.

9. The XDM Enabler notifies the group members of a change in group membership.

5.1.4.8 Alternative Flow

None

5.1.4.9 Operational and Quality of Experience Requirements

- Both group administrator and service provider are authenticated before all XDM transactions.
- End-users are able to manage groups in an end-user friendly way.
- End-users will receive acknowledgements of all transactions performed.
- End-users can be charged according to the number of transactions in some time period, or may be charged as part of another service.

5.1.5 Use Case – Group Visibility

5.1.5.1 Short Description

Group visibility defines who is able to see the group identifier when performing a search. The following classes exist: the group is visible to group members only, and the group is visible to all end-users.

The administrator can define group visibility. If the group visibility is "the group is visible to group members only", only the member can retrieve the group identifiers. And if the group visibility is "the group is visible to all end-users", all the end-users will be able to see that group when performing a search.

5.1.5.2 Actors

Alice: a teacher, who creates a group with the group identifier "STUDENTS"and defines its visibility as "the group is visible to group members only". At the same time, she is a music fan, so she creates another group with the group identifier "MUSIC"and defines its visibility as "the group is visible to all end-users".

Bob: The student of Alice, and also a member of the group "STUDENTS", who wants to use the search function of the XDM.

Charlie: An end-user who is a music fan, but not a member of the group "STUDENTS" & "MUSIC", who wants to use the search function of the XDM.

5.1.5.3 Actor Specific Issues

Alice wants the group "STUDENTS" visible only to the group members, which are her students in this case. And she wants the group "MUSIC" visible to all the end-users in order to contact other music fans.

Bob wants to find the "STUDENTS" group using searching, and communicate with his classmates.

Charlie wants to find the "MUSIC" group using searching, and communicate with other music fans.

5.1.5.4 Actor Specific Benefits

Alice can define the group "STUDENTS" only visible to the group members, and the group "MUSIC" visible to all the end-users.

Bob can find the group "STUDENT" using searching.

Charlie can find the group "MUSIC" using searching, but cannot find the group "STUDENT" using searching.

5.1.5.5 Pre-conditions

Alice is provisioned to use the XDM function to define the group visibility.

Bob and Charlie are provisioned to use the search function of the XDM.

Bob is a member of the group "STUDENT", but Charlie not.

5.1.5.6 Post-conditions

When performing a search, the group "STUDENT" is visible to Bob but invisible to Charlie and the group "MUSIC" is visible to Charlie and Bob.

5.1.5.7 Normal Flow

1. Alice creates a group with the group identifier "STUDENT" and defines its visibility is "the group is visible to group members only". She adds Bob to the group.

2. Alice creates a group with the group identifier "MUSIC" and defines that its visibility is "the group is visible to all end-users".

3. Bob uses the search function of the XDM and sees "STUDENT" and "MUSIC" on the search result list.

4. Charlie uses the search function of the XDM and sees "MUSIC" on the search result list.

5.1.5.8 Alternative Flow

None.

5.1.5.9 Operational and Quality of Experience Requirements

The administrator must be able to define visibility of the group using his client, and the server should know the visibility of the groups.

The end-user must be able to use the search function of the XDM.

5.1.6 Use Case - Assigning Permissions

5.1.6.1 Short Description

In this scenario, a Sales Representative of an enterprise creates a group list to discuss the best sights and places to visit in San Francisco, where a big Sales Convention is to be held. The list is to contain some of her colleagues plus some Sales Representatives from other companies whom she knows well and likes to socialises with. As group creator, she is allowed to authorise other members to perform certain management functions. The use case also shows how some actors automatically get assigned some or all permissions to perform XDM operations.

5.1.6.2 Actors

Mobile Service Provider

An enterprise, owning the mobile device subscriptions of its employees

Maria, Sally, Molly and John who are employees of the same enterprise and use Mobile devices

Employees of other enterprises who are added to the group list

5.1.6.3 Actor Specific Issues

The group creator (Maria) wants to allow other members of the group to perform certain XDM functions

The enterprise wants to be able suspend or delete the group if necessary

5.1.6.4 Actor Specific Benefits

All members of the group can communicate quickly and effectively using a group list

Maria can give permission to other members of her group list to manage the group on her behalf

The enterprise can offer its employees a flexible way to communicate in groups

The Service Provider generates revenue

5.1.6.5 Pre-conditions

Maria, Sally, Molly and John's mobile service subscriptions are owned by their company

Maria and her colleagues can use an IM service as part of the mobile service subscription owned by their company

As part of the subscription that the enterprise has with the Service Provider, the group creator (Maria) is allowed to grant permissions to other group members to perform some XDM functions.

Some of the potential group members have service subscriptions with different service providers

5.1.6.6 Post-conditions

The chat group is suspended.

5.1.6.7 Normal Flow

Maria and her sales colleagues, Sally, Molly and John think it would be a good idea to set up a discussion forum to discuss places to visit and sights to see in San Francisco, the location of a big industry sales convention. They think it is a good idea to invite sales representatives from other companies who will also be there

Maria creates a group initially comprising herself Sally, Molly and John. As group creator, Maria is assigned full administrative rights and is also allowed the right to assign permissions to other members

The enterprise who owns Maria's subscription is automatically given 'group suspend' and 'group delete' permissions as part of the contract it has for XDM enablers with the Service Provider. [The enterprise does NOT have permission to 'add' or 'delete' members, or to hand out those permissions to anyone else. Also, the permission to delegate the 'group suspend' command and the permission to delegate the 'group delete' command are separate from permission to perform 'suspend' and 'delete'; the latter permissions are automatically available to the enterprise.]

Maria authorises Sally, Molly and John to be able to add members to the list from their sales contacts in other companies who are coming to the convention. Maria also gives Sally the right to delete members from the group. Maria gives Sally the right to delegate (i.e., pass on) the "add member" and "delete member" permissions to other people; Maria withholds such delegation permission from Molly and John.

Sally, Molly, and John are notified that they have been given additional administrative permissions for this group.

Sally, Molly and John add Sales reps from other companies as members to Maria's trip discussion group.

John has second thoughts about Bill who is a rival from another company, who he has already added to the group. When accessing the group list data, John finds out that he has not been assigned rights to delete other members from the group.

John sends a text message to Maria. Maria is busy so she asks Sally to delete Bill from the group

Weeks of happy instant messaging follow discussing the best places to visit, eat, drink and take customers to in San Francisco.

David, a colleague of Maria's from San Francisco hears about Maria's chat forum and decides to ask their enterprise IT department to add him as a member of the group. David is informed that he must contact the group administrator.

Just before leaving for the convention, Maria requests her enterprise IT department to suspend the group during the week of the convention, but she thinks it will be a good idea to keep the group list and resume discussions just before the next convention in Miami.

5.1.6.8 Alternative Flow

None

5.1.6.9 Operational and Quality of Experience Requirements

End-users with appropriate rights shall be able to manage groups in a user friendly way.

The look and feel of group data should be uniform regardless of device used to access it.

Administrative access should be possible from any device type, over any network type.

5.1.7 Use Case - Access Control Lists

5.1.7.1 Short Description

This use case describes the role of Access Control lists. It shall be possible for Access Control lists to be created, modified and deleted by the subscriber or another authorised end-user.

5.1.7.2 Actors

Corporation: Acme Communications pays the subscription for Push to Talk service and Instant Messaging Service for Corporate Communications purposes.

Corporate Users: Atul, Andrew, Paul, Sunny, Nick, Gary, Adrian are all end-users of Push to Talk service and Instant Messaging Service who are employed by Acme Communications.

Individual Subscribers: Nadja, Izumi, "Mr Spammer", "Mr Angry", "Mr Hacker" and "Mr Abusive", are individual subscribers to and end-users of the Push to Talk service and Instant Messaging Service not affiliated with Acme Communications.

Service provider: Is the organisation, could be the Network operator, which provides the subscribers and end-users with the Push to Talk service and Instant Messaging Service.

5.1.7.3 Actor Specific Issues

Acme Communications

- Want to ensure that their corporate end-users have access to all the other employees and cannot be blocked by an individual employee
- Want secure transport of the contents of their Access Control lists

- Want a practical way to Create and Manage Access Control Lists using fixed corporate computer resources (not restricted to provisioning using a handset)
- Want to maintain employee morale by allowing employees to add and remove other non Acme employees to their Access Control lists but not allow them to fully modify the Access Control settings of other employees.

Corporate Users

- Want to add and remove other friends and family to their Access Control lists.
- Want to prevent unauthorised end-users having access to or being able to modify their Access Control Lists
- Want to prevent abusive Push to talk calls and block spammers
- Want a practical way to Create and Manage Access Control Lists using personal computer resources in addition to using a handset.
- Want the flexibility to use the same Access Control lists for the Push to Talk service and Instant Messaging Service and other services.

Individual Subscribers

- Want to add and remove friends and family to their Access Control lists.
- Want to prevent unauthorised end-users having access to or being able to modify their Access Control Lists.
- Want to prevent abusive Push to talk calls and block spammers.
- Want a practical way to Create and Manage Access Control Lists using personal computer resources in addition to using a handset.
- Want the flexibility to use the same Access Control lists for the Push to Talk service and Instant Messaging Service and other services.

Individual Subscriber "Mr Spammer",

- "Mr Spammer" wants to send unsolicited Instant Messages for his lottery winner fraud scam to end-users of the Instant Messaging service.

Individual Subscriber "Mr Angry",

- "Mr Angry" wants to place Push to Talk calls to people and pick arguments with them.

Individual Subscriber "Mr Abusive",

- "Mr abusive" wants to place abusive Push to Talk calls to people and also send obscene Instant Messages to them.

Individual Subscriber "Mr Hacker",

- "Mr Hacker" likes to break into computer systems and gain access to or change the personal information of people that is stored there. He often sells this information to "Mr Spammer".

5.1.7.4 Actor Specific Benefits

Acme Communications

- Confidence that the service they are paying for is useful for corporate purposes.
- Confidence that their corporate employee information is private and secure.

End-users and Individual Subscribers

- Have services that they can use without becoming victims of the activities of "Mr Spammer", "Mr Angry", "Mr Hacker" and "Mr Abusive".
- Have simple easy to use configuration of authorisation policies for different services.

Service Provider

- Reduces complaints from subscribers regarding SPAM.

5.1.7.5 Pre-conditions

Acme Communications and all the Individual Subscribers have a valid subscription to the Push to Talk service and Instant Messaging Services. The end-users have access to a Network for Push to Talk service and Instant Messaging Services.

The Individual Subscribers have mobile terminals which support creation and modification of Access Control lists.

"Mr Spammer", "Mr Angry", "Mr Hacker" and "Mr Abusive" may have access to modified terminals that provide access to the Access Control Lists and other XDM functions with the ability to modify parameters or spoof identities,

5.1.7.6 Post-conditions

Acme Communications, all the End-users and Nadja and Izumi all have a satisfactory communication experience which enhances their ability to communicate for both business and social purposes.

"Mr Spammer", "Mr Angry", "Mr Hacker" and "Mr Abusive", find that their anti social and often illegal activities are frustrated.

5.1.7.7 Normal Flow

- Acme Communication Corporation creates using their fixed corporate computer resources an Access Control list containing a list of the identities of Acme end-users Atul, Andrew, Paul, Sunny, Gary, Nick and Adrian. This Access Control lists is assigned as an Accept List and allocated to all the Acme End-users.
- Different attributes are assigned to the Accept lists of each of the end-users – Atul, Andrew, Paul, Sunny, Nick, and Adrian are all allocated attributes that indicate that this Access Control list applies to both the Push to Talk service and Instant Messaging Service, While the Access Control list of Gary indicates that this only applies to the Instant Messaging Service since Gary does not use the Push to Talk service.
- Acme corporation creates an associated authorisation policy for the accept list that only allows their network administrators to delete, or modify these entries on the accept list but allows the end-user to whom the list applies to add additional entries to the accept list and to modify and remove those additional entries added by the end-user as well as allowing that end-user to create, add modify, remove and delete their reject list.
- Adrian adds his friend Izumi's telephone number to his accept list using his mobile terminal. Izumi adds Adrian to her accept list using her PC from home. Andrew adds his friend Nadja's SIP URI to his accept list using his PC from the office. Nadja requests her Service Provider to add Andrew's SIP URI to her accept list.
- "Mr Hacker" attempts to hack into the Access control lists of other Paul and Nick using his mobile terminal and his PC but is prevented by strong security mechanisms that authenticate and prevent the spoofing by "Mr Hacker" of Paul and Nick's identities. "Mr Hacker" also manages to hack into an intermediate router and get packets routed to himself but is unable to gain any information about the end-users because the Access Control list information is securely encrypted.
- "Mr Spammer" discovers Gary's identity from a business card and sends him an instant message from his mobile terminal anonymously with details of his lottery winner scam. Gary decides he does not want to receive any more SPAM from "Mr Spammer" so he uses the capability of his mobile terminal to add the anonymous end-user that sent him the SPAM to his reject list. The network entities are able to resolve the anonymous address of "Mr Spammer" and add "Mr Spammer" to Gary's Reject list. Further SPAM instant messages from "Mr Spammer" to Gary are rejected based on "Mr Spammer" being on his Reject List.

- Izumi receives and abusive instant message from "Mr Abusive". Izumi adds "Mr Abusive" to her Reject List. Further instant messages from "Mr Abusive" to Izumi are rejected based on "Mr Abusive" being on her Reject List.
- Sunny accepts a PoC Call from "Mr Angry" who gets upset on the call and starts shouting. Sunny terminates the PoC Call but "Mr Angry" calls again. Since Sunny is set up so that calls from end-users not on the accept list are manually answered he does not have to accept the call. Sunny then adds "Mr Angry" to his Reject List. Further PoC Calls from "Mr Angry" to Sunny are rejected based on "Mr Angry" being on his Reject List.

5.1.7.8 Alternative Flow

None.

5.1.7.9 Operational and Quality of Experience Requirements

- Access Control Lists SHALL be transported securely
- It SHALL be possible to prevent unauthorised users to access or modify their Access Control Lists
- Users SHALL be able to add/remove content from their Access Control Lists
- Users SHALL be protected from spam and abusive PoC calls
- End-users SHOULD have the ability to create and manage Access Control Lists using either a Personal Computer or mobile device
- It SHOULD be possible to use the same Access Control Lists for both PoC, IM and other applications

5.1.8 Use Case - Blocking or Granting communication from different end-users

5.1.8.1 Short Description

John is setting up his access rules so that certain persons may contact him while others are not able to contact him. This is done both by grouping of end-users, URI lists, by individual end-users as well as by different communication types.

This use case currently only contain blocking of individuals – to be expanded later to cover blocking based on URI lists, and by different communication types.

5.1.8.2 Actors

John: The recipient of communication.

Lisa: Initiating communication with John, but John does not want to be contacted by Lisa.

Jeff: Initiating communication with John and it is ok for John to be contacted by Jeff.

Access List Service: A service for storing and managing of Access List that are used for blocking and granting an end-user the ability to communicate with a particular end-user.

Communication Service: A service used by end-users to communicate, such as, PoC or messaging.

5.1.8.3 Actor Specific Issues

John – wants to control who is able to contact him.

5.1.8.4 Actor Specific Benefits

John – will be able to choose who will be able to contact him.

5.1.8.5 Pre-conditions

John, Lisa and Jeff all have subscriptions and devices for a communication service.

The communication service can contact the Access List Service.

5.1.8.6 Post-conditions

Lisa was not able to communicate with John.

Jeff was able to communicate with John

5.1.8.7 Normal Flow

- John accesses his Access List Service
- John blocks Lisa so she is not able to contact him using a particular communication service.
- John grants Jeff the right to contact him using the same communication service.
- List tries to establish communication with John using the communication service.
- The communication service verifies with the Access List Service if Lisa is allowed to contact John.
- Lisa is not allowed to contact John; therefore the communication is blocked.
- Jeff tries to establish communication with John
- The communication service verifies with the Access List Service if Jeff is allowed to contact John.
- Jeff is allowed to contact John and the communication is established.

5.1.8.8 Alternative Flows

None.

5.1.8.9 Operational and Quality of Experience Requirements

- Access Control Lists shall be transported securely.
- It shall be possible to prevent unauthorised users to access or modify their Access Control Lists.
- Users shall be able to add/remove content from their Access Control Lists.
- Users shall be protected from spam and abusive PoC calls.
- End-users should have the ability to create and manage Access Control Lists using either a Personal Computer or mobile device.
- It should be possible to use the same Access Control Lists for both PoC, IM and other applications.

5.1.9 Use Case – Retrieving a List of Lists

5.1.9.1 Short Description

This use case describes the need for an end-user to populate his terminal with information about the various lists and groups that he maintains. This may be because he has a new terminal, to which he wishes to restore his previous data on his groups and lists, or because he has accidentally deleted the data on his existing terminal.

John has created various URI lists of his buddies, as well as joined various PoC groups. He maintains this list on the network so that he can access them from anywhere and from any device. Recently John has purchased a new terminal, and he would like to populate his terminal with the names of his groups and lists so that he may continue to modify them.

5.1.9.2 Actors

John: Owner of various URI Lists and a member of various Groups.

List Management Service: Entity which maintains John's groups and list information on his behalf.

5.1.9.3 Actor Specific Issues

The end-user needs a place to store his list of all his lists for future retrieval.

5.1.9.4 Actor Specific Benefits

The end-user can easily synchronise his group and list information between different terminals.

5.1.9.5 Pre-conditions

The end-user's terminal must be capable of retrieving and manipulating such stored data.

The end-user must be made aware of the address where he can retrieve his list of lists. This can be done via configuration, not requiring end-user intervention.

John is authorised sufficiently to the list server.

5.1.9.6 Post-conditions

The end-user is able to retrieve his list of lists.

From this list of lists, he can download, as needed, the contents of each list and therefore repopulate his new device.

5.1.9.7 Normal Flow

The steps to download the list of lists are as follows:

1. John's terminal downloads the list of lists.
2. John's terminal compares the received list of lists with the stored list of lists if available locally on the terminal.
3. John's terminal downloads all the lists that are not stored on the terminal from the server.
4. John can access those lists, or information derived from those lists, by using appropriate applications on his terminal.

5.1.9.8 Alternative Flows

None.

5.1.9.9 Operational and Quality of Experience Requirements

- Based on the applications available on John's terminal, he will only be offered the list of lists pertaining to that application. Thus, if he only has a PoC application on his terminal, he will be offered the ability to download his PoC Group and Access List. If his terminal is also Presence enabled, he will be offered the ability to download his Presence List as well as his Presence Authorization Policy document.
- The access to the URI list should be secure so that only John can access it.

The performance for accessing the list of lists should be fast to give a good end-user experience.

5.2 Service Enabler Specific Use Cases

The service specific use cases define the behaviour, information elements and actors that are common for all OMA services elements using XDM.

5.2.1 Push to talk over Cellular (PoC)

5.2.1.1 Use Case - Creation and Advertising Group List

"SHOPPING LIKE CRAZY" (Reference: OMA-RD_PoC-V1_0-20040506-C Use Case A).

5.2.1.1.1 Short Description

This sub clause provides the prose description of the basic PoC service from the beginning to the end.

A group of people shopping together decided to keep in touch with each other using a PoC service to inform on the most challenging bargains. Therefore, one of them, Mary, requests the PoC service provider to set-up the PoC service for them.

As soon as the PoC service provider has set up the service, all the invited people get an indication on their terminal, asking whether they would accept the service. This service invitation contains the name of the inviting host (Mary) as well as the name of the group: "*SHOPPING LIKE CRAZY*". In addition, the PoC service provider has relayed the right to accept additional participants to Mary.

Most of the invited people accept the service offer, becoming participants in the PoC group. However some do not accept, since they have other preferences.

In the department store they meet another friend who would like to join. Being given the name of the group he sends a request to Mary to join the group. Mary allows him to join.

Susie suddenly discovers an extremely cheap shoe shop, which she simply has to tell her friends of. So she pushes the talk button.

As someone is speaking right now and Manfred had pushed the button before, Susie's request to speak is queued.

Hearing Manfred talk, Susie realises that Manfred is already talking about this shoe shop. So she cancels her request to speak. Alternatively, after Manfred had finished speaking, Susie would have received an indication, that she is now "*on air*".

The voice is immediately distributed to the other participants. For the listeners, when they are ready to listen, their terminals receive the voice of the speaker without prior indication.

One of the participants receives an incoming phone call. As determined by the preferences of the owner, the phone switches to "*not ready to listen*" mode of the PoC service. In this mode the PoC service silently continues in the background, after the end of the phone call the participant decides to return to listening to the PoC service.

After a while Manfred gets bored with all this gossip and decides to leave the PoC group. He simply sends the unregister-request indication to the PoC service. The rest of the participants get an indication that Manfred has left the PoC group.

5.2.1.1.2 Actors

PoC Participants: Susie, Manfred and others are acting as participants.

PoC Host: Mary is acting as the host.

PoC Group Member: PoC End-user who has been added to the group, may or may not be PoC Participant.

Service provider.

5.2.1.1.3 Actor Specific Issues

PoC Participants

Want to be able to communicate quickly using voice.

Want easy to use handsets.

Want good voice quality.

PoC Host:

Want to be able to control the PoC group.

Service Provider

Wants to attract corporate customers to new infrastructure.

Wants to maximise potential for VoIP services.

5.2.1.1.4 Actor Specific Benefits

PoC Participants:

Increased productivity.

- Ease and speed of placing voice calls.

PoC Host

Takes authority to control and administer the PoC group.

Service Provider

Takes revenue from PoC voice calls.

5.2.1.1.5 Pre-conditions

All PoC group participants are enabled to use the PoC service and using PoC compatible terminals with PoC client.

All PoC group participants have connectivity to PoC Service Provider.

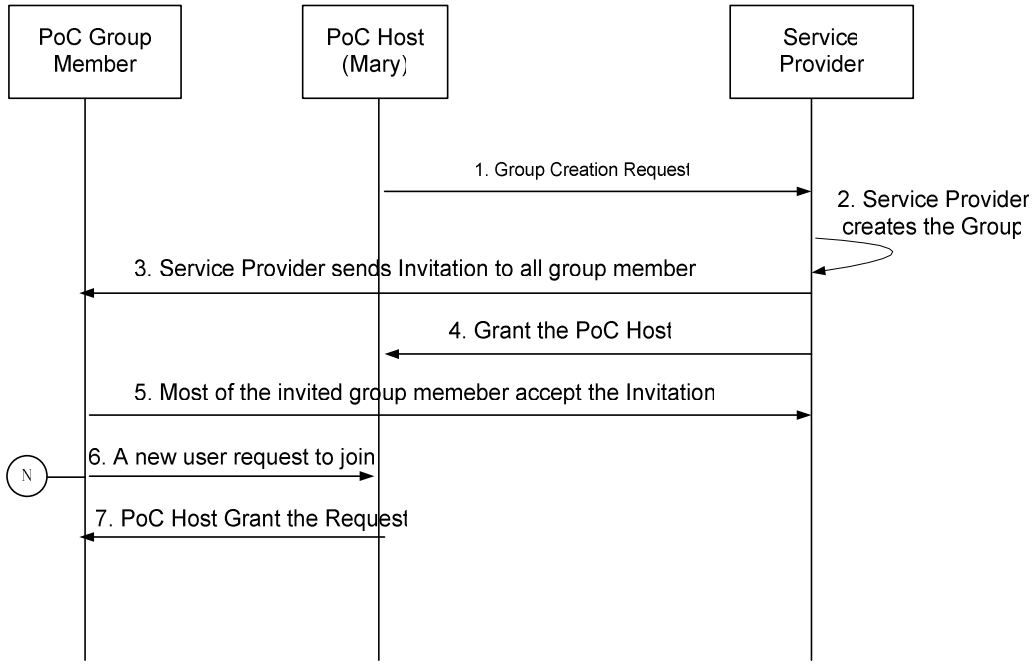
5.2.1.1.6 Post-conditions

When the group came to an end, the administrator may unregister all the participants and stop the service for this group. For another group, there is their PoC service running, but, as all the participants have left the service, the administrator may decide to terminate the service. In the both cases, the administrators give back their authority to the PoC service provider.

5.2.1.1.7 Normal Flow

The following flow provides the prose description of the PoC group creation by a PoC end-user.

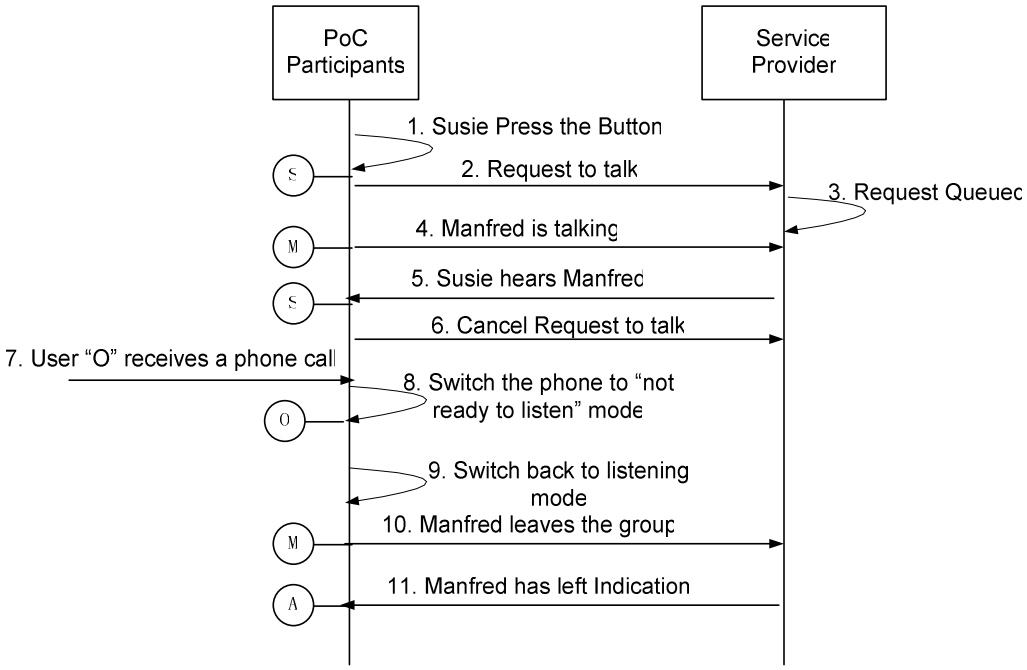
1. A PoC end-user (Mary) sends a request to create a PoC Group to the Service Provider.
2. Service Provider creates the group according to the request.
3. Service Provider advertises the PoC group to all the invited group members with the group name and the PoC Host for the group.
4. The Service Provider grants part of the administrative authority to requestor (Mary), so that the requestor becomes PoC Host.
5. Most of the invited group members accept the invitation and become PoC Participant of the group.
6. A new end-user send a request to PoC Host to join the group
7. PoC Host grants the request to join.



PoC Group Creation

The following flow provides the prose description of the basic PoC service when the end-user starts speaking and listening.

1. A participant pushes the talk button to request that she would like to speak.
2. The request to talk indication is sent to the service provider.
3. The network recognises the request by the end-user and puts the request in a queue since another participant in the group is talking.
4. The other participant speaks.
5. The speaking is delivered to other PoC participants in the same group.
6. The requestor hears the other participant's speech and decides to cancel her request.
7. Another participant in the group receives a circuit-switched phone call.
8. The participant set his PoC configuration to "not ready to listen" mode.
9. After finishing the CS call, the participant switches his PoC configuration back to listening mode.
10. Another participant decides to leave the group.
11. All the other participants in the group receive an indication that this participant has left the group.



PoC Group talk

5.2.1.1.8 Alternative Flow

None.

5.2.1.1.9 Operational and Quality of Experience Requirements

- The request-response time by the network and the distribution of the voice message shall be short enough so as not to irritate the end-users when the end-users take action to speak and to listen.

5.2.1.2 Use Case - User Defined Group for PoC Call One-to-Many

"User Defined Group Call – One-to-Many" (Reference: OMA-RD_PoC-V1_0-20040506-C Use Case G).

5.2.1.2.1 Short Description

Group Call is a half-duplex dispatch audio communications between multiple end-users. In the case of User Defined Group Call, an end-user invokes a Group Call to a group list that end-user previously created via a network provisioning action. An end-user creates and provisions a group which creates a persistent group identifier (which is held in the network and the handset) that the group owner can reference from his/her URI list. The subscriber that creates the group member list is the group owner for that group, and other members cannot change that member list, unless modification permissions are given to those members.

The end-user can define the group member list via web mechanisms in the network, or via handset GUI operations, which allow the end-user to pick people from their URI list, and add those people to a group list definition. The group is given a name or handle, which can then be then referenced in the owners URI list.

If group members are in an automatic accept mode of call acceptance, typically associated with having high audio /speaker phone operation, the called parties are automatically joined to the group call. Otherwise, if they are in an invited mode of call acceptance, the called parties have the option of accepting or rejecting the group call invitation.

5.2.1.2.2 Actors

Participants: Alice, Bob, Charlie, and Dave. Alice has defined a group, "Workteam", consisting of Alice, Bob, Charlie, and Dave. Alice wishes to call the "Workteam", for a short conversation.

Host: In this case, Alice is the owner of the group "Workteam", and will initiate the group call.

Network operator.

Service provider.

5.2.1.2.3 Actor Specific Issues

Participants

- End-users want to respond quickly communicate using voice to a broad number of people, and have all those people participate in a discussion.
- Want easy to use handsets, with fast methods of selecting end-users and initiating a call.
- Want reasonably good voice quality.

Network Provider

- Wants to attract customers to new service.
- Wants to reduce subscriber churn to other network providers.
- Wants to maximise potential for VoIP services, offering new revenue generating service.

5.2.1.2.4 Actor Specific Benefits

Participants

Better productivity – PoC calls are of quick duration, and gets end-users back to more productive tasks (vs. waiting for calls, or participating in calls that typically last longer than PoC calls).

Ease and speed of placing PoC group voice calls. Group Calls far easier to coordinate that establishing conventional conference bridges.

Network Provider

Takes revenue from PoC voice calls. Group Calls can generate large aggregate minutes of use, as many people can be pulled into a call.

5.2.1.2.5 Pre-conditions

Alice, Bob, Charlie, and Dave have PoC capable terminals and service subscriptions, and Alice, Bob, and Charlie have powered-on their phones. Dave has not powered on his phone. Alice's, Bob's, and Charlie's PoC phones have registered with the network for PoC service. The handsets have provided presence information about Alice, Bob, and Charlie to the network (either automatically, or upon their interaction with the handset).

Alice, via a previous provisioning action, created a group called "Workteam" consisting of Alice, Bob, Charlie, and Dave. This group definition exists on both the handset and in the network. The mechanisms for synchronizing the group definitions and the URI lists are outside the scope of this use case.

5.2.1.2.6 Post-conditions

Alice, Bob, and Charlie have finished their User Defined Group Call and ended their session. Dave did not participate in the session.

5.2.1.2.7 Normal Flow

- Alice would follow the same procedure for placing a User Defined Group Call as placing a Private Call, however instead of selecting a specific end-user on the URI list, a specific group would be selected, and in this case, it would be called "Workteam". In this case, no presence information is provided for a group, as it consists of multiple members with obviously difference presence states (Bob and Charlie are "online", Dave is "offline").

- When Alice selects the "Workteam", she then presses and holds the "PoC" button/key, indicating to the network that she would like to speak. The network attempts to reach all the group members. Alice hears a talk-proceed-tone as soon as the first group member handset joins the call, indicating that she can now begin to speak. As members are added to the call, Alice is notified as members join the call. For example, if Bob's handset automatically joins the call first, and Charlie's handset joins a few seconds later, Alice would be informed that Bob joined the group, and then a bit later Charlie joined the group. This way, members can be apprised as to who is on the call.

- All of the active target members of the "Workteam", Bob and Charlie, will hear a tone to announce the incoming group call. A visual indicator (along with Caller ID of the originator) will be provided to Bob and Charlie to indicate that this is a Group Call verses a Private Call. Each member of the talk group will be able to respond and participate in the call using the previously outlined method for Private Call. PoC subscribers will not be able to participate in more than one group call at a time. The group call will continue with the "Workteam" as long as two or more members are engaged in the call. As soon as only one member exists on the call, or no group activity is detected, the "Workteam" group call session is terminated.

5.2.1.2.8 Alternative Flow

A number of alternative flows or methods exist for this User Defined Group Call;

- Call Start Criteria – The talk-proceed could be held off until all active members join. However, if invite methods are required at the target, this could significantly hold up the call start. Therefore, it is recommended that call start occur on the first join of any the group members.

- Call Tear Down Criteria – Based on the billing models, it might be desirable to terminate the group call as soon as the originator leaves the call, especially if the group call is paid for by the calling party. This should be a PoC system configuration capability.

- Missed Call Notifies - Members of the group who are on another PoC call and not available for the User Defined Group Call will receive an indication on their handset that a Group Call from the call originator was missed.

- Invite Based Call Treatment - Invitation based call treatment at the target should be supported as in the Private Call.

- Callbacks – Even though Bob and Charlie don't own this group definition, the Group ID will show up in their recent call list. Since Bob and Charlie participated in the "Workteam" call, they can call that group back through their recent call list.

- Call Re-Join – In similar fashion to callbacks, if the one of the "Workteam" members drop off the call (tunnel, took another call, etc.), the members may re-join a group call in progress through initiating a PoC call to the Group ID in their recent call list.

5.2.1.2.9 Operational and Quality of Experience Requirements

PoC Terminals should support the following (as a minimum):

- The same ergonomic elements called out for the Private Call support (PoC buttons, comfort tones, URI lists, speaker phones, recent calls lists, active group member lists, visual indicators of floor control).

- Caller ID of the group originator should be provided to all parties of the group call. Additionally, the friendly group name, "Workteam" should also be provided.

- Current talker ID for the group should be provided.

- A list of active group member participants should be provided by the handset to the end-user.
- The initial call setup (first "PoC") exchange can take longer than subsequent PoC setups in the same session.

5.2.1.3 Use Case - User Defined Private Group

"Private Chat Group Support – One-to-Many" (Reference: OMA-RD_PoC-V1_0-20040506-C Use Case I).

5.2.1.3.1 Short Description

Chat groups in PoC have similar operational behaviours as conventional group calls, with the following main differences;

- When an end-user builds/defines a Chat Group, it is a private group, and specific members are invited to the chat group. The Chat Group ID is provided by the PoC service to all selected members of the group.
- End-users may join the Chat Group via selecting the Chat Group ID from their URI list (or other chat group lists) and pushing 'PoC'. However, joining a chat group does not result in inviting all the members of the group, as in group call. Members join the group of their own volition.
- Once end-users join, they stay attached or bound to that group in a static fashion, whether there are discussions in the Chat Group or not.
- If no one is speaking in the Chat Group, the radio resources may be released by the network after a period of time. Upon activity in the group, the audio will be transmitted to the end-users attached to the group, which may result in activating the RF channels for those end-users.
- End-users participate in the Chat Group in a half-duplex fashion as in the Group Calls.
- When a end-user wishes to unattach from the group, this will require a end-user action on the device to signal to the network to remove him from that Chat Group session.

Chat Groups really differ from a group call in the sense that people join and leave as they wish, and members are not actively pulled into a call as people join. It is "permanently" created by an owner, and has properties similar of a conference bridge.

Concerns exist on the feasibility of public PoC Chat Groups that would be created by a PoC service provider. Issues of privacy, name hiding, group moderation and supervision, control / overloading, and the basic utility must be explored more fully.

5.2.1.3.2 Actors

Participants: Alice, Bob, Charlie, Dave. Alice has defined a chat group, "Sales Chat Room", consisting of Alice, Bob, Charlie, and Dave. Alice wishes to have a quick "conference call" at 9 am with Bob, Charlie, and Edward for a fast sales status review.

Host: In this case, Alice is the creator of the "Sales Chat Room", including Bob, Charlie, and Edward. After she creates the Chat Group, the notification of the "Sales Chat Room" is sent to Bob, Charlie and Edward.

Network operator.

Service provider.

5.2.1.3.3 Actor Specific Issues

Participants

- Chat Group creator wants to create a fast access "conference bridge" that is persistent, and can be used at any time. The group is closed, but readily accessible for all approved members.
- Want easy to use handsets, with fast methods of selecting end-users and initiating a call.

- Want reasonably good voice quality.

Network Provider

- Wants to attract customers to new service.
- Wants to reduce subscriber churn to other network providers.
- Wants to maximise potential for VoIP services, offering new revenue generating service.

5.2.1.3.4 Actor Specific Benefits

Participants

- Chat Group provides very fast access "conference bridge service". Very likely more cost effective than paying for conventional bridging service. Also, Chat Group ergonomics will likely shorten meeting times compared to normal conference bridge sessions.
- Chat Group allows people to participate in "Group Call" like sessions, without being bothered with an invitation to join the group call. People join the group on as their schedule allows, vs. being immediately pulled into a group call.
- Ease and speed of placing PoC chat group calls. Group Chat calls far easier to coordinate that establishing conventional conference bridges, and are permanent.
- Better productivity – PoC calls are of quick duration, and gets end-users back to more productive tasks (vs. waiting for calls, or participating in calls that typically last longer than PoC calls).

Network Provider

- Takes revenue from PoC chat groups. Like Group Calls, Chat Groups can generate large aggregate minutes of use, as many people can join the call.

5.2.1.3.5 Pre-conditions

Alice has previously defined a chat group, "Sales Chat Room", consisting of Alice, Bob, Charlie, and Dave, and this Chat Group ID / name has been sent and stored in their devices. Alice wishes to have a quick "conference call" at 9 am with Bob, Charlie, and Edward for a fast sales status review, so Alice sends an SMS message to Bob, Charlie, and Dave requesting them to join the "Sales Chat Room" at that time.

5.2.1.3.6 Post-conditions

The "Sales Chat Room" call is over, and all members have exited (un-attached) from the "Sales Chat Room".

5.2.1.3.7 Normal Flow

- Alice, Bob, Charlie and Dave would follow a similar procedure for joining a Chat Group as placing a Private Call, however instead of selecting a specific end-user on the URI list, a specific Chat Group would be selected, and in this case, it would be called "Sales Chat Room". In this case, no presence information is provided for a chat group, as it may consist of multiple members with obviously difference presence states (Bob and Charlie are "online", Dave is "offline").
- When Alice finishes selecting the "Sales Chat Room", she may press and release ("Quick key") the "PoC" button/key, indicating to the network that she would like join the group. The push and release method is suggested so that she can use the PoC button as the method to join the chat group, which will cause her to join and be put into a listen mode. This way, if group members have already joined, they may already be speaking and have the floor. She will begin to hear dialog on the next talk burst after joining. If Alice does not hear anyone speak, she may request the floor via pushing the "PoC" button again.
- Alternatively, she may press and hold the button after selecting the "Sales Chat Room", and if provided the talk proceed tone, she may immediately begin speaking. However there is a chance that she will be rejected if someone

else in the Chat Group is already speaking. Therefore, the press release method is suggested as the preferred behaviour to join a Chat Group.

- As members join, the handset devices display the Caller ID's of the joining parties in the Chat Group. Additionally, an 'entry' audio tone is played on the handsets, indicating that a person joined the group.

- Alice was the first person to join the Chat Group, Bob joined a few minutes later, and then Charlie and Dave joined the Group near the same time. Once Alice has determined that all the group members are on the call (confirmed through her handset display), she has a discussion with each of the team members on their sales contacts status, in a back and forth half duplex manner as in Group Call. When Alice has all of her status from the team members, she says goodbye and leaves the Chat Group. Bob and Charlie stay in the Chat Group for a while longer to talk about some sports related topics, and Dave is not interested and leaves the chat group. When the members want to leave the chat group, each of the participants detach from the Chat Group via an option on the handset GUI. It should be emphasised that there is no session timer for Chat Groups, and if there is a large amount of time between talk spurts, the chat session is not terminated by the PoC service. Exiting the Chat Group requires a manual action from the member.

5.2.1.3.8 Alternative Flows

- Handset Automatically Logs Off Chat Group if Idle - A handset client may have additional functionality to provide an automatic logoff from a chat group if there has been no activity on the group for a period of time, configured by the PoC end-user.

- Creator Privacy Control – The creator of the Chat Group should have the ability to specify if only the provisioned end-users may join the group, or if the chat group is open to other non-provisioned members if they are given the Chat Group name/ID.

5.2.1.3.9 Operational and Quality of Experience Requirements

PoC Terminals should support the following (as a minimum):

- The same ergonomic elements called out for the Private Call support (PoC buttons, comfort tones, URI lists, speaker phones, recent calls lists, active group member lists, visual indicators of floor control).

- Caller ID of all chat group participants should be provided to all parties of the group call. As end-users join and leave, the handset devices should display the participant lists to reflect the current membership status. Also, join and leave tones should be played at the handset as member join / leave.

- End-users must explicitly join and leave the chat group through actions on the handset. No automatic joins, or automatic session teardowns occur for chat groups.

- Current talker ID in the chat group must be provided.

5.2.1.4 Use Case - Multiple Group Operation

"Use of Multiple Group Operation" (Reference: OMA-RD_PoC-V1_0-20040506-C Use Case K).

In this use case, Julie is a cleaner in a hotel, and her work also includes responsibility to coordinate workflow with the hotel laundry.

5.2.1.4.1 Short Description

Julie participates both in the group "cleaners" and in the group "laundry". The group "cleaners" is used whenever the cleaners need any kind of assistance of each other, and when any other related person has something to communicate to or request from the cleaners. In this example, the groups are chat rooms that are joined by the persons involved at the beginning of their work shift, but the use case can be applied to other types of groups as well.

Julie is hearing voice from the group "laundry".

Now the hotel receptionist selects the group “cleaners” on his/her PoC end-user equipment. Presses the talk button and starts to talk to ask if there is any vacant, single room already cleaned up.

Because the group “cleaners” is related to Julie’s primary duties, the transmission of the receptionist will override her reception of the group “laundry” and she will hear the voice of the receptionist.

Note that the communication in the laundry group is not disturbed in any way. In addition, if Julie is talking in the “laundry” group, she is not interrupted.

Julie sees on the PoC end-user equipment display that the “cleaner” group communication is received and receptionist is talking.

Julie presses the talk button, when she sees on her display that the receptionist talk burst is over and tells that she has a room # 274 available.

The receptionist thanks Julie and gives the room to the customer.

After a certain period, if there is no subsequent traffic in the group “cleaners”, Julie starts to hear the group “laundry” again (if there is traffic).

5.2.1.4.2 Actors

Participants

- Hotel receptionist, who needs to be able make requests to cleaners.
- Julie, a cleaner, who needs to keep informed of the situation in the hotel laundry.
- Other cleaners.
- Laundry personnel.

Host

- Hotel management

Network operator.

Service provider.

5.2.1.4.3 Actor specific issues

Participants

- want to be able to receive “handsfree” information related to their work
- want to be able to reach people related to their own work quickly and easily
- want to keep informed of the activities of groups related to their own work, by monitoring traffic in such groups
- want to give priority to the particular group

Hotel management

- wants to optimise the efficiency of their operations
- wants to minimise the communication cost to support the workflow

Network provider

- wants to minimise the resources used for a given revenue

5.2.1.4.4 Actor specific benefits

Participants

- Each participant hears only the traffic that is relevant to her work

Network provider

- A more efficient solution, because it allows using two small groups instead of one large one, so that less resources are used

5.2.1.4.5 Pre-conditions

All parties have PoC capable terminals and PoC service subscriptions. Receptionist and all cleaners on working duty are beforehand joined in the same group “Cleaners”. Julie, one of the cleaners, has joined the group “cleaners” as her primary group and additionally the group “laundry”.

5.2.1.4.6 Post-conditions

Receptionist has found a cleaned room.

5.2.1.4.7 Normal Flow

- Julie activates group “cleaners” as her primary group and the group “laundry” as an additional group.
- Julie hears traffic from the group “laundry” if there is no traffic in the group “cleaners”.
- Receptionist selects the group “cleaners” to talk to, presses the talk button and asks if any single room is already cleaned.
- All group members see that receptionist is talking and hear that she/he is asking a cleaned room. Those group members, who have “cleaners” as their primary group, hear the receptionist even if they were just hearing another group.
- One of the group members has a room ready made and she presses the talk button, when the previous talk burst is over and talks to receptionist, that she has a room. All other group members hear also, that room was found and there is no need anymore to talk with receptionist.

5.2.1.4.8 Alternative Flows

None.

5.2.1.4.9 Operational and Quality of Experience Requirements

A PoC end-user shall be able to be joined-in to more than one group at a time for group communication. There can be two levels of groups for an end-user: one of the joined-in groups may be his primary group and the rest of the groups are secondary.

In case an end-user only has secondary groups, the main requirements are:

- If there is traffic in more than one group at the same time, there shall be a means to filter the traffic so that the end-user hears a single conversation
- The end-user shall start to hear traffic from any group that starts first
- The end-user shall continue hearing the same discussion (i.e., traffic from the same group) rather than hopping from group to group, unless there is a period of silence to indicate that the discussion has ended
- Because the end-user will be receiving voice from multiple groups in sequence, there shall be a means to identify which group is being received

- There may also be means to allow end-user to hears multiple groups at the same time
- When the end-user wants to talk into a group, she shall be able to select to which group to talk. The selection may also be implicit (e.g., the transmission is to the group that was most recently heard).

In case the end-user has a primary group and secondary group(s), the following additional requirements are

- If there is no traffic in the primary group, the end-user shall receive traffic from secondary groups according to the requirements described above
- Voice in the primary group shall be received immediately, even if the end-user was receiving voice in secondary group
- As long as there is traffic in the primary group, the end-user shall continue hearing it, until there is a period of silence to indicate that the discussion has ended.
- When the end-user wants to talk into a group, it shall be possible to have the primary group as the default target
- The end-user shall be able to change her primary group
- When the end-user is talking, her transmission should not be interrupted because of traffic in another group
- The end-user shall be able to lock herself temporarily into one group and thus, suspends the listening of the other groups.

5.2.1.5 Use Case - User Defined Temporary Group

"Ad-hoc Chat Group Support – One-to-Many" (Reference: OMA-RD_PoC-V1_0-20040506-C Use Case M).

5.2.1.5.1 Short Description

PoC Host creates an ad-hoc PoC Group a week before an important meeting. The PoC Group ID is circulated on a company's internal mailing list. The PoC Host's colleagues, who plan to attend the meeting, register with the ad-hoc PoC Group individually using the PoC Group ID. (A colleague gives the Group ID to his friend; this friend is not part of the group who plans to attend the meeting.) A corresponding buddy list is automatically created; any of the PoC participants in the PoC Group can see who is online/offline.

5.2.1.5.2 Actors

- Participants (10): Paul, George, Ringo, John, Yoko, Billy, Bob, Eric, Elton and Michael. Paul has defined an ad hoc PoC group called "Meeting Chat Room". (The chat room consists of no members yet. Later on, other people will register themselves to the chat room in a simple manner described later in this paper.)
- PoC Host: Paul is the PoC Host. He creates the "Meeting Chat Room", which now includes no members. After he creates the ad hoc PoC group, a PoC Group ID (numerical or alphanumerical) is displayed on his screen. Paul sends this information to the appropriate members via his email account
- Network operator (or PoC service provider): At registration the network operator provides the facility to check if the entered PoC IDs (PoC end-user identities) belong to the PoC participant. For this ad hoc PoC service, PoC IDs are of the nature of MSISDNs or SIP URIs so other PoC participants can identify who is in their PoC group. However, in case of public PoC chat rooms, nicknames can be supplemented for PoC IDs.

5.2.1.5.3 Actor Specific Issues

Participants

- PoC Host wants to create an ad hoc PoC Group on the fly, but he does not want to be bothered with the administrative actions[1]; he wants to have each member register him/herself. Therefore, all members have some administrative rights.

- To maintain some level of security/privacy when a PoC participant registers himself using his Group ID the corresponding MSISDNs or SIP URIs are checked by the network operator and are shown on each PoC Group participant's screen. Any PoC participant can see the list on his/her terminal.

- In some cases, a malicious PoC end-user, who is an outsider, could steal the PoC Group ID by eavesdropping, and secretly join the PoC Group. A PoC Host has the right to remove any PoC members from the ad hoc PoC Group and to block him/her from future registration.

    - Additionally the PoC Host can also grant rights to any participant to remove/block PoC members.

Network Operator (or PoC Service Provider)

- The network operator (PoC service provider) checks the registrants' PoC IDs (PoC end-user identities) at registration. All PoC Group participants are visible to each participant. A cooperated operation between the network operator and the PoC service provider is necessary to archive a certain level of security. Additionally, cooperation of participants (including the Host) can be a measure of fraud avoidance.

Three levels are provided for PoC group communications

- Prearranged (already defined)
- Ad Hoc (already defined)
- Chat Mode
    - *Members-only* - Anybody can join the group if he/she has membership via a PoC Group ID.

- His (MSISDN/URI) information is displayed.

    - *Public* - Anybody can join the group if he/she has membership via a PoC Group ID.

- His nickname may be displayed.

5.2.1.5.4 Actor Specific Benefits

Participants

- **Simplicity and quickness for ad-hoc PoC grouping** -- for the PoC Host, administrative actions are limited to the request of the PoC Group ID and the creation of the chat room. This is requested to either a network operator or to a PoC service provider. The PoC host can also define the expiration time (optional) for 1, talk sessions and 2, termination of the group itself (for, say, 2 days after the meeting).

- **Openness** -- anybody who knows the PoC Group ID can join the PoC Group. This is, in a sense, similar to a typical IM chat room.

Network Provider

- **More PTT usage expected** -- PoC usage will increase by providing more open access levels; *members-only* access and *public* access.

[1] Ad hoc PoC Group communications are intended for casual ad hoc communications mimicking the legacy walkie-talkie operations. Degraded security/privacy might be a trade-off.

5.2.1.5.5 Pre-conditions

Paul registers and obtains a PoC group ID via the PoC end-user interface on his terminal. Paul then sends the ID to his colleagues via his company's internal mailing list. His colleagues, who plan to attend the meeting see Paul's message. They get the ID and store it (on paper or via some device). Paul set the PoC Group to terminate 24 hours after the last day of the meeting.

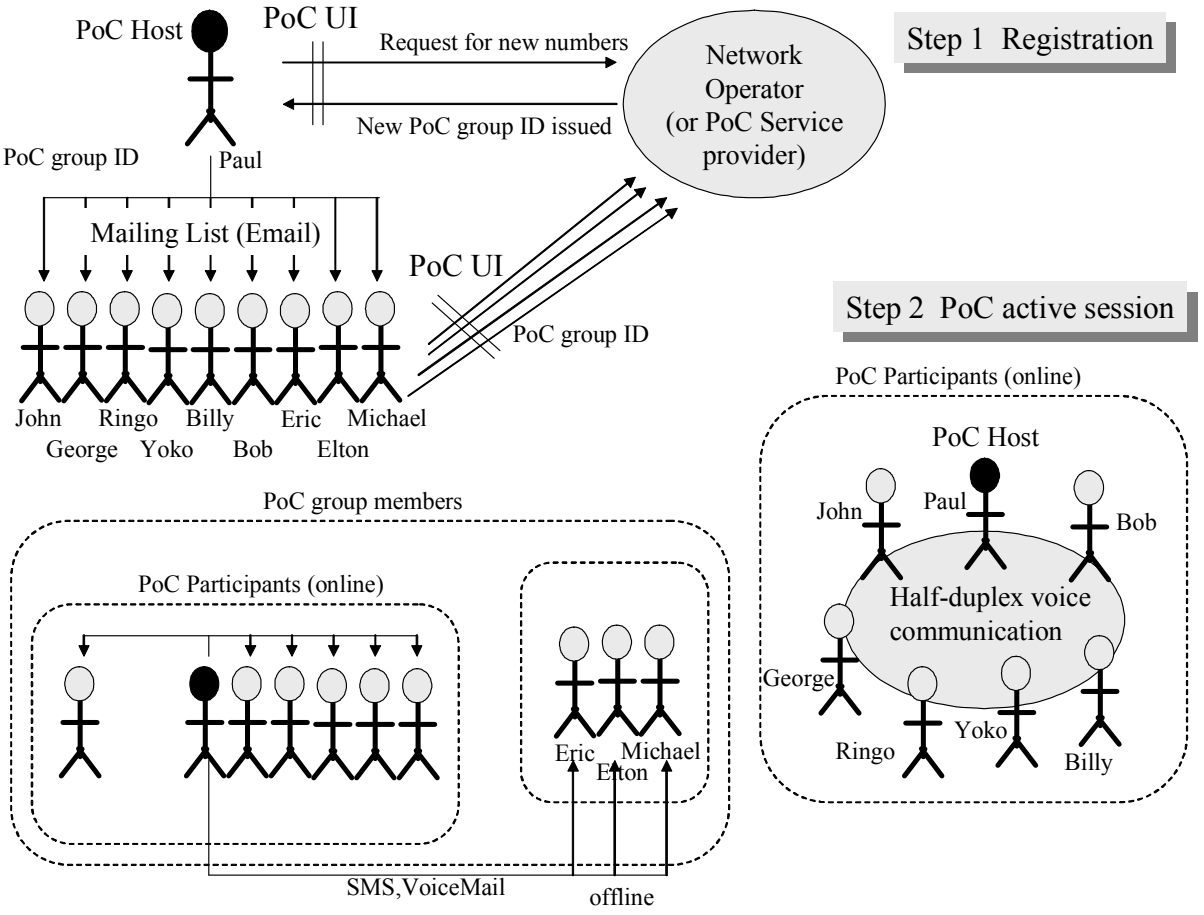
5.2.1.5.6 Post-conditions

The meeting is over, and all the members have no use for this PoC Group Chat Room. In 24 hours from the last meeting day (designated by the Host), the PoC Group is terminated.

5.2.1.5.7 Normal Flow

The figure below explains the service steps schematically.

Step 1 is divided into two sub-steps; Sub-step 1, the Host requests a PoC group ID, and Sub-step 2, Participants register to the group by entering the PoC group ID via the PoC end-user interface (PoC UI).



Step 1 Registration

- A week before the meeting, John, George and six other colleagues receive an email form Paul (making 9 total members), which says, "Let's create an ad hoc PoC Group for our upcoming meeting. Please join the PoC Group with this PoC group ID". Some of the members register to the PoC Group at once. But some others do not.

- The morning of the first meeting day, Ringo meets Elton. Elton says to Ringo, "Have you already registered with the PoC Group?" Ringo says, "Darn, I forgot! I lost the ID". Elton jots down the ID on a sheet of paper and says, "You are so forgetful. Here you are", and gives the paper to Ringo. Ringo registers with the PoC Group.

- Yoko comes across Michael in the main venue just near finishing time. Although Michael is not one of the original 9 members, he is one of Yoko's buddies and Yoko wants Michael to join his PoC Group as they will soon go out for beers. Yoko hands Michael the ID.

Step 2 PoC active session

- John, who has already registered to the PoC Group, finds a guy named Michael is suddenly on the list. He is disgruntled and makes a PoC Private Call (one-to-one), "Who on earth are you?" Michael says, "I used to sing with Yoko's husband. Yoko invited me but perhaps she has not notified the group yet. I will log off so that nobody else is surprised. Hope you don't mind me coming with you tonight for drinks and dinner. "

- Around half past 6pm, the group is ready to drink and eat. Paul makes a PoC Alert Call to all the PoC Group participants. Seven participants are logged-in (PoC Participants – online, active), but three other participants (Eric, Elton and Michael) are offline. After waiting for a few minutes, Paul makes a PoC Group Call by pressing Talk Button, "Guten Abend! I used to live in this area when I was in college. The beer was great. Are we all ready?"

- John replies, "I want to have Eisbein mit Sauerkraut! And beer, of course! My favourite is Berliner Kindle".

- Ringo asks the group, "Say, where shall we dine? I happen to be walking in Europe Centre, a popular shopping mall in West Berlin. I see a German restaurant called Alt-Nuernberg. It looks good. I can even go through the menu while I am talking to you. Group agreed to discuss the menu over the PoC session

- Paul, "After our call I'll send an SMS or voice mail to those offline (Eric, Elton and Michael) with a message, **Eating out, Alt-Nürnberg in Europe Centre, 7PM, Tel:030 2614397".**

5.2.1.5.8 Alternative Flows

None.

5.2.1.5.9 Operational and Quality of Experience Requirements

PoC Terminals support the following:

- Chat Mode PoC Group end-user interface is provided. An end-user requests and obtains a PoC Group ID that is issued by a network operator/PoC service provider via the user interface. The end-user enters via the UI, the PoC Group ID to become one of the PoC Group participants. The registered participant is automatically and dynamically added to the buddy list belonging to the PoC Group ID.

- The PoC IDs are tied into either MSISDNs or SIP URIs of all registered participants to the PoC Group and are visible on the PoC Group list. Optionally end-user names, for example, "John Doe" in this SIP From header field [From: John Doe <sip: Jdoe@necam.com>], are displayed.

A network operator (and PoC service provider) supports the following:

- Chat Mode PoC group services are provided with the following access levels – *members-only* and *public*.

- For *members-only* and *public* access levels, a network operator has to give part of the administrative rights to every PoC group member to let him manage his own PoC group registration.

- For *members-only* and *public* access levels, a network operator has to grant the PoC Host with administrative rights. For example, PoC Host may remove any PoC group member (and block him/her from future participation) in the PoC Group.

  - Additionally a PoC Host may grant a participant with the same rights

- For *members-only* and *public* access levels, a network operator has to perform some form of authentication for PoC Group member registrations.
- Anonymous access or nicknames may be allowed and are at the discretion of the PoC Host or network operator (PoC service provider).
- For *members-only* access level a 'buddy list' is created when the PoC Group ID is issued or when the first PoC end-user logs into the 'chat room' of the PoC Group.
- For *public* access level a 'buddy list' may not be created when the PoC Group ID is issued or when the first PoC end-user logs in the 'chat room' of the PoC Group. However, a network operator must create a 'buddy list' when the PoC end-user requests a certain level of security/privacy.

5.2.1.6 Use Case - Private Group for Secure PoC Corporate Chat

"Corporate Chat" (Reference: OMA-RD_PoC-V1_0-20040506-C Use Case O).

Many situations exist where a quick and efficient communication method is needed but the need for confidentiality is very high and closed user groups are demanded.

5.2.1.6.1 Short Description

In this example a small workgroup needs to communicate quickly and privately. They work within the same company and the company has provided them with the PoC enabled terminals from the same service provider.

A collection of stock traders from company X is considering a major move in the stock price of a stock that they are involved with.

By mid-day the stock price continues to move and they consider what actions should be taken with the shares.

The most senior member of the workgroup, Mike, knows his fellow traders from company X all have terminals capable of a private and secure PoC conversation.

Mike, acting as host, sends an invitation to his co-workers to start the PoC conversation.

Tom, one of the invitees is caught in another panic trading situation and can't join immediately. He ignores the first invitation and joins a couple of minutes later.

The conversation proceeds and the stocks are traded within a few minutes after the call has started.

5.2.1.6.2 Actors

PoC Participants: Tom, Peter, Paul and Mary.

PoC Host: Mike is acting as the host.

PoC Company: Company X has made it possible for this workgroup to have a PoC conversation and is paying the bill for the PoC service.

Service Provider.

5.2.1.6.3 Actor Specific Issues

PoC Participants

- Want to be able to communicate quickly as stocks are volatile and can have significant financial impact.
- Want easy to use handsets with headsets for hands-free use to allow private conversations.
- Want PoC terminals with good voice quality so trading instructions are understood.

Service Provider

- Provides corporate customers a service for business critical applications.

Company X

- Company X must have closed confidential user groups to ensure that conversations cannot be overheard and that eavesdroppers are excluded.
- Unauthorised disclosure of the actual names of Group members to third parties must be prevented.
- Secure media link so that conversations cannot be intercepted.

5.2.1.6.4 Actor Specific Benefits

PoC Participants:

- Trusted and secure system that enables large value stock trades.

PoC Host

- Efficient workgroup communication, which can be leveraged to increase revenue for the company with a solid coordinated effort in selling or buying stocks.

Service Provider

- Increased revenue from corporate customers.

5.2.1.6.5 Pre-conditions

All PoC group participants are enabled to use the PoC service and have PoC compatible terminals. All PoC group participants have connectivity to PoC Service Provider through their company subscription.

The group has been authorised and made available for designed employees using company-approved methods for confidentiality.

5.2.1.6.6 Post-conditions

When the call comes to an end, the host terminates the call knowing that all will execute the trade instructions.

5.2.1.6.7 Normal Flow

- Mike knows that there is a problem in the morning and might even warn his co-workers via e-mail, Instant Message or PoC that they should be prepared for this afternoon trade discussion.
- In the Afternoon the value of some stock continues to move and Mike decides to initiate a conversation with the team using a predefined group name.
- Various people accept the PoC conversation and get their instructions at that time. Any concerns are voiced and a consensus is reached.
- The trade is agreed to and the stock is traded.

5.2.1.6.8 Alternative Flow

- An alternative situation Mike forgets to warn his co-workers of what he is planning.
- His attempt to schedule a meeting finds only a small subset of the team available.
- Those that are left and have successfully connected to the PoC service, discuss the situation.
- They have the discussion; Mike decides to call off the trade. He then sends an e-mail, or Instant Message to the team to inform them what has happened.

5.2.1.6.9 Operational and Quality of Experience Requirements

- The PoC service entity should allow the company subscriber to affect and authorise the groups that can be used by the end-user.
- The PoC capable terminal should have a headset in addition to the speaker.
- The PoC service entity should allow corporate PoC calls to have integrity and confidentiality.
- The PoC service entity should allow the company to manage naming identities that are commonly used within the company
- The PoC service entity should allow the company to use a name space within the company that is independent from the addressing used within the PoC network.

5.2.1.7 Use Case - PoC Fleet Dispatch: One-to-Many-to-One

"Fleet Dispatch – One-to-Many-to-One" (Reference: OMA-RD_PoC-V1_0-20040506-C Use Case N).

5.2.1.7.1 Short Description

A fleet delivery service or taxi service using PoC for dispatching has similar operational behaviour to group calls, with the following main differences:

- Fleet members and dispatcher use a dedicated PoC group for dispatch management.
- The dispatcher is a distinguished actor with capabilities that are quite distinct from those of the fleet members:
  - All fleet members hear the dispatcher, or,
  - In a more sophisticated version where PoC and Locationing services are both available, only fleet members meeting a given criterion selected by the dispatcher, such as, being within 5 km of a given location, might hear the dispatcher in a given instance.
  - Only the dispatcher hears an individual fleet member. This is different from all other use cases.
  - Optionally, the dispatcher can preempt the channel from the fleet member.

5.2.1.7.2 Actors

Participants: There are two classes of participant:

- The dispatcher, who can interact with all the fleet members or any subset of them
- The individual fleet members, who can only interact with the dispatcher.

Host: The dispatch channel is typically administered independently of the participants. The administrator assigns dispatch and fleet roles to the participants.

Network Operator: Provides the network and radio resources used for the communications.

Service Provider: May be the network operator, the fleet operator, or some third party provider supporting dispatch as a value-added service.

5.2.1.7.3 Actor Specific Issues

Participants

- The dispatch channel should be permanently available and easily accessible.
- Access to the dispatch channel should be limited to the dispatcher and the fleet members.

- All fleet members need to be able to hear the dispatcher.
- Only the dispatcher needs to hear the fleet members.
- Voice quality only needs to be intelligible.

Host

- Needs to be able to add and remove fleet members from the group
- Needs to be able to assign different employees dispatcher authority
- Needs standard terminals for fleet members, specialised dispatch terminal for dispatcher.
- Wants to reduce communications costs
- Wants to be able to integrate dispatch with other services (e.g., locationing, emergency systems, text messaging).

Network operator

- Wants to replace traditional dispatch channels
- Needs to provide wide coverage
- Opportunity to integrate PoC with other services

Service Provider

- Requires the ability to provide new types of service.

5.2.1.7.4 Actor Specific Benefits

Participants

- Replaces existing capabilities with equivalent services on standard equipment and with upgrades to integration with additional services.

Host

- Lowers costs through use of non-specialised terminals and shared radio resources.
- Integration with other facilities allows improvements in efficiency of fleet management.

Network operator

- Creates additional revenue stream.

Service Provider

- Provides a new type of service.
- Creates additional revenue stream.

5.2.1.7.5 Pre-conditions

The host has previously created the dispatch group, and has identified one member as the dispatcher.

5.2.1.7.6 Post-conditions

The dispatcher may convert the one-to-many-to-one call to a one-to-one call with the fleet member who answers.

After interacting with the fleet members, the dispatcher moves to the next action.

5.2.1.7.7 Normal Flow

- A fleet member may initiate a call to the dispatcher by pressing a Talk button. The dispatcher's response is heard by all fleet members. However the fleet member's side of the conversation is not relayed to the other fleet members. While this conversation is in progress other fleet members may not access the channel.
- The dispatcher initiates a dispatch call by broadcasting to all fleet members, or to a filtered subset meeting certain criteria. The return channel is open until one of the fleet members responds.
- The dispatcher is notified of the identity of the fleet member. Other fleet members may not be notified of the identity of a fleet member that the dispatcher is in discussion with.

5.2.1.7.8 Alternative Flows

If necessary, the dispatcher can cut off a fleet member and open the floor to other fleet members.

5.2.1.7.9 Operational and Quality of Experience Requirements

- The fleet members' PoC terminals should support speakerphone, Talk button, comfort tones, visual indicators of floor control. Certain common features, such as, a visual user interface, may not be required in low-end dedicated terminals.
- The dispatch terminal should support speakerphone, Talk button, comfort tones, visual indicators of floor control, tracking of active fleet members, display of speaker identity, history logs etc. It may have wired or wireless access to the network. It is likely to offer other specialised fleet management capabilities integrated with a PoC end-user interface.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

This section describes the functional requirements that are common to all document management functions.

6.1.1 General

1) The end-user SHALL be able to store his per-user information (e.g., URI Lists) in the network.
2) Such information SHALL be stored as one or more documents described in an extensible and platform-neutral format.
3) Each such document SHALL be identified by at least one globally unique identifier (i.e., a URI according to RFC 2396).
4) Documents SHALL be associated with meta-data which describes certain properties of the document that are not included in its content.
5) A document SHALL be associated with at least the following meta-data:
   a) Primary Principal: By default this value indicates the original creator of the document. The primary principal may be changed by any principal having appropriate permissions.
   b) Creator: The original creator of the document.
   c) Identifier: This property contains the URI of the document.
   d) Visibility: This property determines which principals are able to find this document when performing a search.
   e) Timestamp: This property identifies the last time when any meta-data or content of the document was changed.
   f) Permissions: This property identifies which principals have which rights to perform which operations on this document.
7) The XDM enabler SHALL allow an authorized principal to access and manage stored documents from any capable device type over any capable network.
8) Data consistency of information stored in the XDM enabler SHALL be ensured, particularly if simultaneous access by multiple authorised end-users and/or multiple devices is allowed.
9) The XDM enabler SHALL allow a XDM principal to retrieve a list of all stored documents for which the principal is the Primary Principal.
10) The XDM enabler SHALL allow a XDM principal to retrieve a list of all stored documents for which the principal is the Primary Principal per type of service (e.g., all documents related to his PoC service).
11) It SHOULD be possible to provision the XDM client using existing OMA Device Management and Provisioning enablers.
12) If provisioning data relevant to XDM is present in the smartcard, the XDM client SHALL be able to retrieve that data.
13) XDM documents SHALL support multiple character sets.

6.1.2 Delegation

1) Principals SHALL be able to authorise other principals to perform selected operations on their behalf.

2) For the document management functions identified in Section 6.1.3, there SHALL be a permission which allows principals to delegate those functions to other principals.

3) Having the permission to perform a function SHALL be separate from the permission to delegate the function to other principals.

6.1.3 Document Management Functions

The sub-sections below identify the set of available document management functions.

1) Document management functions SHALL be controlled by permissions which determine the capabilities available to a principal wishing to perform such functions.

2) It SHALL be possible to define "roles" that represent a given set of permissions. Assignment of those roles to particular principals is equivalent to assigning the corresponding set of permissions.

3) The service provider SHALL have permissions to perform all document management functions.

4) Principals MAY be assigned permissions to perform some or all of the document management functions.

5) Permissions MAY be assigned at any time from creation to deletion of the document.

6) Principals who try to perform a document management function SHALL first be authenticated.

7) The creator of a document SHALL become the initial Primary Principal of the document.

8) The Primary Principal SHALL always be allowed to modify the permissions on his/her document.

9) There SHALL always be one and only one Primary Principal of a document.

10) It SHOULD be possible for principals with the appropriate permission to query the permissions applied to a specific document.

11) XDM-based repositories MAY notify authorised principals of updates to documents, upon their request..

6.1.3.1 Create

1) Principals with appropriate permissions SHALL be able to create a document.

2) When creating a document, it SHALL be possible to define document meta-data at a minimum including the meta-data described in Section 6.1.1 (4).

6.1.3.2 Retrieve

1) Principals with the appropriate permission SHALL be able to retrieve a document.

6.1.3.3 Copy

1) Principals with appropriate permissions SHALL be able to copy documents from one repository to the same or another repository.

6.1.3.4 Delete

1) Principals with appropriate permissions SHALL be able to delete a document.

6.1.3.5 Modify

1) Principals with appropriate permissions SHALL be able to modify a document.

2) When modifying a document, it SHALL be possible to add, edit or delete document meta-data.

6.1.3.6 Suspend

1) Principals with appropriate permissions SHALL be able to suspend access to and use of a document.

2) When access to and use of a document is suspended, no operation can be performed on that document, except to take it out of the suspend state or delete it.

6.1.3.7 Resume

1) Principals with the appropriate permission SHALL be able to resume usage of a suspended document.

2) After a resume operation, all operations can be performed on that document (except for the resume operation).

6.1.3.8 Search

1) It SHOULD be possible to search for the existence of certain content (e.g., the identifier of a PoC Group member) in a document.

2) It SHOULD be possible to search for the existence of a document based on meta-data associated with the document.

3) Principals with the appropriate permission SHALL be able to define the visibility of a document when performing a search.

4) It SHALL be possible to limit the number of search results.

5) Searches MAY be limited to documents hosted by the Service Provider.

6) Search results SHALL be subject to Service Provider policy or end-user privacy settings.

7) Wildcards MAY be used when searching for documents.

6.1.3.9 Administration and Configuration

Principals with appropriate permissions SHALL be able to configure the following:

1) Different values for the maximum number of documents that can be created for different principals.

2) Different values for the maximum number of documents that can be created for different document types.

3) Permission to receive notification of administration or configuration changes.

6.1.4 Security

1) XDM protocol SHALL support:

   a) Mutual authentication of the XDM server and XDM client implementations.

   b) Integrity and confidentiality of XDM message exchanges.

2) It SHALL be possible to log all XDM interactions.

3) If there is a mechanism to perform the security functions mentioned above in a common way, the XDM protocol SHOULD support the use of such a mechanism instead of duplicating such functionality.

6.1.5 Charging

1) Mechanisms SHALL be provided for the Service Provider to charge for the use of XDM.

   Examples of charging events include:

   - The creation, modification or deletion of a document.

- The number of documents for which the end-user is the Primary Principal.

2) Mechanisms SHALL be provided for the Service Provider to charge for the use of XDM as part of another service enabler.

6.1.6 Usability

1) The XDM protocol SHOULD support version control of documents that it manages.

2) The XDM client MAY use a version control mechanism to avoid unnecessary document retrievals prior to document manipulation.

6.1.7 Interoperability

Interoperability of the XDM enabler is provided through the definition of open interfaces and a consistent format of documents and XDM functions in compliance with the requirements presented in this document. The XDM functions, open interfaces and document formats SHALL provide interoperability to include at least the following:

1) Administration of documents.

2) Transfer of documents over open interfaces.

3) General structure of the documents transferred over open interfaces.

4) Collection and general format of charging information.

6.1.8 Privacy

1) Access to XDM information SHALL conform to privacy requirements specified in [Privacy].

6.2 System Elements

This section contains high-level requirements on the basic functionality required by any system that implements the XDM specifications (e.g. a data repository containing shared documents, a data repository containing PoC-specific documents, a terminal accessing repositories as a XDM client, a PoC server accessing repositories as a XDM client, etc.).

6.2.1 XDM Clients

The XDM client SHALL:

1) Support document management functions identified in Section 6.1.3.

2) Support secure communications with the XDM Server.

The XDM client MAY:

3) Subscribe to and receive notifications regarding updates to documents.

6.2.2 XDM Servers

The XDM Server SHALL:

1) Support document management functions identified in Section 6.1.3.

2) Support secure communications with the XDM client.

3) Support charging mechanisms.

The XDM Server MAY:

4) Notify authorised principals of updates to documents.

6.2.3 Network Interfaces

6.2.3.1 Interface Between XDM Clients and XDM Servers

The interface between the XDM client and XDM server:

1) SHALL be access technology neutral.

2) SHALL support the secure exchange of XDM messages.

3) SHALL support document management functions as described in Section 6.1.3.

4) SHALL support the secure provisioning of XDM client parameters.

5) SHOULD support the synchronisation of changed data.

6.2.3.2 Interfaces to XDM Servers from Applications/Enabler Implementations

Applications and/or Enablers would assume the role of a XDM Client, and therefore the above requirements apply.

6.3 Document Types

6.3.1 Shared Documents

1) It SHALL be possible to share the following types of documents such that they can be used by multiple enablers (e.g. PoC, Presence, IM, etc.):

6.3.1.1 URI List

1) A URI List SHALL have the following meta-data, in addition to those properties specified in Section 6.1.1:

   a) Display name: A human readable name.

2) A URI list SHALL contain zero or more URI List members.

3) The following requirements apply to URI List members:

   - Every URI List member SHALL be identified by a globally unique identifier (i.e., a URI as defined in RFC 2396).
   - A URI List member MAY have a human readable display name.

4) The following requirements apply to URI List management, in addition to those specified in Section 6.1.3:

   a) The service provider SHALL be able to set the maximum number of URIs in a URI List.

6.3.2 PoC-specific Documents

This section describes additional functional requirements that are specific to document types needed to support the PoC enabler.

6.3.2.1 PoC Group Document

1) A document describing a PoC Group SHALL have the following content, in addition to the meta-data specified in Section 6.1.1:

   a) Display name: This is a human readable name.

b) Session Type: This identifies the nature of the PoC Group, which is one of two – "chat" or "instant". (In chat group sessions, members join a group session individually, whereas in an instant group session, whether pre-defined or an ad-hoc group, all other members are invited simultaneously at a group member's request.)

c) Membership: This identifies the nature of the membership in the PoC Group, which is one of two – "open" or "restricted".

d) Session initiation policy: Session initiation policy: This describes who, apart from the Owner, may initiate a PoC group session..

e) Group member list: This provides a list of end-users and/or URI lists who will be invited to a PoC session.

f) Group reject list: This is the list of end-users and/or URI lists who SHALL be barred from joining a PoC chat session. (Only for Session Type = "chat").

g) Maximum number of members: This is the maximum number of end-users who can be active in the session.

h) Anonymous access allowed: This is used to reveal, or not reveal, the end-user identities of all members of a "Chat" type group session taking the values - "yes" or "no", respectively.

2) Each entry in a Group member list or Group reject list SHALL be a tuple consisting of a URI and, optionally, a display name.

3) Each URI in the Group member list SHALL be unique.

4) Each URI in the Group reject list SHALL be unique.

The following requirements apply to PoC Group document management, in addition to those specified in Section 6.1.3:

Create:

5) The service provider SHALL be able to set the maximum number of members that can be added to a group member list or group reject list in a PoC Group document.

6) A principal with appropriate management permissions MAY be able to set the maximum number of members in a PoC Group document to a value that does not exceed the maximum number set by the service provider.

7) It SHALL be possible to create a PoC Group document that contains members in the group member list or group reject list that belong to different service providers.

Copy:

8) PoC Group members MAY use PoC Groups to which they belong to create a new PoC Group document by copying an existing PoC document, subject to service provider policy and access rules.

Get:

9) Principals SHALL be able to retrieve the Group members list contained in PoC Group documents.

6.3.2.2 PoC Access Control Policy Document

A PoC access control policy document SHALL be described by the following:

1) Accept List: A list of end-users from whom requests are accepted.

2) Reject List: A list of end-users from whom requests are rejected.

6.3.3 Presence-specific Documents

This section describes additional functional requirements that are specific to document types needed to support the Presence enabler.

6.3.3.1 Presence Policies

The following types of documents related to presence authorization policies SHALL be supported:

1) A document that defines how incoming subscription requests are handled. This document SHALL be able to utilize Accept, Reject, Polite Block and Deferred lists. Depending on how the subscription policy document combines those lists, they Presence Server will determine whether to accept, reject, politely block, or defer the handling of an incoming subscription request.

2) A document that defines what presence information will be disseminated to the watchers of a particular presentity.

3) A document that defines what conditions will trigger a presence notification for a particular presentity.

6.3.3.2 Presence Subscription Lists

Presence Subscription Lists (PSLs) are used to support the end-user to watch for presence information for a list of URIs with a list of requested attributes for every member. Following the requirement to support subscriptions to parts of the presence information, it is meaningful to link the requested presence information tuples with the PSL.

1) URI lists (as stored in the XDM server and the terminal) SHALL be supported as a reference for members of a PSL.

2) PSL SHALL support a presence attribute request list for every list member.

3) PSL SHALL support a presence attribute request list common for some list members.

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_GM-V1_0	29 Sep 2004	All	Clean version of final RD with all agreed change bars accepted for submission to OMA TP Approval
Draft Version OMA-RD_XDM-V1_0	29 Jan 2005	All	Updates from Consistancy Review
Candidate Version OMA-RD-XDM-V1_0	04 Feb 2005	n/a	Status changed to Candidate by TP: OMA-TP-2005-0060-XDM_1_0--for-candidate-approval
Candidate Version OMA-RD-XDM-V1_0	22 Feb 2005	6 2.1	Added note CR PAG-2004-0835R03 Added XDM AD reference CR PAG-2004-0835R03
Candidate Version OMA-RD-XDM-V1_0	17 Mar 2005	4.1 6	CR TP-2005-0095 implemented.