Liberty ID-WSF 2.0
Marketing Requirements Document

Version: 1.0

Notice:

This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact the Liberty Alliance to determine whether an appropriate license for such use is available.

Implementation of certain elements of this document may require licenses under third party intellectual property rights including, without limitation, patent rights. The Sponsors and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. **This Specification is provided "AS IS", and no participant in the Liberty Alliance makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose.** Implementers of this Specification are advised to review the Liberty Alliance Project's website (http://www.projectliberty.org/) for information concerning any Necessary Claims Disclosure Notices that have been received by the Liberty Alliance Management Board.

Abstract:

This combined marketing requirements document covers the primary marketing requirements for the Liberty ID-WSF 2.0 release. These consist of People Service, a combination of the Principal Referencing and the Groups and Roles marketing requirements sub-documents, and the Subscriptions and Notifications marketing requirements sub-document.

Filename: **liberty-id-wsf-2.0-mrd-v1.0.pdf**

Contents

People Service 6
1 Principal Referencing 6
1.1 Introduction 6
1.2 Requirements 7
1.3 Use Cases 8
1.3.1 Principal Invites a Friend 8
1.3.1.1 Main Description 8
1.3.1.2 Targeted Scenarios 8
1.3.1.3 Business Justification 8
1.3.1.4 Dependencies with Other Use Cases 8
1.3.1.5 Details 8
1.3.2 Invited Principal Responds to Invitation 9
1.3.2.1 Main Description 9
1.3.2.2 Targeted Scenarios 9
1.3.2.3 Business Justification 9
1.3.2.4 Dependencies with Other Use Cases 9
1.3.2.5 Details 9
1.3.3 Invited Principal Accesses Resource 10
1.3.3.1 Main Description 10
1.3.3.2 Targeted Scenarios 10
1.3.3.3 Business Justification 10
1.3.3.4 Dependencies with Other Use Cases 10
1.3.3.5 Details 10
1.3.4 Principal Manages List of Friends 10
1.3.4.1 Main Description 10
1.3.4.2 Targeted Scenarios 11
1.3.4.3 Business Justification 11
1.3.4.4 Details 11
2 Groups and Roles 12
2.1 Introduction 12
2.1.1 Business Needs 12
2.1.1.1 Group Membership-Based Access Control 12
2.1.1.2 Role-Based Access Control 12
2.1.1.3 Group as a Family of Principals 12
2.1.1.4 Operations on Principals in a Group 12
2.1.2 Definitions 13
2.2 Requirements 14
2.3 Use Cases 15
2.3.1 Principal Is Authorized for a Service at SP Based on a Membership Status Maintained at another SP 15

2.3.1.1 Main Description 15
2.3.1.2 Targeted Scenarios 15
2.3.1.3 Business Justification 15
2.3.1.4 Dependencies with Other Use Cases 15
2.3.1.5 Details 15
2.3.2 Principal Requests Actions on Members in a Group 17
2.3.2.1 Main Description 17
2.3.2.2 Targeted Scenarios 17
2.3.2.3 Business Justification 17
2.3.2.4 Dependencies with Other Use Cases 17
2.3.2.5 Details 18

Subscription and Notification 19
3 Subscription and Notification 19
3.1 Introduction 19
3.1.1 Overview and Problem Statement 19
3.1.2 Requirements 19
3.1.3 Sample Use Cases 21
3.1.3.1 Personal Profile Data Subscription (Relatively Static Data) 21
3.1.3.2 Location Data Subscription (Specifying Quality of Service) 21
3.1.3.3 Periodic notification 21
4 New Overall Glossary Terms 22
4.1 Friend 22
4.2 Invitation 22
4.3 Group Manager 22

People Service

People Service is a combination of the marketing requirements documents for Principal Referencing and Groups and Roles.

1 Principal Referencing

1.1 Introduction

Principal Referencing enables a Principal to directly reference another Principal. Liberty has defined strong mechanisms for protecting a user's privacy that include the use of pseudonyms when two parties interact regarding a Principal such that the user's actual identifier at either party is not known to the other party, just the pseudonym is known. This works because our model is based upon a federation event where the user was authenticated to both parties at the same time and then the parties chose the pseudonym to use for the Principal.

This model works well when a Principal is doing things on his own behalf. However it does not work well when a Principal is trying to do something about or with a second Principal (e.g., I want to give my wife access to my calendar so she can add social events that she has scheduled). The problem is that I don't have a pseudonym for my wife because she hasn't federated with my calendar service and therefore a pseudonym hasn't been created. While I may have a public identity for her (e.g., her email address), there is no current mechanism in the protocols for my calendar to validate that a requestor has that public identity, so there is no way for federation to take place and therefore no way for my calendar to get a pseudonym.

Principals should be able to reference other Principals within an IdP or across multiple IdPs without breaking the privacy protection of any of the involved Principals' pseudonyms.

1.2 Requirements

Req#	UC #	Requirements
1	1.3.1	Means by which a Principal, when visiting an SP, can view the list of his "friends" maintained at his IdP.
2	1.3.1	Means by which a Principal, when visiting an SP, can specify that a Principal (or multiple Principals) should be allowed to access some resource maintained at that SP without requiring that the invited Principal establish an account at the SP.
3	1.3.1	Means by which a Principal can be notified that he is authorized to access a resource owned by another Principal.
4	1.3.2	Means by which a Principal can respond to an invitation to access some resource and give appropriate consent.
5	1.3.3	Means by which a web service consumer (WSC) can request a SIS resource belonging to one Principal on behalf of another.
6	1.3.3	Means by which a WSC, for a particular Principal, can determine the location of the SIS resources of those Principals who have authorized that Principal to access those resources.
7	1.3.1	Means by which a WSC can discover the network location of a given Principal's list of friends.
8	1.3.4	Means by which a Principal, when visiting a WSC, can manage his list of friends stored elsewhere, e.g., add new friends, delete friends.

1.3 Use Cases

1.3.1 Principal Invites a Friend

1.3.1.1 Main Description

A Principal invites a friend to access some resource.

1.3.1.2 Targeted Scenarios

B2C, B2B, B2E

1.3.1.3 Business Justification

Many online interactions involve one Principal accessing a resource "owned" by another. The accessing Principal must be alerted to the possibility of this access through an invitation.

1.3.1.4 Dependencies with Other Use Cases

Liberty ID-FF Federation and SSO

1.3.1.5 Details

Title/ID	Principal invites a Friend
Pre-Conditions	- Principal_1 has federated accounts at SP1 & IdP1. - Principal_1 has resource at SP1. - Principal_1 has been authenticated by IdP1.
Constituents	Principal_1, Principal_2, SP1, IdP1
Use Case	1. Principal_1 requests that some resource held at SP1 be shared. 2. Principal_1 shown list of available friends from which a selection can be made. 3. Principal_1 specifies that Principal_2 from the list (known by some label supplied by Principal_1) be allowed to access resource held at SP1. Principal_1 specifies any constraints that are to be placed on this access. 4. Appropriate invitations(s) are created and delivered to Principal_2 by Principal_1.
Post Conditions	Principal_2 receives the invitation.
Alternate Courses of Action	- Principal_2 may not be on the list of available friends. Principal_1's request that the friends be allowed to access the resource would ensure that Principal_2 be added to the list for potential future invitations. - The invitation may be delivered to Principal_2 by some provider on behalf of Principal_1 rather than directly by Principal_1. - Whether the resource is browser-based or WSF-accessed.

1.3.2 Invited Principal Responds to Invitation

1.3.2.1 Main Description

An invited Principal presents the invitation he received from the inviting Principal in order to access the relevant resource.

1.3.2.2 Targeted Scenarios

B2C, B2B, B2E

1.3.2.3 Business Justification

The Principal for which authorization to the resource is to be granted must be actively involved in the process in order to ensure that he is informed of the nature of the invitation and potential implications. The invitation mechanism ensures that this consent can be given as well as providing the necessary mechanism by which the invited Principal can specify his IdP.

1.3.2.4 Dependencies with Other Use Cases

Liberty ID-FF Federation and SSO

Principal Referencing use case 3.1 - Principal Invites a Friend

1.3.2.5 Details

Title/ID	Invited Principal Responds to Invitation
Pre-Conditions	- Principal_2 has account at IdP2. - Principal_2 has received invitation to access some resource owned by Principal_1 and maintained at SP1. - IdP1 able to determine that Principal_2 has account at IdP2. - Trust can be established between IdP2 and SP1 and/or IdP1.
Constituents	Principal_2, IdP1, SP1, IdP2
Use Case	1. Invitation carries sufficient information to allow Principal_2 to determine whether or not he wishes to proceed. 2. Principal_2 presents invitation(s) to SP1. 3. SP1 provides any additional information not within invitation. 4. Principal_2 consents to "making this happen." 5. Principal_2 authenticates at IdP2 and consents to "making this happen." 6. SP1 assigns permissions so that Principal_2 can access resource when SSO'ing from IdP2.
Post Conditions	Principal_2 attempts to access Principal_1’s resource.
Alternate Courses of Action	- Principal_2 may have previously been invited to access some other resource of Principal_1’s maintained at SP1. - Principal_2 may have previously scoped their consent for accessing resources of Principal_1 such that he needn’t be prompted for additional consent at IdP2. - Resource may be WSF-accessed.

1.3.3 Invited Principal Accesses Resource

1.3.3.1 Main Description

An invited Principal accesses the resource of Principal_1 to which he has previously been invited.

1.3.3.2 Targeted Scenarios

B2C, B2B, B2E

1.3.3.3 Business Justification

"Access" to the resource can mean any of read, write, update, etc. Access can mean through a browser-interface or through a WSF interface.

1.3.3.4 Dependencies with Other Use Cases

Principal Referencing use case 3.1 - Principal Invites a Friend

Principal Referencing use case 3.2 - Invited Principal Responds to Invitation

1.3.3.5 Details

Title/ID	Invited Principal Accesses Resource
Pre-Conditions	- Principal_2 has account at IdP2. - Principal_2 has received invitation to access some resource owned by Principal_1 and maintained at SP1. - Principal_2 has responded to invitation and consented to "making this happen."
Constituents	Principal_2, SP1, IdP2
Use Case	1. Principal_2 attempts to access resource. 2. Principal_2 redirected to IdP2 for authentication. 3. Principal_2 redirected to SP1 and is able to access resource with appropriate permissions.
Post Conditions	N.A.
Alternate Courses of Action	- Principal_2 authenticates at IdP2 before being linked to SP1 resource. - Resource may be WSF-accessed. If action is instigated by invited Principal, he may need to specify which of his friends (that would have previously invited him to see a particular type of resource) resources he wishes to access. For instance, if Bob and Tony have both allowed Mary to see their contact books, if and when Mary tells a WSC to access the contact books of her friends, that WSC will need to ask her "which friend, Bob or Tony?"

1.3.4 Principal Manages List of Friends

1.3.4.1 Main Description

A Principal is able to manage (add/delete, etc.) his list of friends independent of a specific resource to which he may be invited.

1.3.4.2 Targeted Scenarios

B2C, B2B, B2E

1.3.4.3 Business Justification

A Principal may wish to *bulk load* or manage a list of friends in advance of actually inviting them to access some resource/participate in some transaction. Additionally, the ability to remove a friend from the list will be relevant to reflect changing social relationships.

By maintaining this list, the Principal's IdP provides a single management point for the data, removing from individual SPs this burden and simplifying its control for the Principal.

1.3.4.4 Details

Title/ID	Principal Manages List of Friends
Pre-Conditions	1. Principal has an account with an IdP.
Constituents	Principal_1, IdP1, Principal_2
Use Case	1. Principal_1 authenticates to IdP1. 2. Principal_1 asks to manage "Friends." 3. IdP1 displays list of friends, each entry a label previously supplied by Principal_1. 4. Principal_1 edits list. 5. Invitation sent to any new entries added to the list.
Post Conditions	
Alternate Courses of Action	

2 Groups and Roles

2.1 Introduction

Traditionally, groups and roles are an integral part of organizing activities by more than one person. In enterprises, most tasks are conducted by groups of people whose sizes range from small project teams to the entire company. Group members play different roles to organize the tasks. For example, only the Director of the Sales Department can approve the department budget plan. The "Sales Department" is a group. The "Director" is a role in the Sales Department. Groups and roles are also useful in consumer scenarios. For example, a "family" group and "guardian" role are useful in defining the privacy policy for family members.

Another usage of Groups would be to account for the way Telcos and ISPs often identify a "family" of Principals via their connection's network or IP address as this information is usually enough to grant access to pay services such as placing a phone call (e.g., the family account is billed). In this situation, the IdP has no idea as to who the actual person accessing the service really is.

2.1.1 Business Needs

We will discuss four essential business needs for groups and roles in identity management and services:

2.1.1.1 Group Membership-Based Access Control

Principals and SPs are allowed to access services and resources based on whether they are members of specific groups. Because John is a family member, he is allowed to access the attributes of all family members.

2.1.1.2 Role-Based Access Control

Principals and SPs are allowed to access services and resources based on roles to which they are assigned. Because John is a Director of the Sales Department, he can access the salary information of the department staff.

2.1.1.3 Group as a Family of Principals

Groups can act as a user of ISPs and telephone services in which network lines (i.e., telephone numbers) or nodes (i.e., IP addresses) are mainly used for identities. For example, if you subscribe to an ADSL service, all of your family members can use the services.

2.1.1.4 Operations on Principals in a Group

In certain business scenarios, it is important to identify multi-valued attributes as lists/groups and perform certain actions on them. For example, a user may want to send emails to an e-mail distribution list owned by other users. Another example would be to find an available time slot in the calendars of all members of a user's buddy list.

Please note that we do not intend to describe detailed requirements for specific access control mechanisms per se. Rather we will discuss requirements for frameworks that enable the implementation of such mechanisms.

Standardizing specifications for groups and roles ensures interoperability between applications and services for user groups such as collaboration tools. Once Liberty-compliant user groups and roles have been defined, they can be used with any tools that support the Liberty specifications, facilitating the seamless integration of the tools.

2.1.2 Definitions

A Group is an identity that consists of zero or more Principals. Groups, as well as their members, should be handled under the same Liberty framework in a systematic manner. For example, a group should be able to be authenticated and access services in a similar manner in which individual Principals are supported. Just like a molecule that consists of atoms, a group exists and behaves on its own, but can be decomposed into smaller units.

Groups also have attributes, such as names, references to Group Managers, time of creation and last update, and brief description of the groups. Group Managers have rights to access and modify the membership and role assignment status of each member in their Groups by default. Group Managers could be Principals, SP/APs, or IdPs. In Liberty, a group is composed by listing its members, for example, John, Paul, George, and Ringo.

A "role" is an attribute of an identity that defines responsibilities which are associated with access rights to services and resources. Optionally, roles can be "scoped" to make them valid only within corresponding groups. For example, in the case of John, the Director of the Sales Department of X Corporation, his role is legitimate only within this specific scope—he is not the Director of Research Laboratories nor the Director of Sales Department of Y Corporation. Roles can be assigned to groups as well as individual Principals.

The main difference between groups and roles is the notion of "encapsulation." A group represents more than zero identities and can be handled as an identity. In contrast, a role is just an attribute and therefore can not represent identities nor can be handled as an identity.

2.2 Requirements

Req#	UC #	Requirements
1	Generic	Nested structure for a group: a group can be a member of another group.
2	Generic	A Principal can be a member of more than one group.
3	2.3.1	Means by which a Principal can be authorized for a service at SP based on a membership status maintained by a third party (i.e., IdP or another SP).
4	2.3.2	Means by which a Principal can at once request of SP the same action on all members of a particular group defined by a third party (i.e., IdP or another SP).
5	2.3.2	Means by which SP can make the delegated access to attributes of members of a specific group defined by a third party (i.e., IdP or another SP).
6	2.3.2	Means by which a Principal can choose one or more (target) groups with human-readable names and specify chosen groups to SP. A human-readable name should be one of the attributes of a group identity.
7	2.3.2	Means by which SP can retrieve attributes of a specified group defined by third party (i.e., IdP or another SP).
8	Generic	Groups can be created, deleted, etc.
9	Generic	A group's membership can be modified, e.g., members can be added and removed.
10	Generic	A group's membership can be queried and tested.

2.3 Use Cases

2.3.1 Principal Is Authorized for a Service at SP Based on a Membership Status Maintained at another SP

2.3.1.1 Main Description

This use-case allows a Principal to be authorized for a service at an SP based on a membership status in a particular group that is maintained at an IdP or another SP.

In this case, the SP has to check with the IdP or another SP to determine whether a Principal is a member of a particular group and consequently decide whether to provide services to the Principal or not. Optionally, Principals can specify the groups in which they act as members.

A possible service use case is that a music content provider SP offers free download service to the gold members of the IdP (or another SP).

2.3.1.2 Targeted Scenarios

B2B, B2E, B2C

2.3.1.3 Business Justification

This use case facilitates joint promotions between SPs, which generate more traffic for the providers. For example, the Star Alliance™ partner airlines share "gold member" user status and provide those frequent flier users with the same level of privileges, resulting in greater customer loyalty to a specific airline as well as to the Star Alliance.

2.3.1.4 Dependencies with Other Use Cases

(In general, the Groups and Roles MRD is closely related to the Principal Referencing MRD.)

2.3.1.5 Details

Title/ID	Principal Is Authorized for a Service at SP Based on a Membership Status Maintained at Another SP
Pre-Conditions	- Principal_1 wants to use SP1. - SP1 wants to permit the use of its service only if Principal_1 is a member of Group1. - SP1 and IdP1 are in the same authentication domain. - SP1 is authenticated and authorized for the membership inquiry about Group1. - Principal_1 has an account at IdP1. - Group1 is a group at IdP1 and includes Principal_1.
Constituents	Principal_1, SP1, IdP1
Use Case	5. Principal_1 issues a request for using a service at SP1 (not specifying in which group she acts as a member). 6. SP1 issues a request for asserting whether Principal_1 is a member of Group1 at IdP1 or not. 7. SP1 receives a response that Principal_1 is a member of

	Group1. 8. Principal_1 is allowed to use SP1's service.
Post Conditions	
Alternate Courses of Action	- Principal_1 would be asked if he would agree to disclose his membership status. - Principal_1 would be notified that SP1 has obtained his membership status.

2.3.2 Principal Requests Actions on Members in a Group

2.3.2.1 Main Description

SP makes a delegated access to attributes of members in a particular group defined in the IdP or another SP and performs some operations/actions with them.

2.3.2.2 Targeted Scenarios

B2B, B2E, B2C

2.3.2.3 Business Justification

In certain business scenarios, it is important to identify multi-valued attributes as lists/groups and perform certain actions on them. For example, a user may want to send emails to an e-mail distribution list owned by other users. Another example would be to find a free time slot on the calendars of all members of a user's buddy list.

2.3.2.4 Dependencies with Other Use Cases

(In general, the Groups and Roles MRD is closely related to the Principal Referencing MRD.)

2.3.2.5 Details

Title/ID	Operations/Actions on Principals in a Group
Pre-Conditions	- Principal_1, Principal_2, Principal_3, and Principal 4 have an account at IdP. - Principal_1 has an account at SP1, which is federated with the account at IdP. - Each of Principal_2, Principal_3, and Principal_4 has an account at SP2, each of which is federated with that account at IdP. - Principal_2 has a group (perhaps a buddy list) at SP2. Principal 2 is the Group Manager while Principal_3 and Principal_4 are the group members. - Principal_2 has granted access rights to the group attributes at SP2 to Principal_1. - Each member of the group (i.e., Principal_3 and Principal_4) has given appropriate access rights of her attributes at APs to Principal_1.
Constituents	Principal_1, Principal_2, Principal_3, Principal_4, SP1, SP2, APs, IdP
Use Case	7. Principal_1 signs on at the IdP. 8. Principal_1 navigates to SP1. 9. Principal_1 instructs SP1 to resolve group membership for Principal_2's group (perhaps members of the buddy list) or to perform some other action on the group membership (perhaps send email to the members of the buddy list). 10. SP1 finds SP2 that holds a group of which Principal_2 is the owner. 11. SP1 requests from SP2 a member list for Principal_2's group. 12. SP2 sends the member list of specified group. 13. SP1 resolves and finds each member's APs. 14. SP request attributes from each member's APs. 15. For each attribute values from APs, SP1 either presents it back to Principal_1 or performs the requested operation on the values (perhaps send emails to the members in the buddy list like Principal_3 and Principal_4.).
Post Conditions	
Alternate Courses of Action	- Principal_1 would be asked by SP1 to which group Principal_1 wants to request actions.

Subscription and Notification

Subscription and Notification is solely a function of the marketing requirements document for Subscription and Notification.

3 Subscription and Notification

3.1 Introduction

3.1.1 Overview and Problem Statement

Currently, via Liberty ID-WSF DST[1], a web service consumer (WSC) application may request attribute data from a web service provider (WSP) via a query mechanism. However, after such a request has been made and satisfied, the data held at the WSP may change. The WSC would not be aware of such changes and may thus be in possession of "dated" data.

Liberty should standardize a protocol by which a WSC may subscribe to notifications indicating that changes have occurred to data held at a WSP. Notifications may also be sent based on other criteria which may be specified by the subscriber such as a particular time interval or set of intervals. Liberty should also standardize the means by which a WSP may notify a WSC of data in which the WSC is interested.

3.1.2 Requirements

Req#	UC #	Requirements	Included in
1	All	Provide a means by which a Liberty WSC can subscribe to data regarding some resource at a WSP.	Subs[2]
2	All	Provide a means by which a Liberty WSP can notify WSCs who are subscribed to receive change notifications, subject to the corresponding privacy policies that apply to such resource.	Subs
3	3.1.3.1, 3.1.3.2	Provide a means by which a WSC can query subscriptions linked to some resource.	Subs
4	All	Provide a method by which a WSC can cancel her subscription for notifications.	DST and Subs
5	All	Provide a method by which a WSP may inform a WSC that it is cancelling a subscription.	DST and Subs
6	All	Provide a method by which a WSC can update a subscription.	DST and Subs
7	3.1.3.1,	Allow subscriptions to be sent in bulk (I can subscribe to	Subs

[1] Liberty ID-WSF Data Services Template
[2] Liberty ID-WSF Subscriptions and Notifications

	3.1.3.2	changes made to the address and name data in the same request).	
8	All	Allow the subscription to be modified by quality-of-service considerations (e.g., only send me a notification every 5 minutes, even if the data changes every second).	Subs
9	3.1.3.1, 3.1.3.2	Allow notifications to be sent in bulk (e.g., if I am subscribed to receive change notifications on address and name data, and both of these items have changed, send me a single notification with two sub-elements describing the changes).	Subs
10	All	Allow the WSP to notify that the specific set of data have changed, without including the specific data in the notification.	Subs via XPath
11	All	Allow the WSP to indicate a specific (possibly partial) data set be returned as specific data in the notification.	Subs
12	All	Provide a means by which a Liberty WSC can specify the end point that should be receiving the notifications (if different from the WSC's application endpoint).	Subs
13	All	Allow a requester to specify the resource to which the subscription request applies.	Subs
14	3.1.3.1, 3.1.3.2	Allow a requester to make "generic" subscription queries, without indicating a specific resource to which the subscription request applies.	Service Defined in Subs
15	3.1.3.1, 3.1.3.2	Allow the requester to register an expiration date/time for a subscription.	Subs
16	3.1.3.1, 3.1.3.2	Allow the requester to register a start date/time for a subscription.	Subs
17	3.1.3.1, 3.1.3.2	Allow the WSP to override a requested expiration date/time, and communicate the expiration date to the requester.	Subs
18	All	Provide the exchange protocol used with a suitable method to support large batches of changes (i.e., volume data).	Subs

3.1.3 Sample Use Cases

3.1.3.1 Personal Profile Data Subscription (Relatively Static Data)

Blodwyn subscribes to a well-known women's magazine which is delivered to her on a monthly basis by Delivery.com. Delivery.com is dependent on knowing Blodwyn's correct mailing address, but Blodwyn's address is stored securely in her privacy-protected profile service at BPK.com, a large ISP with whom Delivery.com has a trusted business relationship. Blodwyn has authorized BPK.com to share her address data with Delivery.com. Delivery.com has acquired Blodwyn's address and has subscribed to receive updates regarding her address.

However, Blodwyn is sick of South Wales, where she currently lives, and has decided to move to Canvey Island. She updates her profile data at BPK.com. Since Delivery.com has subscribed to receive notifications about Blodwyn's changes of address, BPK.com releases her new address data to Delivery.com.

Blodwyn opens the door to her new house to discover the latest copy of her magazine lying conveniently on the doormat.

3.1.3.2 Location Data Subscription (Specifying Quality of Service)

John is a coffee addict. He also maintains a secure, privacy-protected, geo-location service with Mobile.com. John is such a coffee addict that he subscribes to Mobicaff, a service that sends him a text message whenever he is within 2 km of a Mobicaff café. Mobicaff, however, only has cafes in Rome, Madrid, London, and Dulles, VA. Their service is not very interested when John isn't quite near one of those places because John only really wants to know that a café is quite close to him. They are also not very interested in knowing exactly where John is at every second and John is constantly moving, so his location data is changing rapidly.

Mobicaff has requested that Mobile.com notify Mobicaff of John’s location, but only when John’s location is within the bounds of one of Mobicaff’s cafes.

3.1.3.3 Periodic notification

Send notifications every 5 minutes, regardless of whether the subscribed data has changed.

4 New Overall Glossary Terms

4.1 Friend

A Principal invited by another Principal to access some resource. The first Principal is a friend of the second. The list of friends for a Principal are those that have been, or are likely to be, invited to access some resource belonging to the Principal.

4.2 Invitation

A message sent to one Principal from another informing the recipient that they have been authorized to access some resource associated with the inviting Principal.

4.3 Group Manager

An owner Principal of a group.