Global Permissions Management Requirements

Candidate Version 1.0 – 31 Mar 2009

Open Mobile Alliance

OMA-RD-GPM-V1_0-20090331-C

Contents

Figures

Tables

1. Scope (Informative)

This document provides use cases and requirements for a Global Permissions Management (GPM) enabler that allows principals to manage the permission rules that determine if, when, how and to what extent information about end-users of OMA enabled services (i.e. Permissions Target) is released to Target Attribute Requesters and –Consumers, e.g. applications, enablers or other end-users. GPM would protect information about end-users being requested by other resources as well.

OMA service enablers that enable presence and location services already have specific requirements on how principal related information is released. GPM provides generic permissions checking and permissions management, which can be used by other resources (e.g. OMA service enablers). Therefore, the requirements contained in this document are limited to those generic aspects, e.g. defining the types of permissions, the storage, management, provisioning and re-use of such permissions and of introducing the notion of notifying a Permissions Target of any changes to permissions and of getting users consent to those changes.

The scope of this RD does not include requirements for authorization to access services or service enablers. GPM specifically excludes authorization of an entity accessing another entity.

The scope of this RD is focused on determining whether a user attribute can be accessed for a particular usage, as well as the management of permissions rules and other specific functions including interaction with the user.

Note that this does not prevent the GPM enabler from making use of other generic functions or enablers when its architecture is described or when it is implemented, if they satisfy the GPM requirements. Neither does it prevent other enablers from using the GPM enabler whenever needed to perform the specific functions that the latter will provide.

2. References

2.1 Normative References

[CHARG] "Charging Requirements", OMA-RD-Charging-V1_0
Open Mobile Alliance™, http://www.openmobilealliance.org

[Privacy] "Privacy for Mobile Services Requirements", OMA-RD-Privacy-V1_0
Open Mobile Alliance™, http://www.openmobilealliance.org

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

2.2 Informative References

[DICT] "Dictionary for OMA Specifications", OMA-ORG-Dictionary-V2_2
Open Mobile Alliance™, http://www.openmobilealliance.org

[GEOPRIV] "Common Policy: An XML Document Format for Expressing Privacy Preferences"
http://www.ietf.org/internet-drafts/draft-ietf-geopriv-common-policy-10.txt

[MLS] "Mobile Location Service Requirements", OMA-RD-MLS-V1_0.
Open Mobile Alliance™, http://www.openmobilealliance.org

[OSE] "The OMA Service Environment", OMA-Service-Environment-V1_0
Open Mobile Alliance™, http://www.openmobilealliance.org

[QoE] "Report on Application Performance", OMA-RPT-ApplicationPerformance-V1_0.
Open Mobile Alliance™, http://www.openmobilealliance.org

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

[XDM2RD] OMA XML Document Management Requirements, OMA-RD-XDM-V2_0.
Open Mobile Alliance™, 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 [RFC2119].

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

3.2 Definitions

Ask Request	An enquiry from GPM to the Ask Target for his/her consent for the release of a target attribute.
Ask Target	Any principal (e.g. Permissions Target or Permissions Manager) who receives an Ask Request.
Delegate	To designate specified tasks or management functions by an authorised principal to another principal.
GPM Administrator	An authorised principal that administers the role(s) and GPM management rights of the Permissions Manager(s), e.g. assigning Permissions Targets to Permissions Managers.
GPM Context	Static or dynamic information pertaining to a principal (i.e. a Target Attribute Requester, Target Attribute Consumer or Permissions Target).
GPM Management Right	Entitlement or privileges given to a principal with respect to which Permissions Management functions he/she can perform
GPM Target Request	An enquiry from a Target Attribute Requester with respect to being granted access to target attribute(s). E.g. a service invocation that includes target attributes as service parameters.
GPM Target Response	An expression of the results of a GPM target request
GPM Validity Period	A time period starting when an ask request is sent by the GPM and during which the GPM waits for an answer from the Ask Target
Permission Checking Request	An enquiry from a principal, (e.g. service enabler) to the GPM enabler for permission to grant access to target attributes.
Permissions Checking Response	Message returned in response to the Permissions Checking Request and including the expression of the results of the Permissions Checking
Permissions Manager	An authorised principal, (typically human) that manages (e.g., creates/retrieves/modifies/deletes/sets priority of/delegates GPM management rights with respect to) permissions rules associated with the permission target's attributes. (This actor can be the Permissions Target, an authorised delegate or the GPM Administrator).
Permissions Manager’s Delegate	A principal (typically a human) who has been authorised by a Permissions Manager to perform one or more specific permissions management functions (as defined by section 6.1.2) on his/her behalf.
Permissions Rule	A combination of a condition and a returned decision if the condition is true. The condition is expressed in terms of target attributes and other information (e.g. requester identity, intended usage) and the decision indicates what action the requester should take. E.g. if requestor = “is in my domain” and “target attribute” = “my location” then grant.
Permissions Rules Priority	Information that could be used by the enabler implementation to determine the order of evaluation of permissions rules
Permissions Target	Any principal (or group of principals) whose target attributes are subject to permission rules
Permissions Target Notification	An announcement to the Permissions Target that a GPM target request has been received.
Principal	See [DICT]
Pseudonym	An arbitrary name chosen by any Principal to protect their anonymity within the context of GPM.
Target Attributes	Information pertaining to Permissions Target(s) for which access to is governed by permissions rules. Target attributes can be either static, i.e. that changes relatively infrequently such as information in an

	address book, or dynamic, i.e. that could change more frequently such as user presence or geographical location.
Target Attribute Consumer	A principal (or group of principals) consuming/making use of a target attribute (e.g. for a map showing the location of the Permissions Target). This role will typically be played by an end-user or an application.
Target Attribute Requester	Any principal that originates a GPM Target Request.

3.3 Abbreviations

GPM	Global Permissions Management
IM	Instant Messaging
IMSI	International Mobile Subscriber Identity
IT	Information Technology
LOC	Location Services Enabler
MDN	Mobile Directory Number
MIN	Mobil Identification Number
MLS	Mobile Location Service
MMS	Multimedia Messaging Service
MSISDN	Mobile Station International ISDN Number
OMA	Open Mobile Alliance
OSE	OMA Service Environment
PC	Personal Computer
PCE	Privacy Checking Entity
PCP	Privacy Checking Protocol
PDA	Personal Digital Assistant
PEEM	Policy Evaluation, Enforcement and Management
POC	Push to talk Over Cellular
QoE	Quality of Experience
RD	Requirement Document
SMS	Short Message Service
SUPL	Secure User Plane Location

4. Introduction (Informative)

Mobile service providers will continue to seek new and flexible ways to offer customised services to its subscribers. This may typically involve for example combining the resources of its existing enablers, or it could involve partnering with third-party application providers such as those who may traditionally provide services from different trust domains (e.g. the Internet). So, as services become richer and more diverse, subscribers will make increasing amounts of user-related data available to those services and, have increasingly intricate permissions concerning when and how the data can be used.

In the current service environment framework, user permissions are potentially distributed across multiple sources to address the service-specific solutions required by each enabler. For example, in the case of location services, user permissions typically involve dynamic data about an end-user, i.e. location information that is to be shared only under certain conditions and how specific actions are to be executed in doing so, e.g. of being notified of a positioning request. Functionality to perform location privacy checking is being specified in [MLS]. [MLS] contains an optional privacy checking protocol (PCP) defined over an interface between the location server and a separate privacy checking entity. However mechanisms to allow the end-user to manage the permissions rules governing the release of his/her own location are not clearly specified nor mandated by [MLS].

User presence and availability are other examples of dynamic data. A user's presence may vary according to device status, a users mood or the time of day etc. As in the case of location services, a user may want to set permissions to grant or deny access and to filter information related to it (e.g., show my availability to my boss only on company-supplied devices, show presence to family on all devices).

Common tools to allow principals to manage how they prefer services to be used are clearly more desirable in a richer and more privacy-conscious service environment. However, existing approaches for supporting informational privacy are considered to neither adequately address the requirements of the mobile value chain nor flexibly adapt to the variety of services offered within converged communications networks that cross trust domains or to the types of *context-aware* services envisaged by service providers.

Therefore Global Permissions Management, (GPM) aims to specify an enabler that is capable of generically managing permissions rules across OMA service enablers providing end-users with a global view of their permissions, (hence "Global" Permissions Management). These permissions rules are those that determine if, when, how and to what extent information about permissions target can be released. The underlying market requirements of GPM include:

(i) The reduction in operational costs and complexity of administrating user permissions related to existing and future service enablers.

(ii) Giving end-users more control over managing (create/modify/delete etc) their own permissions rules that determine who may access information about them and under what conditions.

(iii) The flexibility to manage a variety of permissions related to all types of service segments using context aware rules (e.g. both static and dynamic data) and not restricted to informational privacy [Privacy].

The GPM RD specifically identifies use cases and requirements from end-user and service provider perspective that inter alia, illustrate how:

(i) Authorised principals express and manage their permissions rules through user-friendly provisioning tools (not to be specified), and manage related events such as being notified of changes to permissions rules, or when /if consent is required and by whom.

(ii) Permissions rules are evaluated to determine what data can be shared with whom and in what situations

Authorised principals can manage their permissions over time in a logically centralised manner, e.g. by adding new services and having these services re-use existing permission rules.

It should be noted that some of the requirements in this RD might show similarities to requirements that have been identified in RD's of some other enablers, e.g. [XDM2RD]. Some requirements overlap analysis during the GPM AD stage is suggested.

4.1 Actors in the context of GPM

The following diagram is only intended to give an overview of the actors and their potential relationships as defined in this RD and is *not* intended to pre-suppose any particular architecture or necessarily identify interfaces.

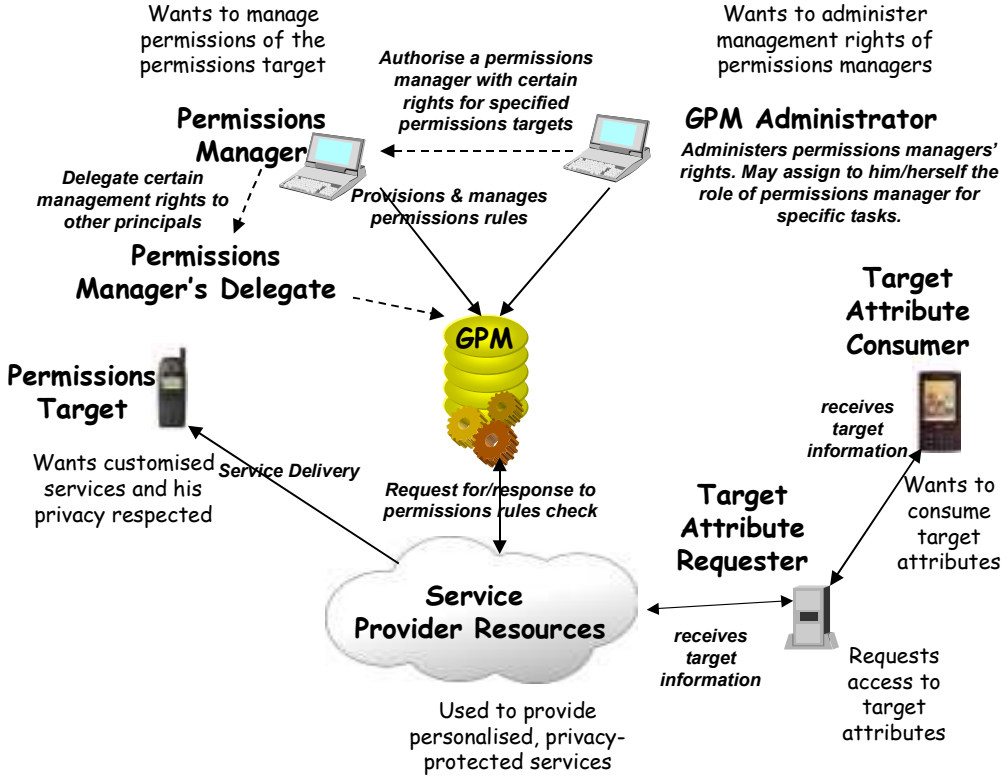

Figure 1: GPM Actors

The **Permissions Target** is the principal who is the subject of **permissions rules** that govern the way other principals access information about him and ultimately how his services are executed. The Permissions Target is usually a human end-user (or a group of human end-users) of services.

The **Permissions Manager** is an authorised principal who manages, (creates, modifies, deletes etc) **permissions rules**. In some cases, the Permissions Manager is the same principal as the Permissions Target, but in many cases the Permissions Manager will be an authorised principal acting on behalf of the Permissions Target such as the person who pays for the subscription or the **GPM Administrator**. GPM takes into account that permissions management operations will have to be performed at a generalised, high level and succinct manner in order to ensure human usability.

The **Permissions Manager's Delegate** is a principal authorised by a Permissions Manager to perform certain responsibilities on his/her behalf. Once such responsibilities have been delegated, the authorised permissions manager's delegate acts in fact in a similar manner to a permissions manager.

The **GPM Administrator** is responsible for determining who the authorised permissions managers are, what their GPM management rights are, and to which permissions targets those rights apply. The GPM Administrator is typically employed by an operator or service provider. It is thought that in some cases a relationship could exist between the GPM Administrator and the Permissions Manager, e.g. where both actors belong to the same enterprise and/or a principal shares both roles. In particular this is the case when it comes to a GPM management right such as determining final relative priority of

permissions rules, or establishing rules based on Service Provider requirements or regulatory constraints. For instance when multiple permissions managers have been assigned to a Permissions Target, then the GPM Administrator can assign priorities to permissions rules created by the permissions managers.

The **Target Attribute Consumer** is any principal that wishes to consume information (**target attributes**) about the Permissions Target either directly or through the invocation of a service. The **Target Attribute Requester** is the actor that requests access to the attributes of the Permissions Target (e.g. on behalf of the Target Attribute Consumer). The Target Attribute Requester may be an application residing in the service provider network of the Permissions Target, or it may be a third party application residing in an external network, or he may be another end-user of services. With GPM, Target Attribute Requesters can therefore discover over standardised interfaces, the extent to which information about Permissions Targets can be accessed or disclosed to them. In some cases a single actor may combine the Target Attribute Consumer role with the Target Attribute Requester role.

The **service provider** will want to use GPM to check permissions set for the Permissions Target before any data about him is disclosed to the Requester as part of its service delivery. Part of this process could involve checking if consent is required and by whom.

5. Use Cases (Informative)

5.1 Is my friend available service

5.1.1 Short Description

User A and User B both subscribed to the service called "Is my friend available?" The "Is my friend available?" service enables the user to know his friend's presence and availability status.

User B wants to know if User A is available through the "Is my friend available?" service. The "Is my friend available?" service sends a presence request to get User A's availability. The request is received by the presence server and processed. The presence information is provided to the service which then provides the information to user B.

5.1.2 Actors

- User A (Permissions Target)
- User B (user of the application service)
- Application Service
- Presence Server (Providing presence data)
- GPM (Global Permissions Management)

5.1.2.1 Actor Specific Issues

- Permissions Target

  The Permissions Target is associated with a set of rules regarding privacy.

- Application

  Application (i.e. Requester) asks for the Permissions Target's presence information.

- Presence Server (Providing presence data)

  Presence Server provides presence data.

- GPM (Global Permissions Management)

  GPM manages rules for targets.

5.1.2.2 Actor Specific Benefits

The Permissions Target's privacy rules must be checked before the presence information is retrieved (i.e. target attributes) and provided to the application. Also, in this use case, the presence information is provided to the application service which then provides it to the requesting end-user. Therefore, both the application and the requesting end-user will need the target's authorisation before retrieving his presence information.

5.1.3 Pre-conditions

An application asks the presence server for the availability of a Permissions Target.

5.1.4 Post-conditions

The Permissions Target's privacy is ensured.

5.1.5 Normal Flow

Flow A-The End User A (the Permissions Target) has set his rules to "GRANT" or "DENY".

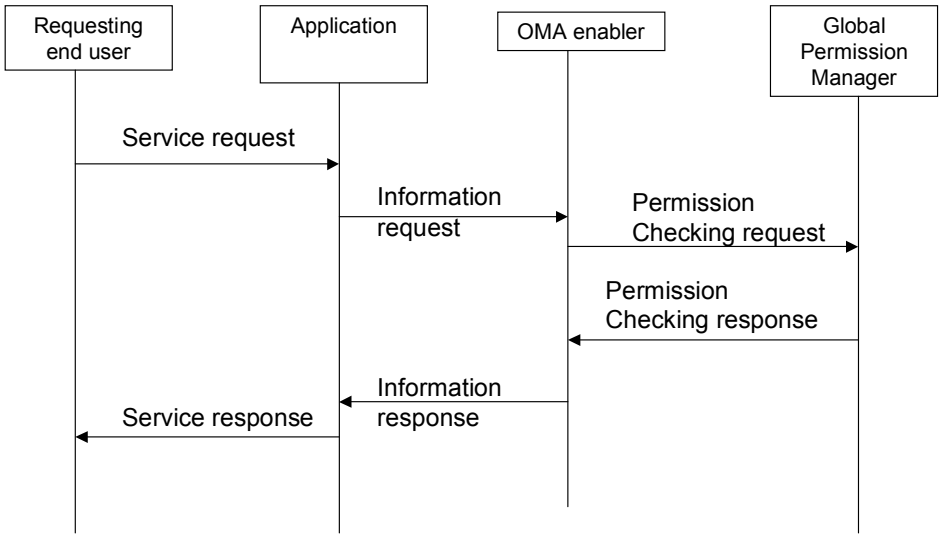

Figure 2: "Is My Friend Available" Normal Flow

1. The requesting end-user asks for his friend's availability
2. The application sends the presence request (i.e. a GPM target request) to the presence server
3. The presence server sends a presence privacy checking request (i.e. a permissions checking request) to the GPM.
4. The GPM checks the relevant permissions rule(s).
5. GPM sends a permissions checking response to the presence server.
6. The presence server sends a presence response (i.e. a GPM target response) to the application.
7. The application provides the information to the requesting end-user

5.1.6 Alternative Flows

Flow B:

Normal Flow. – But permissions checking request handles on 3 different presence (target) attributes X, Y, Z. Grant GRANT is given only for X, Y.

Flow C:

Normal Flow – GRANT given - With Notification to the user A. In this flow the user Permissions Target is notified that his presence information has been requested.

Flow D:

Normal Flow – Denied positioned - With Notification

In this alternative flow, the result of the permissions checking is that the Requester is denied the right to access the presence information of the permission target, after the check of the permissions rules by GPM. Also, the Permissions Target is notified of the request.

Flow E:

User A has provisioned his rules to "Ask", which means that the Permissions Target wants to be asked before his presence information is released – With Yes/No Answer

Flow F:

Alternative flow: User A has provisioned his rules to Ask – with or without answer. There is a Time Out Management that defines the time during which the user can answer and during which Requesters can be notified that GPM is waiting for the answer of user A.

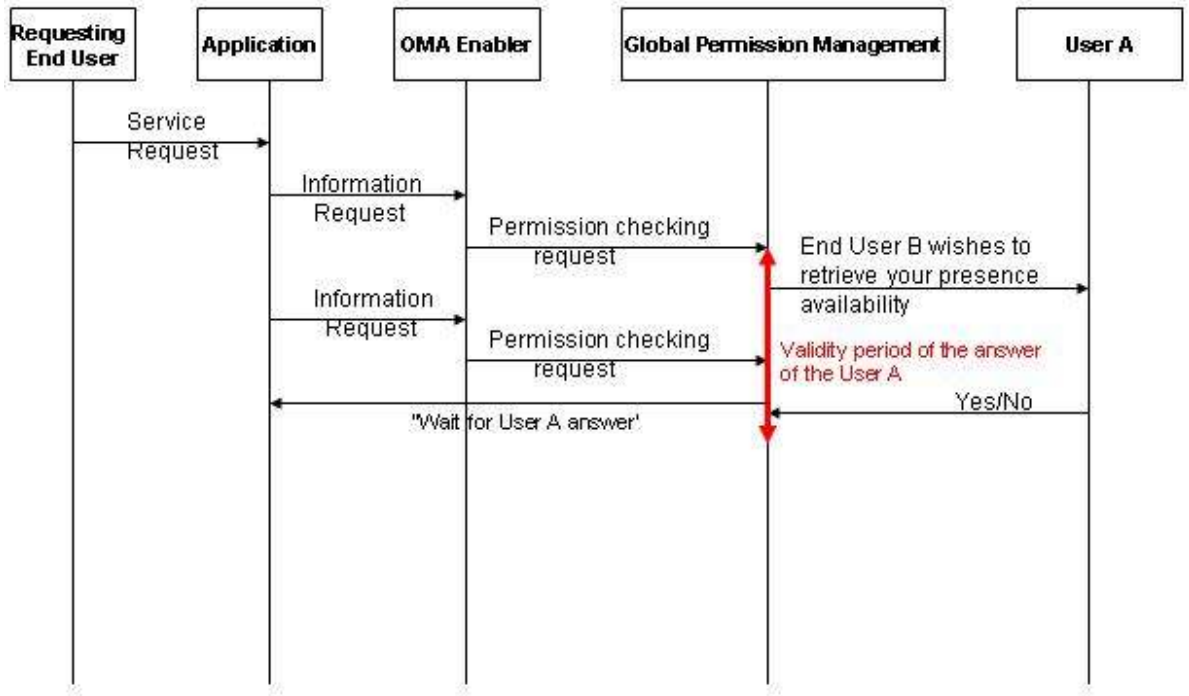

Figure 3: "Is My Friend Available" Alternative Flow F

If another Permissions checking Request arrives on GPM before GPM has received the User A answer and during the GPM validity period, the GPM answers back that it is still waiting for User A answer.

The GPM validity period is parameterised.

5.1.7 Operational and Quality of Experience Requirements

None.

5.2 Service Upgrade and Permissions Rules

5.2.1 Short Description

This use case illustrates potential requirements when end users add new services or upgrade existing ones and allow them to flexibly inherit or adapt their user permissions. The service enablers used in this example are IM and Presence.

This use case is based on some scenarios from the OMA privacy RD. [Privacy].

5.2.2 Actors

- End user of mobile services (Permissions Target)
- Service provider

5.2.2.1 Actor Specific Issues

- End User of a mobile enabled PDA
    - Wants to easily manage his contacts lists
    - Wants to make the most of his device
    - Wants to easily manage his permissions when upgrading an existing application
- Service provider
    - Wants to offer more feature rich upgrades to value added services but retain reliable and trusted mechanism for executing user permissions
    - Wants to obtain consent from user to any changes to user permissions rules

5.2.2.2 Actor Specific Benefits

- End User of a mobile enabled PDA
    - Can upgrade applications and allow them to inherit his existing user permissions rules
    - Can access and configure his user permissions via his mobile device or via a fixed device (e.g. PC)
- Service provider
    - Is seen as a trusted provider of services
    - Provides easy to use and flexible means to change user permissions rules

5.2.3 Pre-conditions

The PDA runs an older version of the IM application in which his contact list is arranged in a flat structure.

His original IM application allows the user to only set presence attributes on a per-contact basis.

The PDA user is authenticated before downloading and executing the IM application upgrade and before making any changes to any user permissions

5.2.4 Post-conditions

End-user David successfully upgrades his IM application and makes use of the more advanced features on his mobile device.

David is able to have his IM application interact with his presence services by setting presence attributes according to each contact profile, as well as being able to change the presence attributes of individual contacts in each profile.

5.2.5 Normal Flow

1. David discovers a new version of his IM chat application, which has new features available
2. After trying out an on-line demo, David decides to subscribe to the new version of this IM application and downloads the new client into his PDA.
3. The IM application set-up package informs David that the flat contact list structure from his existing client will be used unless he wants to make use of a new format for profiling his contact list
4. David uses his PDA for business purposes as well and would really like to arrange the presence attributes of his existing IM contact list according to business, family and social profiles. So, David decides to make use of the new structure for contact lists offered.
5. During the re-configuring of his contact list, David applies rules and preferences according to each of the new categories stored. He consents to any changes to existing settings pertaining to the use of his presence information.
6. The IM application set-up package executes David's requests and the IM application is ready to use.
7. Whilst using his IM application to chat with his work colleagues, David receives an ask request from another colleague not already included in his Business buddy list.
8. David accepts the ask request and his service provider authorises the colleague to access David's presence information according to the permissions rules and preferences he has configured.

5.2.6 Alternative Flow

1. In step 3, David decides not to halt the execution of his new IM client application to save time and preserves his existing flat contact list structure in his upgraded IM client
2. Later, David invokes an application via a secure connection from his PC to the IM service provider's web site and re-configures his contact list, his user permissions and preferences in his user profile. He consents to any changes to existing settings pertaining to the use of his presence information.

5.2.7 Operational and Quality of Experience Requirements

None.

5.3 Permissions Management Delegation

5.3.1 Short Description

Permissions rules related to corporate users are managed by an enterprise Permissions Manager. A Permissions Manager's Delegate can also manage permissions rules according to his assigned GPM management rights.

This use case also demonstrates important requirements related to user experience, e.g., being informed of changes to permissions rules etc.

This use case is based on some scenarios from the OMA Privacy RD [Privacy].

5.3.2 Actors

- Mobile service provider: acts as GPM Administrator
- Enterprise: a representative from the Enterprise IT department authorised by the GPM Administrator, acts as Permissions Manager
- Corporate Sales Team Leader using mobile device: acts as Permissions Manager's Delegate and Permissions Target

- Corporate Sales Team members using mobile devices: act as Permissions Manager's Delegates and Permissions Targets

5.3.2.1 Actor Specific Issues

- Mobile service provider
    - Wants to offer mobility related applications to enterprise customers and preserve user privacy.
    - Wants to allow some device characteristics to be considered as private information (i.e. GPM target attributes) because they could be considered as sensitive e.g. input/output modality may suggest a disability, visual impairment etc.
- Enterprise
    - Wants to provision services to its work force
    - Wants to respect regional and corporate policies with respect to the informational privacy of its work force
- Corporate Sales Team Leader using mobile device
    - Wants to keep his sales team productive
    - Wants to use his device as a work tool
    - Wants to be informed of any changes to his permissions rules
- Corporate Sales Team members using mobile devices
    - Want to use their devices as work tools

    Want to be informed of any changes to their permissions rules

5.3.2.2 Actor Specific Benefits

- Mobile service provider
    - Generates revenue from providing privacy aware services to its corporate clients
- Enterprise
    - Manages the related privacy of its employees
- Corporate Sales Team Leader using mobile device
    - Can manage his permissions rules when changing devices
    - Can manage the permissions rules of his sales team members
- Corporate Sales Team members using mobile devices
    - Maintain their permissions rules and protect their privacy

5.3.3 Pre-conditions

- The enterprise has a subscription with the mobile service provider.
- A representative from the enterprise's IT department manages the permissions rules for its corporate mobile users (Permissions Manager)

Applications (Target Attribute Requester) request target attributes of the Sales Team members, which may include capabilities of the devices they use.

- A designated end-user (Sales Team Leader) can act as a Permissions Manager's Delegate with the right to manage the permissions rules of individual members of his entire sales team.

5.3.4 Post-conditions

- Each individual device user (Permissions Target) can be informed of any changes made to their permissions rules

5.3.5 Normal Flow

1. The Permissions Manager (of the Enterprise IT department) manages permissions rules that protect the privacy of each individual sales team member (Permissions Target), e.g. identity of user, type of applications used, presence and availability information, number and type(s) of device(s) used, calendar information, geographic region they cover etc)
2. The device belonging to a junior team member fails . The Sales Team Leader lends her his own PDA that has a larger screen and better capabilities, and the sales team leader uses another PDA with the same capabilities.
3. The Sales Team Leader modifies the permissions rules related to the releasing of the new device's capability of the junior team member
4. Both the sales team member and team leader continue accessing their applications without further changes to privacy settings.
5. The Sales Team Leader recruits a new sales team member and he makes a request to the company's enterprise IT department to allow this new employee to use the same applications as the rest of the team.
6. The enterprise IT department processes the team leader's new service request and creates new permissions rules for the applications used by this new Sales Team member.
7. The new Sales Team member starts using applications now that his device has the appropriate information

5.3.6 Alternative Flows

- Alternative 1:

  1-6 as Normal Flow

  7. The new Sales Team member starts using the corporate presence application and in doing so sends presence requests to his Sales Team colleagues to get their communication status.

  8. The Sales Team members act as Permissions Manager's Delegates and are able to modify their related permissions rules. That is adding the new team member to their presence buddies list.

- Alternative 2:
  - The GPM Administrator informs each Permissions Manager about their individual corporate rights with regard to managing their permissions

- Alternative 3:
  - The junior team member is informed that his permissions rules related the capabilities of the device have been modified by the Sales Team Leader.

- Alternative 4:
  - The Sales Team Leader accidentally deletes some permissions rules. When saving the changes to his permissions rules, he is informed that he has no right to delete these permissions rules.

5.3.7 Operational and Quality of Experience Requirements

None

5.4 Setting Permissions Rules Using Context Information

5.4.1Short Description

This use case demonstrates how an end-user sets permissions rules using GPM context information that is used to determine if, when, how and to what extent requesters can access information about him.

William, a self-employed consultant is subscribed to a presence service which can provide his presence information to authorised watchers (including his customers) who might want to contact him at different times in the day using presence enabled applications.

William uses a self-provisioning interface to easily create permissions rules based on GPM context information, e.g. "relationship with target attribute consumer/requester" etc and other information such as the time of day and his work location, to make choices about how his presence may be viewed and by which applications

5.4.2 Actors

- William, a self-employed consultant – acts as both the *Permissions Target* and *Permissions Manager*
- Peter, a low priority customer – acts as a *Target Attribute Requester Consumer*
- Susan, a high priority customer - acts as a *Target Attribute Requester Consumer*
- Presence Server
- GPM Service Provider

5.4.2.1Actor Specific Issues

- William
    - Wants to set permissions rules that determine his presence with respect to selective watchers (Target Attribute Consumers) can reach him based on GPM context information such as customer priority, time of day, work situation etc.
    - Wants to easily change his permissions rules when the GPM context of callers change, e.g. the importance of certain customers
    - Wants to stay in touch with selective customers even if he deviates from his normal schedule
- William's Customers
    - Want to obtain William's presence information for communications purposes
- GPM Service provider
    - Wants to handle permissions checking requests from the presence server based on information received in the request, permissions rules based on GPM context information such as buddy lists (e.g. "if watcher is in customer list-A then show my availability only on IM"), calendar schedule (e.g. "if my schedule has no entry between 1pm and 3pm, then…"), caller identity etc.
    - Wants to implement a single, logically centralised permissions management service.
    - Wants to enable its enterprise subscribers with a simple and fast method of capturing permissions rules
- Presence server
    - Wants to know if William's presence information (target attributes) can be presented to Target Attribute Consumers based on information included in the permissions checking request to GPM, (e.g. user identity)

5.4.2.2Actor Specific Benefits

- William
    - Easily provisions and manages his permissions rules via a single application that allows him to use information from various sources/applications, e.g., phonebook, calendar, schedule, location and presence
    - Uses permissions rules to specify when and where he is available and by what communication medium
    - Is able to use one interface to perform permissions management operations for a number of services
- William's Customers
    - Can obtain William's presence information based on his permissions
- GPM Service provider
    - Performs permissions management on behalf of the permission target thereby protecting his privacy
- Presence server
    - Uses GPM to set permissions regarding the target's presence status
    - Turns presence data into more useful availability information about the permissions target

5.4.3 Pre-conditions

- William is a subscriber of the GPM Service Provider and the Presence server
- William, Peter and Sue have devices with presence enabled phonebook clients and both Peter and Sue have subscribed to William's presence information
- All requests for William's presence are handled by William's presence server
- The GPM service provider evaluates the permissions rules to determine if and how William's presence is granted

5.4.4 Post-conditions

William's presence information is released to authorised requesters based on his permissions rules

5.4.5 Normal Flow

- William expresses his presence rules, via a simple permissions management tool. This tool allows him verify his rules by performing some 'what-if' testing. He proposes a test that emulates the presence views of buddies according to their GPM context, (e.g. boss, friend etc). Using this test he is able to verify that his rules are recognised and he confirms his settings.

- For this particular working day, William provisions the following presence rules:
    1. From 0800 to Noon: make my presence "available" on voice, PoC and IM to all customer entries in my business phonebook
    2. From 1300 to 1700 (William works at Acme, another client's premises): block all presence requests from low priority customers but allow high priority customers to see that I am "available" on IM only
        - Peter sees William's presence as "unavailable" on all communications means.
        - Susan sees that William is available on a chat client and communicates with him using IM.
    3. After 1700: Show my availability to all presence enabled applications (voice, PoC and IM) for all customers entered in my customer phonebook
        - At 1900: Susan wants to talk to William. She checks her presence enabled phonebook and sees that he is "busy" for voice communication so decides to send him an IM asking him to call her urgently

- William sees Susan's IM and hangs up. Susan is able to see William's icon for voice communication change state almost immediately, until he calls her.

5.4.6 Alternative Flow

At 1730, William decides to stay at the Acme office where he is consulting to complete an important project, so he provisions an "override" rule via his permissions management screens accessed from his mobile device. The "override" rule sets his presence to "not-available" on all presence-enabled applications.

5.4.7 Operational and Quality of Experience Requirements

1. Permissions Managers are presented with customised front-end interfaces that allow them to express intricate permissions rules in a succinct manner.
2. Permissions management tools adapt to device capabilities
3. Permissions management tools flexibly adapt to the relative simplicity and intricacy of each application and the needs of Permissions Managers (i.e. from technophobes to technophiles)
4. Permissions management tools allow Permissions Managers to express permissions rules based on their GPM context (e.g. activities) on a per-Requester basis.
5. Permissions management tools flexibly adapt as subscriber's subscribe to more services
6. The evaluation of the permissions rules is near instantaneous so that the service is executed within the acceptable limits required.

5.5 Nearest Restaurant

5.5.1Short Description

John, a tourist in Madrid, is looking for a typical "tapas" bar near his location. John has received information about "Nearest Restaurant" service, and he is going to use it.

1. John sends an MMS to the "Nearest Restaurants" application with the text "Tapas".
2. Nearest Restaurant application will send John an MMS with the nearest restaurant to his location. To determine John's location and sends him the MMS, Nearest Restaurants application makes use of LOC[1] and MMS enablers.

LOC and MMS enablers send Permissions Checking Requests to GPM, in order to find out John's permissions rules regarding the attributes Nearest Restaurant application is asking for.

5.5.2 Actors

- John, a tourist with a mobile phone-acts as *Permissions Target and Permissions Manager*.
- InfoMovil.com, a Content Provider which owns several applications (e.g. Nearest Restaurant) - acts as *Requester Administrator*
- Nearest Restaurant, InfoMovil.com application that provides the nearest restaurant to your location – acts as *Requester*.
- Mobile operator offering GPM, LOC and MMS enablers-acts as Service Provider

5.5.2.1Actor Specific Issues

- John,
    - Wants to use Nearest Restaurant to know the nearest tapas bar to his location.

[1] LOC enabler, E.g. Mobile Location Service (OMA). This use case does not reflect current MLS specs, it is only a potential development of a future LOC enabler.

  - Wants to set permissions rules regarding LOC and MMS enablers.
  - Wants his permissions rules to be taken into account when applications ask for his location attributes to LOC enabler or for the possibility to send him an MMS through MMS enabler.

- InfoMovil.com,
  - Wants to offer several applications to mobile user's based on Service Provider Resources.
  - Wants to register/ unregister dynamically new applications (e.g. Nearest Restaurant) using the mobile operator's Service Provider Resources.

- Nearest Restaurant,
  - In order to offer a nice service,
    - Wants to ask for mobile user's location
    - Wants to send an MMS to the mobile user with the nearest restaurant to his location.
- Mobile operator,
  - Wants to establish agreements with third parties content providers to offer as many applications as possible.
  - Wants to offer permissions checking rules system to the mobile user's

5.5.2.2Actor Specific Benefits

- John,
  - Easily establishes his permissions rules and uses interesting applications with his permissions rules checking guaranteed.

- InfoMovil.com
  - Reduces time-to-market for new applications.
  - Offers applications based on enablers.

- Nearest Restaurant
  - Gets mobile user's attributes (location) and uses enablers (multimedia messaging) to offer an attractive service.
- Mobile operator
  - Establishes agreements with third parties content providers to increase its revenues (e.g. LOC and MMS enabler).
  - Offers permissions checking rules to the mobile user's, fulfilling legal and business requirements.

5.5.3 Pre-conditions

- InfoMovil.com content provider has an agreement with the mobile operator such that InfoMovil applications could make use of several enablers (LOC, MMS enablers). This includes an obligation to notify information to GPM. InfoMovil is aware of the use of GPM when accessing LOC and MMS enablers.
- InfoMovil.com has developed recently Nearest Restaurant application and wants to launch it to the market as quickly as possible. Nearest Restaurant application needs a LOC enabler (to get user's location) and an MMS enabler (to send an MMS to a mobile user).
- John makes use of GPM service.

5.5.4 Post-conditions

- MMS containing the nearest tapas bar address, phone number and situation map is sent to John taking account of his permissions rules.

5.5.5 Normal Flow

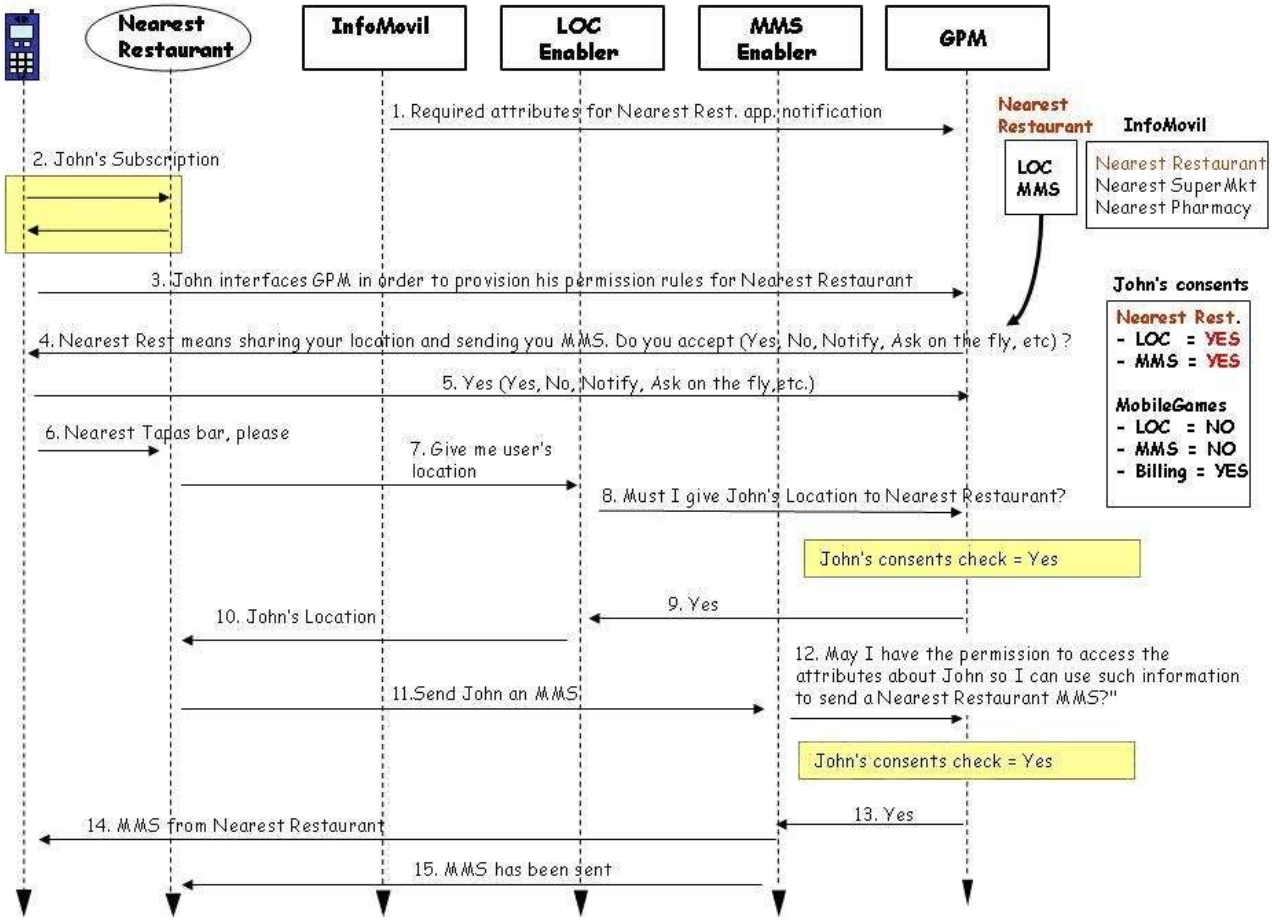

Figure 4: "Nearest Restaurant" Normal Flow

1. InfoMovil.com informs GPM about target attributes it requires (user's location from LOC enabler and sending an MMS through MMS enabler)

2. John subscribes to Nearest Restaurant application, and he is advised to express properly its permissions preferences in GPM service.

3. John, (Permissions Manager) interfaces GPM in order to provision his permissions rules for 'Nearest Restaurant' application

4. GPM, checking the information provided by InfoMovil.com, notifies John all permissions rules required (not only LOC permissions rules) for Nearest Restaurant: sharing Location and permit MMS sending.

5. John agrees for both requirements: sharing location and MMS sending. Permissions rules have just been provisioned.

6-15. After this process, the service can be provided.

5.5.6 Alternative Flow 1

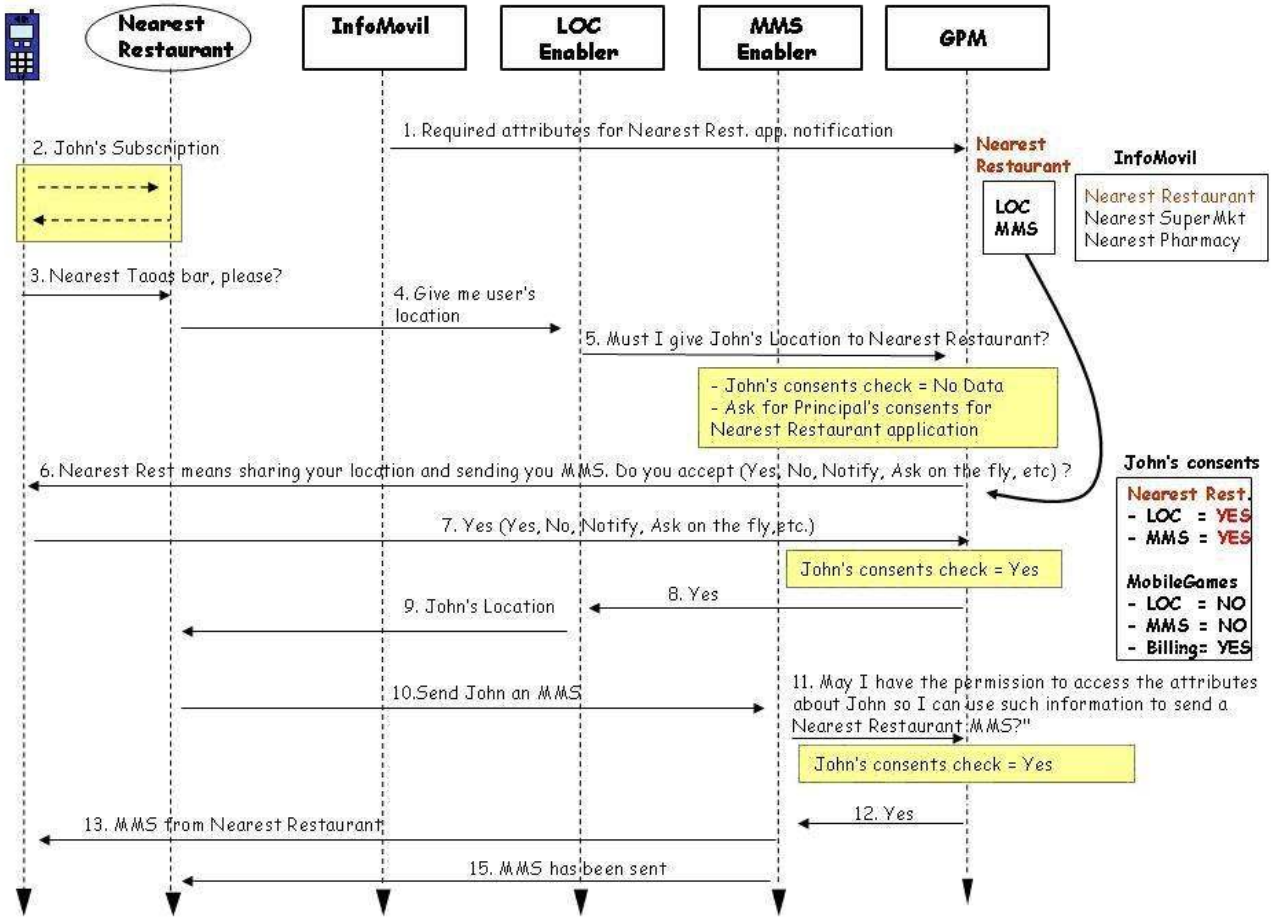

Figure 5: "Nearest Restaurant" Alternative Flow 1

1. InfoMovil.com informs GPM about target attributes it requires (user's location from LOC enabler and sending an MMS through MMS enabler)

2. John subscribes to Nearest Restaurant application, and he is advised to express properly its permissions preferences in GPM service. This alternative flow also applies to no-subscription services, in that case, step 2 disappears (notice dashed arrows).

3. For subscription service, John asks for the nearest tapas bar without notifying GPM about the new subscription and for no-subscription service, John just asks for the nearest tapas bar too.

4. Nearest Restaurant needs to know John's location, so it makes a request to LOC enabler.

5. LOC enabler wants to know if it must provide Nearest Restaurant with John's Location.

6. GPM has no data available to answer LOC request, but it has John default permissions rule applying to applications for which he hasn't set up an specific permissions rule: *ask me to express my permissions preferences about new*

applications requesting my attributes or for a service regarding me. This default rule could also be a default rule for all mobile operator users.

7-15.Same as Normal Flow

5.5.7Alternative Flow 2

1. (See Step 1 Normal Flow) InfoMovil informs GPM about Nearest Restaurants requirements (user location from LOC enabler and sending an MMS through MMS enabler) it sets up location as mandatory (Nearest Restaurant is not able to operate properly if not provided) and MMS optional (Nearest Restaurant is able to operate properly if not provided, but it is desired to fulfil this requirement in order to give a better service).
2. (See Step 7 Normal Flow) John sets up Location sharing to "No" and MMS sending to "Yes".
3. Checking information provided by InfoMovil (Step 1) and permissions settings provide by the user (2), GPM notices that Nearest Restaurant is not able to operate properly enforcing John's permissions rules.
4. GPM notifies John of the inability to request Nearest Restaurant if Location information is not provided to the application and asks John to change its permissions rules in order the application to operate properly.

5.5.8 Alternative Flow 3

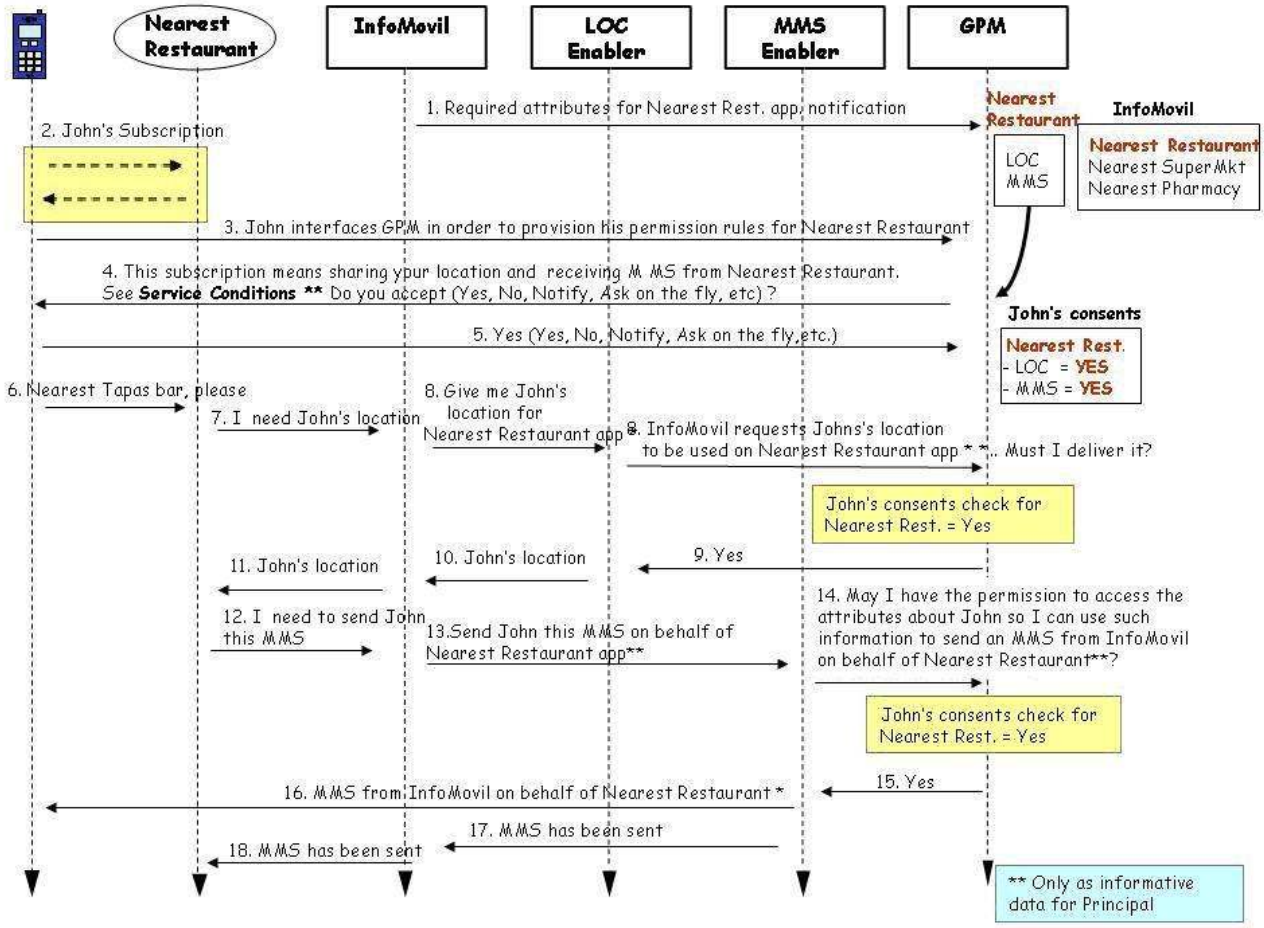

Figure 6: "Nearest Restaurant" Alternative Flow 3

Same as Normal Flow except Infomovil behaviour: Infomovil acts as a Broker or Reseller to Nearest Application, it means:

- Dialog between Nearest Restaurant and GPM takes place through InfoMovil.
- InfoMovil receives Nearest Restaurant's request and passes them to GPM (InfoMovil also sends to Nearest Restaurant GPM response).
- Service Provider Resources (LOC, MMS…) and GPM shall have neither direct communication nor control over Nearest Restaurant.
- GPM information about Nearest Restaurants is provided by InfoMovil.
- (Step 4 in the flow above)GPM shall make John aware of "Service Condition" regarding Nearest Restaurant Nearest Restaurants needs both John's location and sending MMS but this is going to be sent through Infomovil.
- (Step 8 in the flow above) InfoMovil shall inform GPM about the application asking for John's location (Nearest Restaurant) in order to use this information to notify the user (e.g. in Ask on the fly notification), to check the appropriate set of permissions rules (the ones corresponding to the application Nearest Restaurant), …

5.5.9 Alternative Flow 4: Content Provider-GPM Agreement expiration/ cancellation

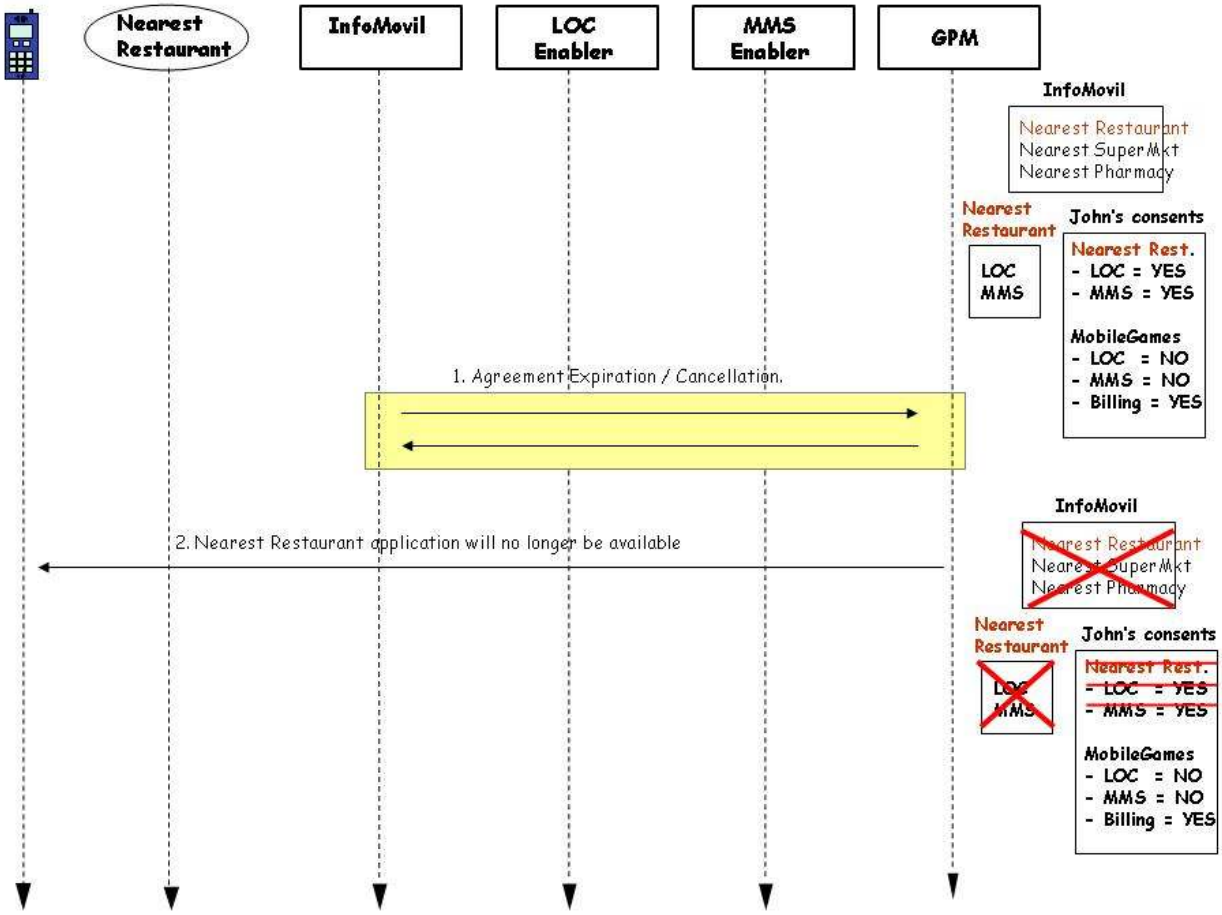

Figure 7: "Nearest Restaurant" Alternative Flow 4

Due to agreement expiration/cancellation between InfoMovil and the Service Provider that owns GPM, GPM removes all information related to InfoMovil: InfoMovil Applications (Nearest Restaurant, Nearest Supermarket)and its requirements (Nearest Restaurant needs MMS and LOC), Permissions Target's preferences (John's consent), …

InfoMovil shall also ask for remove information related only to a subset of its applications (this process could also be GPM initiated).

In addition, GPM shall inform John about the removal of his permissions rules regarding the InfoMovil applications (Nearest Restaurant) that have been just cancelled.

5.5.10 Alternative Flow 5: Unsubscription

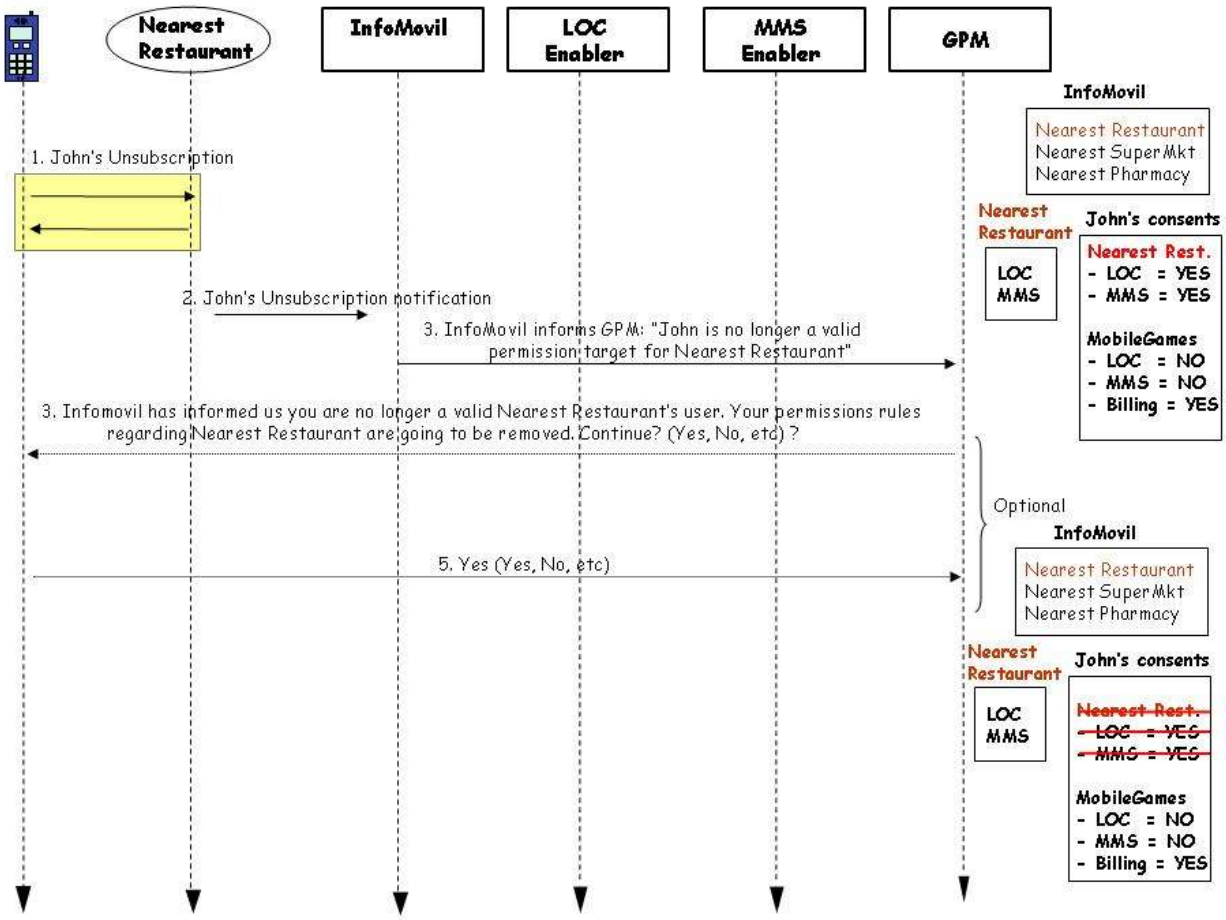

Figure 8:"Nearest Restaurant" Alternative Flow 5

John's unsubscription request triggers unsubscription notification from Nearest Restaurant (through InfoMovil in Broker use case) to GPM. GPM removes all information related to John's preferences about Nearest Restaurant.

In addition, GPM shall ask for consent / inform John about unsubscription taking place and its consequences.

5.5.11 Operational and Quality of Experience Requirements

GPM does not make any assumptions on responses for the same attribute given to different requesters. The responses may differ over time.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
HLF-1	The GPM enabler SHALL enable Permissions Managers and/or Permissions Manager's Delegates to manage per-target permissions rules, within the boundaries of their GPM management rights as set by the GPM Administrator when such operation is required. • At any time • From any capable device type and over any capable network, (e.g. mobile or fixed network). (Use Case 5.2)	GPM 1.0
HLF-2	The GPM enabler SHALL support different permission rules for different Permissions Targets regarding access to and usage of target attributes	GPM 1.0
HLF-3	The GPM enabler SHALL support the use of the same permission rules for multiple different Permissions Targets regarding access to and usage of target attributes	GPM 1.0
HLF-4	It SHALL be possible to request consent for the release of target attributes from any authorized principal, as set by the Permissions Manager or a Permissions Manager's Delegate. (Use Case 5.3)	GPM 1.0
HLF-5	The GPM enabler MAY provide mechanisms for the GPM Administrator to determine the GPM enabler implementation behaviour that applies when changes to permissions rules cannot be made effective immediately, e.g. by notifying the permissions target(s), do nothing, logging etc.. (Use Case 5.3)	Future
HLF-6	A Permissions Target MAY also be a Permissions Manager, or as a Permissions Manager's Delegate	GPM 1.0
HLF-7	A Permissions Manager and/or a Permissions Manager's Delegate that has requested changes to permissions rules SHOULD be notified when the changes are effective or will become effective. (Use Case 5.3)	Future
HLF-8	When using a service for the first time, it SHALL be possible for the Permissions Target to be informed that default permissions rules have been provisioned for him/her	Future
HLF-9	It SHALL be possible to notify a Permissions Target of any changes to permissions rules made on their behalf by a Permissions Manager and/or a Permissions Manager's Delegate. (Use Case 5.3)	Future
HLF-10	The GPM enabler SHOULD make use of existing, unique Identifiers (e.g. MSISDN/IMSI, MDN/MIN, e-mail Address) for addressing Permissions Targets.	GPM 1.0
HLF-11	It SHALL be possible to inform a Permissions Manager or Permissions Manager's Delegate of his/her role, rights and limitations with regard to permissions management. (Use Case 5.3)	Future
HLF-12	In case the Permissions Target is not the same actor as the Permissions Manager or Permissions Manager's Delegate, the Permissions Target SHOULD be informed of the role, rights and limitations of Permissions Manager or Permissions Manager's Delegate with regards to his/her permissions rules	Future
HLF-13	The GPM enabler SHALL be able to support a permissions checking request for either a single attribute or a group of attributes of the permissions target. (Use Case 5.1)	GPM 1.0

HLF-14	The GPM enabler SHALL support returning any permission checking response and associating it to any attribute or combination of attributes, (e.g. GRANT for some attributes and DENY for others.. (Use Case 5.1)	GPM 1.0
HLF-15	GPM SHALL be able to give a permissions checking response based on information associated with • The Target Attribute Consumer (e.g. the identity of a single end-user or the identities of multiple end-users) and the Target Attribute Requester (e.g. the application(s) used) • The Permissions Target identity (e.g. the identity of a single end-user or the identities of multiple end-users). • The requested target attributes In addition to the above, the following information MAY be used: • The intended use of the target attributes (i.e. use that will be made of this information by the application, e.g. to access and modify a target attribute, or sharing medical data with doctors but not students) • User profile information and other relevant GPM context information (e.g. time of day, number of requests per unit time or other information coming from OMA enablers) (Use Case 5.1)	GPM 1.0
HLF-16	Once the permission to access a particular (set of) attributes has been expressed (e.g. GRANT always), it SHALL be possible for the GPM enabler implementation to notify the Permissions Target (or another principal, as required by the permission rule) every time the information is requested. (Use Case 5.1)	GPM 1.0
HLF-17	The Permissions Target notification SHALL contain at least the following: • The Target Attribute Requester identity • Target Attribute Consumer identity • The attributes/group of attributes requested. (Use Case 5.1)	GPM 1.0
HLF-18	The GPM enabler SHALL support permissions rules based on well-defined schema and semantics	GPM 1.0
HLF-19	The GPM enabler SHALL uniquely identify the permissions rules.	GPM 1.0
HLF-20	The Permissions Manager and/or Permissions Manager's Delegate(s) SHALL be able to manage permissions rules according to: • The GPM context of the Target Attribute Requester (e.g., relationship between Target Attribute Requester and Permissions Target) • The GPM context of the Target Attribute Consumer (e.g., relationship between Target Attribute Consumer and Permissions Target) • The GPM context of the target (e.g., user behaviour or situations such as work, home etc)	GPM 1.0

	• Other information (Use Case 5.4)	
HLF-21	The Permissions Target SHOULD be able to view the permissions rules that pertain to him/her.	GPM 1.0
HLF-22	The GPM enabler SHALL provide principals (e.g. Permissions Target, Permissions Manager, Permissions Manager's Delegate, GPM Administrator Ask Target) with the same experiences even when those principals are in a visited network	GPM 1.0
HLF-23	GPM SHALL allow provisioning tools that enable Permissions Managers and/or Permissions Managers' Delegates to manage permissions rules with adequate quality of experience [QoE].	GPM 1.0
HLF-24	The Permissions Manager that has been assigned this specific responsibility by the GPM Administrator, SHALL be able to configure the permissions rules priority.	Future
HLF-25	The GPM enabler SHALL support the ability of network or terminal resources, (e.g. IM, Presence, PoC enabler, SUPL client…) to stay aware of updates performed on the permissions rules associated to the resource.	GPM 1.0
HLF-26	The GPM enabler SHALL be able to apply consistent permission checking, to applications implemented both in a terminal and a network server.	GPM 1.0

Table 1: High-Level Functional Requirements

6.1.1 Types of Permission Rules

Label	Description	Enabler Release
PermTypes-1	Permissions rules SHALL allow the expression of what target attribute(s) can or cannot be accessed by a Target Attribute Requester and/or a Target Attribute Consumer.	GPM 1.0
PermTypes-2	Among the types of rules supported by GPM there MAY be a permissions rule that allows the Permissions Manager to delegate some or all permissions management operations to one or more Permissions Manager's Delegate(s) (Use Case 5.3)	Future
PermTypes-3	Among the types of rules supported by GPM there SHALL be a permissions rule type that allows the Permissions Target (i.e. a principal or group of principals) and/or Permissions Manager and/or Permissions Manager's Delegate to be notified of changes to permissions rules. (Use Case 5.3)	Future
PermTypes-4	Among the types of rules supported by GPM there SHOULD be a permissions rule type that allows a Permissions Target to be notified once changes to his permissions rules take effect. (Use Case 5.3)	Future
PermTypes-5	The GPM enabler SHALL enable permissions rules to express whether a Permissions Target notification is required to be sent to the Permissions Target (i.e. a principal or group of principals)	GPM 1.0

PermTypes-6	If multiple devices are associated with a single Permissions Target, the GPM enabler SHALL support: (a) The same or different permissions rules for each device used simultaneously by one Permissions Target; (b) The same or different permissions rules for each device when one Permissions Target uses only one device at a given time or for a particular service..	GPM 1.0
PermType-7	The GPM enabler SHALL include a mechanism for a Permissions Manager and/or Permissions Manager's Delegate(s) to express the validity conditions for the release of a particular attribute or group of attributes.	GPM 1.0
PermType-8	Permission rules with validity conditions SHALL specify what outcome is to take place if the validity conditions are not met	GPM 1.0
PermType-9	The following types of validity conditions SHALL be supported: • Availability lifetime of target attributes • Target Attribute Requester GPM context information [see HLF-20]	GPM 1.0
PermType-10	Among the types of rules supported by GPM there MAY be a permissions rule type which causes a permission checking response which depends on other contextual information, e.g. information related to earlier permission checking requests, the time of day, the permission target, or the interval between permission checking requests.	GPM 1.0
PermType-11	The GPM enabler SHALL support a mechanism to allow one set of permissions rules to take precedence over a different set of permission rules.	GPM 1.0

Table 2: Types of Permission Requirements

6.1.2 Permissions Management Functions

Label	Description	Enabler Release
PMF-1	It SHALL be possible to assign "roles" to principals that determine the rights for the management of a given set of permissions rules (e.g. a "super permissions manager role" may imply that the authorised principal has the rights to perform all the functions described in PMF-3, a "reading-only permissions manager role" may imply that the authorised principal may only able to read and list the permissions rules).	Future
PMF-2	The roles described in PMF-1 MAY be defined by the GPM Administrator, and/or the Permissions Managers and/or the Permissions Manager's Delegates	Future
PMF-3	Permissions Managers SHALL be able to perform the following permissions management functions as authorised by the GPM Administrator: • Create permissions rules (including default permissions rules) • Read permissions rules • Delete permissions rules • Modify permissions rules • List permissions rules (e.g. according to search or filter criteria)	GPM 1.0: bullet 1-4 and 9 Future: Bullet 5-8 and 10-13

	• Suspend permissions rules (i.e., temporarily halt rules without deleting or modifying them) • Resume permissions rules • Prioritize permissions rules • Overwriting permissions rules priorities • Retrieve GPM management rights • Delegate GPM management rights • Modify delegated GPM management rights • Revoke delegated GPM management rights	
PMF-4	The Permissions Manager's Delegate(s) SHALL be able to perform some or all of the permissions management functions described in PMF-3, depending on their assigned rights.	Future
PMF-5	It SHALL be possible to assign a role to the Permissions Manager's Delegate	Deleted
PMF-6	The Permissions Manager and/or Permissions Manager's Delegate(s) SHALL be able to create permissions rules based on any combination of conditions and actions, e.g. some (or all) of the following: • The Target Attribute Consumer (e.g. the identity of a single end-user or the identities of multiple end-users) and the Target Attribute Requester (e.g. the application(s) used) • The intended use of the target attributes (i.e. use that will be made of this information by the application.) • The Permissions Target (i.e. a principal or group of principals). • Target attributes • GPM Context information (e.g. between 9 and 12 o'clock) (Use Case 5.4).	GPM 1.0
PMF-7	The Permissions Manager and/or Permissions Manager's Delegate(s) SHALL be able to modify existing permissions rules when target attributes are added.	GPM 1.0
PMF-8	When creating or modifying permissions rules, the Permissions Manager and/or Permissions Manager's Delegate(s) SHALL be able to specify a response per permissions rule out of a finite set of multiple possibilities defined by the deployer of the enabler implementation.	GPM 1.0
PMF-9	Permissions Managers and/or Permissions Manager's Delegates SHOULD be able to subscribe to notifications of management operations performed on permissions rules they manage.	Future
PMF-10	It SHOULD be possible for Permissions Managers and/or Permissions Manager's Delegates to be notified once changes to permissions rules take effect	Future
PMF-11	The GPM enabler SHALL enable Permissions Managers and/or Permissions Managers' Delegates to assign at least the following actions to permissions rules: Ask for consent from Ask Target, ('ASK'),	GPM 1.0

	• Grant permission to release target attribute(s), ('GRANT'), • Deny permission to release target attribute(s), ('DENY'). (Use Case 5.1)	
PMF-12	It SHALL be possible to associate any action to any permission rule, e.g.: • ASK, • GRANT once, • GRANT always, • DENY once, • DENY always, for this attribute X and not for the attribute Y. (Use Case 5.1)	GPM 1.0
PMF-13	A Permissions Manager and/or Permissions Manager's Delegate(s) SHALL be able to provision a rule that determines whether a Permissions Target notification is required to be sent to the Permissions Target (i.e. a principal or group of principals)	GPM 1.0
PMF-14	The Permissions Manager and/or Permissions manager's Delegate SHALL be able to assign values to parameters in permission rules that they are allowed to manage, e.g. for the GPM validity period used by the Ask Target to convey his/her answer. (Use Case 5.1)	GPM 1.0
PMF-15	It SHALL be possible for the GPM enabler to send a notification to a resource and/or a designated principal when a permissions rule related to the resource is changed	Future

Table 3: Permissions Management Functions Requirements

6.1.3 Ask Management Requirements

Label	Description	Enabler Release
Ask-1	If the permission checking request, results in an Ask request, and when this Ask request is sent, it SHALL be possible for the GPM enabler to notify the Target Attribute Requester and the resource issuing the permissions checking request.	Future
Ask-2	If the Permissions Manager/Permissions Manager's Delegate(s) has assigned an ASK to a permissions rule, it SHALL be possible for them to assign one or more Ask Target(s).	GPM 1.0
Ask-3	In the case that multiple Ask Targets exist for the same permissions rule, it SHALL be possible for the Permissions Manager/Permissions Manager's Delegate(s) to assign an order of asking (sending Ask Requests) to those Ask Targets.	GPM 1.0
Ask-4	In the case that an Ask Request is sent to multiple Ask Targets for the same permissions rule, it SHALL be possible for the Permissions Manager/Permissions Manager's Delegate(s) to specify which Ask Target's answer takes precedence over the others	Future
Ask-5	It SHALL be possible to notify a Target Attribute Requestor when the Ask Target is the same principal as the Target Attribute Consumer.	Future
Ask-6	It SHALL be possible for the Ask Target to manage 'Once' or 'Always' cases in its 'ask' notification answer. (Use Case 5.1)	GPM 1.0

Ask-7	The Ask request SHOULD present to the Ask Target the Target Attribute Consumer identity and/or Target Attribute Requester identity. (Use Case 5.1)	GPM 1.0
Ask-8	If the permissions rules include an Ask Request, the Permissions Manager SHALL be able to set a GPM validity period for providing an answer regarding a permissions checking request. (Use Case 5.1).	Future
Ask-9	The GPM Administrator or the Permissions Manager or the Permissions Manager's delegate SHALL be able to determine the outcome if multiple permissions checking requests are received for the same permissions rule when the GPM validity period has not yet expired and the Ask Target has not yet responded. E.g.: • By NOT sending repeated Ask request to the Ask Target, and • By notifying the Target Attribute Requester with a predefined message that says that the request was already received and no additional Ask request was sent. (Use Case 5.1).	Future
Ask-10	In the case the Ask Target indicates unwillingness to receive Ask Requests or the GPM validity period expires before the Ask Target has responded, the Target Attribute Requester and/or Target Attribute Consumer SHALL be denied access to target attributes and optionally notified accordingly. (Use Case 5.1).	GPM 1.0
Ask-11	Permissions rules SHALL include a mechanism to specify that consent needs to be explicitly obtained before permission is given to the release of target attributes, i.e. by means of an Ask request.	GPM 1.0
Ask-12	GPM MAY provide a mechanism for Ask Targets to indicate their willingness/unwillingness to receive an ask request	GPM 1.0
Ask-13	It SHALL be possible for GPM to check the Ask Targets' willingness to receive Ask Requests before sending an Ask Request	GPM 1.0
Ask-14	In the case all Ask Targets indicate unwillingness to receive Ask Requests or the GPM validity period expires before any Ask Target has responded, a default permissions rule MAY be applied	GPM 1.0

Table 4: Ask Management Functions Requirements

6.1.4 Delegation

Label	Description	Enabler Release
DEL-1	A Permissions Manager SHALL be able to delegate other principal(s) to be Permissions Manager(s), i.e. create Permissions Manager's Delegate(s).	Future
DEL-2	Depending upon the GPM management rights assigned to the Permissions Manager's Delegate(s), the Permissions Manager's Delegate MAY be able to delegate some or all of the permissions management functions he has been assigned.	Future
DEL-3	Permissions Managers SHALL be able to assign Permissions Manager's Delegate(s) to perform some or all permissions management operations on their behalf. (Use Case 5.3)	Future
DEL-4	It SHALL be possible that the Permissions Manager's Delegate(s) to be notified when their delegation is created or modified.	Future

DEL-5	A Permissions Manager SHALL be able to transfer all GPM management rights over a given Permissions Target to different Permissions Manager's Delegate.	Future
DEL-6	The Permissions Manager SHALL be able to revoke those rights that he/she has previously assigned to a Permissions Manager's delegate.	Future
DEL-7	It SHOULD be possible for the Permissions Target to be informed if Permissions Manager's Delegate(s) is/are created to manage his/her permissions rules.	Future
DEL-8	The Permissions Manager MAY assign one or more of their GPM management rights to one or more Permissions Manager's Delegate(s) to manage per-target permissions rules.	Future

Table 5: Delegation Requirements

6.1.5 Security

Label	Description	Enabler Release
SEC-1	The GPM enabler SHALL support: a) Authentication and authorisation of principals wishing to perform permissions management functions b) Integrity and confidentiality of permissions management operation messages.	GPM 1.0
SEC-2	GPM SHOULD support secure communication between the source requesting permissions checking and GPM	GPM 1.0
SEC-3	The GPM enabler SHOULD use available mechanisms to log all permissions management operations.	GPM 1.0
SEC-4	The GPM enabler SHALL protect against potential security threats, including denial-of-service attacks and identity theft.	GPM 1.0
SEC-5	It SHALL be possible to authenticate and authorise an entity issuing a permissions checking request.	GPM 1.0
SEC-6	GPM SHALL enable logged information to be made available to authorized principals, e.g. authorized representatives of law enforcement authorities.	GPM 1.0
SEC-7	The GPM SHALL store the information pertaining to permissions target securely, (e.g. permissions rule, the identity of permissions target, the log related to permissions target)	GPM 1.0

Table 6: Security Requirements

6.1.6 Charging

Label	Description	Enabler Release
CHRG-1	The GPM enabler SHALL be able to send charging information to the charging enabler [CHARG].	GPM 1.0

Table 7: High-Level Functional Requirements – Charging Items

6.1.7 Administration and Configuration

Label	Description	Enabler Release
ADMIN-1	The GPM Administrator SHALL be able to trace all relevant information related to permissions checking requests.	OSPE 1.0
ADMIN-2	The GPM Administrator SHALL be able to assign Permissions Managers for a Permissions Target (e.g. the Permissions Manager role could be assigned to Permissions Target, or the owner of the GPM subscription, or to the GPM	Future

	Administrator him/herself).	
ADMIN-3	The GPM Administrator SHALL be able to assign specific GPM management rights to a permissions manager (e.g. right to create/retrieve/modify/delete/prioritize/delegate GPM management rights) with respect to the managed permissions targets.	Future
ADMIN-4	The GPM enabler SHALL be able to support multiple principals with the same roles and provide mechanism to detect and handle any possible resulting management conflicts, e.g. by use of a management right to overwrite permissions rules priorities	Future
ADMIN-5	The GPM Administrator SHALL be able to revoke any rights that he/she previously assigned to a Permissions Manager	Future

Table 8: High-Level Functional Requirements – Administration and Configuration Items

6.1.8 Usability

Label	Description	Enabler Release
USAB-1	The GPM enabler SHALL allow Permissions Target who access new services to easily re-use their existing permissions rules for those new services. (Use Case 5.2)	GPM 1.0
USAB-2	The GPM enabler SHALL allow Permissions Managers and/or Permissions Manager's Delegate(s) to apply default permissions rules. (Use Case 5.2)	GPM 1.0
USAB-3	It SHOULD be possible for a Permissions Manager and/or Permissions Manager's Delegate(s) to check the response to the permissions checking request before deploying permissions rules in the service provider domain, (e.g. 'what-if' testing). (Use Case 5.4).	GPM 1.0
USAB-4	It MAY be possible for a Permissions Manager and/or Permissions Manager's Delegate(s) to trace the outcome of permissions rules	OSPE 1.0
USAB-5	The Permissions Manager and/or Permissions Manager's Delegate(s) MAY be able to modify default permissions rules	GPM 1.0
USAB-6	The Permissions Manager and/or Permissions Manager's Delegate(s) SHALL be able to update permissions rules, including override permissions rules that impact (i.e., cancels or pre-empts) an existing permissions rule(s). (Use Case 5.4).	GPM 1.0

Table 9: High-Level Functional Requirements – Usability Items

6.1.9 Privacy

Label	Description	Enabler Release
Privacy-1	The GPM enabler SHALL support the ability of a Permissions Target to use a pseudonym. [Privacy]	GPM 1.0
Privacy-2	The GPM enabler MAY support the ability of a Target Attribute Consumer to use a pseudonym	GPM 1.0
Privacy-3	The GPM enabler SHALL be compatible with managed identities (e.g. anonymized, federated identity etc), where the principals are actors (e.g. Target Attribute Requesters, Target Attribute Consumers, GPM Administrator, Permissions Managers, Permissions Managers Delegate(s), Permission Targets).	GPM 1.0
Privacy-4	The GPM enabler SHALL handle the same managed identities identifiers for the permission rules as it handles the identifiers passed in the request (e.g. identifiers have to match to potentially result into a "grant"). GPM intrinsic functions explicitly SHALL NOT include resolving a pseudonym.	GPM 1.0

Table 10: High-Level Functional Requirements – Privacy Items

6.2 Overall System Requirements

Label	Description	Enabler Release
OSR-1	The GPM enabler SHALL NOT restrict deployment options	GPM 1.0
OSR-2	The GPM enabler SHALL be able to be used by any services applicable to any kind of users or segments	GPM 1.0
OSR-3	It SHALL be possible to represent any relevant information about a Permissions Target as target attributes. The following are examples of target attributes: • Identity • Location information, see [MLS] • Presence information, see [SIMPLE] • Other Personal Data, see [Privacy] • Application specific data (e.g., clock, calendar information, etc) • Preferred device(s) and their capabilities (Use Case 5.4).	GPM 1.0
OSR-4	The interface to the permissions checking request SHALL be able to support multiple formats to ensure consistency between permissions rules and input arguments (Use Case 5.4).	GPM 1.0
OSR-5	The GPM enabler SHALL support permissions checking requests from any resource and any domain (e.g. Service Provider domain or in a Terminal domain).	GPM 1.0
OSR-6	Permissions checking requests SHALL provide at least the following types of data as input arguments: • The Target Attribute Consumer (e.g. the end-user identity) and the Target Attribute Requester (e.g. the application used) • The Permissions Target identity • Target attributes In addition to the above, the following information MAY also be provided to derive an appropriate permission checking response: • The intended use of the target attributes (i.e. use that will be made of this information by the application.) If a GPM target request is initiated by an end-user service request, permissions checking requests SHALL also provide the identity of the end-user (Use Case 5.1 and 5.4)	GPM 1.0
OSR-7	Output arguments SHALL be returned to the source of the permissions checking requests after the permissions rules are checked.	GPM 1.0

OSR-8	Output arguments SHALL include at least the following types of data: • GRANT for all or only a list of attributes • DENY for all or only a list of attributes The permissions checking response MAY contain any combination of the above output arguments (e.g. GRANT the attribute called 'ADRESS TOWN' and DENY all the other requested attributes).	GPM 1.0
OSR-9	If the output arguments include a DENY response, a reason MAY be provided by the GPM enabler	GPM 1.0
OSR-10	The GPM permissions management interface SHALL support any information required for permissions management operations, including the following: • Permissions Managers with different roles (e.g. "Super Permissions Manager") • Different categories (e.g. subscription profiles) of permissions target using a single application • Different device capabilities • The addition/removal of services used by the permissions target	GPM 1.0
OSR-11	The GPM enabler SHALL permit highly scalable implementations	GPM 1.0
OSR-12	The GPM enabler design SHALL maximize reliability, scalability and performance.	GPM 1.0
OSR-13	The GPM enabler SHALL be able to log all relevant information (e.g., errors) and the associated decisions related to permissions checking requests.	GPM 1.0
OSR-14	If the GPM enabler supports mechanisms to log permissions management operations, the information as below SHALL be stored: a) The type of permission management operations (e.g. Create/Modify/Delete) b) The time of operations c) The identity of principal who performed permission management operations d) The permission rules that apply to the relevant permission management operations e) e) The Permissions Target	GPM 1.0
OSR-15	The GPM enabler SHALL support the re-use of a single permissions rule or a group of permissions rules as part of multiple sets of permissions rules.	GPM 1.0
OSR-16	Input arguments to permissions checking requests SHALL be extensible to support data from various sources of permissions checking requests.	GPM 1.0
OSR-17	GPM SHALL define an interface for permissions checking	GPM 1.0
OSR-18	GPM SHALL support mechanisms to make available, to an authorized principal (e.g. the Permissions Manager and/or Permissions Manager's Delegate(s)) via one single interaction from the user perspective, based on provided criteria (e.g. for a specified individual attribute, or for all attributes associated to a particular application, or for all attributes associated to a particular feature of an application (e.g. attribute A, B with feature X, attribute A, B, C with feature Y)) all relevant information (e.g. default permission rules, previously provisioned permission rules) needed to make a	GPM 1.0

	decision on a permissions rule to be set up. (Use Case 5.5)	
OSR-19	In order to enhance usability, the GPM enabler SHALL support mechanisms to ensure that an authorized principal (e.g. Permissions Managers and/or Permissions Manager's Delegate(s)) can: a) Obtain all attributes and features of an application (e.g. core features of an application without which a service cannot be provided properly, optional features of an application without which a service will not be able to provide enhanced information, etc) related to a specific permissions rule. b) Be informed at management time, (by using information provided in A) whether a permission rule would make a particular feature of an application not available (Use Case 5.5)	GPM 1.0
OSR-20	The GPM enabler SHALL support mechanisms to provide, as part of an Ask Request to an Ask Target, additional information received as input parameters in the permissions checking request, as dictated by the permissions rules, such as: • Identifier of the requesting resource (e.g. application) • Identity of the end-user, if the GPM target request is initiated by a user other than the Permissions Target • Identifier of the resource (e.g. application) making use of the target attributes, if the Target Attribute Requester is asking for target attributes on behalf of another resource (e.g. application) (Use Case 5.5)	GPM 1.0
OSR-21	GPM SHALL support mechanisms to: • To capture the list of target attributes needed by an application and • To allow a Permissions Manager and/or Permissions Manager's Delegate(s) to set up their Permissions Rules regarding a certain application in one single step (i.e. from Permissions Manager's perception point of view), in order to enhance the Permissions Manager's experience. (Use Case 5.5)	GPM 1.0
OSR-22	The GPM enabler SHALL limit the repeated sending of Ask Requests, (e.g. by use of a provisionable parameter to determine the number of such "Ask request" in a given time interval) (Use Case 5.5)	GPM 1.0
OSR-23	Default permissions rules MAY include an Ask Request to be sent to the Ask target (Use Case 5.5)	GPM 1.0
OSR-24	The GPM enabler SHALL enable an authorised principal to identify: a) Permissions rules association with attributes of an application and/or features of an application b) Permissions rules association with a Permissions Manager (or a Permissions Managers' Delegate	GPM 1.0

	c) Permissions rules association with a Permissions Target (Use Case 5.5)	
OSR-25	Permissions Managers and/or Permissions Manager's Delegate(s) SHALL be able to provision a default permissions rule regarding permissions rules being removed and the associated outcomes towards the Permissions Target (e.g. "Ask the Permissions Target before any of his/her permissions rules being removed", "notify the Permissions Target before any of his/her permissions rules being removed" etc.) (Use Case 5.5)	GPM 1.0
OSR-26	The GPM enabler SHALL support principals (e.g. Permissions Manager and/or Permissions Manager's Delegate(s), Target Attribute Requester, Target Attribute Consumer, Ask Target etc.) to perform their functions when they are located in a different domain to the Permissions Target.	GPM 1.0
OSR-27	It SHALL be possible to categorize target attributes into target attribute types, e.g. types that are updated more frequently such as raw presence information or calendar information and types that are updated less frequently such as phone book entries or devices used.	GPM 1.0
OSR-28	It SHALL be possible to associate permissions rules with any target attribute type.	GPM 1.0
OSR-29	The GPM enabler SHALL support the ability for a Target Attribute Requester to provide proof that the GPM target request is authorised.	GPM 1.0
OSR-30	When a GPM target request does not satisfy the permission rules set by the Permissions Manager and/or Permissions Manager's Delegate(s), it MAY be possible for the DENY output arguments to include a list of acceptable request criteria for release of the target attributes	GPM 1.0
OSR-31	The authorised principal (e.g. Permissions Manager, Permissions Manager's Delegate, GPM Administrator) SHOULD be able to retrieve the logged information pertaining to the Permissions Target.	GPM 1.0
OSR-32	Default permissions rules MAY be applied to new or updated information contained in a permissions checking request to GPM, (e.g. a new application identity from an existing resource).	GPM 1.0
OSR-33	The GPM enabler SHOULD support deployments where permission rules are distributed rather than centralized (e.g. between network entity(ies) and device(s)). If permission rules are distributed, the GPM enabler SHALL provide mechanisms to ensure their consistency in a secure and efficient manner.	GPM 1.0
OSR-34	GPM SHALL be able to coexist with existing enabler-specific mechanisms for protecting end-user privacy (e.g. SHALL NOT prevent from continuing use of such existing mechanisms).	GPM 1.0
OSR-35	GPM SHALL be able to support the equivalent privacy controls that existing enablers provide (e.g. the way location and presence enablers define privacy controls).	GPM 1.0

Table 11: High-Level System Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-GPM-V1_0	15 Sep 2005	1, 5.1, 6.1, 6.1.7, Appp B	• Added scope, section 6.1 headings and Appendix B from OMA-REQ-GPM-2005-0009R01-Initial_RD_Idea, with changes suggested on CC 8th Sep. • Added use case 5.1 and requirements HLF1, USAB 1 & USAB 2 modified and agreed from OMA-REQ-GPM-2005-0010R01-Use_Case_service-upgrade, as suggested on CC 8th Sep.
	12 Oct 2005	2.1, 3, 5.2, 6.1, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.2	Added use case 5.2 and requirements agreed from OMA-REQ-GPM-2005-0011R02-Use_Case-consent-rights-sharing-trustworthiness
	28 Oct 2005	2.1, 2.2, 3.2, 4, 4.1, 4.2, 5.1, 6.1, 6.1.3, 6.1.7, 6.1.8, 6.1.9, 6.2	▪ Added references and Introduction sections agreed from OMA-REQ-GPM-2005-0021R01-GPM-Introduction. ▪ Added agreed definitions from OMA-REQ-GPM-2005-0020R01-Definitions ▪ Added agreed use case and requirements from OMA-REQ-GPM-2005-0012R02-"Is my friend available" use case, (agreed as R03, see minutes in OMA-REQ-GPM-2005-0023-Oct7-CC-Minutes and OMA-REQ-GPM-2005-0027-Minutes-Sydney) ▪ Added agreed use case and requirements from OMA-REQ-GPM-2005-0022R01-Call_Forward_use_case
	24 Nov 2005	1, 2, 3, 4, 5, 6	• Added Scope clarification agreed in OMA-REQ-GPM-2005-0030R02-GPM_Scope_Clarification. • Amended fig.1 and text in section 4 as discussed and agreed on CC 16th Nov (OMA-REQ-GPM-2005-0033-MINUTES_16Nov2005-CC.doc) • Added all agreed changes to sections 2, 3, 5 and 6 from OMA-REQ-GPM-2005-0034R01-Requirements_terminology-alignment
	8 Dec 2005	1, 3, 4, 5, 6	• Editorial changes to sections 1, 4, 5 and 6 to align terminology, (e.g. 'target principal '-> 'permissions target' and 'requesting principal' -> 'requester' • Added definition of 'target response' omitted in previous draft • Corrected figure 2 in 5.1 • Incorporated requirements from OMA-REQ-GPM-2005-0025R02-added-requirements agreed on CC dated 30th Nov 2005 (added as HLF-18, DEL-2, SEC-2, OSR-16, -17 and modified PMF-2 • Made some corrections from OMA-REQ-GPM-2005-0037-Clarifications_and_open_issues_on_GPM_RD: o Numerous editorial corrections highlighted in 0037 o Corrected 5.3.2.1 o Clarified the text in 4 and 4.2.1 about PCP in MLS • Adjusted OSR-5 as agreed in CC 7th Dec 2005

Document Identifier	Date	Sections	Description
	22 Dec 2005	4, 5, 6	• Changes agreed at Athens F2F Meeting December 2005, (see minutes in OMA-REQ-GPM-2005-0053-MINUTES_12Dec2005-Athens) • Incorporated agreed requirements from OMA-REQ-GPM-2005-0045-clean-up-of-some-requirements o Add Ed. Note to HLF-8 o Added HLF-19. o Modified: HLF-1, HLF-12, PMF-3, ASK-9, OSR-7 and OSR-9 • Incorporated agreed use case (5.5) and requirements (OSR-18 to –25) from OMA-REQ-GPM-2005-0026R03-GPM-Use-Case--Nearest-Restaurant with modifications agreed in Athens • Incorporated changes agreed from OMA-REQ-GPM-2005-0049-comments-to-RD: o Amended section 4.2.1 as proposed o Modified HLF-6, HLF-16, PMF-2, OSR-11, ASK-3 ASK-7, USAB-3 o Removed PermTypes-6
	2 Feb 2006	All	• Incorporated changes from OMA-REQ-GPM-2005-0050R01-Further-Requirements agreed on conference call 11th Jan 06 (see: OMA-REQ-GPM-2006-0002-MINUTES_11Jan2006REQGPM-060111-CC). o Added requirememts to 6.1 (resulted in re-formatting numbering of HLF) o Added requirememts to 6.1.1 (resulted in re-formatting numbering of HLF) o Added requirememts to 6.1.4, 6.1.5, 6.1.6, 6.1.7 and 6.2 • Amended typo in Ask-7 requirement from previous version • Add requirement ‘Ask-8’ which was agreed in Sydney, (see OMA-REQ-GPM-2005-0027-Minutes-Sydney), but were omitted from previous drafts • Incorporated changes from OMA-REQ-GPM-2006-0006-more-requirements agreed on conference calls on 18th Jan 2005 (OMA-REQ-GPM-2006-0008-MINUTES_18Jan2006-CC) and 25th Jan 2006 (OMA-REQ-GPM-2006-0010-MINUTES_25Jan2006REQGPM-060125) o Modified HLF-12 and PMF-2 o Added SEC-5 to –8 o Added requirements to 6.1 o Added OMA-RPT-ApplicationPerformance-V1_0-20031028-A to section 2.2 o Added requirements to 6.2 o Added Ask-9 • Incorporated editorial changes, e.g. capitalised actor terms.
	13 Feb 2006	3.2, 4, 6	• Incorporated new requirements and other changes to existing requirements agreed in Paris, 6th-7th February 2006: o USAB-5 and OSR-32 from OMA-REQ-GPM-2006-0005R01-Registering-enablers/ o Agreed changes from OMA-REQ-GPM-2006-0012-comments-to-RD-20051222 o Agreed changes from OMA-REQ-GPM-2006-0004R04-GPM-ask-6-requirement-rewording o Agreed changes from OMA-REQ-GPM-2006-0003R03-Usage-limits (with HLF- 19 modified as per mail thread on RD-DEV list 07/02/06 o OMA-REQ-GPM-2006-0019-New-notification-requirement

Document Identifier	Date	Sections	Description
	3 Mar 2006	1, 3.2, 5.4, 6.	• Incorporated changes agreed on conference call dated 22nd Feb 2006, i.e: o OMA-REQ-GPM-2006-0024-RD-change-to-OSR05 o OMA-REQ-GPM-2006-0018R01-CR-GPM-1_0-RD-Permission-checking-request-from-a-terminal with agreed changes (HLF-31 and OSR-33) o OMA-REQ-GPM-2006-0026-Ask-Target-and-Ask-Request-definitions o OMA-REQ-GPM-2006-0022R01-GPM-RD-Attribute-Requester-Consumer, with agreed changes • Incorporated changes agreed on conference call dated 1st Mar 2006, i.e: o OMA-REQ-GPM-2006-0011R01-administrator-clarifications, with agreed changes o OMA-REQ-GPM-2006-0028-UC5.4-clarifications
	28 Mar 2006	1, 3.2, 6	• Incorporated changes agreed on conference call dated 8th March 2006, i.e: o OMA-REQ-GPM-2006-0021R01-GPM-RD-notion-of-groups with agreed changes o OMA-REQ-GPM-2006-0032-GPM-RD-Clarifications o OMA-REQ-GPM-2006-0033R01-OSR5-Clarifications with agreed changes • Incorporated changes agreed on conference call dated 15th March, i.e.: o Agreed definition of 'Permissions Rule' according to the first proposal in OMA-REQ-GPM-2006-0038-Definition-Permissions-Rule
	5 Apr 2006	All	• Incorporated changes agreed in Vancouver face-to-face meeting 3rd and 5th April 2006. o OMA-REQ-GPM-2006-0036R02-New-Actor-requirements o OMA-REQ-GPM-2006-0040R01-reword-PMF1 o OMA-REQ-GPM-2006-0042-abbreviation-for-RD o OMA-REQ-GPM-2006-0041R01-about-Ask-Target o OMA-REQ-GPM-2006-0043-for-GPM-RD (with agreed changes) o OMA-REQ-GPM-2006-0044R01-additional-requirement-to-Ask11 o Remove Appendix B and Editor's Notes as per the face-to-face discussions. o Remove Intreroperability Section (no requirements) o Corrected OSR-23 (editor's error) to the wording agreed in Athens (OMA-REQ-GPM-2005-0026R03-GPM-Use-Case--Nearest-Restaurant with modifications agreed in Athens).
	16 Aug	All	• Added HLF-xx from OMA-REQ-GPM-2006-0059--New-requirement-for-GPM-RD-to-address-an-AI as agreed at the Osaka F2F, June 2006. • Applied all changes described in the final RDRR version OMA-RDRR-GPM-V1_0-20060816-D • Ensure consistent use of 'SHALL' instead of 'MUST' in normative sections
	18 Aug	All	Some editorial changes
	24 Aug	All	DSO cleanup + template update prior to Candidate approval following REQ approval in Beijing (OMA-REQ-2006-0149R01)
Candidate Version OMA-RD-GPM-V1_0	28 Sep	All	Conversion to Candidate following approval via TP R&A finishing on 2006-09-27
Draft Version OMA-RD-GPM-V1_0	16 Jan 2009	All	Implemented agreed change: OMA-ARC-GPM-2008-0030R01-CR_CONRR_changes_for_RD Editorial fix: 2009 copyright and cover page
Candidate Version OMA-RD-GPM-V1_0	31 Mar 2009	All	Status changed to Candidate by TP OMA-TP-2009-0117-INP_GPM_V1_0_ERP_for_Candidate_Approval