Global Permissions Management Architecture

Approved Version 1.0 – 22 Nov 2011

Open Mobile Alliance

OMA-AD-GPM-V1_0-20111122-A

Contents

Figures

1. Scope (Informative)

The Global Permissions Management (GPM) enabler provides generic permissions checking and permissions management, which can be used by other resources (e.g. OMA service enablers). This document provides the architecture for the GPM enabler. The role of the GPM enabler is to specify how authorized principals are managing 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), and to specify how permissions checking requests for release of information are defined and processed.

The scope of the Global Permissions Management architecture document is to define the architecture for the Global Permissions Management enabler based on the requirements as described in the Global Permissions Management Requirements Document [GPM-RD]. The scope of this Architecture Document does not include general authorization architecture for verifying access to resources or services.

2. References

2.1 Normative References

[GPM-RD] "Global Permissions Management Requirements", Open Mobile Alliance, OMA-RD_GPM-V1_0, URL:http://www.openmobilealliance.org/

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

[PEEM-AD] "Policy Evaluation, Enforcement and Management Architecture", Open Mobile Alliance, OMA-AD_Policy_Evaluation_Enforcement_Management-V1_0, URL:http://www.openmobilealliance.org/

[PEEM-RD] "Policy Evaluation, Enforcement and Management Requirements", Open Mobile Alliance, OMA-RD_Policy_Evaluation_Enforcement_Management-V1_0, URL: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

[MLS] "Mobile Location Service Requirements", OMA-RD-MLS-V1_0,

Open Mobile Alliance™, http://www.openmobilealliance.org

[OMA-DICT] "Dictionary for OMA Specifications", OMA-ORG-Dictionary-V2_6 URL:http://www.openmobilealliance.org/

[SIMPLE] "Presence SIMPLE Requirements", OMA-RD-Presence_SIMPLE-V1_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 [**Error! Reference source not found.**].

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. (This definition is only valid in the context of GPM).
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 principal requesting access to target attribute(s). E.g. a service invocation that includes target attributes as service parameters.
Permissions Checking	Processing of Permissions Rules
Permissions 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 Permissions Target's attributes. (This actor can be the Permissions Target, an authorised delegate or the GPM Administrator).
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 requester = “is in my domain” and “target attribute” = “my location” then grant.
Permissions Target	Any principal (or group of principals) whose Target Attributes are subject to Permissions Rules
Principal	See [OMA-DICT]
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 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

AD	Architecture Document
GPM	Global Permissions Management
MMS	Multimedia Messaging Service
OMA	Open Mobile Alliance
OSE	OMA Service Environment
PCP	Privacy Checking Protocol
PEEM	Policy Evaluation, Enforcement and Management
PEM-1	PEEM specified callable interface
PEM-2	PEEM specified management interface
RD	Requirements Document
SIP	Session Initiation Protocol
SMS	Short Message Service
WAP	Wireless Application Protocol

4. Introduction (Informative)

Service providers will continue to seek new and flexible ways to offer customised services to their subscribers. This may typically involve for example combining the resources of their 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 complex contexts dictating when and how the data may be used.

In the current service environment framework, some service enablers (e.g. Presence [SIMPLE] and Location [MLS]) already have their own well-defined mechanisms for private information protection; user permissions and their permission checking mechanisms are potentially distributed across multiple sources to address the service-specific solutions required by each enabler. For example, functionality to perform location privacy checking is being specified in [MLS] and includes an optional privacy checking protocol (PCP) defined over an interface between the mobile location server and a separate privacy checking entity. GPM enabler requirements recognize the need to coexist with existing enabler-specific mechanisms for protecting end-user information, and provide in a generic manner at least equivalent functionality with such mechanisms.

The main objective of the Global Permissions Management (GPM) Enabler is to protect the release of information considered private by end-users. In order to enable end-users to effectively control such release, GPM specifies how to define and manage the rules that determine the conditions in which privacy-controlled end-user attributes can be released to a resource that requests them, and how a requester may inquire and obtain a response related to the releasability of the requested information. In a deployment, other resources handle the support of the definition of roles and responsibilities related to managing Permissions Rules.

The Permissions Rules may be associated with specific Permissions Targets and specific attributes, and multiple Permissions Rules may apply in a particular case, such as end-user preferences associated with particular services or resources. A permission rule is comprised of conditions that have to be evaluated, and actions related to the releasability of a Target Attribute. A requester will pass information such as the Target Attribute requested to be released, identity of the requester and identity of the Permissions Target whose Target Attribute is needed, and any other arguments needed in the evaluation of the Permissions Rules. The Permissions Rules are managed by authorized principals [GPM-RD].

4.1 Planned Phases

All the GPM requirements are planned to be fully met in this release. No future releases are currently planned.

Some GPM requirements are dealing with roles and rights assignment/management, listing, suspending and resuming policies and setting priorities. These capabilities are generic in nature and can be resolved in various ways in a solution implementation that do not require interoperability and hence should not be specific to GPM, or developed as part of GPM. The realization of those capabilities is left to the implementation or may become a topic of activity for a future OMA enabler. An implementation for the roles/rights management requirements for Permissions Managers and their delegates is orthogonal to the GPM functionality.

4.2 Security Considerations

Interaction with the GPM enabler implementation may be within the same domain or between different domains. The GPM enabler can be explicitly called by a requesting resource (e.g. other enabler or network element) that may reside in the same domain as the GPM enabler domain and security measures should be considered that allow for secure intra-domain exchanges between the requesting resource and GPM enabler. Alternatively the requesting resource may reside in a different domain from the GPM enabler domain hence security measures should be considered that allow for secure inter-domain exchanges between the requesting resource and the GPM enabler.

Note that different domains may imply: different administrative domains, different security domains and/or the need to traverse insecure networks between the domains.

The GPM enabler may delegate functions to (i.e. make a request to) other resources such as a charging enabler. These other (delegated to) resources may or may not reside in different security or administrative domains and appropriate security measures should be considered for each case. In particular, it is important to be able to ensure that the different resources (GPM and other resources) get access only to the information that they need to know to perform their functions (e.g. payment

details are not made available to authentication resource etc.). When using delegated resources, appropriate key management and encryption may be required and may be specified by the Permissions Rules.

The GPM enabler Permissions Rules are managed (i.e. created, modified, viewed, deleted) through the management interface. It should be possible to authenticate and authorize users of the management interface for both the intra-domain and the inter-domain cases.

5. Architectural Model

5.1 Dependencies

In general, the GPM enabler identifies two main functions in order to support the requirements:

- The Permissions Checking function
- The Permissions Rules management function.

It exposes these functions to other resources via interfaces specified by GPM.

The behaviour of GPM in order to comply with the requirements related to the Permissions Checking function is different than the behaviour of GPM in order to comply with the requirements related to the Permissions Rules management function. There is only loose coupling between the two functions, namely the Permissions Rules need to be accessible to both main functions, but we note here that Permissions Rules storage is out-of-scope for GPM specifications.

This enabler depends on PEEM [PEEM-AD] for its PEEM specified callable interface (a.k.a. PEM-1) and PEEM specified management interface (a.k.a. PEM-2). It also may depend on PEEM [PEEM-AD] for the means to express the Permissions Rules. The GPM Permissions Rules are similar to the PEEM Policy Rules (see [PEEM-AD] and [GPM-RD]). The pattern of requesting a decision from GPM is a callable usage pattern similar to the one defined in PEEM AD (see [PEEM-AD]). The type of information to be passed by a requester to GPM is supported, by the PEEM PEM-1 interface (see [PEEM-AD]). Permissions Rules management is similar to management of policies via PEEM PEM-2 interface (see [PEEM-AD]). This leads to the conclusion that GPM enabler may be realized using PEEM in callable usage pattern, potentially with some changes and/or extensions.

Messages exchanged via GPM.PEM-1 and GPM.PEM-2 between a requester and GPM may themselves be subjected to other application of policies,e.g. to determine whether the requester has appropriate rights to execute the request, or because of the need to issue notifications to other authorized principals at the time such requests are made, or at the time the requests complete. Depending on specific deployment criteria and GPM implementation, this may be realized through the use of the PEEM enabler, in either proxy or callable usage patterns.

5.2 Architectural Diagram

As the GPM enabler is based on the PEEM enabler, this section contains the GPM architectural diagram using PEEM nomenclature [PEEM-AD].

The GPM enabler consists of the Permission Checking and Management component (in Figure 1), which provides two main functions:

- The Permissions Checking function, which is exposed by the GPM.PEM-1 interface.
- The Permissions Rules management function, which is exposed by the GPM.PEM-2 interface.

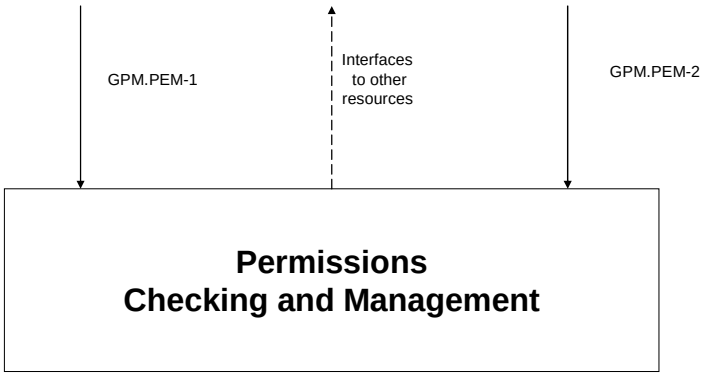

Figure 1. GPM Enabler architecture

Interfaces are based on the requirements that imply interactions with other resources, and are critical for interoperability between those resources. Other requirements point to the behaviour of the architectural component, and may require the use of I2 interfaces in order to be fulfilled (e.g. requirements regarding management of actor roles/rights) but do not necessarily require the specification of I0 interfaces because interoperability between resources is not a GPM issue in this case, and how those roles/responsibility are being assigned does not affect the GPM functionality described in the GPM RD.

5.3 Functional Components and Interfaces

5.3.1 Permissions Checking and Management Component

The Permissions Checking and Management Component has the following features:

- **Processes the Permissions Rules**, i.e. goes through the following steps:
  - Identifies the Permissions Rules associated with the Permissions Checking Request as part of the permission rule processing
  - Evaluates and Processes Permissions Rules using input arguments received from a Permissions Checking Requester (a resource that issues a Permissions Checking Request to GPM enabler) and additional information which it may may acquire from other resources. As part of the processing, there could be an action to ASK (Ask for consent from Ask Target) – an action that the GPM enabler would complete prior to returning the decision to the Permissions Checking Requester.
  - Determines the decisions to return to the Permissions Checking Requester
  - Returns to the Permissions Checking Requester a decision to:
    - GRANT (grant permission to release (a subset of) the Target Attribute(s)) or
    - DENY (deny permission to release Target Attribute(s))

- **Provides the Permissions Rules management functions** to a Management Requester - a resource that issues a request for performing functions such as:
    - creating, reading, deleting, modifying of Permissions Rules
    - associating/disassociating permission rules with attributes, application feature sets, Permissions Targets
- **Notification and Ask Requests:** GPM asks authorized principals for consent on Permissions Checking decisions (e.g. send Ask Request to Ask Target). This may be an action performed during the processing of Permissions Rules. Different mechanisms (though service specific and will not be specified by GPM) can be used to allow setup of subscriptions to notifications, such as:
    - notifying authorized principals when changes occur in permission rules, or protected attributes, or management roles/responsibilities

  When Permissions Managers/Delegates create or modify Permissions Rules (e.g. GPM.PEM-2 input parameters, specific Permissions Rule constructs, etc), the GPM component can identify the need for and the conditions in which notifications need to be sent, and the category of destination (e.g. user, resource). It also can derive from the Permissions Rules most of the destination instances (e.g. actual Permissions Target or actual resource), and can use additional external functions to detect other actual destinations (e.g. I2 or interfaces from other OMA enablers to find the list of Permissions Managers and/or Delegates to be notified). Furthermore, GPM will trigger the notifications to the list of destination targets triggered by the fulfillment of the conditions provided (e.g. before the Permissions Rule are changed, after they are changed or after the changes are deployed and committed).

5.3.2 GPM.PEM-1

This interface is derived from PEM-1 [PEEM-AD], using the PEEM defined process of using templates.

- input parameters in the Permission Checking request
    - Must include all arguments required in the evaluation of the Permissions Rules
        - Permissions Target identity,
        - Requested Permission Target Attributes,
        - Permission Requester identity
        - Target Attribute Consumer
    - May include
        - 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, application specific data, and other relevant GPM Context information (e.g. time of day, number of requests per unit time or other information coming from OMA enablers)
- Output parameters in the Permission Checking response
    - Must include
        - decision rendered by the evaluation of Permissions Rules for each attribute
    - May include
        - If DENY Reason of the decision

5.3.3 GPM.PEM-2

This interface is derived from PEM-2 [PEEM-AD]. It allows Authorized Principals to manage Permissions Rules, i.e. create, read, delete and modify Permission Rules. The authorized principal (the permission manager or permission manager's

delegate) will be able to create permission rules based on any combination of conditions and actions, based on some part (or all) of the following information:

- The Target Attribute Consumer (e.g. the identity of a single end-user or the identities of multiple end-users)
- The Target Attribute Requester (e.g. the application(s) used)
- The intended use of the Target Attributes
- The Permissions Target (i.e. a principal or group of principals).
- Target Attributes
- GPM Context information (e.g. between 9 and 12 o'clock)
- Other information

5.4 Other components and interfaces

In addition to the GPM specified components and interfaces, there are other elements represented in **Error! Reference source not found.** for a better understanding of the architectural diagram. The following is a list of other elements identified in **Error! Reference source not found.** that interact with GPM:

- Interface to other resources
    - Like in the [PEEM-AD, Section 5.3.5], the Interface to other external resources is not specified by GPM. This interface may be used, for example, in the Permissions Rules evaluation process when the evaluation of conditions may require delegation of functions to other resources;
    - In the particular case where an "Ask Request" needs to be performed or when a notification to an authorized principal needs to be sent, the GPM TS does specify the information that is to be exchanged and the binding to one or more protocols.

The "Ask Request" is understood as a message sent to a target, with the expectation of a response. The response is associated to the Ask Request. The notification and the outbound Ask Request can be performed by existing messaging mechanisms, and the key parameters that are to be exchanged over these means are specified in the Technical Specification. One of the aspects here is that the GPM enabler implementation has to ensure correlation between Ask Request and its response. This may involve bindings to: SMS, MMS, WAP PUSH and SIP Push, etc.

5.5 Flows (Informative)

GPM logical architecture is introduced in Section 5.2. This section describes the high-level logical flows for the GPM callable usage pattern. In addition, this section describes the Permissions Rules management flow.

The flows that can happen as a result of processing rules are informative.

5.5.1 GPM Callable Usage Pattern Flow

Figure 2 illustrates the logical flows of GPM enabler in the callable usage pattern.

In the GPM callable usage pattern the Permissions Checking Requester issues a Permissions Checking Request for Permissions Checking (flow#1) to the GPM enabler using the GPM.PEM-1 interface.

- Upon reception of the Permissions Checking Request the GPM enabler identifies the relevant Permission Rules and starts the process of evaluating them. During this process, the GPM enabler may interact with Other Resources using "interface to Other Resources" (flow#2 and #5).
- The GPM enabler will always return a Permissions Checking Response (flow#6) of GRANT and/or DENY to the Permissions Checking Requester, but before that, the GPM enabler itself may execute an Ask Request (flow#3, 4).
- In the latter case, GPM enabler sends Ask Request for consent for the release of Target Attribute (flow#4) to one or more Ask Targets through the "interface to Other Resources" and possibly notifies the Target Attribute Requester

that it is interacting with the Ask Target (s) for consent. The GPM enabler will finally make a decision based on response(s) (flow#4) that are returned from the Ask Target(s) and other context data, and then returns a Permissions Checking Response(flow#6) to the Permission Checking Requester.

- Upon reception of the response the Permissions Checking Requester executes its own action as dictated by the response of GPM.

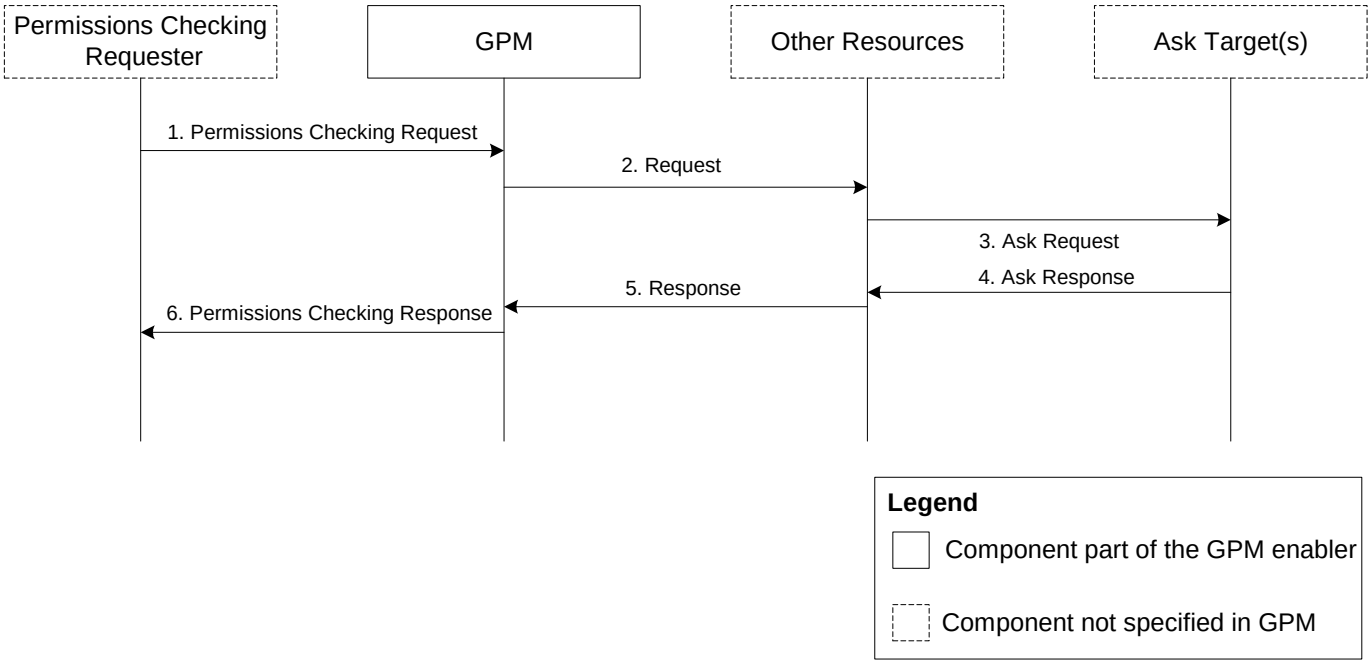

Figure 2. Logical Flow for GPM Callable Usage Pattern

5.5.2 Permissions Rule Management Flow

Figure 3 illustrates the logical flows of the GPM enabler for management of Permissions Rule.

In the GPM Permissions Rule management flow the Management Requester issues a request for Permissions Rule Management (flow#1 in **Error! Reference source not found.**) to the GPM enabler, through the GPM.PEM-2 interface. Upon reception of the request the GPM enabler identifies the type of Permissions Rule Management request (e.g., create, delete, read, modify etc), performs the appropriate function and returns the results to the Management Requester (flow#2 in **Error! Reference source not found.**).

When executing a management operation, management policies may be triggered. This may be used for example to notify some principals or send an Ask Request, and in the latter case possibly await confirmation before proceeding with the management operation.

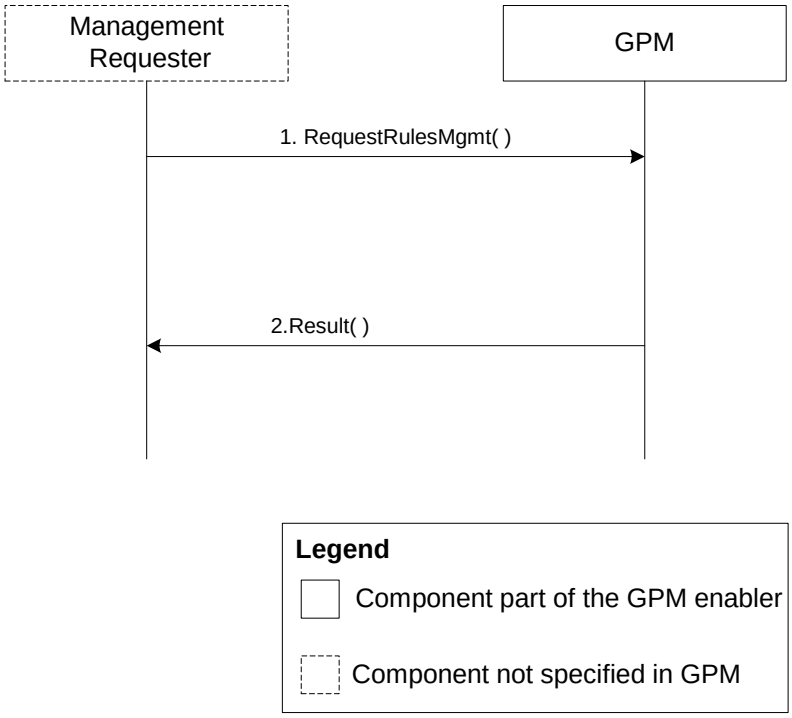

Figure 3. Logical Flow for GPM Permissions Rule management

5.6 Permissions Rules Language

GPM Permissions Rules language will include support for specific names to identify different identities (e.g. Permissions Target, Target Attribute Consumer, resources, etc).

The Permission Rule language used by GPM may include support to express policies that apply to GPM Permission Rule management.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-AD-GPM-V1_0-20111122-A	22 Nov 2011	Approved by TP Ref TP Doc# OMA-TP-2011-0413-INP_GPM_1_0_ERP_for_Final_Approval