Global Permissions Management Technical Specification

Approved Version 1.0 – 22 Nov 2011

Open Mobile Alliance

OMA-TS-GPM-V1_0-20111122-A

Contents

Tables

1. Scope

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 technical specification for the GPM enabler. The scope of this GPM technical specification is to define how the GPM enabler extends the PEM-1 interface for permissions rule checking and the PEM-2 interface for permissions rule management. One or both of the PEL options may be used for Permissions Rules, without extending the PEL options.

2. References

2.1 Normative References

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

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

[GPM INPUT TEMPLATE XSD] XSD definition file for GPM Input Template, Open Mobile Alliance™, OMA-SUP-XSD_GPM_PEM1InputTemplate-V1_0, URL: http://www.openmobilealliance.org/

[GPM OUTPUT TEMPLATE XSD] XSD definition file for GPM Output Template, Open Mobile Alliance™, OMA-SUP-XSD_GPM_PEM1OutputTemplate-V1_0, URL: http://www.openmobilealliance.org/

[PEEM FAULT WSDL] "PEEM WSDL definition file for the PEM-1 Faults", Open Mobile Alliance, OMA-SUP-WSDL-PEM_1_faults-V1_0, URL: http://www.openmobilealliance.org/

[PEEM INPUT TEMPLATE XSD] "PEEM XSD definition file for Policy Input Template", Open Mobile Alliance, OMA-SUP-XSD_PEM_1_GenericInputTemplateData-V1_0, URL: http://www.openmobilealliance.org/

[PEEM OUTPUT TEMPLATE XSD] "PEEM XSD definition file for Policy Output Template", Open Mobile Alliance, OMA-SUP-XSD_PEM_1_GenericOutputTemplateData-V1_0, URL: http://www.openmobilealliance.org/

[PEEM REQ WSDL] "PEEM WSDL definition file for the PEM-1 Request Interface", Open Mobile Alliance, OMA-SUP-WSDL-PEM_1_REQ-V1_0, URL: http://www.openmobilealliance.org/

[PEEM RSP WSDL] "PEEM WSDL definition file for the PEM-1 Response Interface", Open Mobile Alliance, OMA-SUP-WSDL-PEM_1_RSP-V1_0, URL: http://www.openmobilealliance.org/

[PEL TS] "PEEM Policy Expression Language Technical Specification", Open Mobile Alliance, OMA-TS-PEEM_PEL-V1_0, URL:http://www.openmobilealliance.org/

[PEM-1 TS] "Policy Evaluation, Enforcement and Management Callable Interface (PEM-1) Technical Specification", Open Mobile Alliance, OMA-TS-PEEM_PEM1-V1_0, URL:http://www.openmobilealliance.org/

[PEM-2 TS] "Policy Evaluation, Enforcement and Management – Management Interface (PEM-2) Technical Specification", Open Mobile Alliance, OMA-TS-PEEM_PEM2-V1_0, URL:http://www.openmobilealliance.org/

[PXSMS] "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Open Service Access (OSA); Parlay X Web Services; Part 4: Short Messaging, Release 7", 3GPP, 3GPP TS 29.199-4 V7.2.0, URL: http://www.3gpp.org

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

[RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL:http://www.ietf.org/rfc/rfc4234.txt

[RFC4825] "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", J. Rosenberg, March 2007, http://www.ietf.org/rfc/rfc4825.txt

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version 2.7, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_7, URL:http://www.openmobilealliance.org/

[XDM_Shared_Policy] "Shared Policy XDM Specification", Candidate Version 1.0, Open Mobile Alliance™, OMA-TS-XDM_Shared_Policy-V1_0, URL: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. (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 [OMADICT]
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
MSISDN	Mobile Station International Subscriber Directory Number
OMA	Open Mobile Alliance
OSE	OMA Service Environment
PEEM	Policy Evaluation, Enforcement and Management
PEL	Policy Expression Language
PEM-1	PEEM specified callable interface
PEM-2	PEEM specified management interface
RD	Requirements Document
SMS	Short Message Service
TS	Technical Specification
URI	Uniform Resource Identifier
XCAP	XML Configuration Access Protocol
XML	Extensible Markup Language

4. Introduction

The Global Permissions Management (GPM) enabler provides two main functions related to the permission rules for access to attributes of a principal, by other resources (e.g. OMA service enablers, applications):

1. Permissions Checking function
2. Permissions Management function

The GPM Permission Rule Checking interface exposes the Permissions Checking function [GPM AD]]. This interface is derived from PEM-1 [PEM-1 TS], using the PEEM defined process of using templates. This technical specification will define the GPM.PEM-1 Standard GPM Input Template, for the Permission Checking request, and the GPM.PEM-1 Standard GPM Output Template, for the Permission Checking response, along with the required parameters.

The GPM Permission Rule Management interface exposes the Permissions Rules management function [GPM AD]]. This interface is derived from PEM-2 [PEM-2 TS]. This technical specification will define how the Permissions Rules management functions available to a Management Requester are mapped to the PEM-2 Policy Management Operations.

The GPM Permissions Rules themselves conform to PEL [PEL TS].

The Permissions Checking function requests Asks Targets for her/his consent for the release of Target Attributes (i.e. send Ask Request to Ask Target). This may be an action performed during processing of Permissions Rules.

4.1 Version 1.0

Version 1.0 of this GPM technical specification addresses all requirements from [GPM RD], unless otherwise indicated in the [GPM RD].

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.

5. GPM Technical Specification

This chapter contains the specification of the GPM V1.0 enabler's

- Permissions Rule Checking interface which is derived from PEM-1 (see section 5.1);
- Permissions Rule Management interface which is derived from PEM-2 (see section 5.3);
- Ask Consent interface (see section 5.4 and 5.5);
- Permissions Rules' description (see section 5.2).

5.1 Permissions Rule Checking Interface

The GPM Permission Rule Checking interface is derived from PEM-1 [PEM-1 TS], using the PEEM defined process of using templates. This section specifies:

- The GPM extensions to the PEM-1 Standard Input Template, for the Permission Checking request.
  - Header parameters
  - Permission Rule Identification parameters
  - Input parameters
- The GPM extensions to the PEM-1 Standard Output Template, for the Permission Checking response.
  - Header parameters
  - Status parameters.

5.1.1 GPM Input Template

5.1.1.1 Header parameters

The following section defines the values for the GPM Input Template Header parameters.

- The `templateID (type STRING)` for this template SHALL be `OMA_GPM_1.`
- The `templateVersion (type STRING)` for this template SHALL be `V1.0.0.`

5.1.1.2 Permissions Rules Identification Parameters

For internal Permissions Rules (i.e. those managed by the Permissions Rule Management interface / GPM.PEM-2):

- The GPM input template MUST support the Internal Policy Reference Standard PEM-1 Template in order to pass internal Permissions Rules by reference.
- In addition the GPM input template MAY optionally support the External Policy Reference Standard GPM.PEM-1 Template.

5.1.1.3 Input Parameters

The GPM input template for GPM.PEM-1 specifies the following input parameters:

- `permissionsTargetID (type ARRAY of URI)`: Permissions Target identity (one or more), the principal (or group of principals) whose Target Attributes are being requested.
- `permissionsRequesterID (type STRING)`: Permission Requester identity, the principal requesting the permission to GPM for accessing the Target Attributes of the Permissions Target.

- `targetAttributeConsumer (type STRUCT):` information pertaining to the Target Attribute Consumer, the 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.
  - `consumerID (type ARRAY of URI)`: **one or more** Target Attribute Consumer identity/ies (i.e. end-user)
  - `serviceID (type STRING):` identity of the service or application, that requests the Target Attributes, that is being used by the end-user (ConsumerID).
  - `serviceProviderID (type STRING)(optional):` identity of the Service Provider that offers this service or application.
- `requestedAttributes (type ARRAY of STRUCT)`: The requested Permission Target attribute(s) (one or more), information pertaining to Permissions Target(s) for which access 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. This is a sequence of:
  - `targetAttributeName (type STRING)`: The name of the Target Attribute.
  - `targetAttributeUse (type STRING) (optional)`: The intended use of the Target Attribute. If present, the parameter indicates for which purpose the application is requesting access to the attribute (e.g. to modify a Target Attribute, or sharing medical data with doctors but not students)
- `contextInformation (type STRUCT) (optional)`: If present, the parameter indicates contextual information pertaining to the GPM Target Request. Examples of contextual information include e.g. 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). This is a sequence of:
  - `contextInfoType (type STRING)`: Indicating the data type of the GPM Context information (data type MUST be one of the PEM-1 parameters data types specified in [PEM-1 TS])
  - `contextInfo (type STRING)`: GPM Context information of type `contextInfoType`.

The GPM input template is specified as a file named `GPM_PEM1InputTemplate-v1_0.xsd` with the following contents [GPM INPUT TEMPLATE XSD]:

```
<?xml version="1.0" encoding="UTF-8"?>
 <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:pem1-i="urn:oma:xml:peem:pem1-input-template:1.0"
  xmlns="urn:oma:xml:gpm:pem1-input-template:1.0"
  targetNamespace="urn:oma:xml:gpm:pem1-input-template:1.0">

 <xs:import namespace="urn:oma:xml:peem:pem1-input-template:1.0"
    schemaLocation="http://www.openmobilealliance.org/tech/profiles/PEM_1_GenericInputTemplateData-v1_0.xsd"/>

  <xs:complexType name="GPM_pem1InputTemplate-V1_0Type">
   <xs:complexContent>
    <xs:extension base="pem1-i:inputTemplateType">
     <xs:sequence>

      <xs:element name="permissionsTargetID" minOccurs="1" maxOccurs="unbounded">
       <xs:complexType>
        <xs:simpleContent>
         <xs:extension base="xs:anyURI">
          <xs:attribute name="permissionsTargetIDType" type="xs:string"/>
         </xs:extension>
        </xs:simpleContent>
```

```
      </xs:complexType>
    </xs:element>

    <xs:element name="permissionsRequesterID">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
            <xs:attribute name="permissionsRequesterIDType" type="xs:string"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>

    <xs:element name="targetAttributeConsumer">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="consumerID" type="xs:anyURI" minOccurs="1"
            maxOccurs="unbounded"/>
          <xs:element name="serviceID" type="xs:string"/>
          <xs:element name="serviceProviderID" type="xs:string" minOccurs="0"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>

    <xs:element name="requestedAttributes" minOccurs="1" maxOccurs="unbounded" >
      <xs:complexType>
        <xs:sequence>
          <xs:element name="targetAttributeName" type="xs:string"/>
          <xs:element name="targetAttributeUse" type="xs:string" minOccurs="0"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>

    <xs:element name="contextInformation" minOccurs="0">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="contextInfoType" type="xs:string"/>
          <xs:element name="contextInfo" type="xs:string"/>
        </xs:sequence>
      </xs:complexType>
    </xs:element>

  </xs:sequence>
 </xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:schema>
```

5.1.2 GPM Output Template

5.1.2.1 Header parameters

The following section defines the values for the GPM Output Template Header parameters.

- The `templateID` for this template SHALL be `OMA_GPM_2.`

- The `templateVersion` for this template SHALL be `V1.0.0.`

5.1.2.2 Status Parameters

The GPM output template MUST support the Output Status Standard PEM-1 Template, and describes a single output element, `permissionsResult`, with the following parameter values:

- **Decision**: The decision rendered by the evaluation of Permissions Rules for each Target Attribute passed in the Permission Checking Request. The possible values for the **Decision** attribute, according to [GPM AD]], are "GRANT" and "DENY". The PEM-1 specification (see [PEM-1 TS], appendix D) defines codes for "ALLOW", "DENY" and "SUCCESS" status categories. The scope of "ALLOW" in PEM-1 covers the interpretation of "GRANT" in GPM, and therefore the "ALLOW" codes defined by PEM-1 can be re-used for a GPM "GRANT" decision, which are mapped to specific "ALLOW" codes. Hence, the GPM **Decision** attribute values map to the following PEM-1 Output Status template values (see [PEM-1 TS], appendix D) as follows:
  - The GPM **Decision** attribute with value "GRANT" maps to the PEM-1 Output Template parameter `statusCode (type INTEGER)` with value 2101; in this case no additional Decision parameters have to be passed. This type of GRANT decision is used when in the request one `ConsumerID` (only) has been indicated. The GRANT decision pertains to the indicated (in the request) `ConsumerID(s)` in combination with all requested `targetAttributeName`(s) as indicated in the Input Parameters (5.1.1.3).
  - The GPM **Decision** attribute with value "GRANT" maps to the PEM-1 Output Template parameter `statusCode (type INTEGER)` with value 2102; in this case additional parameters are passed. This type of GRANT decision is used when either a subset of the `ConsumerID`(s) has been granted and/or access to a subset of the `targetAttributeName`(s) has been granted. The GRANT decision pertains to the indicated `ConsumerID`(s) in the output, that are granted access to all explicitly indicated `targetAttributeName`(s), as indicated in the Output Parameters (5.1.2.3).
  - The GPM **Decision** attribute with value "DENY" maps to the PEM-1 Output Template parameter `statusCode` (type INTEGER) with value 2401, in case no additional parameters have to be passed.
  - The GPM **Decision** attribute with value "DENY" maps to the PEM-1 Output Template parameter `statusCode (type INTEGER)` with value 2402 in case additional parameters have to be passed..
- **Reason** (*optional*): In the case of either GRANT or DENY, an optional reason for the decision may be passed in the Permission Checking Response, regardless of the use of specific **Decision** codes used.The following PEM-1 Output Status template value (see [PEM-1 TS], appendix D) mapping applies:
  - The GPM **Reason** attribute maps to the PEM-1 Output Template parameter `statusText (type STRING)`.

5.1.2.3 Output Parameters

The GPM output template for GPM.PEM-1 specifies the following parameters:

- `targetAttributeConsumer (type STRUCT):` information pertaining to the Target Attribute Consumer, the principal consuming/making use of a Target Attribute (e.g. for a map showing the location of the Permissions Target). This parameter MUST be supplied in case of a GRANT decision with value 2102, when a subset of the `consumerID`(s) is granted access.
  - `consumerID (type ARRAY of URI)`: one or more Target Attribute Consumer identity/ies (i.e. end-user).
  - `serviceID (type STRING):` identity of the service or application, that requests the Target Attributes, that is being used by the end-user (ConsumerID).
  - `serviceProviderID (type STRING) (optional)`: identity of the Service Provider that offers this service or application.

- `requestedAttribute (type ARRAY of STRUCT)`: The requested Permission Target attribute(s) (one or more). This parameter MUST be supplied in case of a GRANT decision with value 2102, when a subset of the `targetAttributeName`(s) is granted access to. This is a sequence of:
  - `targetAttributeName (type STRING)`: The name of the Target Attribute.
  - `targetAttributeUse (type STRING) (optional)`: The intended use of the Target Attribute.

The GPM output template is specified as a file named `GPM_PEM1OutputTemplate-v1_0.xsd` with the following contents [GPM OUTPUT TEMPLATE XSD]:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:pem1-o="urn:oma:xml:peem:pem1-output-template:1.0"
  xmlns="urn:oma:xml:gpm:pem1-output-template:1.0"
  targetNamespace="urn:oma:xml:gpm:pem1-output-template:1.0">

<xs:import namespace="urn:oma:xml:peem:pem1-output-template:1.0"
    schemaLocation="http://www.openmobilealliance.org/tech/profiles/PEM_1_GenericOutputTemplateData-v1_0.xsd" />

  <xs:complexType name="GPMOutputTemplateType">
    <xs:complexContent>
      <xs:extension base="pem1-o:outputTemplateType">
        <xs:sequence>
          <xs:element name="permissionsResult">
            <xs:complexType>
              <xs:attribute name="decision">
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="GRANT"/>
                    <xs:enumeration value="DENY"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:attribute>
              <xs:attribute name="reason" type="xs:string" use="optional"/>
            </xs:complexType>
          </xs:element>

          <xs:element name="targetAttributeConsumer">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="consumerID" type="xs:anyURI" maxOccurs="unbounded"/>
                <xs:element name="serviceID" type="xs:string"/>
                <xs:element name="serviceProviderID" type="xs:string" minOccurs="0"/>
              </xs:sequence>
            </xs:complexType>
          </xs:element>

          <xs:element name="requestedAttributes" maxOccurs="unbounded">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="targetAttributeName" type="xs:string"/>
                <xs:element name="targetAttributeUse" type="xs:string" minOccurs="0"/>
              </xs:sequence>
            </xs:complexType>
```

```
        </xs:element>

      </xs:sequence>
    </xs:extension>
  </xs:complexContent>
 </xs:complexType>
</xs:schema>
```

5.2 Permissions Rules

A GPM permission rule (i.e. a PEEM policy) SHALL be represented as an XML document. The schema for such a GPM permission rule (i.e. a PEEM policy) SHALL conform to [PEL TS]. One or both of the PEL options (i.e. Ruleset Framework and/or Business Processes) may be used for Permissions Rules.

The optional function call extension to the PEEM Ruleset [PEL TS] is considered NORMATIVE for this GPM specification: the PEEM Ruleset function call extension MUST be supported in order to be able to realize the user consent interaction.

When reusing the GPM enabler in another specification or as part of a solution and if the GPM enabler needs to call out to other resources (including other enablers), then the GPM function call extension (see above) can be used to implement such a callout to a resource (e.g. to retrieve location information). It is advised to not standardize such callout as typically such callout will be on implementation (e.g. java) level and not on external interfacing level. One may choose instead to specify which standardized interface should be by used by GPM to retrieve the information from the other resource (e.g. location information).

In case GPM needs to work with external documents that for instance capture the privacy settings of end-users or employees, such as e.g. a document that expresses such preferences as per the standardized [XDM_Shared_Policy] or e.g. a potential future location authorization policy, then it is assumed that such documents are defined outside this GPM specification.

5.3 Permissions Rule Management Interface

The GPM Permission Rule Management interface is derived from PEM-2 [PEM-2 TS]. This implies the following:

- The PEM-2 interface SHALL be used to manipulate GPM permission rules [PEM-2 TS].
- The GPM Permissions Rule identifier (i.e. Policy identifier) SHALL be an XCAP URI [RFC4825].
- The GPM Permissions Rule Management interface SHALL use the PEM-2 Application Usage as specified in [PEM-2 TS].

In addition, and in accordance with [PEM-2 TS], it SHALL be possible to use a Permissions Target identifier as a path segment of the document selector of the XCAP URI (see [RFC4825]) to identify the path to a Permission Rule. Note that this does not imply that the Permissions Target must be the root selector. The Permissions Target tree MAY be a sub-tree of another tree. It does imply the support of a directory structure where one or more Permissions Rules are put as a sub-tree of the Permissions Target tree.

5.3.1 Permissions Rules management functions

The Permissions Rules management functions available to a Management Requester include the ability to create, read, delete, modify Permissions Rules [GPM-AD]. GPM.PEM-2 defines four Policy Management Operations [PEM-2]. This section defines how the Permissions Rules management functions map to the PEM-2 Policy Management Operations:

- The PEM-2 Create Policy operation defined in [PEM-2 TS] SHALL be used to “create” a permission rule.
- The PEM-2 Modify Policy operation defined in [PEM-2 TS] SHALL be used to “modify” a permission rule.
- The PEM-2 Delete Policy operation defined in [PEM-2 TS] SHALL be used to “delete” a permission rule.

- The PEM-2 View Policy operation defined in [PEM-2 TS] SHALL be used to "read" a permission rule.

In the [GPM RD] there is a mentioning of suspending and resuming of policies. These type of management actions are perceived of a different nature than the ones described above; the suspend/resume operations target the activation/deactivation of the managed policies to be carried out in an operation modus in a policy processing implementation (as opposed to managing; creating, modifying, deleting them). In a solution such activation/deactivation operations can be addressed with management tools; the suspend/resume operations are considered out of scope.

In the [GPM RD] there is a mentioning of listing of policies. This management action can be addressed with management tools that make use of the GPM.PEM-2 View Policy operation [PEM-2 TS]; the list operation is considered out of scope.

In the [GPM RD] there is a mentioning of management mechanisms to prioritize permissions rules. It is noted here that there are various ways to implement prioritization systems that do not require an explicit priority management interface; for example the permissions processing entity could derive the priority from other pieces of information that are part of the permissions rules and/or from the context information. As such, the mechanism to explicitly manage prioritization of permissions rules is considered out of scope.

5.4 Ask Consent Interface

The Ask Consent interface consists of the following messages:

- a request to the Ask Target for its consent (5.4.1);
- the response from the Ask Target (5.4.2);
- an optional verification to the Ask Target about the implications of its consent and how these may be undone (5.4.3).

5.4.1 Ask Target for Consent

The request message, to ask the Ask Target for its consent, MUST support the following parameters, unless indicated otherwise:

- `AskTargetID (type URI)`; Ask Target identity, the principal whose consent is being requested.
- `ConsumerID (type URI)`: Target Attribute Consumer identity (i.e. end-user)
- `RequestedAttributes (type ARRAY of STRUCT)`: The requested Permission Target attribute(s) (one or more). This is a sequence of:
  - `targetAttributeName (type STRING)`: The name of the Target Attribute;
  - `targetAttributeUse (type STRING) (optional)`: The intended use of the Target Attribute.
- `ConsentPeriod (type INT)`: The period during which the Ask Target's consent will be valid. The period will start immediately after a positive Ask Target response has been received (e.g. a amount of hours or days).
- `ConsentCommands (type STRING)`: The Ask Target can use these commands in its response (e.g. "Allow", "Deny", "Revoke" or "yes", "no", "undo", etc.).
- And at least one of the following parameters MUST be supported:
  - `SessionID (type STRING)`: An identifier that can be used to correlate the response message with the request message.
  - `ServiceProviderID (type STRING)`; identity of the Service Provider that offers this service or application.
  - `ServiceID` (type `STRING`); identity of the service or application, that requests the Target Attributes, that is being used by the end-user (ConsumerID). The ServiceID can contain the fullfledged name of the service/application, e.g.

"Ultimate Bargain Finder.com". Depending on the binding, the ShortServiceID may be sent instead; this will be outlined in the bindings section.

- `ShortServiceID (type STRING)`; shortened version of the identity of the service or application, that requests the Target Attributes, that is being used by the end-user (ConsumerID). The ShortServiceID contains an abbreviated name of the service/application, e.g. "UBF" and can be used in particular bindings, such as SMS (where it may be assumed that the Ask Target's terminal display may have limited capabilities).

5.4.2 Ask Target response

The Ask Target response to the request for consent MUST support the following parameters, unless indicated otherwise:

- `ConsentCommand (type STRING)`: The Ask Target can use these commands in its response (e.g. "Allow", "Deny", or "yes", "no", etc.).
- And at least one of the following parameters MUST be supported:
  - `SessionID (type STRING)`: An identifier that can be used to correlate the response message with the request message.
  - `ServiceProviderID (type STRING)`; identity of the Service Provider that offers this service or application.
  - `ServiceID (type STRING)`; identity of the service or application, that requests the Target Attributes, that is being used by the end-user (`ConsumerID`). The `ServiceID` can contain the fullfledged name of the service/application, e.g. "Ultimate Bargain Finder.com". Depending on the binding, the `ShortServiceID` may be sent instead; this will be outlined in the bindings section.
  - `ShortServiceID (type STRING)`; shortened version of the identity of the service or application, that requests the Target Attributes, that is being used by the end-user (`ConsumerID`). The `ShortServiceID` contains an abbreviated name of the service/application, e.g. "UBF" and can be used in particular bindings, such as SMS (where it may be assumed that the Ask Target's terminal display may have limited capabilities).

Notice that the Ask Target response may immediately follow the request, for instance when the Ask Target allows/grants or denies a Target Attribute Consumer to retrieve her location (e.g. ALLOW 0001 or DENY 0001).

Another possibility is that the Ask Target initially allows/grants access to her attributes and later on decides to revoke that decision; the Ask Target can then send an additional Ask Target response to undo the initial allow/grant (e.g. "Revoke 0001"); see section 5.4.3 and 5.4.4.

5.4.3 Verification to Ask Target (Optional)

The verification message to the Ask Target is meant to inform the Ask Target how to undo an already sent allow/grant Ask Target response. In this case any of the parameters as specified in section 5.4.1 MAY be supported, but at least the relevant ConsentCommands (type STRING) SHOULD be supported as well as at least one of the following parameters SHOULD be supported:

- `SessionID (type STRING)`: An identifier that can be used to correlate the response message with the request message.
- `ServiceProviderID (type STRING)`; identity of the Service Provider that offers this service or application.
- `ServiceID (type STRING)`; identity of the service or application, that requests the Target Attributes, that is being used by the end-user (ConsumerID). The ServiceID can contain the fullfledged name of the service/application, e.g. "Ultimate Bargain Finder.com". Depending on the binding, the ShortServiceID may be sent instead; this will be outlined in the bindings section.
- `ShortServiceID (type STRING)`; shortened version of the identity of the service or application, that requests the Target Attributes, that is being used by the end-user (ConsumerID). The ShortServiceID contains an

abbreviated name of the service/application, e.g. “UBF” and can be used in particular bindings, such as SMS (where it may be assumed that the Ask Target’s terminal display may have limited capabilities).

5.4.4 Response to Verification (Optional)

The definition of the Ask Target response to the Verification message is the same as the Ask Target response (see section 5.4.2). There is a difference in usage: the returned `ConsentCommand` will have a different value than in the earlier sent Ask Target response (e.g. “Allow”), such as for instance “Revoke”.

5.4.5 Data Types

The table below represents the supported data types:

Ask Consent Interface Data Types	Description
int	4 byte signed: -2147483648 to 2147483647
float	Floating-point number, 3.4e +/- 38 (7 digits)
array	Arrays (lists) of objects of a given type (e.g. arrays if integers, or characters, or floats).
function	A type that returns object of a given type.
struct	A complex type that contains a sequence of objects of different types.
string	A sequence (array) of characters
bool	A type that can only take the values TRUE or FALSE
URI	A type derived from string, with a well-specified structure as per [**Error! Reference source not found.**]

Table 1: Ask Consent Interface parameters data types

5.5 Ask Consent Interface Bindings

GPM enabler implementations SHALL offer at least one of the following bindings for the Ask Consent Interface:

- SOAP; reuse Parlay X Short Messaging [PXSMS], see section 5.5.1.

Other bindings are not precluded, and may be described in future versions of this specification.

5.5.1 Parlay X Short Messaging Interface Binding

5.5.1.1 Ask Target for Consent

The `SendSmsRequest` message as specified per [PXSMS] SHALL be used to request the Ask Target for consent; the `AskTargetID` as specified in section 5.4.1 (the document you are reading) maps to the `SendSmsRequest Adresses`-parameter in [PXSMS], e.g. the MSISDN.

The `SessionID` and `ServiceID` or `SessionID` and `ShortServiceID` as specified in section 5.4.1 (the document you are reading) maps to the `SendSmsRequest SenderName` parameter in [PXSMS] coded as a concatenated string, e.g. "UBF99887766" or "33399887766", where the initial part of the string is the `ServiceID` or `ShortServiceId` of the service and the latter part the `SessionID`. In the example UBF or 333 is the `ShortServiceID` and the 99887766 is the `SessionID`. The [PXSMS] web service implementation takes care of mapping this information into the actual SMS message that is to be sent by the underlying enabler to the Ask Target; this mapping is out of scope of this specification.

All other parameters indicated in section 5.4.1 are to be described as part of the textstring value of the SendSmsRequest Message-parameter in [PXSMS] as indicated per the following list:

- The ConsumerID, TargetAttributeName, ConsentPeriod, ConsentCommands MUST be described as part of the textstring value of the SendSmsRequest Message-parameter

- The TargetAttributeUse MAY OPTIONALLY be described as part of the textstring value of the SendSmsRequest Message-parameter.

- At least one of the parameters SessionID, ServiceProviderID, ServiceID, ShortServiceID, MAY OPTIONALLY be described as part of the textstring value of the SendSmsRequest Message-parameter.

- Additional descriptive freeformatted text MAY OPTIONALLY be described as part of the textstring value of the SendSmsRequest Message-parameter (to allow customization of the message).

The exact position and order of the parameters within the SendSmsRequest Message-parameter are not specified, to allow for sufficient freedom to facilitate each GPM provider to be able to distinguish itself or particular applications that it supports.

5.5.1.2 Ask Target Response

The NotifySmsReceptionRequest or the GetReceivedSMS message as specified per [PXSMS] MUST be used to return the Ask Target response to the GPM enabler:

- The ConsentCommand MUST be described as part of the textstring value of the NotifySmsReceptionRequest Message-parameter.

- The SmsServiceActivationNumber SHALL be used to correlate the response with the previously sent Ask Target Request. The SmsServiceActivationNumber parameter contains the ShortServiceID or ServiceID combined with the SessionID as described above.

- At least one of the parameters SessionID, ServiceProviderID, ServiceID, ShortServiceID, MAY OPTIONALLY be described as part of the textstring value of the NotifySmsReceptionRequest Message-parameter.

5.5.1.3 Verification to Ask target (Optional)

The SendSmsRequest message as specified per [PXSMS] MAY be used to send a Verification message to the Ask Target response; any of the parameters as specified in section 5.5.1.1 MAY be supported, but at least the relevant ConsentCommands SHOULD be supported as well as at least one of the following parameters SHOULD be supported: SessionID, ServiceProviderID, ServiceID, ShortServiceID.

5.5.1.4 Response to Verification (Optional)

The NotifySmsReceptionRequest or the GetReceivedSMS message as specified per [PXSMS] MAY be used to return the Ask Target response to the GPM enabler; the definition of the Ask Target response to the Verification message is the same as the Ask Target response (see section 5.5.1.2). There is a difference in usage: the returned ConsentCommand will have a different value than in the earlier sent Ask Target response (e.g. “Allow”), such as for instance “Revoke”.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-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

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [SCRRULES].

B.1 SCR for Permissions Rule Checking

B.1.1 SCR for Permissions Rule Checking Client Request

Item	Function	Reference	Requirement
GPM-PRC-REQ-C-001-M	Support GPM.PEM-1 interface [GPM TS]	5.1	PEEM-PEM1: MCF (see [PEM-1 TS])
GPM-PRC-REQ-C-002-M	Support GPM specified PEM-1 extensions	5.1	
GPM-PRC-REQ-C-003-M	Support Header parameters	5.1.1.1	
GPM-PRC-REQ-C-004-M	Support Internal Policy Reference Standard GPM.PEM-1 Template	5.1.1.2	
GPM-PRC-REQ-C-005-O	Support Internal Policy Reference Standard GPM.PEM-1 Template	5.1.1.2	
GPM-PRC-REQ-C-006-M	Support Permission Rule Checking Input parameters	5.1.1.3	

B.1.2 SCR for Permissions Rule Checking Client Response

Item	Function	Reference	Requirement
GPM-PRC-RES-C-001-M	Support GPM.PEM-1 interface [GPM TS]	5.1	PEEM-PEM1: MCF (see [PEM-1 TS])
GPM-PRC-RES-C-002-M	Support GPM specified PEM-1 extensions	5.1	
GPM-PRC-RES-C-003-M	Support Header parameters	5.1.2.1	
GPM-PRC-RES-C-004-M	Support Permission Rule Checking Status parameters	5.1.2.2	
GPM-PRC-RES-C-005-M	Support Permission Rule Checking Output Parameters	5.1.2.3	

B.1.3 SCR for Permissions Rule Checking Server Request

Item	Function	Reference	Requirement
GPM-PRC-REQ-S-001-M	Support GPM.PEM-1 interface [GPM TS]	5.1	PEEM-PEM1: MSF (see [PEM-1 TS])
GPM-PRC-REQ-S-002-M	Support GPM specified PEM-1 extensions	5.1	
GPM-PRC-REQ-S-003-M	Support Header parameters	5.1.1.1	
GPM-PRC-REQ-S-004-M	Support Internal Policy Reference Standard GPM.PEM-1 Template	5.1.1.2	
GPM-PRC-REQ-S-005-O	Support Internal Policy Reference Standard	5.1.1.2	

Item	Function	Reference	Requirement
	GPM.PEM-1 Template		
GPM-PRC-REQ-S-006-M	Support Permission Rule Checking Input parameters	5.1.1.3	

B.1.4 SCR for Permissions Rule Checking Server Response

Item	Function	Reference	Requirement
GPM-PRC-RES-S-001-M	Support GPM.PEM-1 interface [GPM TS]	5.1	PEEM-PEM1: MSF (see [PEM-1 TS])
GPM-PRC-RES-S-002-M	Support GPM specified PEM-1 extensions	5.1	
GPM-PRC-RES-S-003-M	Support Header parameters	5.1.2.1	
GPM-PRC-RES-S-004-M	Support Permission Rule Checking Status parameters	5.1.2.2	
GPM-PRC-RES-S-005-M	Support Permission Rule Checking Output Parameters	5.1.2.3	

B.2 SCR for Permissions Rule Management

B.2.1 SCR for Permissions Rule Management Client

Item	Function	Reference	Requirement
GPM-PRM-C-001-M	Support GPM.PEM-2 interface [GPM TS]	5.3, 5.3.1	PEEM-PEM2: MCF (see [PEM-2 TS])
GPM-PRM-C-002-M	Support Permissions Target Identifier as a path segment in the request	5.3	

B.2.2 SCR for Permissions Rule Management Server

Item	Function	Reference	Requirement
GPM-PRM-S-001-M	Support GPM.PEM-2 interface [GPM TS]	5.3, 5.3.1	PEEM-PEM2: MSF (see [PEM-2 TS])
GPM-PRM-S-002-M	Support Permissions Target Identifier as a path segment in the request	5.3	

B.3 SCR for Ask Consent

B.3.1 SCR for Ask Consent Client

Item	Function	Reference	Requirement
GPM-ASKCONSENT-C-001-M	Support request message to ask the Ask Target for its consent	5.4, 5.4.1	
GPM-ASKCONSENT-C-002-M	Support the response of the Ask Target to the request for consent	5.4, 5.4.2	
GPM-ASKCONSENT-C-003-O	Support verification message to the Ask Target	5.4, 5.4.3	
GPM-ASKCONSENT-C-004-O	Support the response of the Ask target to the verification message to the	5.4, 5.4.4	

Item	Function	Reference	Requirement
	Ask Target		
GPM-ASKCONSENT-C-005-M	Protocol binding	5.5	GPM-ASKCONSENTBIND: MCF AND GPM-ASKCONSENTBIND: OCF

B.3.2 SCR for Ask Consent Server

Item	Function	Reference	Requirement
GPM-ASKCONSENT-S-001-M	Support request message to ask the Ask Target for its consent	5.4, 5.4.1	
GPM-ASKCONSENT-S-002-M	Support the response of the Ask Target to the request for consent	5.4, 5.4.2	
GPM-ASKCONSENT-S-003-O	Support verification message to the Ask Target	5.4, 5.4.3	
GPM-ASKCONSENT-S-004-O	Support the response of the Ask target to the verification message to the Ask Target	5.4, 5.4.4	
GPM-ASKCONSENT-S-005-M	Protocol binding	5.5	GPM-ASKCONSENTBIND: MSF AND GPM-ASKCONSENTBIND: OSF

B.4 SCR for Ask Consent interface binding

B.4.1 SCR for Ask Consent interface binding Client

Item	Function	Reference	Requirement
GPM-ASKCONSENTBIND-C-001-M	SOAP protocol binding, using Parlay X Short Messaging [PX SMS]	5.5	
GPM-ASKCONSENTBIND-C-002-M	Support request message to ask the Ask Target for its consent	5.5.1.1	
GPM-ASKCONSENTBIND-C-003-M	Support the response of the Ask Target to the request for consent	5.5.1.2	
GPM-ASKCONSENTBIND-C-004-O	Support verification message to the Ask Target	5.5.1.3	
GPM-ASKCONSENTBIND-C-005-O	Support the response of the Ask target to the verification message to the Ask Target	5.5.1.4	

B.4.2 SCR for Ask Consent interface binding Server

Item	Function	Reference	Requirement
GPM-ASKCONSENTBIND-S-001-M	SOAP protocol binding, using Parlay X Short Messaging [PX SMS]	5.5	
GPM-ASKCONSENTBIND-S-002-M	Support request message to ask the Ask Target for its consent	5.5.1.1	
GPM-	Support the response of the	5.5.1.2	

Item	Function	Reference	Requirement
ASKCONSENTBIND-S-003-M	Ask Target to the request for consent		
GPM-ASKCONSENTBIND-S-004-O	Support verification message to the Ask Target	5.5.1.3	
GPM-ASKCONSENTBIND-CS005-O	Support the response of the Ask target to the verification message to the Ask Target	5.5.1.4	

B.5 SCR for GPM Server supporting Permission Rules

Item	Function	Reference	Requirement
GPM-PR-S-001-M	Support of XML schema as defined in [PEL TS] to represent a permission rule	5.2	PEEM-PEL-S-001-M (see [PEL TS])
GPM-PR-S-001-M	Support of function call extension to the PEEM Ruleset PEL [PEL TS]	5.2	