



Guidelines for RESTful Network APIs

Approved – 27 Feb 2014

Open Mobile Alliance

OMA-WP-Guidelines_for_RESTful_Network_APIs-20140227-A

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2014 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

- 1. SCOPE 4
- 2. REFERENCES..... 5
- 3. TERMINOLOGY AND CONVENTIONS 6
 - 3.1 CONVENTIONS 6
 - 3.2 DEFINITIONS..... 6
 - 3.3 ABBREVIATIONS 6
- 4. INTRODUCTION 7
- 5. PRINCIPLES FOR DEFINING RESTFUL NETWORK APIS IN OMA 8
 - 5.1 API DOCUMENTATION..... 10
 - 5.1.1 API Data Types..... 10
 - 5.2 ERROR HANDLING 11
 - 5.3 EXAMPLES 12
 - 5.4 COMMON DATA FORMATS..... 12
 - 5.4.1 XML..... 12
 - 5.4.2 JSON..... 12
 - 5.4.3 Application/x-www-form-urlencoded..... 13
 - 5.5 INTERNATIONALIZATION 13
 - 5.6 BACKWARDS COMPATIBILITY 14
 - 5.6.1 XML based APIs..... 14
 - 5.6.2 JSON based APIs 15
 - 5.7 FORWARD COMPATIBILITY, EXTENSIBILITY 16
 - 5.7.1 XML based APIs..... 16
 - 5.7.2 JSON based APIs 17
 - 5.8 ENCODING AND SERIALIZATION DETAILS FOR MIME FORMAT..... 17
 - 5.9 LIGHT-WEIGHT RESOURCES 19
- APPENDIX A. CHANGE HISTORY (INFORMATIVE) 24
- APPENDIX B. PRINCIPLES FOR DEFINING REST BINDINGS FOR PARLAY X WEB SERVICE APIS (INFORMATIVE) 25

Figures

- Figure 1 Clients using older versions of the API..... 14
- Figure 2 Backwards compatibility for operations..... 15
- Figure 3 Upgraded servers returning a response to legacy clients 16
- Figure 4 New versions of clients making requests to existing, non-upgraded servers 16

Tables

- Table 1: API Data Type Example..... 11

1. Scope

This White Paper (WP) contains guidelines for the development of RESTful Network API specifications in OMA.

2. References

- [Fielding] “Architectural Styles and the Design of Network-based Software Architectures”, Roy Fielding, 2000, [URL:http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm](http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm)
- [HTML_FORMS] “HTML Forms”, W3C Recommendation, [URL:http://www.w3.org/TR/html401/interact/forms.html](http://www.w3.org/TR/html401/interact/forms.html)
- [JSON] Java Script Object Notation, [URL:http://www.json.org/](http://www.json.org/)
- [OMADICT] “Dictionary for OMA Specifications”, Version 2.8, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_8, [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [REST_NetAPI_Common]
- [REST_NetAPI_Common] “Common definitions for RESTful Network APIs”, Open Mobile Alliance™, OMA-TS-REST_NetAPI_Common-V1_0, [URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [RFC1738] “Uniform Resource Locations”, T. Berners-Lee, L. Masinter, M. McCahill, December 1994, [URL:http://www.ietf.org/rfc/rfc1738.txt](http://www.ietf.org/rfc/rfc1738.txt)
- [RFC2046] “Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types”, N. Freed, N. Borenstein, November 1996, [URL:http://www.ietf.org/rfc/rfc2046.txt](http://www.ietf.org/rfc/rfc2046.txt)
- [RFC2387] “The MIME Multipart/Related Content-type”, E. Levinson, August 1998, [URL:http://www.ietf.org/rfc/rfc2387.txt](http://www.ietf.org/rfc/rfc2387.txt)
- [RFC2388] “Returning Values from Forms: multipart/form-data”, L. Masinter, August 1998, [URL:http://www.ietf.org/rfc/rfc2388.txt](http://www.ietf.org/rfc/rfc2388.txt)
- [RFC2616] “Hypertext Transfer Protocol -- HTTP/1.1”, R. Fielding et. al, June 1999, [URL:http://www.ietf.org/rfc/rfc2616.txt](http://www.ietf.org/rfc/rfc2616.txt)
- [RFC3986] “URI Generic Syntax”, T. Berners-Lee et al., January 2005, [URL:http://www.ietf.org/rfc/rfc3986.txt](http://www.ietf.org/rfc/rfc3986.txt)
- [RFC4627] “Application/json media type”, D. Crockford, July 2006, [URL:http://www.ietf.org/rfc/rfc4627.txt](http://www.ietf.org/rfc/rfc4627.txt)

3. Terminology and Conventions

3.1 Conventions

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

For the purpose of this WP, all definitions from the OMA Dictionary [OMADICT) apply.

3.3 Abbreviations

API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CLRF	Carriage Return Line Feed
CRUD	Create, Read, Update, Delete
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
JSON	Java Script Object Notation
MIME	Multipurpose Internet Mail Extensions
MMS	Multimedia Message Service
OMA	Open Mobile Alliance
REST	REpresentational State Transfer
SMS	Short Message Service
SP	SPace
TS	Technical Specification
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UTF	Universal Transformation Format
WP	White Paper
XML	Extensible Markup Language

4. Introduction

This WP is intended to provide the guidelines for defining RESTful Network APIs in OMA.

The REST (REpresentational State Transfer) architecture was defined in 2000 by Dr Roy Fielding [Fielding]. The key principles of REST are that clients and servers (typically in an HTTP system) interact via requests and responses. These requests/responses transfer representations of a resource; which is identified and addressed by a Uniform Resource Locator (URL). REST promotes the use of HTTP verbs (GET, POST, PUT, and DELETE) to allow the client to query the current state of the resource, or to change it. By reusing these verbs, as well as HTTP principles of authentication, caching and content negotiation; it is possible to build relatively simple APIs based on existing Web standards [RFC2616].

5. Principles for defining RESTful Network APIs in OMA

1. A key guideline is that RESTful Network APIs are intended for use by typical web developers. These developers are assumed not to have a detailed understanding of telecoms services and will need to be able to leverage the OMA specified RESTful services as simply as they would leverage services from major web players, service providers or platforms.

Therefore, OMA-specified RESTful Network APIs should provide the same level of easy-to-use as other popular RESTful services provided on the Web. Wherever technically feasible, RESTful Network APIs would be used by applications acting on behalf of the end user (e.g. web site, portal), other specialized applications (SMS campaign managers, various notification services etc) or applications located on the end user device (e.g. mobile phone, dvd player). The cases where the OMA specified RESTful Network APIs specified do not serve well a particular client environment have to be identified, analyzed, documented and addressed (in the same Work Item, or a different Work Item, as deemed appropriate).

2. RESTful Network API specifications should conform to the REST & HTTP practices, in particular:
 - a. Services should be defined in terms of resources that are addressable as URLs.
 - b. Use of nouns in URLs is recommended over the use of verbs
 - URLs identify resources
 - HTTP methods identify Operations
 - c. Use HTTP verbs, i.e. POST, GET, PUT, DELETE for CRUD (Create, Read, Update, Delete) operations, for all interfaces for which CRUD is a good fit , using the following mapping:
 - POST
 - POST maps to Create, if the HTTP client sends a request to the HTTP server to create a subordinate of the specified resource (a.k.a. creating a new member of the resource collection), using some server-side algorithm.
 - POST maps to Update if the HTTP client sends a request to the HTTP server to partially update the specified resource, or to update one or more subordinates of the specified resource
 - Note: In certain cases, POST may be used when the operation cannot be mapped to a CRUD operation. For example transformational update of the resource space is usually difficult to map to a CRUD operation (e.g. batch update, etc).
 - GET maps to Read. GET must be safe (i.e. it cannot change a resource), and must be idempotent (i.e. the outcome of calling it multiple times is the same as calling it once - unless somebody else changed the resource between calls)
 - PUT
 - In case the URL addressed by the PUT operation points to an existing resource, PUT maps to a complete Update of the resource, and must be idempotent.
 - In case the URL addressed by the PUT operation does not point to an existing resource, PUT maps to Create of that resource, if that operation is permitted.
 - DELETE maps to Delete, and must be idempotent
 - d. Use standard HTTP Status codes in responses for both successful and failed operations. In the case of a failed operation additional status information (if available) will be returned in the body of the response.

Use of HTTP status codes in response should be consistent with [RFC2616] and in case of successful operations it is recommended to use the following Status codes:

POST: for successful response, these are the allowed values:

200 (OK): when no resource URL is provided in the response but the response includes the entity that describes the result.

201 (Created): if a resource has been created on the origin server, the message SHOULD contain an entity which describes the status of the request and refers to the new resource, and a Location header

204 (No content): when no resource URL is provided in the response and it does not provide a body.

303 (See other): when the POST operation resulted in a change that is reflected in another resource (e.g. when using POST to do call transfer in a call API), the message SHOULD contain an entity which describes the status of the request and refers to the other resource, and a Location header

PUT:

200 (OK) or 204(No Content): they are used when the existing resource has been modified (idempotent).

201 (Created): MUST be used when a new resource has been created.

GET: (idempotent)

200 (OK): successful response that includes the entity requested.

DELETE: (idempotent)

200 (OK): for a successful response if the response includes an entity describing the status.

202 (Accepted): if the action has not yet been enacted.

204 (No Content): if the action has been enacted but the response does not include an entity.

3. The content type used in responses is established using the following methodology:

As a general rule, content type used in response message body must match content type used in request body. In case this is not possible, content type negotiation can be used. The methodology for content type negotiation is based on the “Accept” HTTP header in the request to signal the supported content types. A parameter of name “resFormat” can be given to override the information in this header. The methodology for content type negotiation is specified further in [REST_NetAPI_Common].

At least XML and JSON content types are supported, with other content types optionally supported on a case-by-case basis to be specifically documented (e.g. simple name-value pair parameters may be accepted in the URL when using GET and application/x-www-form-urlencoded may be supported for the request message body when using POST).

4. It is recommended to specify API versioning by inserting the API version in the resource URL path (e.g. “v1”) version is a completely separate set of resources/endpoints from the previous 1.0 version).
 - a. Minor API revisions are backwards compatible (in general, unknown parameters should be ignored for forwards compatibility) and major revisions are a distinct set of paths.
 - b. If a change is made to the XML request/response format that is not backwards compatible, the major version number must be incremented, otherwise the minor version number is incremented.
 - c. The namespace URN of the XML schemas only contains the major version number (e.g. urn:oma:xml:rest:netapi:common:1).
 - d. The full version number (major and minor version number separated by a “.” character) is given in the “version” attribute in the <schema> element of the XML schema.
 - e. The resource URL only includes the major version number in the path, following the letter “v” (e.g. “v1”).

Example: If service, for example “messaging” service, supports version 1.0, 1.1, .. and 2.0, 2.1, etc, then the API versioning in the resource URL should be indicated as:

http://example.com/exampleAPI/messaging/v1/ for the 1.0, 1.1, 1.x version, and

http://example.com/exampleAPI/messaging/v2/ for the 2.0, 2.1, 2.x version of the “messaging” service.

5. Callback APIs specification and client implementations of the callback APIs have to comply with the remaining set of guidelines in this WP. Wherever necessary, callback functionality (i.e. the ability for the server to notify the application of particular events subscribed to) will be supported in the most appropriate manner consistent with the general REST architectural style chosen.
 - a. For example, in the case when the client resides in a server-like environment a request URL may be passed by the client on which it can be notified of particular events that the client subscribed to.

- b. In all cases, other approaches may be followed on a case-by-case basis, using an analysis of specific client access particularities.
6. The API specifications should include examples. The examples in the RESTful Network API description should avoid using real host and real company name (use “www.example.com” instead of “www.carrier.com” and “myapp.developer.com”).
7. If multiple attachments need to be sent as part of the client request or callback request from the server, then MIME Content-Type multipart/related should be used.
8. APIs should support ability to add extra data elements in the request/reply body and extra query parameters in the URL to enhance usability.

Note: Client and server should ignore unrecognized parameters and data elements for forward compatibility reasons.

9. If a message contains sensitive data, such as passwords, account numbers, and card numbers (as in account management and payment APIs), security consideration to protect these information is required.
10. The HTTP protocol does not place any a priori limit on the length of a URL according to [RFC2616]. However, some old implementations have a limitation, that is, 256 bytes, while other implementations have at least 4000 characters limitation. GET-based forms with a URL above 255 bytes may get response including 414 (Request-URI Too Long) status code. In the case where the URL would exceed 4000 characters, the API design would consider using POST method instead of GET on a case by case basis.

5.1 API Documentation

Each RESTful Network API should be specified in a resource-oriented manner and the resources used by the API should be defined and explained. Use cases and sequence diagrams should be provided. Each RESTful Network API specification must include the following definitions:

- API resource definitions, together with an overall structure if multiple resources are defined in the API.
- Definition of HTTP operations (HTTP verbs: GET, POST, PUT, DELETE) for each resource:
- Data type definition, such as complex data type and enumeration type.
 - Description of the operation
 - Request
 - Response
 - Referenced faults

All parameters in URLs must be URL encoded, for example an ‘endUserId’ and description parameters would be encoded as endUserId=tel%3A%2B19585550100 and description=Some%20billing%20information.

5.1.1 API Data Types

RESTful Network API data types and enumeration types must be specified with an associated detailed description including optionality. This will enable a developer to understand how to use the parameter. API data type definitions must be consistent and follow recognized standard definitions; the following table gives an example:

Element	Type	Optional	Description
destinationAddress	xsd:anyURI	No	Number associated with the invoked messaging service, i.e. the destination address used by the terminal to send the message (e.g. 'sip' URI, 'tel' URI, 'acr' URI)

senderAddress	xsd:anyURI	No	The address of the sender to whom a responding message may be sent (e.g. 'sip' URI, 'tel' URI, 'acr' URI). If senderAddress is also part of the request URL, the two MUST have the same value.
dateTime	xsd:dateTime	Yes	Time when message was received by operator
resourceURL	xsd:anyURI	Yes	Self referring URL. The resourceURL SHALL NOT be included in POST requests by the client, but MUST be included in POST requests representing notifications by the server to the client, when a complete representation of the resource is embedded in the notification. The resourceURL MUST also be included in responses to any HTTP method that returns an entity body, and in PUT requests.
link	common:Link[0..unbounded]	Yes	Link to other resources that are in relationship with the resource
messageId	xsd:string	Yes	Server generated message identifier. This field MUST be present when the type of the message differs from a plain text SMS, i.e. the element in the choice below has a type other than InboundSMSTextMessage.
inboundSMSTextMessage	InboundSMSTextMessage	Choice	Inbound SMS text message
inboundMMSMessage	InboundMMSMessage	Choice	Inbound MMS message
inboundIMMessage	InboundIMMessage	Choice	Inbound IM message
destinationAddress	xsd:anyURI	No	Number associated with the invoked messaging service, i.e. the destination address used by the terminal to send the message (e.g. 'sip' URI, 'tel' URI, 'acr' URI)

Table 1: API Data Type Example

Furthermore, common data types should be reused consistently across multiple APIs.

5.2 Error Handling

After receiving and interpreting a REST request message, a server responds with an HTTP response message, as defined in [RFC2616].

```

Response = Status-Line
          *(( general-header
             | response-header
             | entity-header ) CRLF)
          CRLF
          [ message-body ]
Status-Line = HTTP-Version SP Status-Code SP Reason-Phrase CRLF

```

Standard values for status code and reason phrase are used for “Status-Code” and “Reason-Phrase” above. For all faults additional information should when applicable, be returned to the requestor in the message body. The message body should

contain the error details, such as an error code as well as an error description if available. The information returned should be self-contained, so the client does not need to save any state information. For examples provide tables with the supported resource formats.

5.3 Examples

The API specifications should include examples. Examples in the RESTful Network API description should avoid using real host and real company names, for example use “www.example.com” instead of specifics such as “www.carrier.com” or “myapp.developer.com”.

Furthermore the RESTful Network API description should include detailed sample request and response messages, in HTTP-XML format for the convenience of the reader. For example, a sample REST <GetMessageDeliveryStatusRequest> Request should include:

```
GET /exampleAPI/messaging/v1/outbound/tel%3A%2B19585550151/requests/req123/deliveryInfos HTTP/1.1
Accept: application/xml
Host: example.com
```

And the resulting sample REST Response should include:

```
HTTP/1.1 200 OK
Content-Type: application/xml
Content-Length: nnnn
Date: Thu, 04 Jun 2009 02:51:59 GMT

<?xml version="1.0" encoding="UTF-8"?>
<msg:deliveryInfoList xmlns:msg="urn:oma:xml:rest:netapi:messaging:1">
  <resourceURL>http://example.com/exampleAPI/messaging/v1/outbound/tel%3A%2B19585550100/requests/req123/deliveryInfos
  </resourceURL>
  <deliveryInfo>
    <address>tel:+19585550103</address>
    <deliveryStatus>MessageWaiting</deliveryStatus>
  </deliveryInfo>
  <deliveryInfo>
    <address>tel:+19585550104</address>
    <deliveryStatus>MessageWaiting</deliveryStatus>
  </deliveryInfo>
</msg:deliveryInfoList>
```

5.4 Common Data Formats

5.4.1 XML

POST and PUT requests may include data in XML format. An “application/xml” body should be used in these cases. This XML format needs to be compliant with the corresponding XML Schemas for the data types. If the XML contains pointers to the OMA SUP schema files, it can be validated online.

Responses may also include XML body.

5.4.2 JSON

POST and PUT requests may include data in JSON format [JSON]. Details on this format can be found in JSON [RFC4627]. Responses may also include bodies in JSON format. In [REST_NetAPI_Common] serialization rules for JSON encoding in HTTP Request/responses are specified.

5.4.3 Application/x-www-form-urlencoded

As an alternative to XML or JSON, input data in requests (but not responses) may be submitted in application/x-www-form-urlencoded format as specified in [HTML_FORMS]. Usually, this format is used as the last portion of a URL as defined by [RFC2616]. In RESTful Network APIs, this applies to GET/DELETE requests where this format can be used in query parameters.

In POST requests, this format can also be used, to support the use case of submitting a representation of a data structure directly from HTML forms by a web browser. This will imply the inclusion of an application/x-www-form-urlencoded body. As web browsers use POST to submit these forms, it usually does not make sense to use this format for the body of PUT requests. The format is subject to some restrictions in the character set of the exchanged information – unsafe and reserved characters must be escaped using “percent encoding” [RFC3986]. I.e., a character is replaced by the string as %HH where HH stands for the hexadecimal representation of the ASCII code of the character.

5.4.3.1 Serialization guidelines for application/x-www-form-urlencoded in requests

The following are general rules for mapping between the XML and application/x-www-form-urlencoded formats:

- a. When using this serialization in POST requests, data will be included in the body of the request and not in the URL. To do this, Content-Type: application/x-www-form-urlencoded will be used.
- b. Where one of the elements is a complex type, only the simple type child sub (or sub-sub)-elements will be included in the URL encoded data.
- c. In the absence of XML hierarchy issues, encoding shall look like:
 - subelement1=valueA&
 - subelement2=valueB&
 - attribute=valueC

The use of application/x-www-form-urlencoded should be specified for each API on a case-by-case basis. This should be documented by means of a table with the result of removing XML hierarchy levels.

Within application/x-www-form-urlencoded bodies, there is neither an indication of the first `<?xml version="1.0" encoding="UTF-8" ?>` nor the declaration of namespaces or schemaLocations.

5.5 Internationalization

XML Serialization: in REST requests/responses, internationalization comes through the use of UTF-8 encoding in XML bodies..

```
Content-Type: application/xml;

<?xml version="1.0" encoding="UTF-8"?>
<tns:example>
.....
</tns:example>
```

For JSON serialization, UTF-8 encoding will be used as default, as specified in application/json [RFC4627].

```
Content-Type: application/json
Content-Transfer-Encoding: 8bit
<json UTF-8 data>
```

For application/x-www-form-urlencoded serialization, internationalization support is more restricted. According to [RFC1738] and [HTML_FORMS], only alphanumeric ASCII characters [0-9, a-z, A-Z] and some other (\$_.,+!*'()) may be included directly. Other unsafe and reserved characters may be exchanged too but must be escaped (" ,?, etc.).

This applies to GET/DELETE query parameters and application/x-www-form-urlencoded bodies in POST/PUT requests, as in the example below.

```
Content-Type: application/x-www-form-urlencoded
message=quedar%EDamos+ma%F1ana&address=621444448
```

For the exchange of binary data, base64 will be taken as Content-Transfer-Encoding.

5.6 Backwards Compatibility

APIs evolution should offer backwards compatibility for clients using older versions of the API. Backwards compatibility should be guaranteed for previous upgrades (i.e. minor revisions) within the same release (i.e. major revisions).



Figure 1 Clients using older versions of the API

5.6.1 XML based APIs

In order to support for received API requests, at server's side, the following guidelines will be followed in APIs:

a. Data Types – Elements:

- A new version of a data type may be created, including new elements within a XML sequence/choice, but they will be always optional (minOccurs=0).
 - Example: a new element called “wapsupport” is included, but as optional. Former parameters (brand, model) are kept

```
<xsd:complexType name="UserTerminalInfoType">
  <xsd:sequence>
    <xsd:element name="brand" type="xsd:string"/>
    <xsd:element name="model" type="xsd:string" />
    <xsd:element name="wapsupport" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

- Example: a new, possible third choice is included

```
<xsd:complexType name="AChoiceType">
  <xsd:choice>
    <xsd:element name="choice1" type="xsd:string"/>
    <xsd:element name="choice2" type="xsd:string"/>
    <xsd:element name="choice3" type="xsd:string"/>
  </xsd:choice>
</xsd:complexType>
```

- A new version of a data type may be created, changing the cardinality of some attribute or parameter, but always changing from mandatory to optional, never changing from optional to mandatory.
 - Example: brand and model are now made optional

```
<xsd:complexType name="UserTerminalInfoType">
  <xsd:sequence>
    <xsd:element name="brand" type="xsd:string" minOccurs="0"/>
    <xsd:element name="model" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
```

- New attributes may be defined for REST. However, they will always be optional (absence of use="required").
 - Example: a new attribute called "lastUpdated" is included but as optional.

```
<xsd:complexType name="UserTerminalInfoType">
  <xsd:sequence>
    <xsd:element name="brand" type="xsd:string" minOccurs="0"/>
    <xsd:element name="model" type="xsd:string" minOccurs="0"/>
  </xsd:sequence>
  <xsd:attribute name="lastUpdated" type="xsd:string" use="optional"/>
</xsd:complexType>
```

b. Data Types – Enumerations:

- New enumerated values may be included, but always maintaining the former ones.
 - Example: a new value is included in the enumeration (pound), keeping the two other, existing formerly.

```
<xsd:simpleType name="CurrencyType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="euro"/>
    <xsd:enumeration value="dollar"/>
    <xsd:enumeration value="pound"/>
  </xsd:restriction>
</xsd:simpleType>
```

c. Operations:

- Operations may be evolved, adding new parameters. But new parameters will always be optional. Existing parameters will always be kept, for compatibility.
 - Example: over an existing operation, a new, optional input parameter is included, "maxItems".

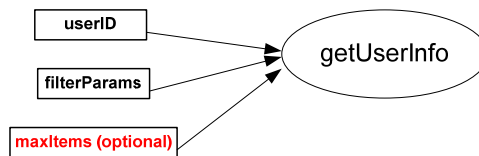


Figure 2 Backwards compatibility for operations

- New operations may be added, but existing operations will always be kept, for compatibility.

5.6.2 JSON based APIs

Above considerations are given for XML based API requests. For the JSON case, existing parameters in previous versions of the API will be kept in API specifications, for backwards compatibility.

5.7 Forward Compatibility, Extensibility

APIs should be designed to offer forwards compatibility towards new versions of the API. This compatibility will typically apply between upgrades under a same Release, in two ways:

- Upgraded servers returning a response to legacy clients
- New versions of clients making requests to existing, non upgraded API servers



Figure 3 Upgraded servers returning a response to legacy clients



Figure 4 New versions of clients making requests to existing, non-upgraded servers

5.7.1 XML based APIs

Considering XML format, extensibility and evolution of the data exchanged over APIs is possible by means of extensible XML Schemas.

Thus, the following technical guidelines will be followed for the design of extensible APIs:

a. Extensions in sequences.

- It is recommended to include extensibility points in root XML types or any other which is expected to evolve in the future, with “processContents=lax” processing model, so that receivers are not forced to validate these extended elements. Extensions over the same namespace will go under a wrapper and extensions over other namespaces may go directly under parent data. However, if the elements included belong to a known namespace, server will try to parse these XML elements.

o Example

```

<s:complexType name="ExtensionType">
  <s:sequence>
    <s:any processContents="lax" minOccurs="0" maxOccurs="unbounded" namespace="##any"/>
  </s:sequence>
  <s:anyAttribute/>
</s:complexType>
  
```

And then, in the complex element definitions include also a direct wildcard to include directly additional elements from other namespaces (to avoid XML determinism problems):


```

<xsd:complexType name="MyType">
  <xsd:sequence>
    <xsd:element name="e1" type="xsd:string"/>
    <xsd:element name="e2" type="xsd:string"/>
    <xsd:element name="Extension" type="tns:ExtensionType" minOccurs="0" maxOccurs="unbounded"/>
    <xsd:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xsd:sequence>
  <xsd:anyAttribute/>
</xsd:complexType>

```

Note: “choice” and “all” complex data types are not extensible and thus can not be modified within a release.

b. Extension of attributes:

- The possibility of any future attribute is given by means of the inclusion of the “anyAttribute” wildcard, as indicated in the example above.

c. Extension of enumerations

- The possibility of any future value in the enumeration is given by means the definition of the enumeration as a union of the current enumerated values plus a possible string.
 - o Example:

```

<xsd:simpleType name="DeliveryStatusType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="DeliveredToTerminal"/>
    <xsd:enumeration value="DeliveryImpossible"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:element name="deliveryStatus">
  <xsd:simpleType>
    <xsd:union memberTypes="tns:DeliveryStatusTypes xsd:string"/>
  </xsd:simpleType>
</xsd:element>

```

This procedure consists in the ‘Must Ignore’ rule, in which receivers may omit extended elements which they don’t understand in syntactically correct XML documents (typically, the validation should then be performed by the application logic on top of the API).

Note: Whether to follow this ‘Must Ignore’ rule - along with the extensibility mechanisms above - or not is a design decision that must consider deployment dependent aspects as well as the specific usage that is desired for the API itself.

5.7.2 JSON based APIs

Above considerations are given for XML based API requests. However, JSON is an inherently extensible serialization format. As a string, any data may be additionally included, although if server is not upgraded they will merely be ignored

5.8 Encoding and Serialization Details for MIME format

A MIME multipart message is used in some APIs (e.g. the RESTful Messaging API) to represent content that consists of several parts (such as an MMS message).

There are different options available for MIME multipart messages, namely multipart/related [RFC2387], multipart/form-data [RFC2388] and multipart/mixed [RFC2046]. The selection of the multipart format to use in a particular API needs to consider multiple factors, such as the conventions in the domain in which the API is defined, how tightly the API is to be coupled to the underlying systems, and how easy the format is to use in the Web community and in browser environments.

When simplicity and better suitability to the internet developer community and browsers are keys, it is suggested to use multipart/form-data [RFC2388] and [HTML_FORMS].

A MIME multipart message usually contains within the HTTP request or response a root structure which carries the representation of the REST resource (usually a parameter set in XML, JSON or application/x-www-form-urlencoded format), and one or more multimedia content attachments expressed as MIME body parts.

Rules how to compose a multipart/form-data message with a root part are given in [REST_NetAPI_Common]. Messages with one attachment are represented differently than those with multiple attachments.

The following uses the example of MMS to illustrate how to encode and send a MIME multipart/form-data message using forms when the root fields are represented in XML and when more than one MMS content is sent:

```
POST /exampleAPI/messaging/v1/outbound/tel%3A%2B19585550100/requests HTTP/1.1
```

```
Host: example.com
```

```
Other http headers
```

```
Content-Type: multipart/form-data; boundary="asdfa487";
```

```
--asdfa487
```

```
Content-Disposition: multipart/form-data; name="root-fields"
```

```
Content-type: application/xml
```

```
Content-Length: nnnn
```

Here the XML representation of the MMS root fields "OutboundMessageRequest"

```
--asdfa487
```

```
Content-disposition: multipart/form-data; name="attachments"
```

```
Content-type: multipart/mixed; boundary="BbC04y"
```

```
--BbC04y
```

```
Content-disposition: attachment; filename="textBody.txt"
```

```
Content-Type: text/plain; charset="UTF-8"
```

```
Content-Transfer-Encoding: 8-bit
```

... text of the MMS ...

```
--BbC04y
```

```
Content-disposition: attachment; filename="file2.gif"
```

```
Content-type: image/gif
```

```
Content-Transfer-Encoding: base64
```

```
...contents of file2.gif...
```

```
--BbC04y
```

Other attachment may come here (correctly delimited by the boundary string)

```
--BbC04y--
```

```
--asdfa487--
```

The following uses the example of MMS to illustrate how to encode and send a MIME multipart message using forms when the root fields are represented in JSON, and when a single content is sent:

```
POST /exampleAPI/messaging/v1/outbound/tel%3A%2B19585550100/requests HTTP/1.1
Host: example.com
Other http headers
```

```
Content-Type: multipart/form-data; boundary="asdfa487";
```

```
--asdfa487
Content-Disposition: multipart/form-data; name="root-fields"
Content-type: application/json
```

Here the JSON representation of the MMS root fields "OutboundMessageRequest"

```
--asdfa487
Content-disposition: multipart/form-data; name="attachments"; filename="picture.jpeg"
Content-type: image/jpeg
```

...contents of picture.jpeg...

```
--asdfa487--
```

5.9 Light-weight resources

A term called "light-weight resources" is used to describe resources that enable access to a part of a data structure or individual elements in a data structure. This is in a contrast to other resources that operate on the entire data structure and are regarded as heavy-weight resources. A data structure could be any kind of XML/JSON structure representing the heavy-weight resource that is created using POST or PUT. A light-weight resource is basically a URL pointing out a resource representing a sub-structure inside the data structure.

For light-weight resources the following apply.

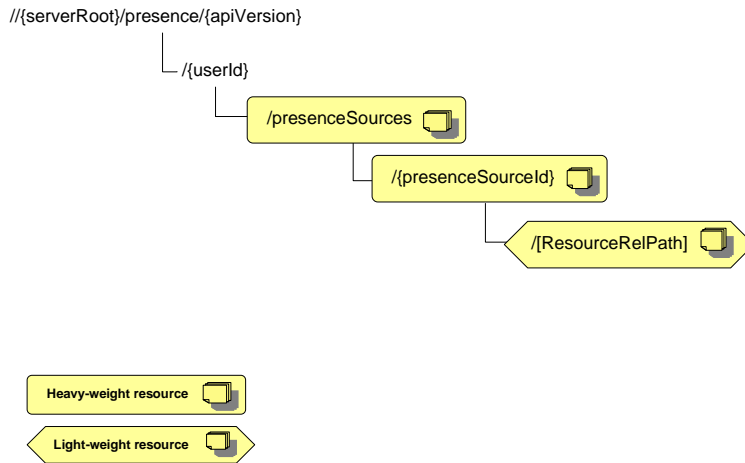
- Only PUT, GET and DELETE operations can be used (PUT will create the resource if it does not exist).
- Precondition for using light-weight resources is that the ancestor heavy-weight resource exists.
- There may be several levels of light-weight resources below the ancestor heavy-weight resource, depending on the data structure (i.e. ../parent/child/grandchild)
- The entire light-weight resource URL is built up of the heavy-weight URL path and the relative resource path for light-weight resource.
- HTTP Etag value MAY be reused from the ancestor heavy-weight resource. Applications MAY also assign individual ETag values per light-weight resource.

The following text (steps 1-3) describes how light-weight resources should be described in API technical specifications.

Step 1: Resources Summary (Section 5.1 in TS):

The light-weight resources should be illustrated in the resource tree as [ResourceRelPath] (i.e. a relative path of the resource) surrounded by a hexagon shape. The heavy-weight resources are illustrated by using a rectangular shape.

Example:



The resource table should describe the name of the light-weight resource as well as applicable operations:

Example:

Resource	Base URL: http://{{serverRoot}}/presence/{{apiVersion}}	Data Structures	HTTP verbs			
			GET	PUT	POST	DELETE
Individual presence source attribute	/{{userId}}/presenceSources/{{presenceSourceId}}/[[ResourceRelPath]]	<i>The data structure corresponds to the element within the PresenceSource pointed out by the request URL.</i> (Used for GET/PUT)	Retrieves the value of the specified presence attribute	Updates presence attribute	no	Removes presence attribute

Step 2: Data Structure (Section 5.2.2.x in TS):

Data structures that contain elements that could be accessed by using light-weight resources should include a column called "[ResourceRelPath]". This column includes string(s) and each of these strings represents a resource relative path for light-weight resource that needs to be appended to the corresponding heavy-weight resource URL in order to create light-weight resource URL for accessing corresponding element in the data structure. The root element and data type of the resource associated with the [ResourceRelPath] are defined by the "Element" and "Type" columns in the row that defines the [ResourceRelPath].

Example: 1

5.2.2.x Type:Presence

Element	Type	Optional	[ResourceRelPath]	Description
person	PersonAttributes	Yes	person	The presence attributes related to a person.

5.2.2.y Type:PersonAttributes

Element	Type	Optional	[ResourceRelPath]	Description
mood	Mood	Yes	person/mood	The user's mood (e.g. Angry, Confused, Happy, etc.) [RFC4480]

root element when accessed as light-weight resource

light-weight resource

Sub-elements in a data structure that are used to identify a particular instance of the parent element are regarded as key properties (keys) of the element; for example for element service, key properties are service Id and service version. In case the key(s) are used to identify a light-weight resource representation, it should be indicated in both the [ResourceRelPath] and in the description part of the corresponding data structure(s). In addition, for keys: the following apply:

- Keys are not accessible individually using light-weight resources (“[ResourceRelPath]” column should indicate “Not applicable”)
- When assessing a parent element with light-weight resource, the key(s) shall not be altered (this should be stated in the description column of the corresponding data structure(s)).
- Where applicable, keys in column “[ResourceRelPath]” should be surrounded by curly brackets ({..}).

Example 2:

5.2.2.m Type: Presence

Element	Type	Optional	[ResourceRelPath]	Description
service	ServiceAttributes [0..unbounded]	Yes	service/{serviceld}/{version}	The presence attributes related to services. For description of "serviceld" and "version" see 5.2.2.n. The sub-elements "serviceld" and "version" of the type ServiceAttributes are key properties for service element and SHALL NOT be altered when this element is accessed as a light-weight resource.

5.2.2.n Type: ServiceAttributes

Element	Type	Optional	[ResourceRelPath]	Description
serviceld	xsd:token	No	Not applicable	Identifier of the service. It is a key property of the service and SHALL NOT be altered when included in the light-weight resource URL.
version	xsd:token	No	Not applicable	The version of the specified service. It is a key property of the service and SHALL NOT be altered when included in the light-weight resource URL.
statusIcon	StatusIcon	Yes	service/{serviceld}/{version}/statusIcon	Contains a link to an icon of the user. [RFC4480]

"serviceld and "version" are key properties of the service

Step 3: Detailed resource operation description (starts with Sections 6.X in TS)

Typically a URL for light-weight resource should look like

http://{Heavy-weight resource path}/[ResourceRelPath]

Table 6.X.1 Request URL variables should include description for [ResourceRelPath].

Example:

The following request URL variables are common for all HTTP commands:

Name	Description
serverRoot	server base url: hostname+port+base path. Port and base path are OPTIONAL. Example: example.com/exampleAPI
apiVersion	version of the API client wants to use. The value of this variable is defined in section 5.1.
xyz	Some data...
[ResourceRelPath]	Relative resource path for a light-weight resource, consisting of a relative path down to an element in the data structure. For more information about the applicable values (strings) for this variable see 6.X.1.1

The description part of [ResourceRelPath] refers to another section-table (6.X.1.1) that is specific for light-weight resources and that should to be created too. The table should describe what types of light-weight resources can be accessed by that particular heavy-weight resource, what methods are available, and the link to the data structure (section 5.2.2.X) that contain possible strings (relative resource paths) that could be used for [ResourceRelPath].

Example:

6.X.1.1 Light-weight relative resource paths

The following table describes the types of light-weight resources that can be accessed by using this resource, applicable methods, and links to data structures that contain values (strings) for those relative resource paths.

Light-weight resource type	Method supported	Description
A type of the light-weight resource	GET, PUT, DELETE	Description of the type of light-weight resource that can be accessed. Here also shall be included a reference to the section with the Data Structure where such light-weight resource type is specified. The data structure in the column “[ResourceRelPath]” contains values (strings) for relative resource path,[ResourceRelPath].

Appendix A. Change History (Informative)

Document Identifier	Date	Sections	Description
OMA-WP-Guidelines_for_RESTful_Network_APIs-20130702-A	02 Jul 2013	n/a	Status changed to Approved by TP TP Ref # OMA-TP-2013-0207- INP_REST_NetAPI_Guidelines_V1_0_RRP_for_Final_Approval
OMA-WP-Guidelines_for_RESTful_Network_APIs-20140227-A	27 Feb 2014	n/a	Status changed to Approved by TP TP Ref # OMA-TP-2014-0053- INP_REST_NetAPI_Guidelines_V1_0_1_RRP_for_Notification

Appendix B. Principles for defining REST bindings for Parlay X Web Service APIs (Informative)

In the previous sections, this document provides generic guidelines and best practices for the specification of RESTful Network APIs in OMA. This appendix provides additional guidelines and best practices for the set of APIs that are based on a Parlay X baseline.

1. For APIs based on a Parlay X baseline, the general principles in section 5 apply. In addition, the following guidelines apply:
 - a. As far as possible, when the goal is to use a REST architectural style in transforming APIs previously bound to a different set of protocols, the operations available through RESTful Network APIs should provide an equivalent level of functionality as was provided by the original set of APIs, and should use similar data elements (when applicable accordingly with the chosen REST architectural style). The operations made available through the RESTful Network API should provide an equivalent level of functionality to the Parlay X SOAP API subset selected for such transformation, and should use similar data elements (when applicable accordantly with the chosen REST architectural style).
 - b. It is recommended that REST binding operations are based on the latest version of 3GPP TS 29.199 series, release 8. Exceptions should be noted in the specific TS document.
2. For the documentation of APIs based on a Parlay X baseline, the guidelines in section 5.1 apply. In addition, for each operation a mapping to the original Parlay X SOAP API should be included in an Annex, where applicable.
3. For error handling in APIs based on a Parlay X baseline, the guidelines in section 5.2 apply. In addition, the fault definitions of the REST binding should follow those of the Parlay X SOAP binding. Proprietary extensions might be supported.
4. For MIME encoding and serialization in APIs based on a Parlay X baseline, the guidelines in section 5.8 apply.
5. Most APIs based on a Parlay X baseline define a application/x-www-form-urlencoded representation at least for some POST messages in an Appendix. In case no such message formats are defined in a particular specification, it is recommended to include information about why this has been omitted; otherwise, the serialization guidelines in section 5.4.3.1 apply.