Mobile Web Services Requirements

Approved Version 1.1 – 28 Mar 2006

Open Mobile Alliance

OMA-RD-OWSER-V1_1-20060328-A

Contents

Figures

Tables

1. Scope (Informative)

This document provides OMA requirements for mobile web services

The requirements are primarily based on the use cases compiled by the Mobile Web Service Group.

The output of the OMA Architecture use cases, OMA REQ use cases and use cases produced by other working groups further refined the requirements specified in this document.

The requirements specified in this document shall be adhered to by all OMA Web Services:

- OMA Web Services Enabler release
- OMA service enablers exposing their capabilities as Web services

Because the OMA MWS specifications in general provide web services realizations respectively of the OMA architecture and components of the OMA architecture (enablers), the present document has also implications on the OMA architecture and enabler specifications.

2. References

2.1 Normative References

[ARCH-PRINC] "OMA Architecture Principles", ArchitecturePrinciples-V1_1-20030401-A,
URL: http://www.openmobilealliance.org/ftp/PD/OMA-ArchitecturePrinciples-V1_1-20030401-A.zip

[CREQ] "Specification of WAP Conformance Requirements", OMA-WAP-221-CREQ-20010425-a.

[EEN] "Execution Environment Neutrality Task Force: Technical Report of the EEN Task Force to the OMA Technical Plenary", OMA-TP-2003-0063-ExecutionEnvironmentNeutralityTR ,
URL: http://www.openmobilealliance.org/ftp/TP/ID/03/OMA-TP-2003-0063-ExecutionEnvironmentNeutralityTR.doc

[rfc2219] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997,
URL: http://www.ietf.org/rfc/rfc2119.txt

[WSAR] "Web Services Architecture Requirement" W3C Working Draft, 14 November 2002,
URL: http://www.w3.org/TR/2002/WD-wsa-reqs-20021114

[OMAPrivacy] "Privacy Requirements for Mobile Services", OMA-Privacy-V1_0_0-20031001-D
URL:http://www.openmobilealliance.org/ftp/PD/OMA-Privacy-V1_0_0-20031001-D.zip

2.2 Informative References

[OASIS WS Provisioning] OASIS Provisioning Services TC, URL: http://www.oasis-open.org/committees/provision/

[Oasis-WS-S] OASIS Web Services Security TC, URL: http://www.oasis-open.org/committees/wss/

[OMA-REQ] OMA Requirements working group,
URL: http://www.openmobilealliance.org/member/technicalPlenary/requirements/index.htm

[OWSE-Overview] "OMA Web Service Enabler Overview",
URL: http://www.openmobilealliance.org/ftp/PD/OMA-OWSF-Overview-V0_12_1-20031031-D.zip

[W3C-WS] W3C Web service activity,URL: http://www.w3.org/2002/ws/

[WS-I] Web Service Interoperability Consortium, URL: http://www.ws-i.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

OMA Web Services Enabler	one or more specifications defining technology intended for use in the development, deployment or operation of OMA enablers that expose their capabilities as Web services
OMA MWS Specifications	The Specifications that together comprise the OMA Web Services Enabler
Web Service	A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards. . (Source: [WSGloss])

3.3 Abbreviations

OWSE	OMA Web Services Enabler
MNO	Mobile Network Operator
MWS	Mobile Web Services
PLMN	Public Land Mobile Network

4. Introduction (Informative)

The mobile telecommunications industry faces new challenges to bring to market diverse, useful and sophisticated services to users. To meet these challenges, the industry must promote interoperability, functional and operational standards. Interoperability standards will ensure that mobile services can be developed which can connect users with all types of services providers and enterprises. Mobility and roaming represent key characteristics constraining such interactions. Users and enterprises expect to be able to use services no matter where they are. Availability of services regardless of user location promises to increase productivity and quality of life. It also provides venues for greater overall revenue per user.

The industry has experimented and successfully rolled out several generations of mobile services, including ones that are based on mobile Internet browsing and mobile commerce.

However, such services have suffered from a number of drawbacks:

- They have been created through tightly-coupled, costly and close alliances between value-added service providers.
    - Such business-driven alliances need to be made more loosely coupled, cheaper and user-driven.
- They have been created based on a mixture of mostly propriety models (e.g. propriety interfaces) and disparate, and sometimes overlapping, standards (WAP, Location, MMS, Presence, Identity, etc.)
    - Such standards need to be harmonized. This is under way at OMA.
    - Sophisticated use cases involving multiple of these standards need to be envisioned.
- These standards have been devised specifically for the mobile environment from the ground up (witness WAP 1.0).
    - Internet and Web Services standards need to be leveraged.
- The deployment, integration and use of services is complex and requires skills that are hard to find.

This document focuses on the mobile environment and on the relevant Internet and Web Services standards that need to be leveraged to produce the next generation of sophisticated mobile services.

The document provides a general analysis of such requirements and specifies a set of priorities.

4.1 OMA Web Services Enabler

OMA Web Services Enabler specifications describe how Web Service standards and technologies can be applied to OMA enabler specifications to

- facilitate the integration of OMA enablers
- expose enabler capabilities at the application-level as web services and therefore take advantage of all the common benefits of web service technologies.
- To simplify the task of integrators, developers and implementers of enablers by providing them with common mechanisms and protocols for interoperability of enablers

Mobile web services are envisioned to support the following interactions:

- Server-to-server
- Server-to-mobile terminal
- Mobile terminal-to-server
- Mobile terminal-to-mobile terminal (or peer-to-peer)

4.2 Market Considerations.

Markets needs have been taken into consideration when selecting and prioritizing the requirements.

The OMA Web Service Enabler Release is motivated by the need to:

- Reduce cost of deployment and integration of mobile services
- Exploit infrastructure, skills and tools from e-Business IT deployments and solutions
    - Declarative, human readable exchanges
    - Independent of the transport protocols and underlying network technologies
- Achieve interoperability across a wide range of platforms and systems:
    - In particular across declarative, imperative and script execution environments.
- Allow integration, composition and coordination of enablers and services provided by numerous parties.

Web services can potentially address all these needs and receive significant support across a wide range of industries. Critical mass can be reached to develop the different technologies and framework needed to achieve efficient deployments. By adopting Web services, the mobile space can re-use these technologies and interoperate with interaction partners realized as Internet-based Web services. Examples of such candidate technologies include the outputs of: WS-Security (e.g. [Oasis-WS-S]), WS-Provisioning [OASIS WS Provisioning], Web service interoperability profiles [WS-I], etc

5. Use Cases (Informative)

The following use cases were considered during the development of MWS Requirements. Not all requirements in this document are explicitly identified or exposed by the use cases. Many requirements were inferred during the analysis.

Note that the use cases were developed using an early drat of the use case templates, hence not all sections of the current template are present and, additional sections not in the current template may be present in some cases.

5.1 Use Case: Device Management.

5.1.1 Short Description

This case describes how local device parameters associated with a service or application may be provisioned remotely by a provisioning service without requiring the device user to manually enter those parameters locally using a device UI. The end user needs only to subscribe to a particular service and that service will be transparently configured by the provider as, for example, voice and SMS services are today.

5.1.2 Actors

- End user wanting to use new services.
- The subscriber's mobile device, which support a new service.
- Service provider targeting a segment of end users

5.1.2.1 Actor Specific Issues

Not Specified

5.1.2.2 Actor Specific Benefits

Not Specified

5.1.3 Pre-conditions

1. The end user wishing to use the new service has a device supporting the new service.
2. The operator provides a device management service and authenticates the service provider to manage relevant configurations in the device
3. The service provider can access the management server in the operator's network via a device management web service

5.1.4 Post-conditions

The application/service settings are provisioned correctly in the device and the end user is able to use the service immediately without trouble.

5.1.5 Normal Flow

Step Number	Action(s)
1	Operator exports a web service interface for device management to service providers.
2	Service provider contracts with the operator for the right to manage a selected set of configuration parameters in devices supporting a particular service
3	Service provider accesses the device management Web service and requests for delivery of

	relevant configuration data to the handsets.
4	The Device management server maintained by the operator authenticates the service provider and delivers configuration data to end-user's devices in the network according to service agreement.
5	Service provider is able to promote the new service.
6	End users are able to subscribe the service provider's service and the service works easily with no trouble, because the settings for the subscriber's device is done automatically.

5.1.6 Alternative Flow

none

5.1.7 High Level Diagram

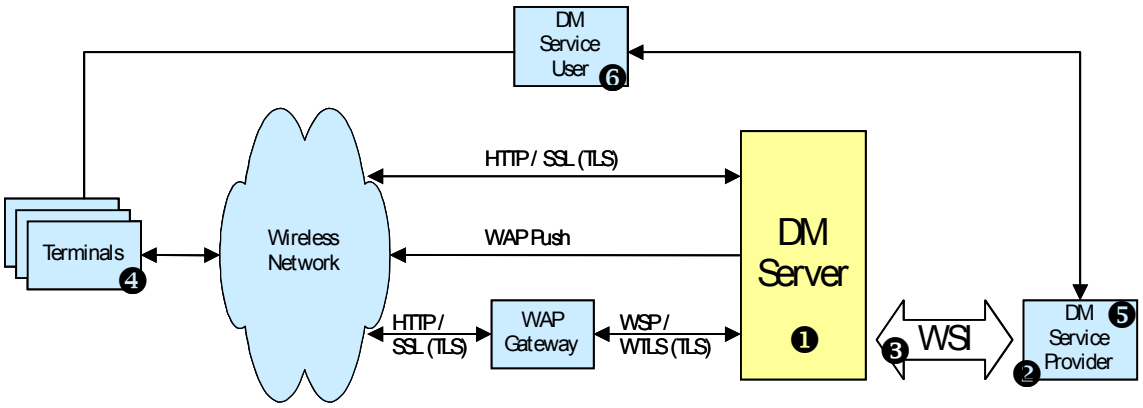

Figure 1: High level diagram Device Management

5.1.8 Web Service Operations

Operation Number	Originator	Operation	Purpose
1	DM service provider	DeliverConfigurationDataRequest	To deliver configuration data to mobile devices
2	DM server	DeliverConfigurationDatAck	Give indication that requested configuration data is delivered

5.2 Use Case: Game Download

5.2.1 Short Description

This case describes how a content provider may utilize a delivery service to download a game to mobile device. The download is verified, and the user's account is billed appropriately.

5.2.2 Actors

- User – Entity that "owns" the terminal to which the game is downloaded
- Content provider – the entity hosting the site or portal where the game is made available for download
- Service Provider – The entity with which the user contracts for mobile data services
- Billing Agent – the entity provides billing services

No business model assumptions are implied by these roles. A single business entity may assume all roles, or they may be distributed among several independent business entities

5.2.2.1 Actor Specific Issues

Not Specified

5.2.2.2 Actor Specific Benefits

Not Specified

5.2.3 Pre-conditions

- The Content Provider has a contract with the Service provider that allows the Content provider to access the delivery service.
- User is allowed to download game applications from the Service Provider's delivery service

5.2.4 Post-conditions

- Game has been successfully downloaded to the user's device
- User's account has been charged (if applicable) for the game

5.2.5 Normal Flow

Step Number	Action(s)
1	Content Provider registers the game application with the Service Providers Delivery service
2	Delivery service caches the game application and applies appropriate Digital Rights Management transforms
3	Content Provider informs the user that the game is available by sending a notification request to the Service Providers Notification service
4	Service Provider delivers the game notification to the user
5	User decides to download the game and initiates a connection to the Service Provider's delivery service (e.g. via a browser)
6	Service Provider delivers the game to the user
7	Service provider verifies that the download completed successfully and requests the billing agent to charge the user's account for the game

5.2.6 Alternative Flow

none

5.2.7 Web Service Operations

Operation Number	Requestor	Responder	Purpose
1	Content Provider	Service Provider	Request that the user be notified that the game is available for download
2	Service Provider	Billing Agent	Charge the user for the game

5.3 Use Case: Presence Service Subscription

5.3.1 Short Description

This case describes how a presence services user may "register" with the Presence Server in order to receive notifications when the presence information of selected other users is updated in the presence server.

5.3.2 Actors

- Presence Services User – person or application making presence service request. In this use case the Presence Services User participant assumes one of two roles
  1. Subscriber – the user requesting a subscription to presence information of one or more other users
  2. Publisher – the user named by a subscriber in a subscription request
- Presence service provider – entity providing presence information to Presence Service Users
- Presence server – entity storing and exposing mobile user's presence information

5.3.2.1 Actor Specific Issues

Not Specified

5.3.2.2 Actor Specific Benefits

Not Specified

5.3.3 Pre-conditions

- The Subscriber is registered and authenticated with the Presence Service Provider
- Presence service provider is authorized to subscribe to presence information maintained by the Presence Server
- Publisher has registered his/her presence information to presence server in operator network
- Publisher allows his/her presence information to be delivered to Subscriber by Presence Service Provider.

5.3.4 Post-conditions

The Subscriber is registered with the presence server to receive updates when presence information for the selected users is updated

5.3.5 Normal Flow

Step Number	Action(s)
1	Presence Service User requests to subscribe to presence information of another user from Presence Service Provider e.g. through browser or dedicated presence client.
2	Presence Service Provider validates the request and makes presence information subscription through WSI to presence server in mobile network.
3	Presence server in mobile network validates the request and stores subscription information.
4	Presence server delivers presence information of subscribed users as presence notification to Presence Service Provider through WSI.
5	Presence Service Provider delivers presence information of subscribed users to subscribing user e.g. through dedicated presence client.

5.3.6 Alternative Flow

none

5.3.7 High level diagram

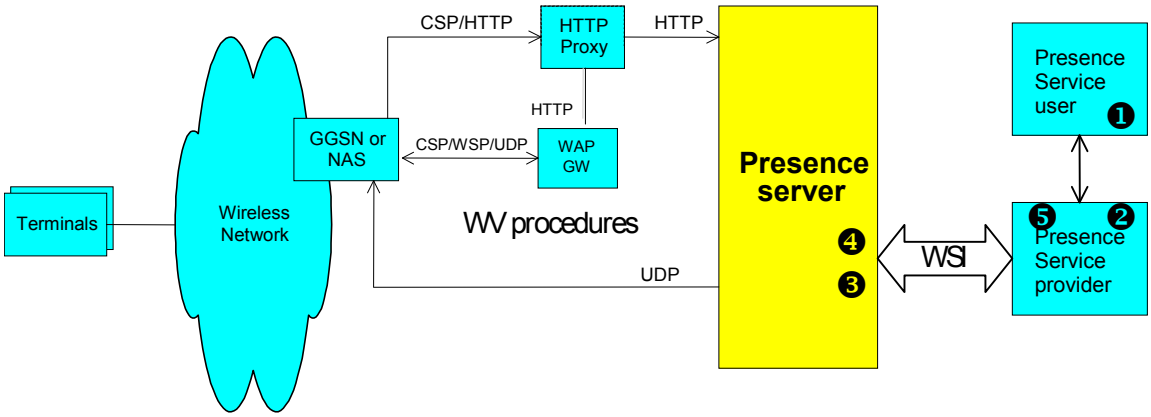

Figure 2: High level diagram Presence Service Subscription

5.4 Use Case:

5.4.1 Short Description

This use case involves a Presence Service User (person or application connected to mobile or fixed internet) who wants to get presence information about other Presence Service Users from a Presence Service Provider. The Presence Service Provider requests presence information from a Presence Server via a Web Service Interface. The Presence Service User uses presence information to determine how to establish communication with mobile subscriber.

Presence is an enabling technology for the mobile Internet. In the desktop world presence has come to mean a technology where users have been able to announce their status to authorized recipients, facilitating instant messaging.

In the mobile environment Presence takes on a richer meaning. It may include things like:

- Client device availability (my phone is on/off, in a call)
- User status (available, unavailable, in a meeting)
- Location
- Client device capabilities (voice, text, GPRS, multimedia)
- Searchable personal statuses such as Mood (happy, angry) and Hobbies (football, fishing, computing, dancing)

5.4.2 Actors

- Presence Services User – person or application making presence service request. In this use case the Presence Services User participant assumes one of two roles
    1. Subscriber – the user requesting presence information of one or more other users
    2. Publisher – the user named by a subscriber in a the request
- Presence service provider – entity providing presence information to Presence Service Users
- Presence server – entity storing and exposing Publisher's presence information

5.4.2.1 Actor Specific Issues

Not Specified

5.4.2.2 Actor Specific Benefits

Not Specified

5.4.3 Pre-conditions

- The Subscriber is registered with the Presence Service Provider
- The Presence service Provider can access presence information from Presence Server in operator network through a Web Services Interface
- Publisher has registered his/her presence information to the Presence Server in operator network
- Publisher allows his presence information to be delivered to the Subscriber by Presence Service Provider.

5.4.4 Post-conditions

- The Presence Service User gets the requested presence information from Presence Service Provider

5.4.5 Normal Flow

Step Number	Action(s)
1	Publisher stores the presence information to Presence Server using appropriate protocol (e.g. WV)

2	Subscriber requests presence information from Presence Service Provider e.g. through browser or dedicated presence client.
3	Presence Service Provider validates the request and requests presence information through WSI from presence server in mobile network
4	Presence Server in mobile network validates the request and compares it with user defined authorisation parameters.
5	If allowed by user authorisation parameters, Presence Server delivers requested presence information through WSI

5.4.6 Alternative Flow

none

5.4.7 High level diagram

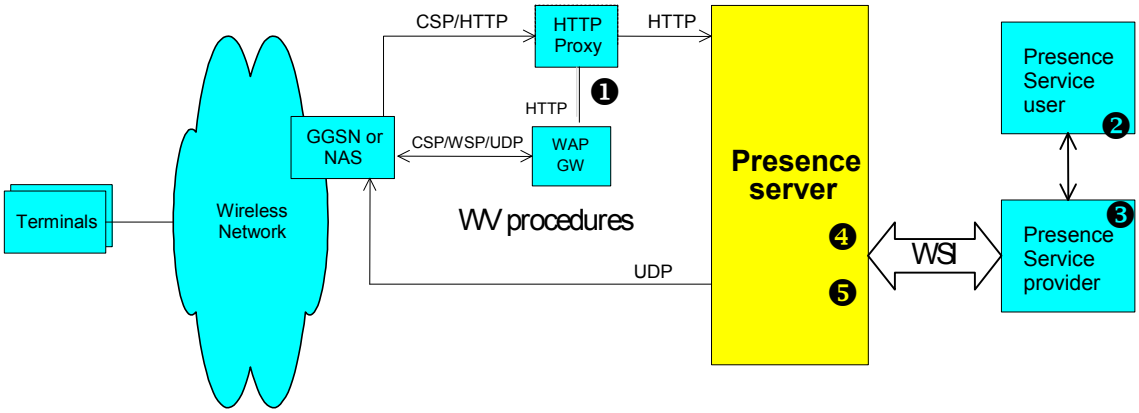

Figure 3: High level diagram

5.4.8 Web Service Operations

Operation Number	Originator	Operation	Purpose
1	Presence Service Provider	Get Presence Information	Presence Service Provider requests mobile users presence information from Presence Server
2	Presence server	Presence Information Delivery	Presence Server delivers mobile users presence information to Presence Server Provider in response to Get Presence Information operation

5.5 Use Case: Presence Information Update

5.5.1 Short Description

This use case describes how presence information may be updated by a Presence Services User.

5.5.2 Actors

- Presence Services User – entity requesting a presence information update
- Presence Service Provider –entity providing presence service to Presence Services Users
- Presence Server – network entity storing and exposing user's presence information

5.5.2.1 Actor Specific Issues

Not Specified

5.5.2.2 Actor Specific Benefits

Not Specified

5.5.3 Pre-conditions

- The Presence Service User is registered with the Presence Service Provider
- The Presence service Provider is allowed to update presence information in Presence Server in operator network via the Exposed Presence Web Service

5.5.4 Post-conditions

- Updated presence information is stored in the Presence Server

5.5.5 Normal Flow

Step Number	Action(s)
1	Presence Service User updates presence information to Presence Service Provider e.g. through browser or dedicated presence client.
2	Presence Service Provider validates the request and makes presence information update through WSI to presence server in mobile network.
3	Presence server in mobile network validates the request and stores the updated presence information.

5.5.6 Alternative Flow

none

5.5.7 High level Flow Diagram

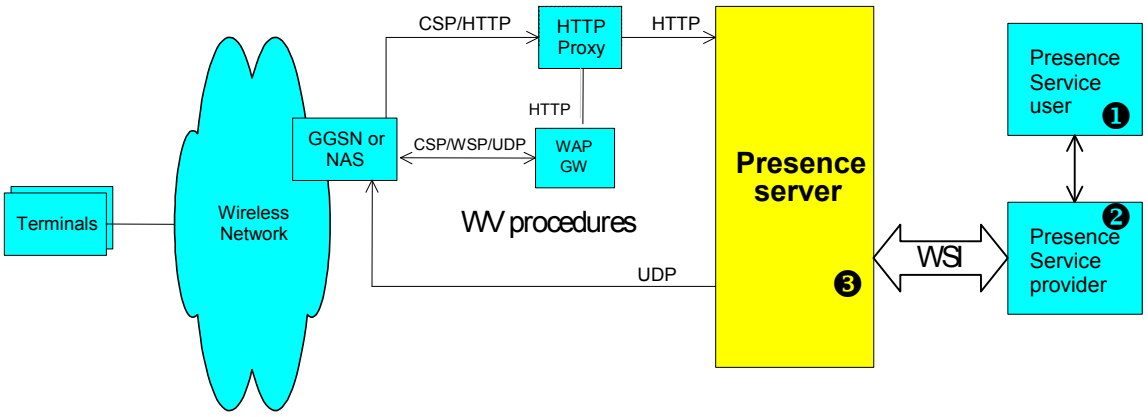

Figure 4: High level diagram Presence Information Update

5.5.8 Web Service Operations

Operation Number	Originator	Operation	Purpose
1	Presence Service Provider	Update Presence Information	Presence Service Provider to update mobile users presence information

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
HLF-1	The OMA MWS specifications MUST enable application providers to easily and efficiently deliver their services / applications through mobile networks.	OWSER 1.0
HLF-2	The OMA MWS specifications MUST support the deployment of mobile services / applications that take advantage of mobile enablers	OWSER 1.0
HLF-3	The OMA MWS specifications MUST provide and rely on standardized network neutral application-level Web Service messages and interfaces to expose mobile enablers.	OWSER 1.0
HLF-4	In the MWS Specifications, the Web Service messages and interfaces MUST be Execution Environment Neutral to allow interoperability and binding to platform / language specific realizations ([EEN]).	OWSER 1.0
HLF-5	The MWS specifications MUST rely on standard internet and web based technologies (based on IP and HTTP)	OWSER 1.0
HLF-6	The MWS specifications MUST be evolutionary	OWSER 1.0
HLF-7	The MWS specifications MUST re-use existing technologies and system components (e.g. authentication framework, load balancing, …)	OWSER 1.0
HLF-8	The MWS specification MUST support extension of existing IT infrastructures	OWSER 1.0
HLF-9	The MWS Specifications MUST enable re-use of authoring and integration tools.	OWSER 1.0
HLF-10	The MWS specifications MUST be interoperable with the wired internet	OWSER 1.0
HLF-11	When needed, the MWS specifications MUST rely on standardized interfaces to access and control entities that enable network-dependent mobile enablers (i.e. APIs to control layer)	OWSER 1.0
HLF-12	MWS specifications MUST enable any actors across the value chain to provide, or aggregate mobile enablers and services), except when an enabler requires resources that can not be distributed or accessed by other actors (e.g. services that can be supplied only by specific actors who own certain PHYSICAL resources (like carrier who has location finding equipment based on cell towers) or because of privacy considerations)	OWSER 1.0
HLF-13	The MWS specifications MUST enable full distribution of functions across actors and value chain	OWSER 1.0
HLF-14	All actors SHOULD be able to make choice on who handles authentication, billing, storage of user profile, etc	OWSER 1.0
HLF-15	The MWS specifications MUST permit different and adaptive function splits between device/terminal and servers and between servers	OWSER 1.0
HLF-16	The MWS specifications MUST enable access to mobile applications over a variety of mobile access mechanisms (different devices, networks, modalities)	OWSER 1.0
HLF-17	The MWS specifications MUST allow deployments where there is a distinction between mobile enablers that provide (possibly new) service features and features common across most enablers and applications NOTE: The analysis work to identify specific “common functions” is currently ongoing in the OMA ARCH and REQ groups.	OWSER 1.0

HLF-18	The MWS specifications MUST facilitate the implementation and deployment of enablers in a manner that permits consistency, reliability, scalability, security, privacy, availability, a consistent user experience and avoids unnecessary user interaction	OWSER 1.0
HLF-19	The OMA Web Services Enabler SHOULD allows the delegation of processing associated with common cross-enabler capabilities (e.g., authentication, authorization, charging, etc) to entities other than the enabler itself.	OWSER 1.0
HLF-20	The MWS specifications MUST reduce TCO for all actors in the value chain	OWSER 1.0
HLF-21	The OMA Web Services Enabler MUST allow service enablers to be discoverable, composable and distributable, in an automated fashion,	OWSER 1.0
HLF-22	Default behaviors and functions MUST be available to all mobile services	OWSER 1.0
HLF-23	The MWS specification MUST support roaming and mobility across networks and applications	OWSER 1.0
HLF-24	The MWS specifications SHOULD enable backward compatibility with Web Service specifications of mobile enablers that are already exist or provide migration path for enabler already deployed	OWSER 1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
SEC-1	OMA MWS specifications MUST provide security guidelines in its policies and specifications. These MUST be consistent with the architecture and security specifications	OWSER 1.0
SEC-2	The OMA MWS specifications MUST only specify solutions compliant to these guidelines, policies and recommendations	OWSER 1.0
SEC-3	The OMA Web Services Enabler MUST provide secure access to web services and associated exchanges. Addressing these requirements MAY require (non-exhaustive) the following and mechanisms to achieve these SHALL be supported a. Confidentiality of the exchanged information. b. Client exchanges shall be accepted only from and to trusted / authorized parties. Integrity protection.	OWSER 1.0
SEC-4	The OMA Web Services Enabler MUST be no less secure against interruption, interception, modification, impersonation, fabrication and other security attacks than current systems that have been deployed according to generally-accepted security standards and practices.	OWSER 1.0
SEC-5	The OMA Web Services Enabler MUST support setting various levels of security policies: e.g. different levels of authentications or authorization for mobile web services in order to restrict service access to authenticated and authorized parties.	OWSER 1.0
SEC-6	The policies supported by OMA Web Services Enabler MUST be versatile enough to comply with local regulatory requirements.	OWSER 1.0
SEC-7	The OMA MWS Web Services Enabler MAY enable non-repudiation.	OWSER 1.0
SEC-8	The OMA Web Services Enabler must enable deployments that leverage underlying network bearer security mechanisms	OWSER 1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.2 Charging

Label	Description	Enabler Release
CHARG-1	The OMA Web Services Enabler MUST allow appropriate charging model such as: a. Service and content providers for usage of the service. b. Users for usage of the service c. For all the actors in the value chain of a web service enabler (e.g. referral fee)	OWSER 1.0
CHARG-2	2. The OMA Web Services Enabler MUST support various charging models such as: a. Per usage or instance b. Per usage time c. Per volume / data rate Per subscription (flat rate)	OWSER 1.0
CHARG-3	The OMA Web Services Enabler MUST support different billing and payment models on top of the different charging model d. Percentage of transaction e. Free f. With different payment models: i. Pre-pay ii. Post-pay	OWSER 1.0

Table 3: High-Level Functional Requirements – Charging Items

6.1.3 Administration and Configuration

Label	Description	Enabler Release
ADM-1	It MUST be possible for service and content providers to control access to mobile web services based on the subscription and personalization information of the user	OWSER 1.0
ADM-2	1. The OMA Web Services Enabler SHOULD detail: o How is the subscription and personalization information expressed o How is the subscription and personalization information requested / accessed and exchanged How are all the parties involved with a web services informed of a particular subscription, authorization or preference of the user. This is especially important for use cases like a portal with sign up for services that are provisioned and executed elsewhere.	OWSER 1.0

ADM-3	2. Access to subscription and personalization information MUST be authenticated, authorized and performed based on pre-set policies established by the user and information repository E.g. with masking of information (e.g. identity, Social Security number, etc…)	OWSER 1.0
ADM-4	Retrieval of users profiles MUST ensure the integrity, confidentiality, , of the subscription and personalization information.	OWSER 1.0
ADM-5	It MUST be possible that mobile web services be provided by any actor in the value chain (terminal, network operator, playing the role of service providers for these web services, as well as third service party providers).	OWSER 1.0
ADM-6	The administration of mobile web services (authorization, registration, activation, configuration, optimization, delegation of trust) MUST be under the control of the one or multiple administrators the web service and available to other actors when authorized.	OWSER 1.0
ADM-7	Within the OMA Web Services Enabler it MUST be possible to easily administer and configure users and service providers.	OWSER 1.0
ADM-8	Within the OMA Web Services Enabler, all services and users SHOULD have specified configuration and administration information exposed through MWS interfaces; when authorized	OWSER 1.0

Table 4: High-Level Functional Requirements – Administration and Configuration Items

6.1.4 Usability

Label	Description	Enabler Release
USAB-1	The OMA Web Services Enabler SHOULD enable users to manage the security policies.	OWSER 1.0
USAB-2	The OMA Web Services Enabler MUST enable users to manage privacy.	OWSER 1.0
USAB-3	The OMA MWS specifications MAY optimize the support of web services with a user interface to minimize delays for the user.	OWSER 1.0
USAB-4	The OMA Web Services Enabler SHOULD allow the user to customize web services that are explicitly exposed to the user. It means that it SHOULD be possible to adapt the user interface of MWS web services or enablers to the characteristics of the device or access mechanism (mode).	OWSER 1.0

Table 5: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

See section 6.2.2.

6.1.6 Privacy

Label	Description	Enabler Release
PRIV-1	The OMA Web Services Enabler MUST enable setting security and privacy policies for mobile web services and in accord to regulatory rules.	OWSER 1.0
PRIV-2	The OMA Web Services Enabler MUST make it possible to protect the privacy of the user according to the broad range of privacy regulations that exist.	OWSER 1.0
PRIV-3	Privacy requirements on the OMA Web Services Enabler MUST be at least as good as for other mobile services or voice sessions:	OWSER 1.0

PRIV-4	It MUST (per regulations) be possible to prevent exchange of the user's true identity, location and other terminal or user related information when required.	OWSER 1.0
PRIV-5	MWS may enable the service provider or content provider to collect information about the user or usage. This information should be treated according to the policies in place for data and voice (e.g. human to human operator or human to automated service) services. The OMA Web Services Enabler SHOULD NOT add additional privacy risks.	OWSER 1.0
PRIV-6	The OMA Web Services Enabler SHOULD be associated to mechanisms that let the user specify the use that can be done of any information, even transient, exchanged by mobile web services.	OWSER 1.0
PRIV-7	Mobile web services SHALL produce schemas or mechanisms to describe the handling and use of the information or allow automation of the acceptance of privacy policies.	OWSER 1.0
PRIV-8	Trust and resolution mechanisms MUST be provided to enable the user to accept the particular service and configuration on the basis of the usage that will be made of such information or the management options provided to the user.	OWSER 1.0
PRIV-9	The Web Services Enabler MUST allow the choice in identity provider, identity services.	OWSER 1.0
PRIV-10	In addition to the MWS Privacy requirements above see [OMAPrivacy] “Privacy Requirements for Mobile Services” for additional normative Privacy requirements that apply to all enabler work within OMA.	OWSER 1.0

Table 6: High-Level Functional Requirements – Privacy Items

6.2 Overall System Requirements

6.2.1 Programming Models

Label	Description	Enabler Release
PROG-1	In the OMA MWS specifications, MWS MUST adhere to interfaces expressed with a common syntax and semantic.	OWSER 1.0
PROG-2	The OMA MWS specifications SHOULD recommend that there be only one Web service interface per functional	OWSER 1.0
PROG-3	The OMA MWS specifications MUST remain neutral with respect to the programming environments as per platform / OS independence requirements proposed as part of OMA charter, ARCH principles [ARCH-PRINC] and Execution Environment Neutrality [EEN].	OWSER 1.0
PROG-4	The OMA MWS specifications SHOULD be message based instead of APIs.	OWSER 1.0
PROG-5	The OMA MWS specifications MUST support version control for service enabler instances to indicate which version of a given interface they are supporting:	OWSER 1.0
PROG-6	Version information MUST be discoverable by Web Services clients.	OWSER 1.0
PROG-7		OWSER 1.0

Table 7: Overall System Requirements – Programming Models

6.2.2 Interoperability

Label	Description	Enabler Release
INTEROP-1	The OMA MWS specifications MUST rely on mechanisms for describing, discovering and interacting with web services that are aligned or compatible with emerging Web service standards from W3C and other organizations like OASIS, WS-I, WSDL, UDDI, SOAP and related technologies.	OWSER 1.0
INTEROP-2	The OMA MWS specifications MUST support different styles of interactions between web services e.g., synchronous and asynchronous message exchanges.	OWSER 1.0
INTEROP-3	The OMA Web Services Enabler and specification MUST support access to enablers that rely on Web services for their implementation from the whole range of OMA devices (e.g, different phones and PDAs).	OWSER 1.0
INTEROP-4	The OMA Web Services Enabler and specifications MUST support access to enablers that rely on Web services for their implementation from different modalities, in multi-modal or multi-device mode.	OWSER 1.0
INTEROP-5	The OMA Web Services Enabler MUST allow binding to different transport protocols and network technologies.	OWSER 1.0
INTEROP-6	1. The OMA Web Services Enabler must support mobile web services with services exchanges that are: a. Server-to-server b. Server-to-mobile terminal c. Mobile terminal-to-server Mobile terminal-to-mobile terminal (or peer-to-peer)	OWSER 1.0

Table 8: Overall System Requirements – Interoperability

6.2.3 Openness

Label	Description	Enabler Release
OPEN-1	The OMA MWS specifications MUST rely on open, published and interoperable interfaces.	OWSER 1.0
OPEN-2	The OMA MWS specifications MUST provide for discoverable interfaces.	OWSER 1.0
OPEN-3	Within the OMA Web Services Enabler, multiple actors (service providers, operators, enterprises), multiple devices across multiple networks SHOULD be able to participate in the realization of a given service	OWSER 1.0
OPEN-4	Within the OMA Web Services Enabler, it SHOULD be possible for all actors to advertise their enabler into a repository and then be plugged into the service infrastructure for a user, by user selection	OWSER 1.0

Table 9: Overall System Requirements – Openness

6.2.4 Integration with the World Wide Web

Label	Description	Enabler Release
WWW-1	Web Services MUST be able to rely on standard protocols used on the WWW (such as HTTP, HTTPS) wherever possible.	OWSER 1.0

WWW-2	Service provisioning MUST be compatible with WWW web service standards (e.g. [OASIS WS Provisioning])	OWSER 1.0
WWW-3	Service security MUST be compatible with WWW web service standards (e.g. [Oasis-WS-S])	OWSER 1.0
WWW-4		
WWW-5	Formats and profiles MUST be able to interoperate with WWW web service standards	OWSER 1.0
WWW-6	The OMA Web Services Enabler SHOULD satisfy whenever possible the requirements expressed in [WSAR]	OWSER 1.0

Table 10: Overall System Requirements – Integration with the World Wide Web

6.2.5 Web Services QoS

Label	Description	Enabler Release
QOS-1	The MWS specifications MUST provide mechanism to optimize web service performances (delays, bandwidth for delays).	OWSER 1.0
QOS-2	The MWS specifications SHOULD expose the quality of service e.g., Delays, available bandwidth, response time	OWSER 1.0

Table 11: Overall System Requirements – Web Services QoS

6.2.6 Distributed modularization and loose coupling

Label	Description	Enabler Release
DIST-1	The OMA MWS specifications MUST support the deployments of applications that result from combination and composition of loosely coupled web services from different service and content providers (any actors including terminals), each maintaining its separate administrative boundary and trust domain.	OWSER 1.0
DIST-2	The OMA MWS specifications MUST enable web services to discover other instances by their names or by other structured attributes. These may be specific to the mobile aspect of the web service. such as coverage that include a particular present or target location, etc…	OWSER 1.0
DIST-3	The OMA MWS specifications MUST support Web service with a user interface on terminal devices e.g. in the form of suitable mark-up pages with embedded scripts, or similar. i.e., mobile-to-server communication should be possible using this technology.	OWSER 1.0
DIST-4	The MWS specifications SHOULD enable an application or enabler to aggregate, combine or compose Mobile web services on the server, in the network or on the mobile device.	OWSER 1.0
DIST-5	The OMA MWS specifications SHOULD allow accommodation to future evolution of technology and business models.	OWSER 1.0
DIST-6	Within the OMA Web Services Enabler, enablers and applications SHOULD be able to control the composition and usage of web services	OWSER 1.0

Table 12: Overall System Requirements – Distributed modularization and loose coupling

6.2.7 Reliability

Label	Description	Enabler Release
REL-1	The OMA Web Services Enabler MUST be designed to provide reliable exchanges especially when exchanges take place over the mobile network e.g. events / updates, user interface exchanges or Web service coordination exchanges	OWSER 1.0
REL-2	1. The OMA MWS specifications MUST enable usage of Mobile Web Services when connectivity is intermittent: a. Connectivity of the terminal b. "visibility" or presence of the service i. Service roaming ii. Service address changes Service instances switches	OWSER 1.0
REL-3	Mobile services in general require very high degrees of reliability and stability of service. This MUST be provided by the OMA Web Services Enabler. For example, once a user selects an identity services provider the service MUST remain reliable and be evolvable over time.	OWSER 1.0

Table 13: Overall System Requirements – Reliability

6.3 System Elements

6.3.1 Terminal Devices

Label	Description	Enabler Release
TERM-1	The OMA Web Services Enabler SHOULD enable support for both Web Service Requestors and Web Services on mobile terminals. Such support MAY involve Mobile profiles of Internet/Web services protocols	OWSER 1.0

Table 14: System Elements – Terminal Devices

6.3.2 Network interfaces

Label	Description	Enabler Release
NET-INT-1	The OMA MWS specifications MUST provide interfaces and supporting protocols (e.g. discovery) that can be accessed across the network.	OWSER 1.0
NET-INT-2	The OMA MWS specifications MUST enable all actors (e.g. service providers and operators) to provide each other with an HTTP/TCP/IP-based network interface	OWSER 1.0
NET-INT-3	The OMA Web Services Enabler SHOULD be agnostic w.r.t. terminal-to-base station network interface and the base station-to-PLMN interfaces.	OWSER 1.0

Table 15: System Elements – Network interfaces

Appendix A. Normative

Label	Description	Enabler Release
APP1-1	The OMA MWS specifications SHOULD support exposing location-related functions as Web services.	OWSER 1.0
APP1-2	The OMA MWS specifications SHOULD support exposing notification, push or messaging -related functions as Web services..	OWSER 1.0
APP1-3	The OMA MWS specifications SHOULD support exposing billing, charging and rating-related functions as Web services.	OWSER 1.0
APP1-4	The OMA MWS specifications SHOULD support exposing presence-related functions as Web services	OWSER 1.0
APP1-5	The OMA MWS specifications SHOULD support exposing device management-related functions as Web services.	OWSER 1.0
APP1-6	The OMA MWS specifications SHOULD support exposing download-related functions as Web services.	OWSER 1.0
APP1-7	The OMA MWS specifications SHOULD support exposing DRM-related functions as Web services.	OWSER 1.0
APP1-8	The OMA MWS specifications SHOULD support exposing payment and M_COMMERCE-related functions as Web services.	OWSER 1.0
APP1-9	The OMA MWS specifications SHOULD support multimodal synchronization if the user interfaces between modalities or devices (UI events and presentation manipulations).	OWSER 1.0
APP1-10	The OMA MWS specifications SHOULD support exposing profiles, personalization and preference-related functions as Web services.	OWSER 1.0
APP1-11	The OMA MWS specifications SHOULD support exposing and enabling backup of personal data that is on mobile terminal.	OWSER 1.0
APP1-12	The OMA MWS specifications SHOULD support exposing QoS, bandwidth and other network measure needed to optimize or adapt applications.	OWSER 1.0
APP1-13	The OMA MWS specifications SHOULD support exposing interfaces and controls for administration of users, of available mobile web services and providers as web services.	OWSER 1.0
APP1-14	The OMA MWS specifications SHOULD support exposing smartcard-related functions as Web services. a. Motivated for example by M-COMMERCE, security use cases, DRM and UICC	OWSER 1.0
APP1-15	The OMA MWS specifications SHOULD support data synchronization-related functions as Web services.	OWSER 1.0
APP1-16	The OMA MWS specifications SHOULD support data authentication and security-related functions as Web services e.g., credential check, single sign-on, encryption, …	OWSER 1.0
APP1-17		OWSER 1.0

A.2 Deployment considerations

The following requirements are specific to implementation or deployments. They affect the OMA MWS specifications in the sense that these implementation should be supported by them.

Label	Description	Enabler Release
DEP-1	The OMA Web Services Enabler SHOULD support appropriate delegation of trust to intermediaries (e.g. to intermediaries)	OWSER 1.0
DEP-2	OMA MWS realizations SHOULD be able to satisfy all the requirements stated at originator and requestor as well as at intermediaries.	OWSER 1.0

DEP-3	It SHOULD be possible, according to some negotiated settings, for intermediaries to join a circle of trust in a system relying on the OMA Web Services Enabler.	OWSER 1.0
DEP-4	The MWS specifications SHOULD support that any OMA mobile terminals, and any other actors, plays the role of intermediary in MWS exchanges.	OWSER 1.0
DEP-5	The OMA MWS specifications SHOULD support exchanges: a. Within the IP network b. Within the Core network (expected to be conventional web services) c. Between the mobile and the core network d. Within the mobile network	OWSER 1.0
DEP-6	Through the OMA MWS interfaces, the service enablers MUST appear as web services to the consumer of the service. a. Web services features MAY be delegated to intermediaries to achieve this. b. Protocol and interface conversions MAY be implemented by intermediaries to achieve this.	OWSER 1.0
DEP-7	It SHOULD be possible for an operator to present the user with a list of service providers. a. Once a user has selected a service provider, it SHOULD be possible that the service provider always remain available on the menu of choices provided to the user or as the preferred provider for the service.	OWSER 1.0
DEP-8	The OMA Web Services Enabler MUST support mobile web services (SAP, Intermediaries) that can be hosted: a. On the server-side (e.g. service providers, enterprises, content providers) -- within the core network and beyond. b. on mobile terminals. i. A case in point is a location service that distributes sensor information from a small device.	OWSER 1.0
DEP-9	The OMA MWS specifications SHOULD support suspend and resume mode of operation for web services or enablers. Resume could be with a different device or modality.	OWSER 1.0

Appendix B. Change History (Informative)

B.1 Approved Version History

Reference	Date	Description
OMA-MWS_RD-V1_0-20031120-A.doc	20060328	OWSER 1.1 Approved TP reference OMA-TP-2006-0096-OWSER_v1_1_for_final_approval
OMA-MWS_RD-V1_0-20031120-A.doc	20031120	OWSER 1.0 Approved