



# Mobile Social Network Enabler

Draft Version 1.0 – 14 Sep 2011

---

**Open Mobile Alliance**  
OMA-ER-MobSocNet-V1\_0-20110914-D

DRAFT

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.**

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.

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

# Contents

<b>1. SCOPE</b> .....	<b>4</b>
<b>2. REFERENCES</b> .....	<b>5</b>
<b>2.1 NORMATIVE REFERENCES</b> .....	<b>5</b>
<b>2.2 INFORMATIVE REFERENCES</b> .....	<b>5</b>
<b>3. TERMINOLOGY AND CONVENTIONS</b> .....	<b>8</b>
<b>3.1 CONVENTIONS</b> .....	<b>8</b>
<b>3.2 DEFINITIONS</b> .....	<b>8</b>
<b>3.3 ABBREVIATIONS</b> .....	<b>8</b>
<b>4. INTRODUCTION</b> .....	<b>10</b>
<b>4.1 VALUE CHAIN</b> .....	<b>11</b>
<b>4.2 VERSION 1.0</b> .....	<b>11</b>
<b>5. REQUIREMENTS (NORMATIVE)</b> .....	<b>13</b>
<b>5.1 HIGH-LEVEL FUNCTIONAL REQUIREMENTS</b> .....	<b>13</b>
<b>5.2 HIGH-LEVEL MANAGEMENT REQUIREMENTS</b> .....	<b>14</b>
5.2.1 User Management Requirements .....	14
5.2.2 Generic Management Requirements .....	14
<b>5.3 GATEWAY REQUIREMENTS</b> .....	<b>15</b>
<b>5.4 DEVICE RELATED REQUIREMENTS</b> .....	<b>15</b>
<b>5.5 DEVICE API REQUIREMENTS</b> .....	<b>16</b>
<b>5.6 NETWORK API REQUIREMENTS</b> .....	<b>16</b>
<b>5.7 SECURITY AND PRIVACY REQUIREMENTS</b> .....	<b>17</b>
<b>6. ARCHITECTURAL MODEL</b> .....	<b>18</b>
<b>6.1 DEPENDENCIES</b> .....	<b>18</b>
<b>6.2 ARCHITECTURAL DIAGRAM</b> .....	<b>18</b>
<b>6.3 FUNCTIONAL COMPONENTS AND INTERFACES DEFINITION</b> .....	<b>18</b>
6.3.1 MobSocNet Enabler Functional Components.....	18
6.3.2 Entities External to the MobSocNet Enabler (Informative).....	19
6.3.3 Interfaces definition .....	20
<b>APPENDIX B. USE CASES (INFORMATIVE)</b> .....	<b>21</b>
<b>B.1 GATEWAY SCENARIO</b> .....	<b>21</b>
B.1.1 Short Description .....	21
B.1.2 Market benefits .....	21
<b>B.2 FEDERATED SCENARIO</b> .....	<b>22</b>
B.2.1 Short Description .....	22
B.2.2 Market benefits .....	22
<b>B.3 MULTIPLE DEVICES SUPPORT</b> .....	<b>22</b>
B.3.1 Short Description .....	22
B.3.2 Market benefits .....	23
<b>B.4 MULTIPLE DEVICE APPLICATIONS SUPPORT</b> .....	<b>23</b>
B.4.1 Short Description .....	23
B.4.2 Market benefits .....	24

# 1. Scope

This Enabler Release (ER) document is a combined document that includes requirements, architecture and technical specification of the Mobile Social Network (MobSocNet) Enabler.

The MobSocNet Enabler scope covers the following items:

- the requirements and reference architecture to allow interoperability between clients and servers and server-to-server federation of OMA Compliant SNs, supporting at least features such as:
  - profile discovery;
  - publication and sharing of contents, activities and follow-up actions;
- the interface between an MobSocNet Client entity and an MobSocNet Server entity (intra-domain or UNI) that support the identified features;
- the interface between MobSocNet Server entities (inter-domain or NNI) that support the identified features;
- a set of Device APIs and Network APIs, to easily integrate OMA Compliant SN with external applications, as well as an appropriate privacy framework to control access to information through these APIs;
- a set of guidelines to reuse existing OMA enablers for providing additional features (e.g. profile search using OMA MSF);

In particular, with respect to interface specification, it is in the scope of this Enabler:

- to consider the endorsement of OStatus-related specifications, in particular for server-to-server interactions;
- to consider the endorsement of OpenSocial REST protocol and/or AtomPub, in particular for client-server interactions;
- to consider the endorsement of OpenSocial JavaScript APIs as Device APIs;
- to consider to reuse OAuth 2.0 and related specifications as privacy framework for APIs;
- to consider to reuse OMA Push enabler to support notifications to MobSocNet Client entities (e.g. for follow-up actions delivery, private message delivery, user status notification, etc).

Connections with External SNs are expected (through gateways implementing proprietary interfaces) but the definition of which External Social Network will be interconnected (and how) is out-of-scope of this activity.

MobSocNet Enabler will reuse as much as possible existing technologies.

## 2. References

### 2.1 Normative References

- [RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997,  
[URL:http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)
- [RFC4234] “Augmented BNF for Syntax Specifications: ABNF”. D. Crocker, Ed., P. Overell. October 2005,  
[URL:http://www.ietf.org/rfc/rfc4234.txt](http://www.ietf.org/rfc/rfc4234.txt)
- [OSE] “OMA Service Environment”, Open Mobile Alliance™,  
[URL :http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [SCRRULES] “SCR Rules and Procedures”, Open Mobile Alliance™, OMA-ORG-SCR\_Rules\_and\_Procedures,  
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)

### 2.2 Informative References

- [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/)
- [WP-MSN] “White Paper on Mobile Social Network Work Item Investigation”, 26 April 2011, Open Mobile  
 Alliance™, URL: <http://www.openmobilealliance.org/>
- [ACTIVITYSTREAMS] URL: <http://activitystrea.ms/>
- [ATOMPUB] <http://www.ietf.org/rfc/rfc5023.txt>
- [CMIS] Content Management Interoperability Services (CMIS) Version 1.0  
 URL: <http://docs.oasis-open.org/cmisis/cmisis-v1.0/cmisis-spec-v1.0.html>
- [FOAF] The Friend of a Friend (FOAF) project. URL: <http://www.foaf-project.org/>
- [HCARD] hCard 1.0. URL: <http://microformats.org/wiki/hcard>
- [HOST-META] Hammer-Lahav, E., Cook, B., “Web Host Metadata”, Internet-Draft, Work In Progress  
 URL: <http://tools.ietf.org/html/draft-hammer-hostmeta-16>
- [MagicSig] Panzer, J., Laurie, B., and D. Balfanz, “[Magic Signatures.](#)”  
 URL: <http://salmon-protocol.googlecode.com/svn/trunk/draft-panzer-magicsig-01.html>
- [OAUTH] OAuth 2. URL: <http://oauth.net/2/>
- [OEXCHANGE] URL: <http://www.oexchange.org/>
- [OExchange-Spec] “OExchange Technical Specification”  
 URL: <http://www.oexchange.org/spec/>
- [OMA- Autho4API] “Authorization Framework for Network APIs (1.0)”, Open Mobile Alliance™,  
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMACAB] “Converged Address Book”, Open Mobile Alliance™, OMA-ERP-CAB-V1\_0,  
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMACAB\_APIs] “Converged Address Book APIs”, Open Mobile Alliance™, OMA-WID\_0215-CAB\_APIs-V1\_0,  
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMACAB1.1] “Converged Address Book v.1.1”, Open Mobile Alliance™, OMA-WID\_0217-CAB-V1\_1-20110301-A,  
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMACMI] “Content Management Interface”, Open Mobile Alliance™, OMA-ERP-CMI-V1\_0,  
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMACPM] “Converged IP Messaging”, Open Mobile Alliance™, OMA-ERP-CPM-V1\_0,  
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)

[OMACSEA]	“Client-Side Enabler API”, Open Mobile Alliance™, OMA-RRP-CSEA-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMADCD]	“Dynamic Content Delivery”, Open Mobile Alliance™, OMA-ERP-DCD-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMADPE]	“Device Profiles Evolution”, Open Mobile Alliance™, OMA-ERP-DPE-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMAMSF]	“Mobile Search Framework”, Open Mobile Alliance™, OMA-ERP-MsrchFramework-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMANGSI]	“Next Generation Service Interfaces”, Open Mobile Alliance™, OMA-ERP-NGSI-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMANGSI-S]	“SOAP Binding for NGSI V1.0”, Open Mobile Alliance™, OMA-ERP-NGSI_S-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMAParlayREST2]	“RESTful bindings for Parlay X Web Services v.2.0”, Open Mobile Alliance™, OMA-ERP-ParlayREST-V2_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMAPOC]	“Push to talk over Cellular”, Open Mobile Alliance™, OMA-ERP-PoC-V2_1, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMA-Privacy]	“Privacy Requirements for Mobile Services”, Open Mobile Alliance™, OMA-RRP-Privacy-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMAPSA]	“Parlay Service Access”, Open Mobile Alliance™, OMA-RRP-PSA-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMAPUSH]	“Push Over The Air”, Open Mobile Alliance™, OMA-TS-PushOTA-V2_3, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMARC_APIs]	“APIs for Rich Communications”, Open Mobile Alliance™, OMA-WID_0213-RCS_APIs-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMASCAB]	“CAB architecture simplification with new market requirements”, Open Mobile Alliance™, OMA-WID_0214-SimplifiedCAB-V1_0-20101221-A, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMA-SIMPLE-IM]	“Instant Messaging”, Open Mobile Alliance™, OMA-ERP-SIMPLE_IM-V1_0, <a href="http://www.openmobilealliance.org/">URL: http://www.openmobilealliance.org/</a>
[OMASUPM]	“Service User Profile Management”, Open Mobile Alliance™, OMA-ERP-Service_User_Profile_Management-V1_0, <a href="http://www.openmobilealliance.org/">URL: http://www.openmobilealliance.org/</a>
[OMAWRAPI]	“Web Runtime API”, Open Mobile Alliance™, OMA-WID_0210-WRAPI-V1_0, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[OMAXDM]	“XML Document Management”, Open Mobile Alliance™, OMA-ERP-XDM-V2_1, <a href="http://www.openmobilealliance.org/">URL:http://www.openmobilealliance.org/</a>
[ONESOCIALWEB]	URL: <a href="http://onesocialweb.org">http://onesocialweb.org</a>
[OPENID]	OpenID Foundation website. URL: <a href="http://openid.net/">http://openid.net/</a>
[OPENID-AX]	OpenID Attribute Exchange 1.0 – Final. URL: <a href="http://openid.net/specs/openid-attribute-exchange-1_0.html">http://openid.net/specs/openid-attribute-exchange-1_0.html</a>
[OPENLIKE]	<a href="http://openlike.org/">http://openlike.org/</a>
[OPENSOCIAL]	OpenSocial. URL: <a href="http://www.opensocial.org/">http://www.opensocial.org/</a>
[OSTATUS]	URL: <a href="http://ostatus.org/">http://ostatus.org/</a>
[OStatus-Spec]	Prodromou, E., Vibber, B., Walker, J., Copley, Z., “OStatus 1.0 Draft 2” URL: <a href="http://ostatus.org/sites/default/files/ostatus-1.0-draft-2-specification.html">http://ostatus.org/sites/default/files/ostatus-1.0-draft-2-specification.html</a>
[POCO]	Portable Contacts. URL: <a href="http://portablecontacts.net/">http://portablecontacts.net/</a>
[PuSH]	URL: <a href="http://pubsubhubbub.googlecode.com/svn/trunk/pubsubhubbub-core-0.3.html">http://pubsubhubbub.googlecode.com/svn/trunk/pubsubhubbub-core-0.3.html</a>
[MSRP]	“The Message Session Relay Protocol (MSRP)”, B. Campbell et al, September 2007, URL: <a href="http://www.ietf.org/rfc/rfc4975.txt">http://www.ietf.org/rfc/rfc4975.txt</a>

[SALMON]	Salmon Protocol, <a href="http://www.salmon-protocol.org/">http://www.salmon-protocol.org/</a>
[Salmon-Protocol]	Panzer, J., "The Salmon Protocol" URL: <a href="http://salmon-protocol.googlecode.com/svn/trunk/draft-panzer-salmon-00.html">http://salmon-protocol.googlecode.com/svn/trunk/draft-panzer-salmon-00.html</a>
[SIMPLE]	SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE), <a href="http://datatracker.ietf.org/wg/simple/">http://datatracker.ietf.org/wg/simple/</a>
[SIOC]	URL: <a href="http://sioc-project.org/">http://sioc-project.org/</a>
[SIP]	"SIP: Session Initiation Protocol", J. Rosenberg et al, June 2002, URL: <a href="http://www.ietf.org/rfc/rfc3261.txt">http://www.ietf.org/rfc/rfc3261.txt</a>
[SWAT0]	<a href="http://www.w3.org/2005/Incubator/federatedsocialweb/wiki/SWAT0">http://www.w3.org/2005/Incubator/federatedsocialweb/wiki/SWAT0</a>
[VCARD]	"vCard MIME Directory Profile", <a href="http://www.ietf.org/rfc/rfc2426.txt">http://www.ietf.org/rfc/rfc2426.txt</a>
[W3C-FSW]	W3C Federated Social Web Incubator Group URL: <a href="http://www.w3.org/2005/Incubator/federatedsocialweb/">http://www.w3.org/2005/Incubator/federatedsocialweb/</a>
[WEBFINGER]	URL: <a href="http://webfinger.org">http://webfinger.org</a>
[WebFingerProtocol]	"WebFinger Protocol", <a href="http://code.google.com/p/webfinger/wiki/WebFingerProtocol">http://code.google.com/p/webfinger/wiki/WebFingerProtocol</a>
[WEBID]	WebID 1.0. URL: <a href="http://payswarm.com/webid/">http://payswarm.com/webid/</a>
[XFN]	XHtml Friends Network. URL: <a href="http://gmpg.org/xfn/">http://gmpg.org/xfn/</a>
[XMPP]	XMPP Standards Foundation. URL: <a href="http://xmpp.org/">http://xmpp.org/</a>
[XRD]	Extensible Resource Descriptor (XRD) Version 1.0. URL: <a href="http://docs.oasis-open.org/xri/xrd/v1.0/xrd-1.0.html">http://docs.oasis-open.org/xri/xrd/v1.0/xrd-1.0.html</a>

DRAFT

## 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

<b>Aggregation</b>	This is defined as the ability to connect to External Social Networks using the SN service specific credentials to access information related to friends (e.g. status, contact details, activities) via the exposed interfaces. Aggregation in SNs is related to only Inbound interaction.
<b>Cross-posting</b>	This is defined as the ability to connect to External Social Networks using the SN service specific credentials to share information (e.g. status, media) via the exposed interfaces. Cross-posting in SNs is related to only Outbound interaction.
<b>External Social Network</b>	A social network that is not-OMA Compliant and made available through either proprietary or non-proprietary mechanism and/or interfaces
<b>Federated Social Networks</b>	This is defined by a set of social networks that share some level of trust or set of rules, data formats and protocols, while, each social network retains its own administrative control and structure. The trust or set of rules binding the social networks govern the information that can be shared/searched/exchanged among users who are part of the respective social network.
<b>Inbound/Outbound interactions</b>	Inbound interactions relate to the concept of Aggregation of activities and media from External Social Networks, making thus possible to allow users that own accounts on multiple External SNs to access aggregated information about their friends (e.g. contact information, activities) on these networks. Outbound interactions, on the opposite, relate to the ability of Cross-posting activities and/or media to multiple External SNs. In this way, users could potentially share their activities over all their External SNs at once.
<b>OMA Compliant Social Network</b>	This is defined as a social network that conforms to the MobSocNet Enabler, essentially to ensure seamless interoperability and satisfaction of various actors in a social network. OMA Compliant Social Networks are natively Federated Social Networks.

### 3.3 Abbreviations

<b>API</b>	Application Programming Interface
<b>JSON</b>	JavaScript Object Notation
<b>MSISDN</b>	Mobile Subscriber ISDN Number
<b>MSN</b>	Mobile Social Network
<b>OMA</b>	Open Mobile Alliance
<b>NNI</b>	Network to Network Interface
<b>RCS</b>	Rich Communication Suite
<b>RDF</b>	Resource Description Framework
<b>RSS</b>	Really Simple Syndication
<b>SDO</b>	Standards Development Organization
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SN</b>	Social Network

<b>SNS</b>	Social Network Service
<b>SSL</b>	Secure Sockets Layer
<b>TLS</b>	Transport Layer Security
<b>UNI</b>	User to Network Interface
<b>URI</b>	Uniform Resource Identifier
<b>URL</b>	Uniform Resource Locator
<b>XML</b>	Extensible Markup Language
<b>XMPP</b>	Extensible Messaging and Presence Protocol

DRAFT

## 4. Introduction

Thanks to Web 2.0 technologies, the World Wide Web has turned into a social space, moving from document links to people links. Individuals and organizations are now linked and leverage on user-generated content, communities, networking and social interaction.

Whilst the Web is becoming increasingly social, social networking itself is heavily fragmented due to the multitude of disparate services that are popular among users.

The existing hundreds of social network sites available on the Internet are based on centralised isolated systems and works standalone, ignoring other siblings, implementing a “walled garden” approach. Users on one Social Network (SN) cannot (easily) interact with users on another Social Network and people will often have to sign up for an account on multiple SNs to keep in touch with different groups of friends.

Unfortunately, or fortunately, there is no single social graph (or even multiple which interoperate) that is comprehensive and decentralized. Rather, these several disperse social graphs are often operated by a single company, sometimes small and with unproven record. This inconvenience ultimately results in a few very large networks with an inordinate amount of control over peoples’ most personal data and a lack of choice and privacy for users.

In this regard, such walled gardens are data silos where user data can easily be inserted, but only accessed and manipulated via proprietary interfaces for humans and machines. This further prevents users from moving easily from one SN provider to another as their social data cannot be shared across networks.

The MobSocNet Enabler aims at allowing large-scale deployments and interoperability of MobSocNet Clients and MobSocNet Servers in a timely manner, further guaranteeing social network federation so that users can easily communicate with users on other SNs and migrate their data. In particular, this document identifies a coherent subset of functionalities specific to MobSocNet representing a core specification.

The Figure 1 shows the overall ecosystem related to Mobile Social Network Enabler. In particular, the user (within the red circle) owns an account on a specific OMA Compliant SN (“his/her SN”), and interacts with users belonging either to his/her SN, or to another OMA Compliant SN, or to an External SN through the gateway functionality. Users access MobSocNet functionalities through multiple devices, each of them capable of running multiple applications.

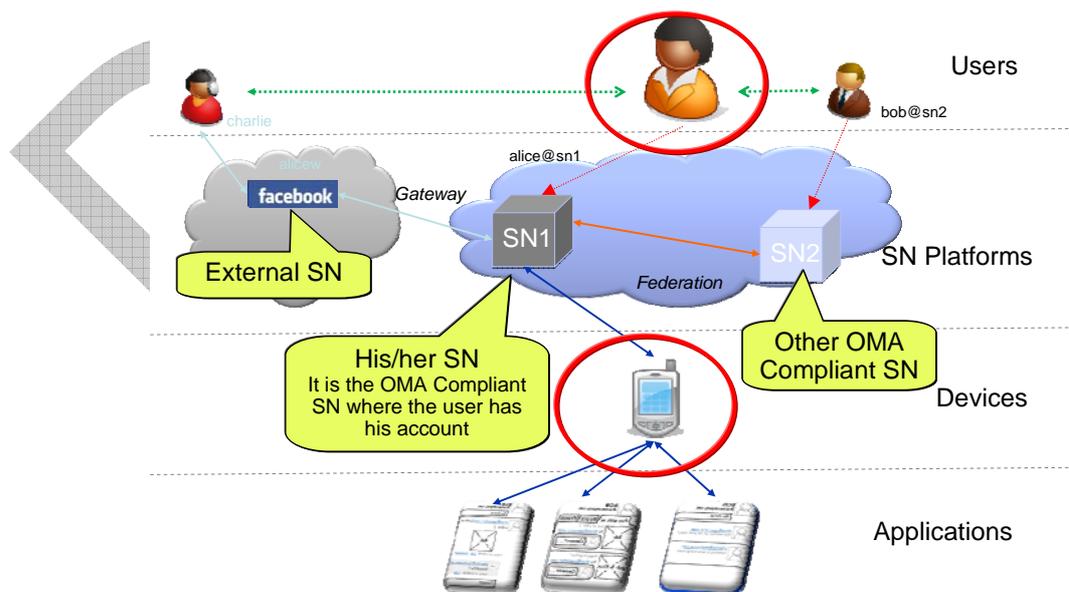
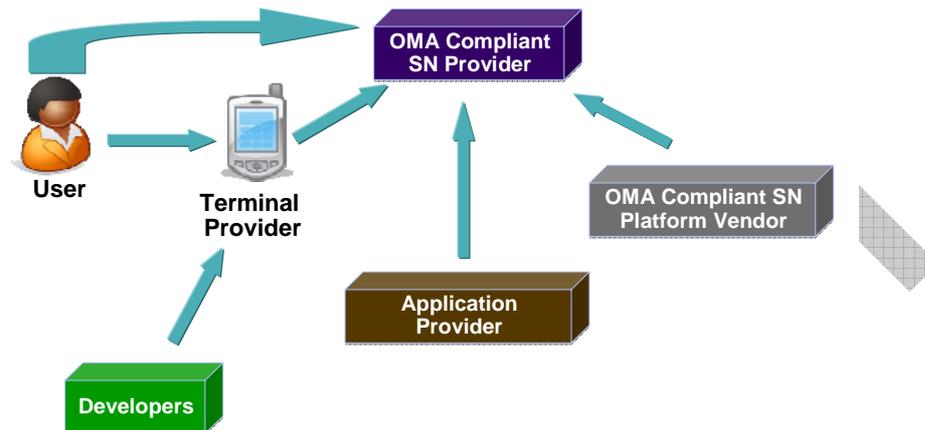


Figure 1: Social Network ecosystem.

## 4.1 Value Chain

In the ecosystem of mobile social networks, the interoperability will effectively connect all dots together and benefit all stakeholders in the value chain. The aspects of the Mobile Social Network (MobSocNet) value chain are provided in Figure 2.



**Figure 2: Mobile Social Network Value Chain**

Subscribers / end users will have more options and freedom to use the mobile social network services which they feel more valuable without having to switch operators or devices. End users and their friends will be able to interact with each other more conveniently across mobile social networks.

Operators (MobSocNet provider) will have more customer loyalty and will be able to retain customers by letting subscribers communicate with friends across different social network services. Furthermore, operators will also be able to increase their customer base and improve ARPU by offering unique, differentiated value of their mobile social network service to subscribers. Platform migration across vendors will be seamless for core features.

Manufacturers will be able to provide devices that can connect to all social network services irrespective of the operators. Thus, the manufacturers will benefit from customer loyalty, lowering the development cost, shortening the time to market, and increasing the market share by outreaching the broader market.

Vendors will be able to differentiate their offering by providing rich appealing features within a single social network, whilst all of them offering basic and common interoperable features.

Authorized Providers will be able to access end users' social data from the mobile social network, thus enabling them to provide richer services and applications to attract the user and thereby generate revenue.

Developers will also benefit this value chain by providing richer applications or widgets according to the mobile social network APIs. It will be for example possible to arrange an application store combined with mobile social network for expanding the usage of the applications and widgets.

## 4.2 Version 1.0

The version 1.0 of the MobSocNet Enabler SHALL cover at least:

- the interoperability between clients and servers and server-to-server federation of OMA Compliant SNs, supporting at least features such as:
  - profile discovery;
  - publication and sharing of contents, activities and follow-up actions;
- a set of Device APIs and Network APIs, to easily integrate OMA Compliant SN with external applications, as well as an appropriate privacy framework to control access to information through these APIs

DRAFT

## 5. Requirements (Normative)

This section identifies the requirements necessary for the Mobile Social Network Enabler to support end-to-end interoperability across different devices, networks, service providers and network operators.

The requirements below are related to the Use Cases described in Appendix B.

### 5.1 High-Level Functional Requirements

This section identifies the high-level functional requirements for the Mobile Social Network Enabler.

Label	Description	Release
MSN-HLF-001	The MobSocNet Enabler SHALL allow a user to perform at least the following activities: <ul style="list-style-type: none"> <li>• posting a text (e.g. update his status, write a blog post);</li> <li>• upload a multimedia content (e.g. image, video, audio);</li> <li>• share a link (e.g. video link, audio link, website link);</li> <li>• perform check-in on an entity (e.g. check-in a place).</li> </ul>	1.0
MSN-HLF-002	The MobSocNet Enabler SHALL allow a user to perform at least the following follow-up actions on existing activities: <ul style="list-style-type: none"> <li>• like;</li> <li>• comment.</li> </ul>	1.0
MSN-HLF-003	The MobSocNet Enabler SHALL allow a user to follow another users activities and follow-up actions on his/her SN.	1.0
MSN-HLF-004	The MobSocNet Enabler SHALL allow a user to follow another users activities and follow-up actions on another OMA Compliant SN.	1.0
MSN-HLF-005	The MobSocNet Enabler SHALL allow a user to perform activities and/or follow-up actions in relation with at least the following entities: <ul style="list-style-type: none"> <li>• user;</li> <li>• content;</li> <li>• place.</li> </ul>	1.0
MSN-HLF-006	The MobSocNet Enabler SHOULD allow a user to perform activities and/or follow-up actions in relation with at least the following entities: <ul style="list-style-type: none"> <li>• group;</li> <li>• event.</li> </ul>	1.0
MSN-HLF-007	The MobSocNet Enabler SHALL allow a user to be identified through a globally unique identifier across OMA Compliant SNs through the use of at least one of the following form: <ul style="list-style-type: none"> <li>• MSISDN;</li> <li>• Email-like address (user@domain).</li> </ul>	1.0
MSN-HLF-008	The MobSocNet Enabler SHALL allow notifying users ("push"-mode) of activities or follow-up actions they are related to (e.g. friend updates, picture tagging notification, comment received, etc), including activities or follow-up actions from users of other OMA Compliant SNs.	1.0
MSN-HLF-009	The MobSocNet Enabler SHOULD support interacting with External SNs in Inbound and/or Outbound directions (gateway functionality).	1.0
MSN-HLF-010	The MobSocNet Enabler SHALL provide means for users to share links when browsing external websites (e.g. through a "share" button).	1.0

MSN-HLF-011	<p>The MobSocNet Enabler SHOULD allow a user to enquire through which users he/she can contact another user within his/her SN.</p> <p><b>Informational Note:</b> User A would like to get acquainted with User B. User A has a friend User 1, who is also a friend of User 2, and User 2 is in the friend list of User 3. User 3 knows User B very well. Thus, we have the following user chain: User A -&gt; User 1 -&gt; User 2 -&gt; User 3 -&gt; User B. With this user chain, User A will be able to be introduced to User B. The internal process of how these users in the chain are identified is out of scope</p>	1.0
MSN-HLF-012	<p>The MobSocNet Enabler SHALL allow a user to exchange private one-shot messages with one or more other users on his/her SN.</p> <p><b>Informational Note:</b> One-shot messages refer to messages sent to another user not related to a conversation session. On the other side, conversation messages enable users to exchange messages in a conversation session.</p>	1.0
MSN-HLF-013	<p>The MobSocNet Enabler SHOULD allow a user to exchange private one-shot messages with one or more others users on other OMA Compliant SN.</p>	1.0

## 5.2 High-Level Management Requirements

This section identifies the high-level management requirements for the Mobile Social Network Enabler. The detailed requirements are further identified in the following sections according to the detailed functions identified.

### 5.2.1 User Management Requirements

Label	Description	Release
MSN-UMG-001	<p>The MobSocNet Enabler SHALL allow a user to perform the following actions:</p> <ul style="list-style-type: none"> <li>• Create an account and obtain an identity on an OMA Compliant SN;</li> <li>• Delete his/her account and all related information (e.g. profile, activities) from his/her SN.</li> </ul>	1.0
MSN-UMG-002	<p>The MobSocNet Enabler SHALL allow a user to delete specific activities and follow-up actions he/she performed previously.</p>	1.0
MSN-UMG-003	<p>The MobSocNet Enabler SHOULD allow a user to update the activities and follow-up actions he/she performed previously (e.g. the user has uploaded an image with a misspelled title and he/she wants to fix the title).</p>	1.0
MSN-UMG-004	<p>The MobSocNet Enabler SHOULD allow to search for a user identity within an OMA Compliant SN, e.g. based on email, name, or other attribute.</p>	1.0
MSN-UMG-005	<p>The MobSocNet Enabler SHALL support user's profile to be discovered across OMA Compliant SNs based on user identity and according to user's privacy settings.</p>	1.0
MSN-UMG-006	<p>The MobSocNet Enabler SHOULD allow a user to block reception of specific or all information/messages:</p> <ul style="list-style-type: none"> <li>- from specific users</li> <li>- from specific OMA Compliant SNs</li> <li>- from specific External SNs</li> </ul> <p><b>Informational Note:</b> the exact set of information/messages to be blocked is FFS</p>	1.0

### 5.2.2 Generic Management Requirements

Label	Description	Release
MSN-GMG-001	<p>The MobSocNet Enabler SHOULD allow a user to report abuse/inappropriate activities, follow-up actions, content, users and applications providing a reason for the report.</p>	1.0

## 5.3 Gateway Requirements

This section identifies the detailed gateway requirements for the Mobile Social Network Enabler. These requirements are only applicable when the gateway functionality is supported as in MSN-HLF-009.

Label	Description	Release
MSN-GWR-001	The MobSocNet Enabler SHALL allow a user to associate his/her identity on External SNs with his/her SN account.	1.0
MSN-GWR-002	The MobSocNet Enabler SHALL allow a user to delete the association between his/her identity on External SNs and his/her SN account.	1.0
MSN-GWR-003	The MobSocNet Enabler SHALL support importing/aggregating at least the following information from the External associated SNs, when supported by the External SNs: <ul style="list-style-type: none"> <li>• user own activities (e.g. status update, link sharing, follow up actions, etc)</li> <li>• friends activities.</li> </ul>	1.0
MSN-GWR-004	The MobSocNet Enabler SHALL allow a user to select External SNs for Outbound interactions.	1.0
MSN-GWR-005	The MobSocNet Enabler SHALL support performing at least the following actions towards the selected External SNs, when supported by the External SNs: <ul style="list-style-type: none"> <li>• posting user own activities (e.g. status update, link sharing, follow up actions, content upload, etc).</li> </ul>	1.0

## 5.4 Device related Requirements

This section identifies the requirements for the device-side of the Mobile Social Network Enabler related to the support of multiple applications running in a device that interact with SNs. The interactions with External SNs are only applicable when the gateway functionality is supported as in MSN-HLF-009.

Label	Description	Release
MSN-DEV-001	The MobSocNet Enabler SHALL allow different applications running in a device to bidirectionally communicate with OMA Compliant SNs and, provided that the gateway functionality is supported, with External SNs.	1.0
MSN-DEV-002	The MobSocNet Enabler SHALL rely on a component on the device, which centralizes communications between device applications and the OMA Compliant SN and (through the gateway functionality) External SNs	1.0
MSN-DEV-003	The MobSocNet Enabler SHALL rely on a component on the device to locally cache information uploaded to or downloaded from an OMA Compliant SN / External SNs to make it available to local device applications.	1.0
MSN-DEV-004	When a device application requests information, the MobSocNet Enabler SHALL ensure that the component on the device first accesses locally cached information on behalf of the device application, subject to the policies relevant for that specific application, prior to have it retrieved from the network.	1.0
MSN-DEV-005	When the component on the device receives information from the OMA Compliant SN, the MobSocNet Enabler SHALL ensure that: <ul style="list-style-type: none"> <li>- when the information relates to a deleted action, that action is deleted from the local cache so that it is not available anymore to local device applications;</li> <li>- when the information relates to an updated action, that action is updated in the local cache so that its new version becomes available to local device applications.</li> </ul>	1.0

MSN-DEV-006	The MobSocNet Enabler SHALL rely on a component on the device to queue user's activities and follow-up actions when offline (or inaccessible due to server problems) and process them automatically when back online (or accessible) removing them from the queue when processed, based on user preferences.	1.0
MSN-DEV-007	The MobSocNet Enabler SHALL allow the user to manage (e.g. remove, edit) items from the activities and follow-up actions queue on the device.	1.0

## 5.5 Device API Requirements

This section identifies the requirements for the Mobile Social Network Enabler related to Device APIs. The interactions with External SNs are only applicable when the gateway functionality is supported as in MSN-HLF-009.

MSN-DAPI-001	The MobSocNet Enabler SHALL mutually authenticate with device applications willing to use the MobSocNet Device API.  <b>Informational Note:</b> mutual authentication means that device applications authenticate themselves to certify their origin and the MobSocNet Enabler component on the device also certifies its authenticity	1.0
MSN-DAPI-002	The MobSocNet Enabler SHALL provide a Device API to device applications that allows them to specify which kind of information/notifications it wants to receive and which kind of activities it wants to perform (see MSN-HLF-001 to MSN-HLF-004) from/towards each OMA Compliant SN / External SN.	1.0
MSN-DAPI-003	The MobSocNet Enabler SHALL provide a Device API to allow device applications to specify data traffic and time constraints (e.g. frequency of polling or notifications from OMA Compliant SNs and External SNs), subject to policies (e.g. service provider policies, device configuration policies).	1.0
MSN-DAPI-004	The MobSocNet Enabler SHALL ensure that device applications using Device API obtain user authorization for the requested interactions (see MSN-DAPI-002).	1.0
MSN-DAPI-005	The MobSocNet Enabler SHALL ensure that only authorized device applications are able to use the MobSocNet Device API.	1.0
MSN-DAPI-006	The MobSocNet Enabler SHALL provide a Device API to device applications that allows them to perform activities and/or receive information/notifications with OMA Compliant SNs and External SNs	1.0
MSN-DAPI-007	The MobSocNet Enabler SHALL allow access to the MobSocNet Device API to multiple device applications simultaneously.	1.0
MSN-DAPI-008	The MobSocNet Enabler SHALL support callback mechanisms in the MobSocNet Device API:  - to allow device applications to register callbacks, - to callback device applications (based on previous registration).  <b>Informational Note:</b> Callback events consist of specific notifications/ messages from OMA Compliant SNs, External SNs and local events (e.g. communication failures).	1.0

## 5.6 Network API Requirements

This section identifies the requirements for the Mobile Social Network Enabler related to Network APIs.

MSN-NAPI-001	The MobSocNet Enabler SHALL provide a Network API to third-party applications that allows them to perform activities and/or receive information/notifications with an OMA Compliant SN.	1.0
MSN-NAPI-002	The MobSocNet Enabler SHALL provide a Network API to third-party applications that allows them to specify which kind of information/notifications it wants to receive and which kind of activities it wants to perform (see MSN-HLF-001 to MSN-HLF-004) from/towards an OMA Compliant SN.	1.0
MSN-NAPI-003	The MobSocNet Enabler SHALL ensure third-party applications be authorized before interacting through the MobSocNet Network API.	1.0
MSN-NAPI-004	The MobSocNet Enabler SHALL ensure that third-party applications using the MobSocNet Network API obtain user authorization for the requested interactions (see MSN-NAPI-002) with an OMA Compliant SN.	1.0

## 5.7 Security and Privacy Requirements

This section identifies the requirements for the Mobile Social Network Enabler related to security and privacy. In particular, such requirements encompass authentication, authorization and privacy mechanisms and settings.

Label	Description	Release
MSN-SEC-001	The MobSocNet Enabler SHALL allow a user to define the privacy level of his activities or follow-up actions to control visibility by other users, including at least: <ul style="list-style-type: none"> <li>• Public: accessible by all users;</li> <li>• Private: accessible only by the user owning the information</li> <li>• Followers: accessible only by the user's followers</li> </ul> <b>Informational Note:</b> other users can pertain to the same or another OMA Compliant SN.	1.0
MSN-SEC-002	The MobSocNet Enabler SHALL allow a user to grant and revoke permissions to external applications (interacting with the MobSocNet Enabler) to access part or all of his/her own related information, including activities and follow-up actions. <b>Informational Note:</b> the exact definition of such permissions is FFS.	1.0
MSN-SEC-003	The MobSocNet Enabler SHALL support authentication mechanisms to authenticate requests among the various MobSocNet components (e.g. client-server, server-to-server), as well as with external applications interacting with the MobSocNet Enabler.	1.0

## 6. Architectural Model

### 6.1 Dependencies

The MobSocNet Enabler has the following dependencies to other OMA Enablers:

- The OMA Push Enabler as described in [OMAPUSH] and [OMAPUSH-PAP];

### 6.2 Architectural Diagram

The following diagram illustrates the Functional Components and Interfaces of the MobSocNet Enabler.

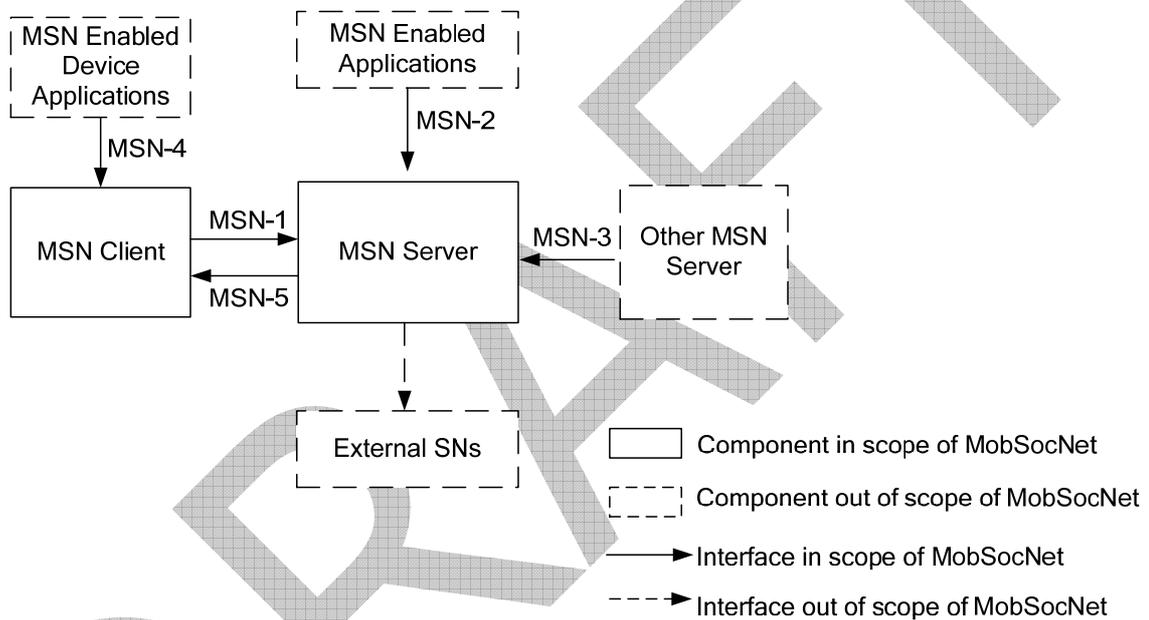


Figure 3: Mobile Social Network reference model

### 6.3 Functional Components and Interfaces definition

The MobSocNet Enabler consists of mandatory components (MSN Server and MSN Client) and interfaces exposed by those components. All other depicted components and interfaces are not specified in this document, but are shown for a better understanding of the interactions with the MobSocNet Enabler.

Both MSN Server and MSN Client are mandatory functional components of the MobSocNet Enabler.

#### 6.3.1 MobSocNet Enabler Functional Components

##### 6.3.1.1 MSN Server

The MSN Server is a MobSocNet Enabler component resident in the network (outside the device) and is the entry point to the enabler for all the requests coming from an MSN Client. It represents the central node of an OMA Compliant SN that federates with other OMA Compliant SNs. It also exposes Network APIs to 3<sup>rd</sup> party applications (MSN Enabled Applications) through the MSN-2 interface.

The MSN Server exposes MSN-1, MSN-2 and MSN-3. It uses MSN-5 exposed by MSN Client and MSN-3 exposed by other MSN Servers for federation.

When using the MSN-5 interface, the MSN Server acts as Push Initiator when using OMA-PAP or as Push Server when using PUSH-OTA.

The core function is the main functionality of the MSN Server responsible for providing mobile social network service to the end user. As user social data centre, it provides management features for user accounts and user activity & follow-up actions (including content management), and the related access to this data to third party applications based on user permissions. It provides native federation features with other MSN Servers, allowing “local” users to interact with users on other OMA Compliant SNs.

The core Functionality can further provide user profile management, social relationship management, and the like, although these features are out-of-scope of this enabler.

The gateway function is an optional functionality responsible for interacting with External SNs. It enables users to interconnect with external SNs on which they already have an account (e.g. Facebook, Twitter) using the proprietary interfaces of such networks.

The gateway function supports inbound interactions to aggregate activities and media from External networks, and outbound interactions for the ability of cross-posting activities and/or media to multiple External SNs. In this sense the gateway function implements the required protocol & data format translation capabilities in relation with the supported External SNs. It also provides the related management features so that users can associate their “local” account with their account on External SNs.

For these reasons there is no common interface with such External SNs identified in this enabler (the interface varies across the specific External SNs), which is thus out-of-scope. Nevertheless, the gateway function itself is defined in the MobSocNet Enabler and is optional.

### **6.3.1.2 MSN Client**

The MSN Client is a MobSocNet Enabler component resident on the device, which enables the user to connect to the MSN Server of an OMA Compliant SN and interact with users on the same or other OMA Compliant SNs, or on External SNs (if the gateway function is provided by the MSN Server).

It has the responsibility for interacting bidirectionally with MSN Server to exchange social network service information, by using MSN-1 interface and by exposing MSN-5 interface to receive push notifications. It also exposes Device APIs to 3<sup>rd</sup> party device applications (Mobile Enabled Device Applications) through the MSN-4 interface.

The MSN Client exposes MSN-4 and MSN-5 and uses MSN-1 exposed by the MSN Server.

## **6.3.2 Entities External to the MobSocNet Enabler (Informative)**

### **6.3.2.1 MSN Enabled Applications**

MSN Enabled Applications represent 3<sup>rd</sup> party applications using the MSN Network APIs exposed by an MSN Server.

### **6.3.2.2 MSN Enabled Device Applications**

MSN Enabled Device Applications represent 3<sup>rd</sup> party applications residing on the device using the MSN Device APIs exposed locally by the MSN Client.

### **6.3.2.3 Other MSN Server**

Other MSN Server represents an MSN Server entity belonging to another OMA-Compliant SN.

### **6.3.2.4 External Social Networks**

See definition.

## 6.3.3 Interfaces definition

### 6.3.3.1 MSN-1

This interface is exposed by the MSN Server and is used by the MSN Client to interact with the OMA Compliant SN.

The supported functions of this interface include:

- User account management,
- User authentication,
- User authorization to 3<sup>rd</sup> party applications to access data,
- User activity & follow-up actions management

### 6.3.3.2 MSN-2

This interface is exposed by the MSN Server to the network-side MSN Enabled Applications. As such, MSN-2 represents a Network API.

### 6.3.3.3 MSN-3

This interface is exposed by the MSN Server to other MSN Servers for realizing the federation between OMA Compliant SNs. It enables the activity, follow-up actions and media exchange between two different OMA Compliant SNs.

As such, this interface is both exposed, and used, by MSN Servers.

### 6.3.3.4 MSN-4

This interface is exposed by the MSN Client to MSN Enabled Device Applications running on the device, according to their specific needs and permissions. As such, MSN-4 represents a Device API.

### 6.3.3.5 MSN-5

This interface is exposed by the MSN Client and is used by the MSN Server to push notification/information (e.g. content, user activities, follow-up actions) to the MSN Client and through it to MSN Enabled Device Applications.

MSN-5 relies on Push-OTA protocol [PUSH-OTA] as underlying interface for receiving push on the MSN Client side. On the MSN Server side, MSN-5 can rely either on the Push Access Protocol (PAP) [PUSH-PAP] or on Push-OTA for point-to-point delivery.

## Appendix B. Use Cases (Informative)

This Appendix provides high-level use cases focused on the users and deployment scenarios point of view, targeting release's requirements.

### B.1 Gateway Scenario

#### B.1.1 Short Description

This scenario aims at enabling users to interconnect with External SNs on which they already have an account (e.g. Facebook, Twitter, others) using the proprietary interfaces of such networks. This scenario introduces the concept of direction in interacting between an OMA Compliant SN and one or more External SNs.

In particular, Inbound interactions relate to the concept of *Aggregation* of activities and media from External networks, making thus possible to allow users that own accounts on multiple External SNs to access aggregated information about their friends (e.g. contact information, activities) on these networks. Outbound interactions, on the opposite, relate to the ability of *Cross-posting* activities and/or media to multiple External SNs. In this way, users could potentially share their activities over all their External SNs at once.

Step 1: User A updates status and gets notification based on comments from User B to the status update:

1. user A associates her identity on External SNs (SN<sub>i</sub> with i=1,2, ...) with its identity on an OMA Compliant SN using the proprietary procedures required by the External SNs
2. At a later stage, user A wants to update her status
3. user A selects to which External SN her status update will be posted and posts it (at least she selects SN 2) (*Cross-posting*)
4. user B2 is a friend of user A2 (other identity of user A) on External SN 2, and sees user's A2 new status
5. user B2 comments the new status of user A2 on External SN 2 (out-of-scope)
6. comment from user B2 gets notified to user A on her OMA Compliant SN (*Aggregation*)

Step 2: User B updates status and User A gets notification based the update:

7. user B2 updates her status on External SN 2, which is seen by user A2
8. user A gets notified of user B2 status update on her OMA Compliant SN (*Aggregation*)

This scenario aims at defining the requirements needed to enable gateway functionalities in a generic way, not addressing the peculiarities of the single External SN.

Furthermore, the concept of activity in this scenario is very generic. Whilst the scenario itself focuses on a status update, media upload and check-in activities are intended as additional valid examples.

#### B.1.2 Market benefits

Mobile operators can provide the social network gateway function in a standalone way or in addition to their own mobile social network. As such it can attract more users and provide competitive services. Users would be attracted by a social network which can provide the gateway function for communication with friends in multiple SNs.

## B.2 Federated Scenario

### B.2.1 Short Description

The federated Social Web community has defined a simple social federation scenario named “Social Web Acid Test - Level 0” [SWAT0] as an integration use case for the federated social web.

This scenario aims at enabling users to interact in a standard way across social networks run by service providers compliant with a set of interoperable specifications.

The generalized flavour of this scenario is copied here for convenience, where “different services” has to be understood as “different services on different Social Networks”:

“

1. user A takes a photo of B from their phone and posts it
2. user A explicitly tags the photo with B
3. B gets notified that they are in a photo
4. C who follows A gets the photo
5. C makes a comment on the photo
6. A and B get notified of the comment

*Where users are on at least 2 (ideally 3) different services [...], and the users only need to have \*one\* account, on the specific service of their choice (requiring the users to have an account on each service that is interacting misses the point of Federation)”*

### B.2.2 Market benefits

Social Network Federation enables users to only have \*one\* account for SN, whilst still giving them the ability to interact with users on different Federated SNs. It is thus possible to enable a Federated SN as the anchor of mobile operator’s service and other services.

The mobile operator can thus operate its own SN thus attracting its own subscribers to an interoperable SN service that allow them to communicate and interact freely with subscribers of other mobile operators.

## B.3 Multiple devices support

### B.3.1 Short Description

This scenario aims at enabling user using different mobile phones or devices to access his mobile social network services. User would like to access the mobile social network from different devices, such as using PC while at home or using a mobile phone while on the road. A user may also use multiple mobile phones to connect the social network sites. The mobile social network services need to be provided as other mobile services which are independent of the devices. Some of the operations that users can carry out in multiple devices scenario are:

1. user A accesses the mobile social network service by PC.
2. user A writes a new blog post.
3. user B accesses the mobile social network service through his mobile phone.
4. user B follows user A and get the notification to the mobile phone that user A has a new blog post.
5. user A accesses the mobile social network service using his mobile phone.

6. user B switches device, e.g. accesses the mobile social network service using his PC.
7. user A updates his status through his mobile phone.
8. user B get the notification to the PC that user A has updated his status.

### B.3.2 Market benefits

The mobile operator would set mobile social network as one major entry in the mobile services if it is device independent.

The subscribers / end users will have more options and freedom to switch mobile phones and enjoy the mobile social network with any device.

The manufacturers will be able to make the mobile phone that can connect to all mobile social network services of all operators. Thus the manufacturers will benefit from lowering the development cost, shortening the time to market, and increasing the market share by outreaching to broader markets.

## B.4 Multiple device applications support

### B.4.1 Short Description

This scenario aims at enabling multiple applications running in a device to benefit from the interworking with SNs in an optimized fashion. In fact there may be multiple applications in a device that require exchanging information with one or several SNs. Instead of managing this interworking with the SNs on their own, the applications may rely on a specialized entity in the device, i.e. the MobSocNet Client, which relieves the applications from this task by centralizing the communication with the user's OMA Compliant Social Network, which in turn interworks with other OMA or non-OMA Compliant Social Networks. The centralization of this interworking through the MobSocNet Client results also in an optimization of the use of air data traffic.

Device applications may have different needs in terms of interworking with SNs, for instance:

- Application 1: Social Network Aggregation Client, that allows a real-time interaction with multiple SNs (A, B and C):
  - Receive push notification of updates from SNs A, B and C
  - Update status and post media to SNs A, B and C
- Application 2: Multimedia Gallery application that stores all pictures from SNs A and C in which the user is tagged
  - Receive push notifications about the user having been tagged in pictures from SNs A and C.
- Application 3, Address Book application, that enriches the contacts with information from SN B
  - On demand access to contact information from SN B

As a first step the different applications have to register to the MobSocNet Client their needs in terms of interaction with the SNs. The user needs to grant permission to each application to access the requested resources and/or perform the requested operations.

Provided that the user grants access, the applications are able from that point of time to interwork with the SNs as requested, that is, the applications are provided with the information from the SNs that match the filters indicated by the application at the registration phase and are also able to post information towards the selected SNs.

A special case occurs when an application posts towards the SNs a piece of information that another application running in the same device is intended to receive. In this case the MobSocNet Client may cache this information to make it available to any other interested applications on the same device, in addition to posting it to the network. In this case there is no need to get this piece of information delivered back from the network to the MobSocNet Client, as it was generated at the device and the MobSocNet Client has already cached it locally.

## B.4.2 Market benefits

Application developers will be able to develop applications that require interaction with SNs more easily, lowering the development cost, shortening the time to market and thus increasing the application portfolio.

The end users will have a wider offer of applications to access the SNs and will get other type of applications enriched with information from the SNs.

Air data traffic will be minimized as every piece of information will be exchanged with the SNs just once even if there are multiple applications on a device that require exchanging that same piece of information with the SNs.

DRAFT