

OMA IMPS (Previously Wireless Village)

Sami I Mäkeläinen, Martin Peter Michael

Abstract— Instant messaging and presence-systems have long been popular in the “fixed” Internet world with tens of millions of PC users. The success has come despite the heterogeneous environment of multiple incompatible IM systems. In the mobile domain, however, instant messaging and presence is a relatively young thing. Hoping to avoid fragmentation in mobile IM and presence, Wireless Village was formed by key industry players to define a standard system for mobile IM and presence. The purpose of this paper is to introduce the Wireless Village initiative currently residing in the Open Mobile Alliance (OMA), its overall architecture, protocols and real life usage.

Index Terms— instant messaging, presence, OMA, IMPS, Wireless Village, WV, chat, mobile IM, mobile presence

I. INTRODUCTION

Instant Messaging services have been provided in the Internet by various vendors for a number of years. These services have proven to be extremely popular among PC users during the last decade. As Internet access became more widely available from mobile devices and capable phones increased in numbers, there arose a need to define a common set of standards for how Instant Messaging and Presence Services (IMPS) would be available from mobile devices. The ideal common standard would be agnostic of the device manufacturer, device type, geographic location, the underlying mobile communication technology and the type of software needed. A commonly accepted standard would prevent marketplace fragmentation, which would lead to multiple incompatible systems. Due to the difficulty of software updates on mobile devices, this problem is especially severe in the mobile device domain. Wireless Village attempts to solve this problem by defining a set of specifications for IMPS specifically on mobile devices.

There are currently close to two billion mobile users in the world and it's estimated that within a few years, more people will be connected to the Internet using their mobile phone than a PC. Lately it has become apparent that the way of communication itself is changing on mobile devices. Instead of just plain voice communication or text messages, there is growing interest in the importance of presence information and the possibilities of instant messaging on mobile devices [6].

This is a seminar paper for the Instant Messaging and Presence-seminar held at the department of Computer Science at the University of Helsinki in the fall of 2005. The authors are MSc students at the department of Computer Science at the University of Helsinki.

Presence is the availability and other status information of any person, application, or device to exchange information with any other person, application, or device. The power of presence is that it promises to make communication more natural and flexible; ideally, people would know beforehand what is the most appropriate way to get in touch with their contacts and when they are available for a chat.

Instant messaging is the act of sending messages to recipients and delivering them more or less instantly, without the need for the recipient to specifically fetch the messages. Combining presence, instant messaging and mobility that can be used anytime and anywhere enables powerful communications possibilities. It opens up new business opportunities as well as creates multiple new services in the mobile communication domain. Not only can mobile users communicate with other mobile users but also with users using PCs, PDAs and other devices.

The Wireless Village initiative was formed by a set of major independent companies in the communication technology area: Ericsson, Motorola and Nokia [4]. The Wireless Village defines a set of specifications for instant messaging and presence. The standard enables interoperability of mobile instant messaging and presence services by defining open standards for the different vendors to abide by. It is aimed to be a powerful catalyst for promoting a universal standard for mobile instant messaging and presence services. It also specifically aims to overcome the limitation of using specific proprietary chat technologies like Yahoo!, MSN Messenger, ICN, Skype etc by opening a well-defined way for cross-system interoperability.

In this paper, the terms OMA IMPS and Wireless Village are used interchangeably. This is due to the fact that while the name of the standardization effort has relocated to OMA IMPS, some elements in the architecture and specifications still bear the Wireless Village name.

II. HISTORY & CURRENT STATUS OF THE INITIATIVE

The Instant Messaging and Presence services have become widely available in the Internet during the last decade. PC users with Internet connections have been enjoying the different services providing ever-increasing number of features for a number of years. In the Internet, there was also a bitter fact that none of the service providers agreed to work together to provide an interoperable solution. Despite this, several of the services were successful. However, mobile devices were completely shut out of the Internet IM systems

for a long time. The closest thing to IM in the mobile world was the widespread use of SMS (Short Message Service) messages. The perceptions of the mobile devices have since changed from simple mobile phones that could only be used to make phone calls to powerful minicomputers. Applications unimaginable only five years ago are now standard on many smartphones.

However, the problem that existed on the fixed side came true for the mobile side as well. There were various manufacturers of devices, proprietary software technologies, access technologies etc. that brought even more headache for the instant messaging and presence services to resolve. The lack of interoperability between the various systems was not limited to IMPS area but also existed in other areas of mobile services.

The Open Mobile Alliance (OMA) was formed in 2002 for solving these kinds of technical issues related to mobile services. OMA defines open specifications for the mobile industry, helping to create interoperable service enablers. There are now approximately 400 companies participating in the OMA work. These include major players in the mobile industries like Nokia, Cingular, Ericsson, Qualcomm, Vodafone and many others. The main principle of OMA is to make products and services not dependent on proprietary technologies but instead create open global standards, protocols and interfaces.

To solve the standardization problem in the instant messaging and presence area, Nokia, Ericsson and Motorola formed the Wireless Village initiative in the year 2001. The first Wireless Village (WV) 1.0 specifications were published on February 2002. The initiative was then consolidated into OMA in October 2002, after which Wireless Village no longer existed as an independent organization. OMA IMPS specification v1.1 was published in November 2002. Based on Wireless Village v1.1 specifications, OMA IMPS v1.2 was published in January 2005. So far over 40 clients and servers have passed the Interoperability Testing.

Nowadays major mobile phone manufacturers often include OMA IMPS compliant applications in their mobile software by default. For example Nokia currently has 25 phone models supporting the standard [12]. There are also service providers providing OMA IMPS services; some for free and others via a subscription plan. Mobile operators, the primary target for the initiative, have so far been somewhat slow in adopting and promoting the standard. In Finland, Saunalahti was the first operator to launch OMA IMPS-compliant instant messaging services in March 2005. Work on the OMA IMPS standard is ongoing and contributors include mobile operators, wireless equipment vendors, information technology companies, content providers and others.

III. ARCHITECTURE

This chapter provides an overview of the OMA IMPS architecture and the protocols used. The reader is assumed to be familiar with the basics of 2.5G and 3G mobile packet data networks as well as the most common protocols and standards used in the Internet.

A. Overview

The conceptual high-level diagram of the solution can be seen from the following diagram. In the diagram, all radio and core network components of the mobile network such as SGSNs, GGSNs and others have been omitted for simplicity. The OMA IMPS server is usually hosted by the mobile operator.

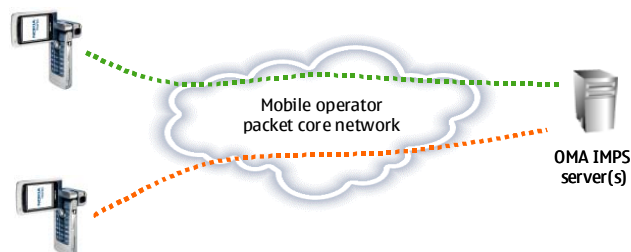


Figure 1: High-level architecture of OMA IMPS.

Immediately apparent from the high-level architecture is that unlike some popular Instant Messaging systems (like Skype or Google Talk) that utilize peer-to-peer connections, the Wireless Village solution is purely a client-server-based solution. Direct client-to-client communications do not exist under any circumstances nor are any protocols defined in the OMA IMPS specification for client-to-client communication.

While the architecture is designed mostly for the wireless environments, OMA IMPS does not limit the client devices to mobile phones; the clients can also include PC-based clients. These clients connect to the OMA IMPS system using the same protocols as clients on mobile device.

When designing the OMA IMPS architecture, principles laid out by the IETF IMPP (Internet Engineering Task Force Instant Messaging and Presence Protocol) working group were kept in mind. While OMA IMPS cannot be called fully “IMPP-compliant”, the architecture bears some resemblance to IMPP specifications. For example, references to the Common Profile for Instant Messaging (CPIM) can be seen in the architecture and the Watcher-structure for receiving presence changes is similar to that defined in IMPP.

A more detailed look at the OMA IMPS architecture and the protocols specified can be seen in Figure 2.

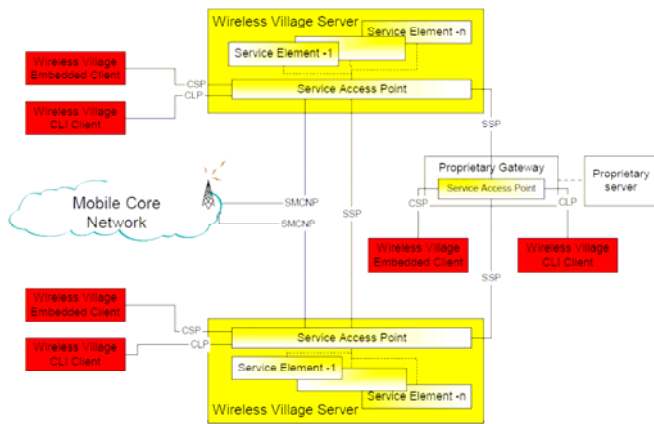


Figure 2: OMA IMPS system architecture: Entities and protocols defined in OMA IMPS specification [1].

The main elements of the architecture are:

- Wireless Village Servers
- Wireless Village Clients: embedded and CLI clients
- Mobile Core Network
- Proprietary Gateway and proprietary server(s)

The Wireless Village (WV) Servers are the core of the solution. WV Servers connect to OMA IMPS-compliant clients using the CSP and CLP protocols, to other OMA IMPS servers using the SSP protocol and to elements of the mobile core network utilizing the SMCNP protocol. A logical element within the WV Servers, Service Access Point, serves as the connection point to the other elements.

One notable feature in the architecture is the presence of an optional element called *Proprietary Gateway*. This gateway, if present, enables the IMPS system to be connected to other external IM systems that do not comply with the OMA IMPS specifications. We will examine interoperability issues more closely in section D of this chapter.

The majority of the system functionality resides in the Wireless Village servers. The following diagram depicts the functional elements of a WV server [1]:

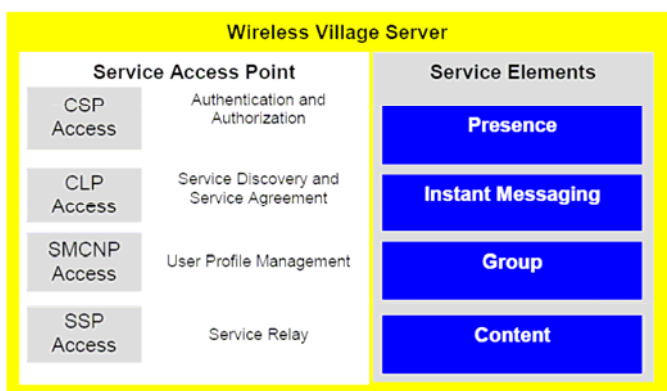


Figure 3: Logical architecture of the Wireless Village Server.

The logical component architecture of a Wireless Village server is split into two subsystems: the *Service Access Point* implements the protocols used to connect to OMA IMPS clients and other network elements and the *Service Elements* provide the actual functional implementations of the features. In addition to basic connectivity, the Service Access Point implements connection-related functions such as authentication, authorization and service discovery.

The OMA IMPS system is session-oriented in the sense that a client must have an active session with the OMA IMPS system to be able to use the service. To establish a session, clients must log in to a Service Access Point. For service discovery, the clients can either be preloaded with the address of a mobile operator’s Service Access Point or they can be manually configured.

Whether or not actual additional authentication is performed when logging in is up to the operator; the Wireless Village Server can also simply rely on the authentication performed by the mobile network. If a separate login is required, either two-way access control through the use of userid/password combination or a four-way access control employing challenge strings can be used.

B. Protocols & standards

OMA IMPS defines separate communication protocols for each of the links between the entities, including two separate protocols for two types of client entities. The defined protocols are:

1) CSP (Client Server Protocol)

CSP is the main protocol used for communication between the client devices and the Wireless Village server(s). An example of a CSP client is a mobile phone with software support for OMA IMPS specification, such as the Nokia 6680 [12]. The CSP protocol is an XML-based protocol and using it, access to the full set of available OMA IMPS services is provided.

The vast majority of the embedded or installable OMA IMPS-compliant clients utilize CSP as their communications protocol towards the Wireless Village Server. More details and examples of the CSP protocol will be presented later.

2) CLP (Command Line Protocol)

Legacy terminals use CLP to connect to the OMA IMPS system. The CLP protocol is a text-based protocol that can be used either from an embedded program or by manually entering commands in an SMS. Using CLP allows practically any existing GSM phone to be used for basic interaction (such as sending and receiving instant messages) with an OMA IMPS system.

As an example, the following is a valid CLP message of sending a message to “John” who is already assumed to be in the sender’s contact list. This SMS can be sent to the WV server, which will then deliver it to John as a normal instant

message, regardless of what protocol he uses to connect to the system.

“WV-John Hi John, how are you?”

CLP provides only a subset of the OMA IMPS services, but by using CLP, it’s possible to perform the most basic functionalities such as adding and removing contacts, fetching presence information, joining a group etc. All in all there are 17 “commands” that can be accessed using the text-based interface to OMA IMPS [15]. While such a command-line interface could be in theory used from any text-based terminal, OMA IMPS has only defined the CLP protocol to be used over an SMS bearer.

3) SSP (Server-Server Protocol)

The Wireless Village servers are connected with the SSP protocol. This protocol is used both intra-domain and inter-domain communication across different service providers (such as different mobile operators). It is also used for the communication between the Proprietary Gateway and the WV Servers. Similarly to the CSP protocol, the SSP protocol is XML-based.

The SSP connections run over HTTP or HTTPS and between two WV servers, at least two TCP connections are established: one for outgoing requests and the other for incoming requests [16]. The exchange of messages between two WV servers typically takes place in one hop over a direct connection to the other WV server. However, the servers also support routing of the messages according to business and service agreements. There is no automatic discovery of the WV servers; the configuration (connections and possible routing agreements) must take place manually.

4) SMCNP (Server Mobile Core Network Protocol)

SMCNP provides the Wireless Village servers access to the mobile core network (e.g. WCDMA CN or 2G/2.5G CN). SMCNP is used to connect to the mobile operator’s core network for the purpose of getting presence and service capability information from the operator’s network. It can also be used to aid the authentication and authorization of the users, clients and OMA IMPS servers.

However, the SMCNP cannot really be considered a protocol but rather a logical connection to the operator’s core network. This is because the OMA IMPS specification does not actually specify anything at all about the protocol. The exact protocol(s) used therefore depends on the deployment.

C. Protocol stack and examples

As seen, the name of the protocol is descriptive of its position in the architecture. Clients always communicate with the servers using either the CSP or the CLP protocol while the servers communicate with each other using the SSP protocol. For interaction with the mobile core network (MCN), the

servers utilize the SMCNP protocol.

The core protocols (CSP and SSP) defined by the OMA IMPS standard are based on XML. The protocol stack below the IMPS protocols is based on various open standards and is depicted in Figure 4:

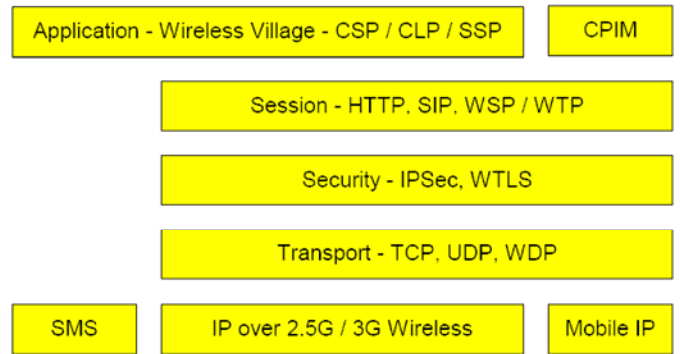


Figure 4: Protocol stack for OMA IMPS protocols.

The protocol stack is a varied collection of mostly standard Internet protocols. On the top level are the OMA IMPS-specified protocols (CSP, CLP and SSP) as well as the IMPP-specified Common Profile for Instant Messaging. The allowed transport protocols vary for the different OMA IMPS protocols.

For example, for the CSP protocol, four transport bindings are specified: WAP Wireless Session Protocol (WSP), Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) and Short Message Service (SMS), of which at least one is required to be supported by the client [10].

Going down the protocol stack, OMA IMPS is bearer-agnostic: the connection itself can be run over TCP, UDP or WDP (WAP Wireless Datagram Protocol) can be utilized. Also, any IP-based mobile or fixed network infrastructure connection can be used to access the system. For mobile networks that do not support packet data connections, an SMS delivery binding is specified for the CSP protocol.

When communicating with the server, most communication between the client and the server is synchronous, i.e. request-reply in its nature. For example, a simple and possibly the most common message is that of a client sending an instant message. The flow of this is depicted in Figure 5:

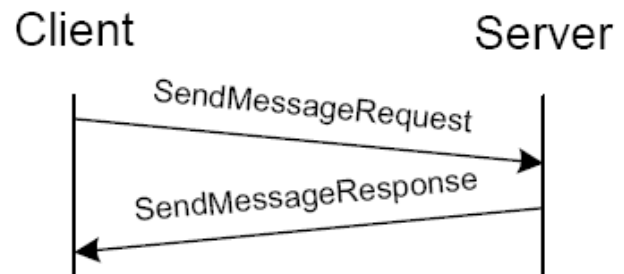


Figure 5: Flow diagram of SendMessageRequest [11].

As was mentioned, the CSP protocol is based on XML. The specified XML protocol structure is quite heavy: with a typical 200-character message, the overhead from the plain-

text XML can be as much as 80% or more of the message length. To alleviate this significant overhead, OMA IMPS has defined binary XML mappings for the Client-Server-Protocol [14]. Binary coding of the XML means “abbreviating” the XML tags with shorter codes (tokens) in order to make the messages shorter. For example, the token “74” is used for the start tag of “TransactionDescriptor”. Listing 1 contains an example message that uses the CSP protocol primitive SendMessageRequest. This primitive is used to send an instant message to other users.

LISTING 1: SENDMESSAGEREQUEST EXAMPLE.

```

<WV-CSP-Message
xmlns="http://www.openmobilealliance.org/D
TD/WV-CSP1.2">
  <Session>
  <SessionDescriptor>
  <SessionType>Inband</SessionType>
  <SessionID>im.user.com#48815@server.com<
/SessionID>
  </SessionDescriptor>
  <Transaction>
  <TransactionDescriptor>
  <TransactionMode>Request</TransactionMod
e>
  <TransactionID>IMApp01#12345@NOK5110</Tr
ansactionID>
  </TransactionDescriptor>
  <TransactionContent
xmlns="http://www.openmobilealliance.org/D
TD/WVTRC1.2">
  <SendMessage-Request>
  <DeliveryReport>T</DeliveryReport>
  <MessageInfo>
  <ContentType>text/plain</ContentType>
  <ContentEncoding>None</ContentEncoding>
  <ContentSize>58</ContentSize>
  <Recipient>
  <User>
  <UserID>wv:he@there.com</UserID>
  </User>
  <Group>
  <ScreenName>
  <SName>Wicked Vicky</SName>
  <GroupID>wv:john/chatgroup@there.com</Gr
oupID>
  </ScreenName>
  </Group>
  <ContactList>wv:john/My_friends@smith.co
m
  </ContactList>
  </Recipient>
  <Sender>
  <User>
  <UserID>wv:john@smith.com</UserID>
  </User>
  </Sender>
  <Validity>600</Validity>
  </MessageInfo>
  <ContentData>
  This is a test message, hurry up people!
  </ContentData>
  </SendMessage-Request>

```

```

</TransactionContent>
</Transaction>
</Session>
</WV-CSP-Message>

```

The above message is over 1200 bytes long. With binary XML encoding, the total message length goes significantly down, but even after binary encoding the message remains over 300 bytes in size. As the “real” absolutely required information consists of significantly less than 100 bytes, there is marked overhead in the CSP protocol even with the binary XML coding.

The simple response from the server to the client to the above message is a equally heavy as shown in Listing 2:

LISTING 2: SENDMESSAGEREQUEST REPLY

```

<WV-CSP-Message
xmlns="http://www.openmobilealliance.org/D
TD/WV-CSP1.2">
  <Session>
  <SessionDescriptor>
  <SessionType>Inband</SessionType>
  <SessionID>im.user.com#48815@server.com</S
essionID>
  </SessionDescriptor>
  <Transaction>
  <TransactionDescriptor>
  <TransactionMode>Response</TransactionMod
e>
  <TransactionID>IMApp01#12345@NOK5110</Tran
sactionID>
  </TransactionDescriptor>
  <TransactionContent
xmlns="http://www.openmobilealliance.org/D
TD/WVTRC1.2">
  <SendMessage-Response>
  <Result>
  <Code>200</Code>
  <Description>Successfully
completed.</Description>
  </Result>
  <MessageID>0x0000f132</MessageID>
  </SendMessage-Response>
  </TransactionContent>
  </Transaction>
  <Poll>F</Poll>
  </Session>
  </WV-CSP-Message>

```

The example plain-text response in Listing 2 consists of over 700 bytes of information; the binary XML equivalent is over 100 bytes in length. Even when using binary encoding, the simple act of sending a very short message and receiving an ACK-like acknowledgement from the server consumes approximately half a kilobyte of traffic. While delay-wise this should not be a cause for concern, it might turn out to be a charging problem if the mobile operator charges their subscribers for the Instant Messaging traffic with normal packet data rates. This charging may come on top of possible charging for the IM service itself. In addition, excessive packet data traffic unnecessarily drains the mobile devices

batteries and degrades the network performance.

D. Interoperability

Interoperability can be divided in two cases: interoperability across different domains both running an OMA IMPS-based system and interoperability with other, possibly proprietary, IM solutions. Interoperability with other OMA IMPS systems is achieved using the standard SSP protocol with the Wireless Village servers running in different domains. The interoperability between WV systems can also include sharing of complementary services – one domain can include the shared content feature that the other does not support. With full interoperability, users of both domains can use services in each other’s domain.

Figure 6 depicts the interoperability scenario between two WV systems [3]. In this scenario, the WV Server on Domain A only implements the IM and Group/Chat services while the server on Domain B implements the full service set. With full interoperability between the domains, Client 1 can also utilize the Presence service even when his/her “local” server does not have the service implemented.

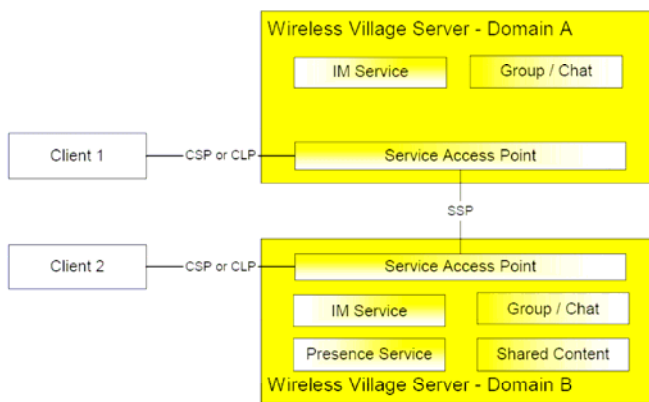


Figure 6: Simple interoperability setup with two Wireless Village server domains.

As was previously mentioned, a noteworthy feature of the OMA IMPS architecture is its explicit support for interoperability with other instant messaging-systems. The interoperability with other IM systems is supported through an element called *Proprietary Gateway* that communicates with

the Wireless Village servers using the SSP (Server-to-Server Protocol). However, the proprietary gateway is not a required element in the OMA IMPS architecture and nothing forces the service providers to provide interoperability with other IM systems – or, indeed, even other operators running an OMA IMPS-compliant system.

The Proprietary Gateway performs the protocol conversions necessary between OMA IMPS and the proprietary system(s). It connects to the proprietary server(s) using whatever protocol they utilize and to the OMA IMPS servers using the SSP protocol. The actual implementation of the protocol conversion(s) and whether or not both (or all) IM services share the same feature set naturally depends on the deployment and which IM service is being connected to. Some features in the other IM service may not be accessible by the OMA IMPS users and vice versa; for example, an attempt by an MSN Messenger user to initiate a video connection with an OMA IMPS user will fail.

Figure 7 presents a simplified message flow-example of sending an instant message to a user residing in another IM system. Client A, an OMA IMPS user, sends an instant message to one of his/her contacts with an ID of “john@hotmail.com” who uses some proprietary IM solution. The message is sent to the WV server as usual, which routes it to the proprietary gateway. The proprietary gateway in turn performs any required protocol conversions and sends the message to the other IM network, where it is routed to the final recipient.

OMA IMPS does not define which other Instant Messaging systems the proprietary gateway should be able to support. Its capabilities are therefore dependant on the vendor’s gateway implementation. There are, for example, implementations connecting to the Yahoo! Messenger service, XMPP (Extensible Messaging and Presence Protocol) and SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions)-based systems. The existence of a dedicated network element to aid interoperability is in contrast with many other IM solutions, which are often purposefully built as “closed” systems with no (allowable) means for interoperability with other IM systems.

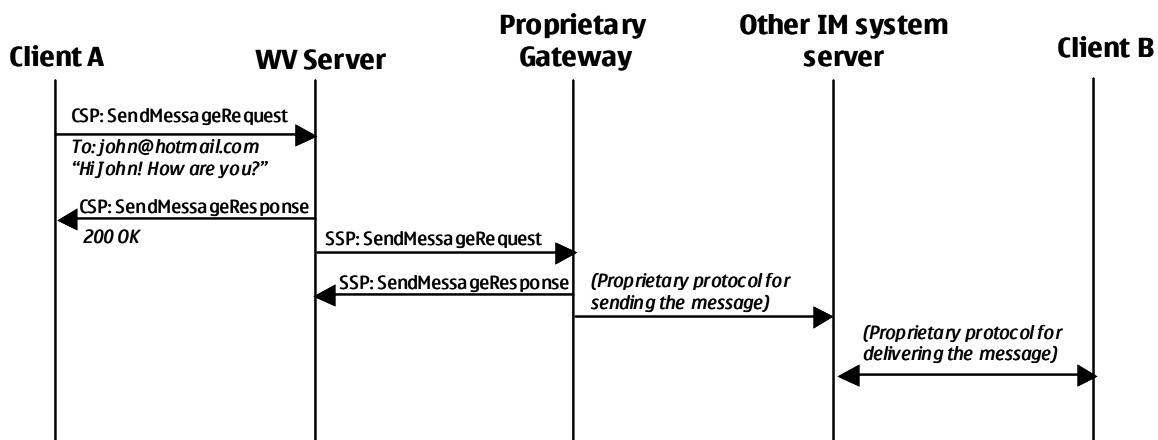


Figure 7: Simple interoperability setup to a proprietary IM system.

E. Implications of chosen architecture

The chosen architecture and protocols for OMA IMPS has a number of important functional and other implications. The choice of a pure client-server architecture would initially imply less than optimal bandwidth utilization as each message will need to traverse through a server. However, in the case of the most common deployment scenario of a mobile operator network, the overhead from the traffic route is likely to be negligible. This is due to the fact that even a “peer-to-peer” message in mobile networks will in any case flow through one or more core network-elements such as the SGSN and the GGSN in GPRS networks [9].

Another implication of the operator-controlled server-centric setup is that it allows for easy legal interception (or even for illegal operator surveillance) of messages exchanged in the system, even if basic encryption is used on the client-server transport. While there is currently no legislation mandating mobile operators to provide for LI (legal interception) for instant messaging or presence services, it is not unreasonable to assume such requirements may arise in some countries.

Companies other than mobile operators can also run the OMA IMPS servers. Considering many mobile operators employ a so-called walled-garden strategy and basically do not allow their users to connect to the general Internet without restrictions, such service providers may see their user base limited by the mobile operators by intentionally or unintentionally blocking traffic to the IMPS servers.

F. Security and network considerations

Since OMA IMPS does not strictly mandate which protocols should be used for transport, there is no single security model available and the security of the different deployments can vary widely. Within one service provider (usually one mobile operator) the security requirements do not play as big a role in OMA IMPS as they perhaps do in other IM systems. This is due to the fact that connections are already reasonably secure due to encryption of GSM traffic and the terrestrial network controlled by the operator can be assumed to be reasonably secure. When sending messages to other domains, security plays a more important role. Even here full message encryption will always break in e.g. the proprietary gateway performing the protocol conversion to other IM systems.

For additional security beyond what the underlying networks provide (and to secure potentially insecure server-to-server connections), OMA IMPS allows standard methods such as HTTPS etc to be implemented. No requirements are placed on encrypting the connections and it can be assumed that most operators, trusting their networks, will deploy the OMA IMPS solution with no additional encryption beyond the existing air-interface encryption.

Full end-to-end security is thus not specified by the OMA IMPS standard and may not even be possible to achieve in an

OMA IMPS system. Even if transport encryption is deployed, due to the nature of the CSP-protocol specification it's inevitable that the encryption breaks at the OMA IMPS servers: as there are no separate headers in the CSP protocol messages, OMA IMPS servers will need to be able to open the XML message to determine who the message should be delivered to. It's clear that significant trust will therefore need to be placed on the service operator – something that especially corporations or governments may not be willing to do.

It is, of course, possible to implement a proprietary method for encrypting the actual message contents sent over the OMA IMPS system. This method would require modified clients that implement the message encryption, possibly an external key management system and knowledge that the other party is able to decrypt the messages sent to him/her.

The OMA IMPS specifications are also somewhat vague on the requirements of user authentication – it is mostly left to the operator to decide what level of additional authentication should be implemented. When deployed in a mobile network, the basic user authentication can be assumed to consist either of an already relatively secure SIM-based authentication or if integration between OMA IMPS and the mobile core network is desired to be minimal, a username/password-combination.

One potentially significant weakness in the OMA IMPS system is the method used for identifying user sessions; once the user has logged in, a session key is used to identify the session. This session ID is a server-generated string with a maximum length of 50 bytes; basically the only thing a malicious user would need to impersonate another user is this session key. While obtaining this key requires sniffing the network traffic or compromising of either the client device or the server, it remains a possible threat especially if no transport encryption is used [8].

A problem with many “Internet” IM systems is the difficulty of traversing through NATs (Network Address Translators) and firewalls. The most common deployment location for the OMA IMPS solution, the mobile operator networks, is typically quite closed and can be considered a relatively secure environment. As the only connection from the clients is to their closest WV server often residing in the same network, dealing with NAT and FW traversal issues is not such a big issue with OMA IMPS. Even if the mobile operator decides to implement a firewall between the mobile terminals and the OMA IMPS servers, they are in the position to configure the firewall to work smoothly with the OMA IMPS system. The WV servers can be e.g. placed in the mobile operator DMZ (DeMilitarized Zone, a network between a company's private network and the outside public network that prevents outside users from getting direct access to servers in the company's internal network) where the servers have convenient access to the OMA IMPS clients as well as other WV Servers outside the operators' network.

IV. FEATURES

This chapter will cover the main features of the OMA IMPS standard. OMA IMPS specifies four main features or feature groups – presence, instant messaging, groups and shared content – which can be implemented modularly with only desired features in place. The different features can also be used for other operator services, such as presence utilized by IP Multimedia System (IMS) services.

A. Presence

Presence is a key element in any instant-messaging solution and can be considered as a backbone for the entire OMA IMPS solution. Presence in many instant-messaging products has come to mean that users are able to announce their availability to authorized persons (“friends” or “buddies”). Often this information is presented simply with a pre-defined status of e.g. “Away”, “Out to lunch” or “Available”. In OMA IMPS, the term presence takes on a somewhat richer meaning. In addition to providing personal status information, it can include information on device availability, location, device capabilities and searchable personal statuses [2].

The OMA IMPS standard defines numerous presence attributes but interestingly, none of these are mandatory. A small subset is defined as “suggested”, with the goal of providing a minimal common set of attributes. These attributes are:

- **OnlineStatus:** shows whether a client is logged on a WV server
- **UserAvailability:** Availability of the user for communication
- **StatusText:** User-specified status text for his or her current presence.

Other attributes defined in the specification contain more detailed information regarding the user’s current presence. These optional items include data such as the user’s geographical location, alias names, information on the client device and contact information in vCard format. Many are further specified; for example, if geographical information is present, longitude and latitude are required parameters but altitude and the locations’ accuracy are optional [2].

When distributing presence information to other users, one key question is who is allowed to see your presence information. OMA IMPS specifies two types of authorization procedures for this: *proactive authorization* and *reactive authorization*.

In the **proactive authorization** model, the subscriber first creates a contact list (of his “buddies”); these contacts are then automatically – proactively – authorized to see the user’s presence information. Once the contact list has been created, the user can further specify which presence attributes he would like people on that particular contact list to see. Multiple contact lists are allowed, so different groups of people can have access to different presence information. For

example, colleagues might be denied access to physical location information that is in turn allowed to family contacts.

In the **reactive authorization** model, users specifically request a certain presence attribute – or all attributes – from another user. The user being asked for the consent can then accept or deny this request for presence information access. Any previous authorization is overridden by the new decision.

The “publisher” of the presence information can at any time revoke any previous authorizations granted, whether proactive or reactive. When presence information changes, the client will notify the server of this. To facilitate updating the presence info to all “interested parties”, the server maintains a Watcher List for each user. All users that have subscribed to presence information of a particular user are in that user’s Watcher List.

B. Instant Messaging

In the OMA IMPS specification, Instant Messaging features are provided by the instant messaging service element in the WV servers. Two types of message delivery mechanisms are specified. The first is a traditional “instant messaging” method of **push-delivery** where the IM service element pushes the message in its entirety to the recipient. This is the delivery mechanism of e.g. SMS messages in mobile networks today.

The second type is a **notification/pull-method**. In this model, a notification of a message instead of the message itself is sent to the recipient. It is then up to the recipient to actually initiate the message transfer by connecting to the server and fetching the message when it’s convenient for the recipient. The notification-style suits better for messages that are large in size. This type of delivery mechanism is used for MMS messages today.

To the end user, the different delivery types may not be visible: for example, most mobile terminals are configured to automatically fetch the MMS message as soon as they receive a notification and notify the subscriber only after fetching the message from the server. On the other hand, the receiving party could also have the option of rejecting the message once the notification is received if configured to prompt the user when the notification is received.

An instant message can be sent either to a group or an individual user. After the message has been submitted (regardless of the delivery method), a delivery report can optionally be delivered to the sender indicating the success or failure of the message delivery.

Similarly to many popular Internet IM-systems, OMA IMPS allows for specific access control for instant messages. Messages and invitations can be filtered using either so-called white- or blacklisting techniques. If these methods are in use, the user specifies the allowed or denied parties respectively. The possible blocking of messages or invitations takes place in the WV servers. Figure 8 shows the decision tree employed when white- or blacklist-based blocking is employed; both lists can be in use at the same time, though the practicality of such a scenario is questionable [11].

Instant messages can deliver any content, including

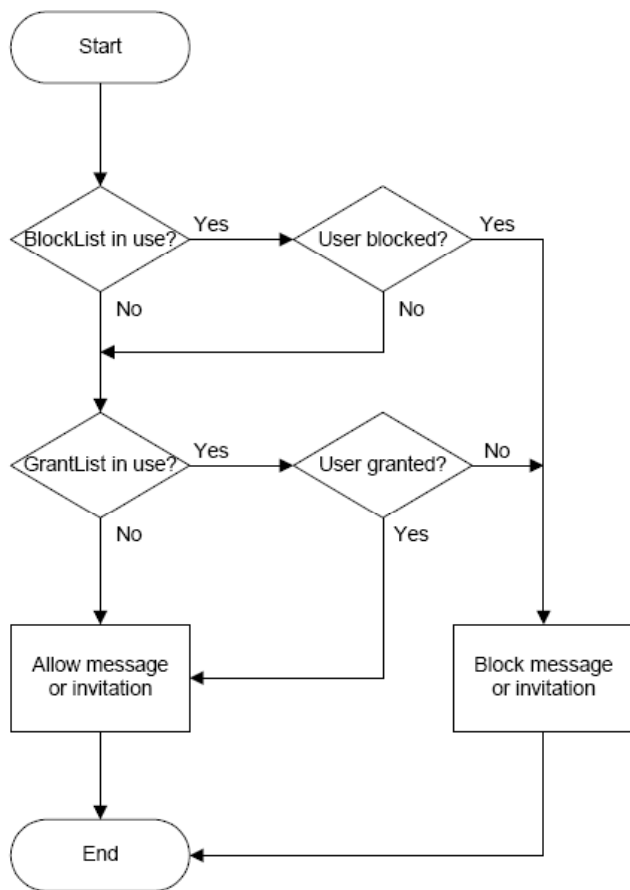


Figure 8: Blocking decision diagram.

multimedia content, but to ensure minimal interoperability, OMA IMPS set a requirement that all messages in OMA IMPS using plain Unicode text with UTF-8 encoding with at least ISO 8859-1 (Latin-1) are to be supported. Suggested content types are the following:

- Multimedia Message (3GPP TS23.140)
- Enhanced Short Message (3GPP TS23.040)
- Business Card (vCard 2.1)
- Calendar Entry (vCalendar 1.0)

1) Offline messaging

When an instant message is sent to the recipient, the user may be offline. This is indicated by the presence attribute that the sending user may or may not check before sending the message to the recipient. If the user is offline, the WV servers can optionally support a store-and-forward type of message delivery where the servers store the message until the recipient becomes available.

When the recipient is online again, the stored messages may be automatically forwarded to them or the system can wait for the client to check for stored messages. As mentioned, this is an optional feature for WV servers and not all deployments may support offline messages. Indeed, it is possible that offline messages can be sent to user A residing in network X

from a user B residing in network Y but not vice versa. The OMA IMPS specification also does not dictate any timeout values for the stored messages.

C. Groups

The concept of a group in OMA IMPS refers to a chat room-type of a discussion forum set up either by the service provider or individual users. This is a closely analogical concept to channels in IRC (Internet Relay Chat). For example, OMA IMPS groups can also have an assigned topic similar to an IRC channel. Messaging to and from the groups is accomplished through the instant messaging feature described above; the main difference is that the group feature at the server acts as a distribution mechanism, sending the messages to all group participants.

It is possible to set up two types of groups; private and public groups. A public group is one created by the service provider while a private group is one set up by the individual users. Private groups may specify a membership list that limits the access to the group. The creator of the private group initially has full control over who is allowed to access the group, but the creator may also assign other users to act as group administrators or moderators.

OMA IMPS specifies all common group management primitives for managing groups: creating and deleting groups, joining and leaving a group and inviting users to a group. In addition to the basic primitives, groups can be searched based on the group's properties and users can subscribe to notifications if the group's features somehow change (e.g. if users join or leave the group).

D. Common features

Two important features are common to multiple other features in the OMA IMPS specification. The first is the *general search feature*, which allows users to search for information and other users. In the OMA IMPS specification version 1.2, the search feature is limited to searching for users and groups. Users can be searched based on their names (or a part of the name) and e-mail addresses while groups can be searched using the group ID, name or topic.

The other common feature is the *general invitation feature*. This enables a subscriber to invite one or more users to an OMA IMPS-related activity such as a group chat or sharing of content. The invitations can include an explanation of the invitation. Users are then expected to respond to the invitation by either accepting or declining it.

In addition to the above, user authorization can also be thought of as a common feature. The OMA IMPS specifications provide means for logging in and out of the service as well as for device capability negotiation between the client device and the OMA IMPS server(s). In device capability negotiation, accepted content types and sizes can be negotiated so that the OMA IMPS server does not attempt to send incompatible content to the clients.

E. Shared Content

One important feature of any social “community”-type of application is the possibility to share content. For this purpose, OMA IMPS provides a framework for sharing content such as photos or music with other individuals or groups in an IM chat session.

However, the actual specification of the shared content feature in OMA IMPS is somewhat light; in the current specification release (v1.2) content sharing is realized by using the *common invitation* feature that has been described above. Using the invitation feature, users send a URL to the content they are willing to share. Users are also assumed to withdraw the invitation when they no longer wish to share the specified content.

Beyond this, OMA IMPS does not provide mechanisms or specifications for uploading, storing or downloading the content itself. Implementing this is up to the vendors and/or service providers. It is clear that the chosen method of content sharing is in its current form somewhat limited and inflexible when compared to other IM systems. The OMA IMPS model does not, for example, currently provide the means to immediately send content to another party – instead, content needs to be uploaded to a server and invitations will have to be sent to the content and care be taken to withdraw the invitations later.

F. Comparisons with other IM systems

OMA IMPS has been specified from a very different perspective than many other Instant Messaging-products or platforms. It is the first serious industry effort to standardize a system that is optimized to be used with mobile devices and provides explicit interoperability support with other IM systems. It’s therefore not very surprising that some of the basic architectural solutions are different from other, Internet-originated IM systems.

Major differences as compared to the IM systems operating in the “Internet domain” include the following:

- OMA IMPS is a purely client-server based system. No information exchange takes place peer-to-peer under any circumstances. While this can create bottlenecks and single points of failure, it’s understandable when one considers the wireless origins of the standard – most wireless devices in current mobile networks are not globally addressable (and thus, contactable) from the general Internet. Instead, a server in the mobile operator network must be in the data path in any case.
- Most IM systems are capable of transmitting files or other content between the session participants. In addition, many of these systems perform the file transfer in pure peer-to-peer fashion without any server involvement, at least when the clients reside in the same subnet. In OMA IMPS, the specified content sharing is conceived via the means of sending a URL

to the content with practically no specification given on how the content is actually to be uploaded, hosted and downloaded by the clients. As a result, the file-sharing feature has potential to cause the emergence of mutually incompatible vendor solutions.

- Compared with the most popular IM solutions in the market, OMA IMPS specifies a relatively light feature-set. No VoIP calls, video streaming, games or other mode advanced features are present and even the general messaging features are rather lightweight in terms of features.
- The protocols specified in OMA IMPS are based on standard transport mechanisms such as HTTP and HTTPS as opposed to many proprietary methods used in some other IM solutions. The specification is completely open (i.e. publicly available) and the main messaging protocols are based on XML.

V. CASE STUDIES

This chapter analyses a few of the popular OMA IMPS contributors who fall under one of the four main categories: Mobile Operators, Wireless Vendors, Information Technology Companies and Content Providers. Many players have entered into the market soon after the OMA’s first WV initiative. The WV clients themselves can be developed for various platforms like J2ME, Symbian, PocketPC, Win32 and proprietary environments.

There are WV clients available from Ecrio, Ericsson, Magic4, MIMT, Motorola, Nokia, OZ Communications, Panasonic, Peramon, Sony Ericsson, WebMessenger, etc. The mobile devices that come pre-shipped with client software supporting the OMA IMPS standard include handsets from Nokia (e.g.. 3220, 5140, 6020, 6630), Motorola (e.g. V180, V547, V3), SonyEricsson (e.g. T630i, K500i, K700i) and Siemens (e.g. CX65, CX70, M65). The servers are provided by, for example, Comverse, Critical Path, Ecrio, France Telecom, Followap, Invertix, Logica, MessageVine, MIMT, OpenWave and OZ Communications.

A. Mobile Operators

Mobile Operators support the OMA IMPS initiative by providing the services to their customers. In the process, they are hoping to find out a way to create new business for themselves. This can include enhancing the business by combining the IMPS services with other existing services; operators do this by deploying the IMPS servers and connecting them to the other servers that provide contents for multimedia services. For example, OMA IMS presence server provides an essential presence service that is used in enhanced services like PoC (Push-to-talk over Cellular) and several IMS services.

Additionally, mobile operators can choose to charge a subscription or usage-based fees for using their instant messaging & presence service – and naturally the mobile operator also gets revenue for the data traffic generated by the

instant messages. As we have seen, this data traffic can be quite large in size. Depending on the pricing models chosen by the operators, this traffic can bring additional revenue for the mobile operators (and costs to the subscribers).

Saunalahti was the first mobile operator in Finland (and also in Nordic countries) [13] who started providing OMA IMPS services on the mobile phones. Its customers can easily make use of these provided services to send Instant Messages and to be aware of the presence of friends or colleagues using the same service. The minimum needed for using these services is a mobile phone that supports the OMA IMPS standard, a mobile phone supporting WAP or a PC. At the moment, only a few percentages of Saunalahti's customers have client devices capable of supporting OMA IMPS and the service is currently offered for free.

B. Wireless Vendors

Nowadays most Wireless Vendors provide the OMA IMPS client implementation in many of their terminals by default. Chat and presence software applications are also common in the popular smart phones and they are freely provided for the latest models.

Nokia is the biggest mobile phone vendor who provides the IMPS supported phones. OMA IMPS is supported by default in all of the new Series 60 Nokia phones. By using a chat application, subscribers can, in addition to mobile operator-provided services, use free OMA IMPS services that are provided by companies like Yamigo.

C. Information Technology Companies

IT companies contribute to the OMA IMPS by providing ready made software solutions to implement the IMPS services, gateways, etc. These products are mainly targeted for the mobile operators in order to deploy the OMA IMPS services for their subscribers to use.

1. Colibria

Colibria is an IT solutions company and one of the contributors to OMA. They mainly focus on providing the solutions for IMPS services. Colibria provides a platform to deploy the IMPS services for the mobile operator's networks and keep the future enhancements like multimedia services, SIP and IMS enabled network in mind. It is one of the important active participants in the interoperability testing conducted by the OMA WV and provides test-server access to the major OMA IMPS client vendors. Colibria has successfully provided OMA IMPS solutions for operators in Europe, Asia and Latin America like Cable & Wireless, Enitel, Globe Telecom, Megatel, Telefonica Moviles, Telenor Mobil and Saunalahti [17].

Anyone can register himself or herself to make use of the IMPS client with Colibria's IMPS WVserver. A PC client is also provided for download but the PC client needs the .NET Framework. Presence service is available even for a web client and a WAP browser can also be used to access the IMPS services. For Norwegian users only, the IM service is also available through SMS text messaging.

Colibria Companion Instant Messaging and Presence Server provides the necessary interfaces to work with the IMS

services and vice versa. It is implemented in a way that it can easily fetch the presence information from other servers in the network and will also work together with other 3GPP and IMS elements thus providing interoperability with other technologies and services. Operators can easily launch new services with the provided flexibility for presence related services extensions. It not only supports OMA IMPS and IMS embedded client but is also open to other ways of accessing the IMPS services through various technologies like J2ME, Symbian, HTML, etc. The support for old phones and PC clients is not forgotten. It also allows the operators to bill the customers and provides a gateway for connecting to other popular IM services in the Internet like MSN, Yahoo, AOL, etc.

Colibria Instant Messaging and Presence Clients also supports legacy users such as using the service over WAP or SMS. Years of experience focused in the OMA IMPS let them not only to develop the PC Clients for the PC users but also HTML-based clients as a lightweight alternative on the devices, XHTML and WAP Clients for users of WAP phones and SMS Clients for people who uses the old or basic mobile phones.

2. Oz Communications

Oz Communications is a private company and also an OMA member that focuses on providing business solutions for extending the IM and presence services to mobile devices [18]. Its partners and customers include companies like AOL, Bell Mobility, Cingular, Microsoft, Motorola, Nokia, Samsung, Siemens, SonyEricsson, Sprint, TCL, Alcatel Mobile Phones and T-Mobile USA. It provides a Mobile IM Gateway for mobile operators, which enables the connection with the existing Internet IM users, Mobile IMPS Clients for mobile operators and for the subscribers to download and an IMPS Server that provides the features and functionalities described in the OMA IMPS specifications.

The Mobile IM Gateway makes it possible for the mobile operator to charge the customers interoperable instant messaging and presence services. This gateway brings the existing Internet IM users and the Mobile IM users together. By using this gateway, mobile operators can make use of the opportunity to increase the revenue from the increase of the messages and the data traffic that uses the interoperable services. Oz claims that it is easily deployable and cost effective. Support is provided for AOL, ICQ, Yahoo! and MSN Internet IM services.

Mobile IMPS Clients are available for J2ME, RIM, BREW and MS Windows Mobile devices and support both IP and SMS-bearers. Oz also provides the support for upgrading and downloading new features for the clients. One significant feature is that the IM presence, portal, and multimedia service such as PoC, picture messaging, and phone book synchronization can all work together.

Oz Communications' IMPS Server is implemented according to OMA IMPS standard and is thus interoperable with other IMPS servers. It also supports presence enhanced phonebook services and can be extended to offer new voice and data services that leverage the presence-enabled contact list. It is customizable and works together with current service

offerings and core network infrastructure, databases, operational systems, billing, and customer care systems. Thus the server can bring the mobile operator additional value for their network services.

D. Content Providers

These are independent companies that provide contents like news, sport events updates etc. in the Internet. These companies typically have little to do with mobile operators.

Yamigo is one example of such a company. Yamigo is independent of any mobile operators and provides OMA IMPS services [19]. The free OMA IMPS services are offered for mobile users regardless of their mobile operator. The mobile operators charge the users for only the data transfer rate. Using some clients like Nokia, Ericsson that use the binary XML version of the CSP protocol, known as WBXML, reduces the amount of data transferred whereas other clients such as Motorola's chat clients use plain XML. Using plain XML in the CSP protocol causes much higher data usage and, therefore, higher prices for the subscribers. The support for connecting the Internet IM communities like Yahoo, MSN, AIM and ICQ is also provided.

IMPS compliant presence-enabled phone chat client should be installed in the mobile device in order to use this service. The client should be configured to point the Yamigo URL <http://www.yamigo.com/wv/control> with the user name and password that can be obtained through free registration.

Service bots like BBC, CNN, Google, weather forecasts etc. are run in the Yamigo server and instant messages for respective services can be received from the servers. Some services are bi-directional: for example, sending an instant message to Yamigo can make a Google search. It was experimentally found out that the messages can take almost 180 seconds before reaching the destination (another IM user). This is because the server polls the messages only approximately every three minutes.

VI. CONCLUSION

The OMA IMPS initiative is an ambitious plan to bring standardized instant messaging to mobile devices. After years of standardization work, however, the resulting standard and especially the state of the surrounding ecosystem in the form of service take up leave a lot to be desired. While OMA IMPS-compliant clients have recently emerged in numbers, few operators have deployed the necessary infrastructure to support the service so far and even fewer provide full interoperability with existing IM systems. Additionally, marketing of the mobile instant messaging services has been minimal by the operators – a critical step in raising subscriber awareness.

At the same time, proprietary clients have been used in mobile phones for some time now and many of these, like Agile Messenger, are independent of the mobile operators and interoperate with other IM systems. However, it is interesting that some operators in North America are offering OMA IMPS clients branded as e.g. Yahoo! IM clients – the OMA IMPS system is then performing the conversion to Yahoo!'s

systems. While this kind of “shadow” usage of OMA IMPS solutions brings business to the parties involved, it does not promote a universal mobile IM standard.

The value of any instant messaging service lies in the size of the user base; if too few people are reachable via the service, it does not make sense for people to use it. Whether or not OMA IMPS is successful depends on a number of things, including how easy the service is to use from the mobile devices, what kind of interoperability options will be offered, how widespread the adoption will be and how the service will be priced by different mobile operators.

As of this writing, it is too early to say what happens. It therefore remains to be seen whether OMA IMPS can gain enough traction in the marketplace to become anything more than a niche player.

REFERENCES

- [1] WV-040 System Architecture Model v1.2, Open Mobile Alliance, January 2005
- [2] WV-049 Presence Attributes v1.2, Open Mobile Alliance, January 2005
- [3] WV-041 Features and Functions v1.2, Open Mobile Alliance, January 2005
- [4] Wireless Village White Paper, Wireless Village Initiative, 2002
- [5] Smith, Brad: Fueling an Instant Messaging Eruption, *Wireless Internet Magazine*, April 15th 2002
- [6] Cremers, de Lussanet: *Mobile Messaging Forecast Europe: 2005 to 2010*, Forrester, March 18th 2005
- [7] Colibria brings its presence message to 3GSM Asia, M2 Presswire, August 2nd 2005
- [8] Stålnacke, Fredrik: *Implementation of an Instant Messaging Client using the OMA IMPS Protocol*. Umeå University, 2003.
- [9] 3GPP 03.60 v7.9.0 General Packet Radio Service Phase 2 System description. 3rd Generation Partnership Project, Sept 2002.
- [10] WV-044 Client-server protocol transport bindings v1.2. Open Mobile Alliance, January 2005.
- [11] WV-042 Client-server protocol sessions and transactions v1.2. Open Mobile Alliance, January 2005.
- [12] Nokia Presence compatible phones. <http://nokia.com/nokia/0,,48546,00.html>
- [13] Saunalahti Press release, March 18th 2005. <http://www.saunalahtigroup.com/bulletin.php?index=1816>
- [14] WV-047 Client-Server Protocol Binary XML Definitions and Examples v1.2.1. Open Mobile Alliance, August 2005
- [15] WV-051 Command Line Protocol v1.2. Open Mobile Alliance, January 2005.
- [16] W-045 SSP – Transport Biding v1.2. Open Mobile Alliance, January 2005.
- [17] Colibria <http://www.colibria.com/>
- [18] Oz Communications <http://oz.com/>
- [19] Yamigo <http://www.yamigo.com/>