

Wireless Village

Open Mobile Alliance

Instant Messaging and Presence Service (IMPS)

Contents

- Introduction
- Background, History and Current status
- Architecture
- Features & Security Aspects
- Real life usage
- Conclusions

Introduction

Wireless Village

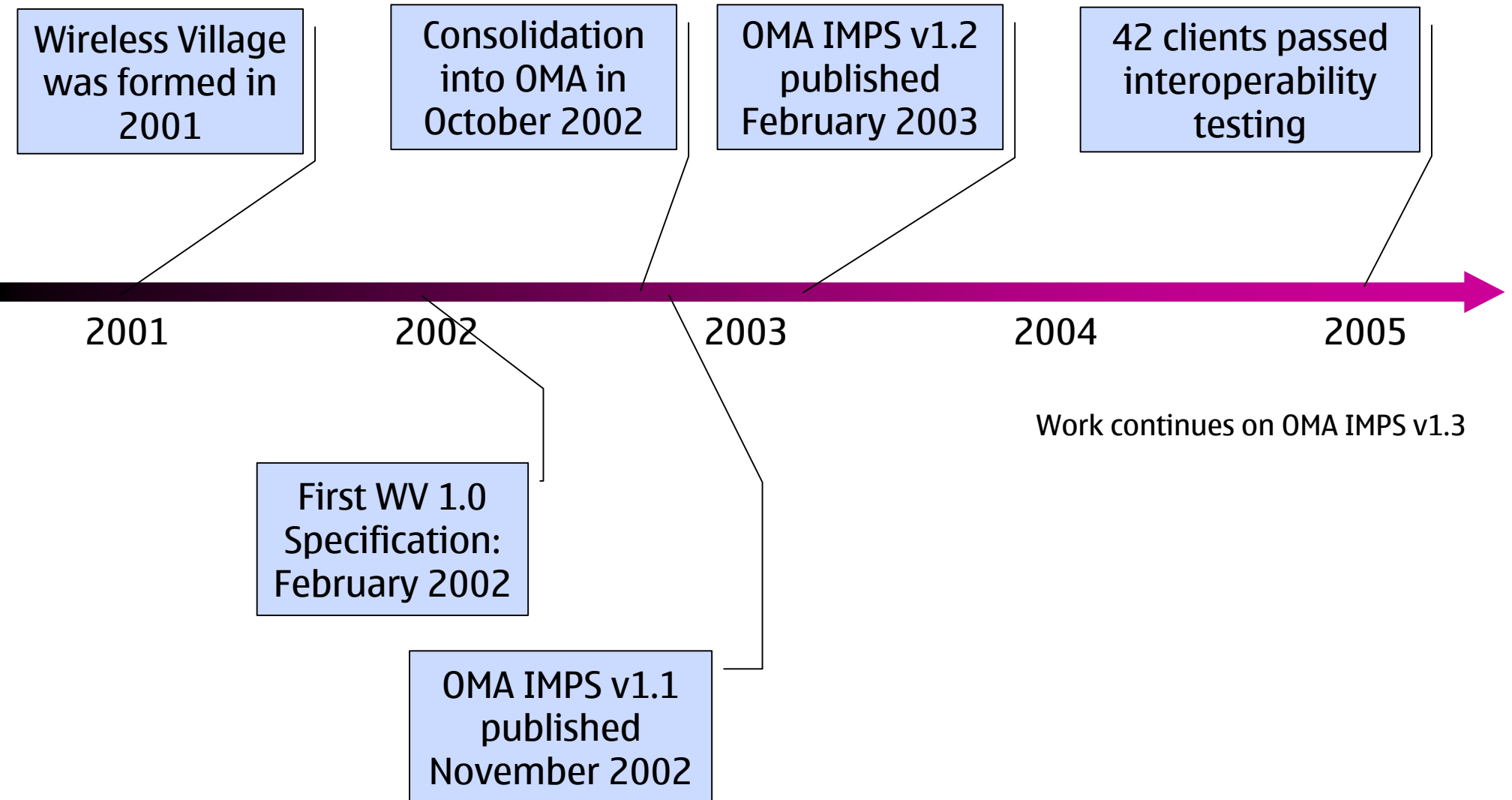
- Wireless Village is a OMA (Open Mobile Alliance) Initiative
- OMA IMPS (Instant Messaging and Presence Service) is the new name for “Wireless Village”
- Interoperability is the key
 - Mobile world
 - PC Internet world
- To avoid the fragmentation
- Industry standard for Mobile IMPS
- Set of open standards and specifications
- Purpose is to bring the mobile world and internet PC world together
 - Presence area
 - Instant Messaging area

Background, History and Current status

Background

- More than 80 billion emails per day
- More than 14 billion IMs per day
- Mobile users approaching two billion
- Mobile internet
 - Wireless access growing
 - Convergence of mobile and internet domains
- Lack of interoperability
 - Many proprietary services exist
 - Lack of openness
- Lack of IMPS services while roaming
 - Mobile users wants the same PC internet world's experience
 - Always want to be connected

History of the Initiative



Why OMA (Open Mobile Alliance)?



- Formed in June 2002, currently over 400 members
 - Mobile Operators
 - Wireless Vendors
 - Information Technology Companies
 - Content Providers & Others
- Main focus
 - Interoperability – bearers, OS, geography, etc
 - Open, global standards
- Center for
 - Mobile service enabler specification work
 - Stimulating and contributing to the creation of interoperable services
- Why

“No matter what device or operating system you have, no matter what service you have, no matter what carrier you use, you can communicate and exchange information.”

Current status

- OMA IMPS is alive and active
- New services are emerging based on “presence”
- Presence
 - Presence enhanced phone book
 - Instant messaging
 - Service discovery
 - Information Channel
 - Push to Talk

Architecture

Architecture: overview

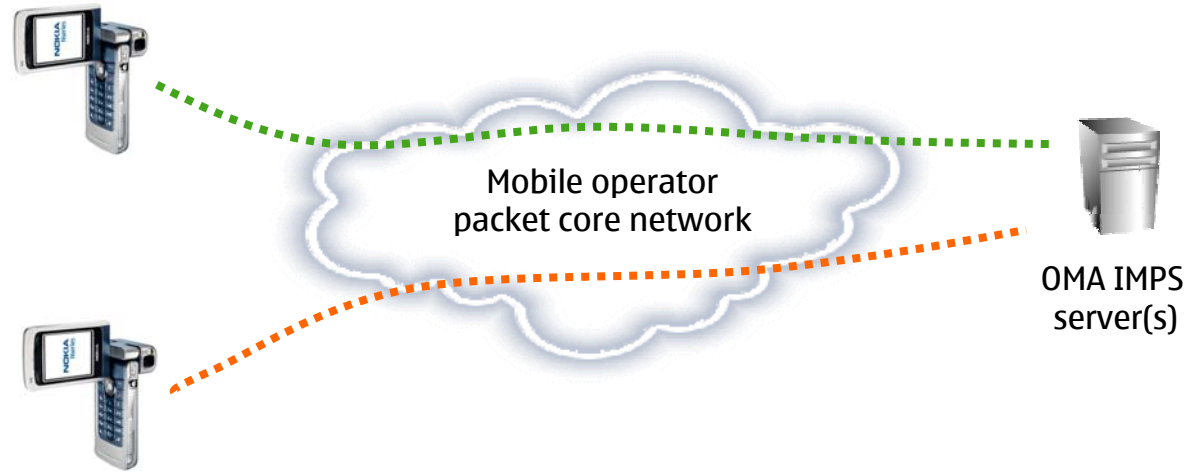
- Pure client-server architecture
 - OMA IMPS does not specify or utilize peer-to-peer connections under any circumstances

- Multiple client types possible
 - Not necessarily just mobile devices but also PCs, PDAs etc.

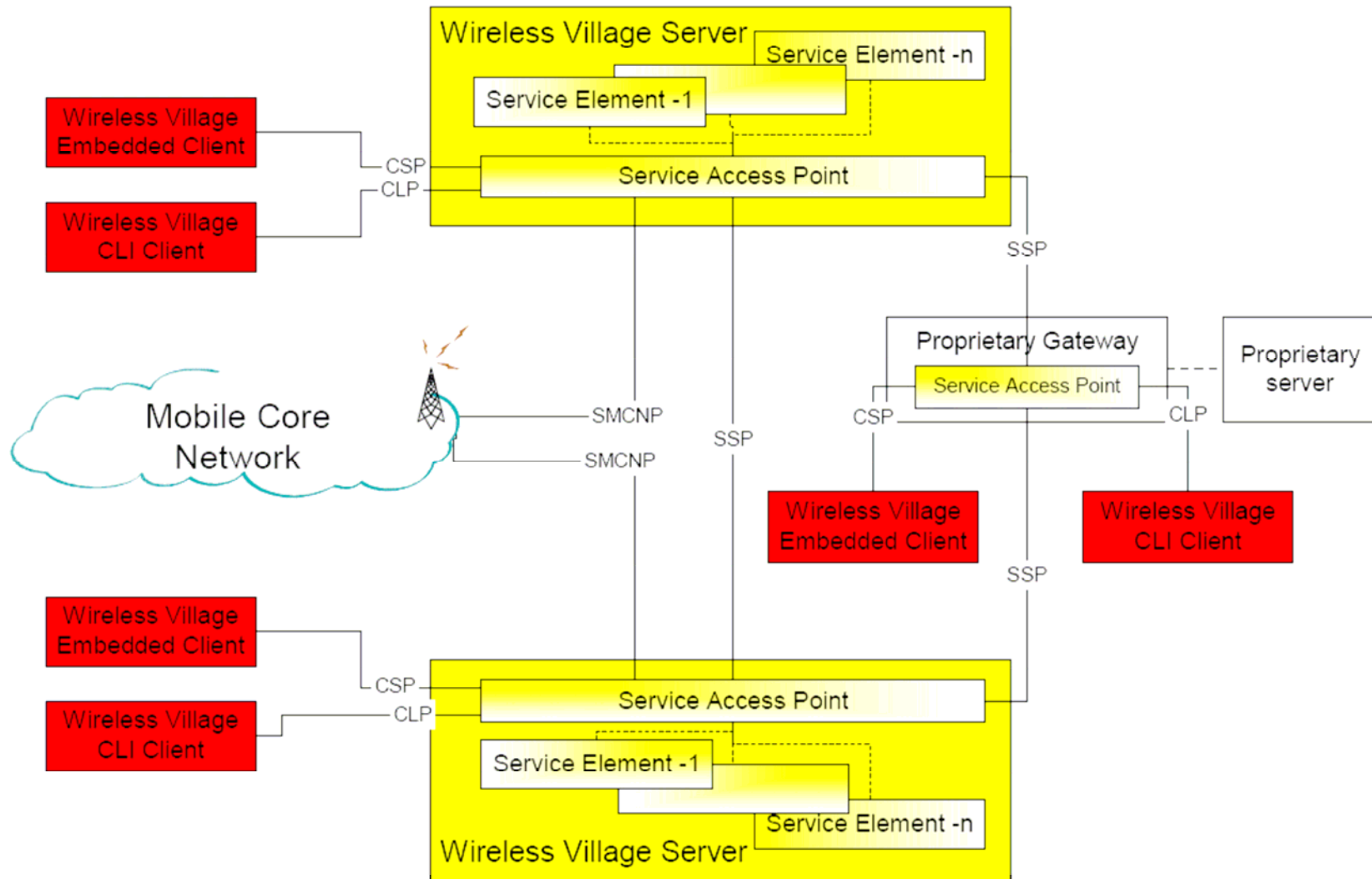
- Specific support for interoperability with other IM systems

- Standards-based where possible:

- XML-based for most important protocols
- E.g. HTTP/S for transport
- Attempt to follow IMPP where appropriate; not “IMPP-compliant” but takes some features from IMPP work

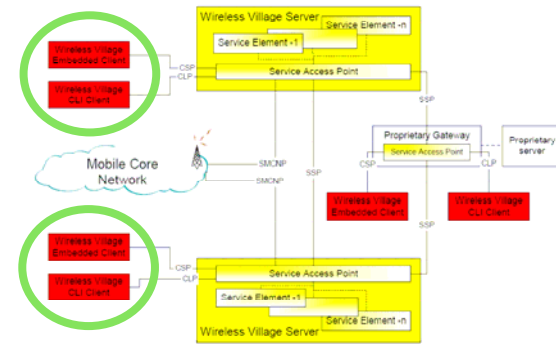


Architecture: OMA IMPS elements - overview



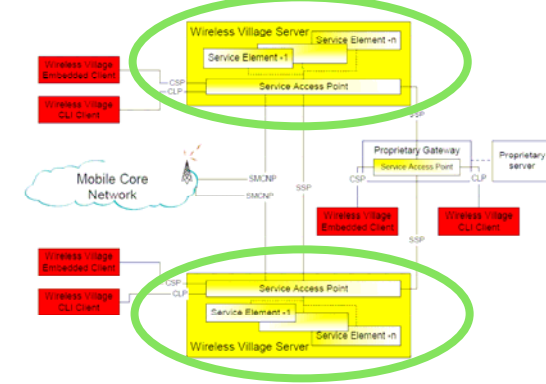
Elements: Wireless Village Clients

- Clients not limited to mobile devices
- Two client types
 - Embedded Clients
 - Mobile phones with an OMA IMPS-capable client (majority)
 - Other devices like PDAs, PCs
 - CLI Clients
 - Legacy terminals communicating via SMS (minority)
- Communicate with the servers using separate protocols



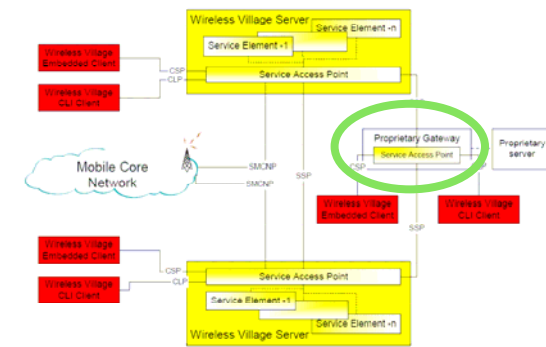
Elements: Wireless Village Servers

- Implement all functionality
 - Modular; not everything needs to be implemented
- Provide interoperability with other domains running OMA IMPS
 - SSP protocol between OMA IMPS servers
 - Servers can share implemented features
- Perform authentication, authorization, message routing, message delivery, group management & maintenance etc.
- Control practically all aspects of the solution
 - Potentially create single points of failure

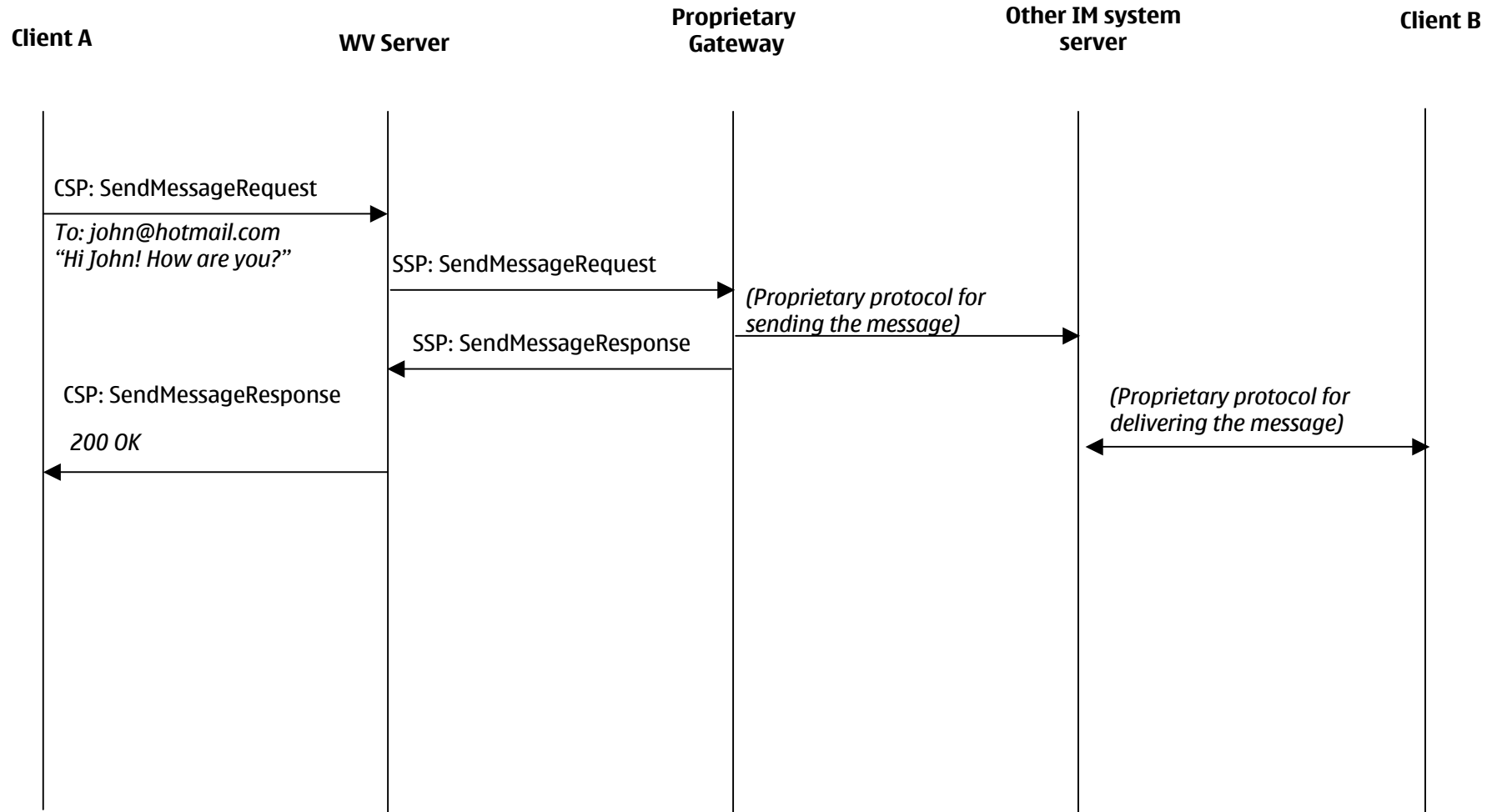


Elements: Proprietary Gateway

- Provides interoperability with proprietary IM systems
 - Optional element
 - Does not have to be implemented
 - An OMA IMPS deployment may not interoperate with any external IM systems unless the operator so wishes *and* the feature has been implemented
 - No mandated “must-support” systems
- Communicates using SSP protocol to WV Servers
- Connects to external systems and performs necessary protocol conversions
- Not all features will be 1-to-1
 - Some functions may fail from both sides
 - Core functionality (basic messaging, presence) should still work both ways
 - *For example: video call attempt by an MSN user to a WV user will fail*

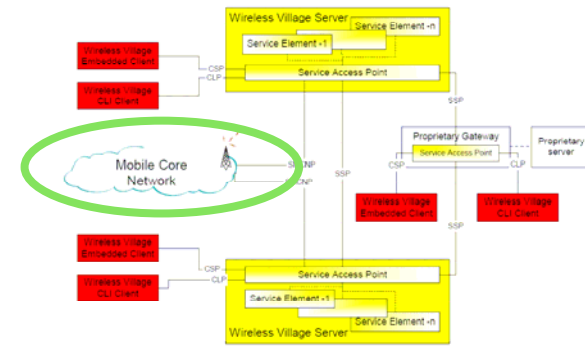


Architecture: Interoperability example



Elements: Mobile Core Network

- Provides mobile terminals the access to OMA IMPS
- OMA IMPS is network-agnostic
 - IP-based: GERAN, UTRAN etc
 - SMS-based if lacking packet-traffic support
- Can also be used as information source:
 - Support for authentication information
 - Fetching other information of the users
- Does not have to be utilized for more than access



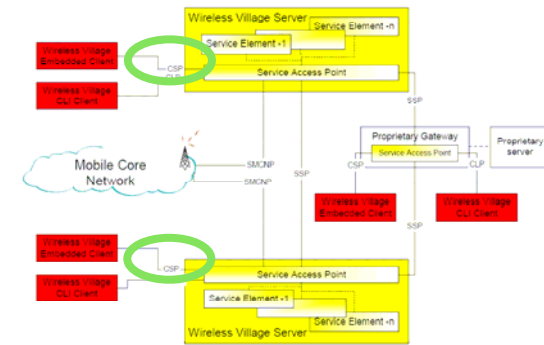
Protocol Structure

- Core protocols (CSP, SSP) based on XML
- Most client-server messages synchronous (request-reply) in nature
 - The only exceptions are PollingRequest and disconnection.
- Application transport layer not strictly mandated, several mappings given:
 - HTTP, HTTPS, WSP, SMS (for legacy terminals)
- Defined protocols surprisingly very heavy
 - Overhead from XML markup up to 80%
 - Defined binary-XML mapping helps, but messages still hundreds of bytes long
 - Not all clients support binary XML
 - Arguably a bad protocol for wireless devices. Potential problems include:
 - Traffic charging
 - Battery life
 - Unnecessary network load

Protocols Defined (1/4)

- **CSP (Client Server Protocol)**

- Used for communication between the client devices and the Wireless Village server(s).
- All communication from and to the clients, including messages to/from other users etc, use either CSP or the CLI protocol.

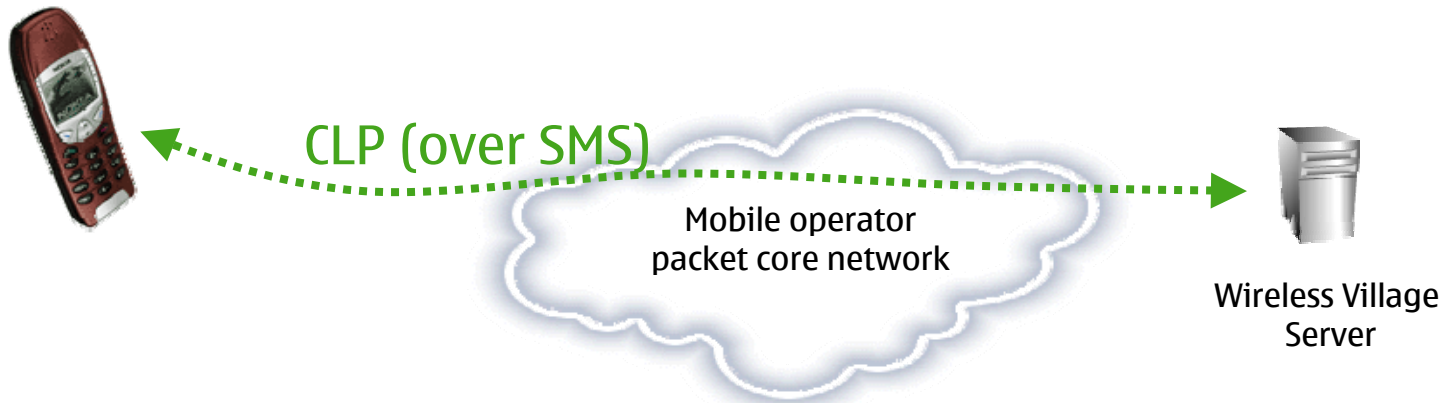
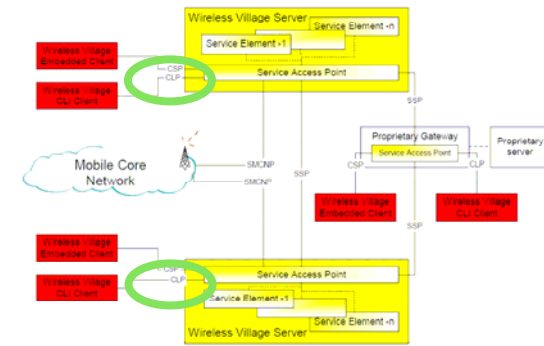


Wireless Village Server

Protocols Defined (2/4)

- **CLP (Command Line Protocol)**

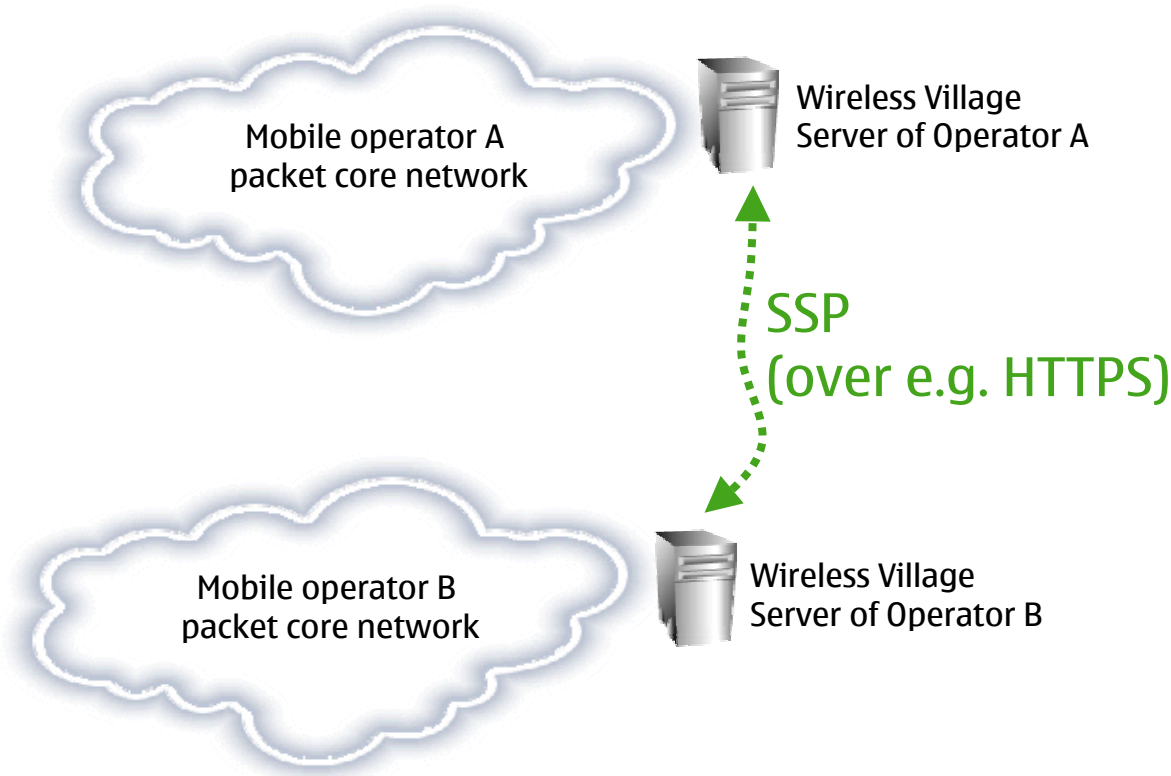
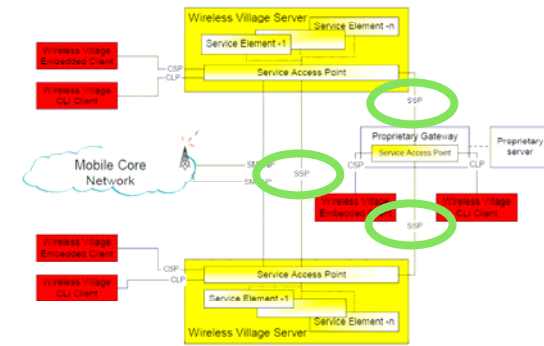
- Used by legacy terminals to connect to the OMA IMPS system.
- Used with SMS messages sent to the WV servers:
 - “WV-John Hey buddy, how’s it going?”
 - “WV-JoinGroup Wireless-village” *to join a group chat*
 - “WV-Logout” *to end the session*



Protocols Defined (3/4)

- **SSP (Server Server Protocol)**

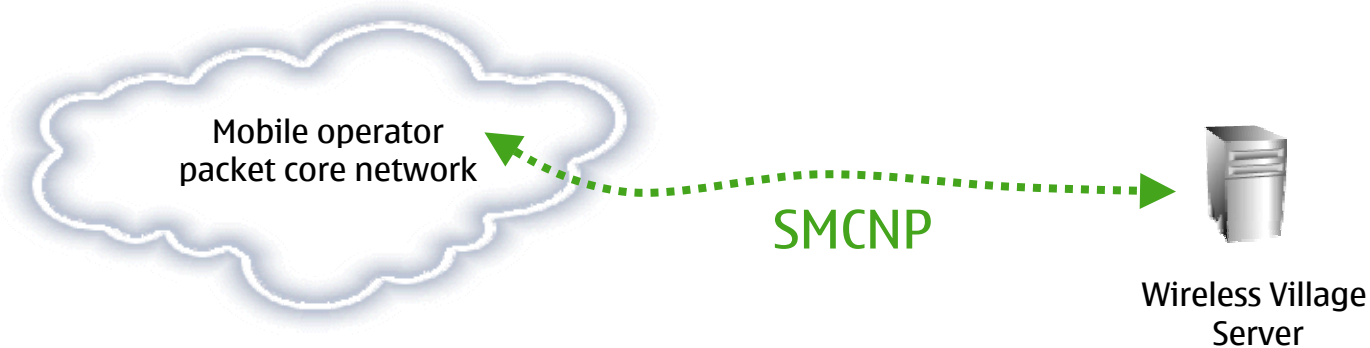
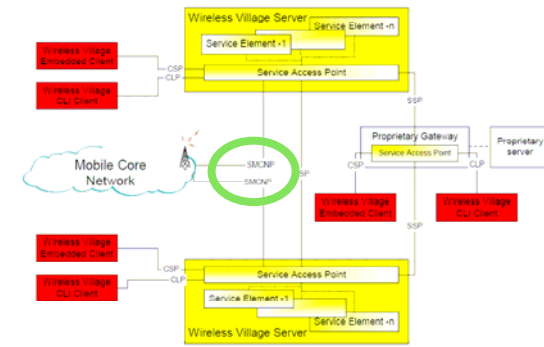
- Used for communication between Wireless Village servers.
- Used both inter-domain and intra-domain communication across different service providers (such as different mobile operators).



Protocols Defined (4/4)

- **SMCNP (Server Mobile Core Network Protocol)**

- Access to the mobile core network for the purposes of e.g.:
 - Authentication of users & clients
 - Getting service capability information
- Not really a specified protocol: OMA IMPS does not specify *anything* about SMCNP except it's intended usage.



Example: Sending a message using CSP

```
<WV-CSP-Message
  xmlns="http://www.openmobilealliance.org/DTD/WV-CSP1.2">
<Session>
<SessionDescriptor>
<SessionType>Inband</SessionType>
<SessionID>im.user.com#48815@server.com</SessionID>
</SessionDescriptor>
<Transaction>
<TransactionDescriptor>
<TransactionMode>Request</TransactionMode>
<TransactionID>IMApp01#12345@NOK5110</TransactionID>
</TransactionDescriptor>
<TransactionContent
  xmlns="http://www.openmobilealliance.org/DTD/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</GroupID>
</ScreenName>
</Group>
<ContactList>wv:john/My_friends@smith.com
</ContactList>
</Recipient>
<Sender>
<User>
<UserID>wv:john@smith.com</UserID>
</User>
</Sender>
<Validity>600</Validity>
</MessageInfo>
<ContentData>
Hurry up; they are ringing the bells in the WV already...
</ContentData>
</SendMessage-Request>
</TransactionContent>
</Transaction>
</Session>
</WV-CSP-Message>
```

**= Total message length of over 1200 bytes
(300bytes even with binary XML)**

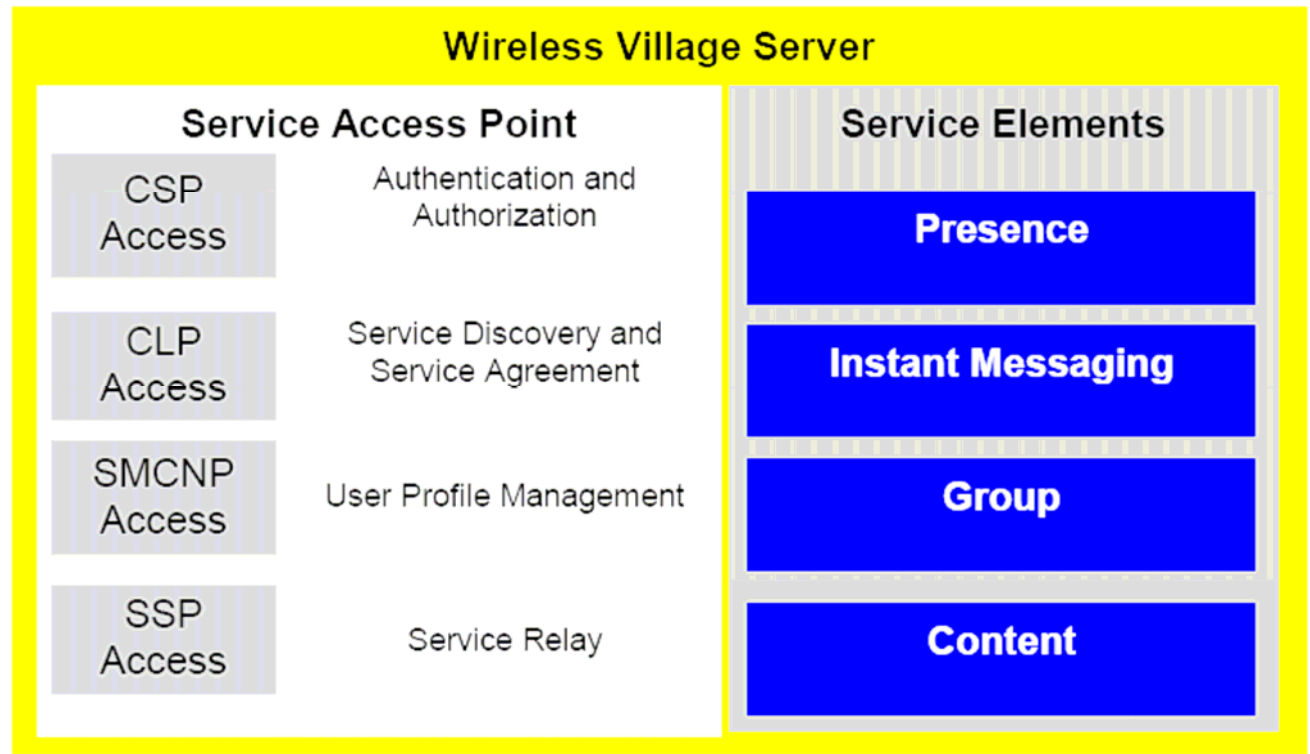
Example: Receiving a reply from the server (CSP)

```
<WV-CSP-Message xmlns="http://www.openmobilealliance.org/DTD/WV-CSP1.2">
  <Session>
    <SessionDescriptor>
      <SessionType>Inband</SessionType>
      <SessionID>im.user.com#48815@server.com</SessionID>
    </SessionDescriptor>
  </Session>
  <Transaction>
    <TransactionDescriptor>
      <TransactionMode>Response</TransactionMode>
      <TransactionID>IMApp01#12345@NOK5110</TransactionID>
    </TransactionDescriptor>
    <TransactionContent xmlns="http://www.openmobilealliance.org/DTD/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>
```

Features & Security Aspects

Wireless Village Server Architecture

- Service Access Points handle the protocols presented earlier
- Service Elements implement the actual feature functionality
- Not all features need to be implemented in a single Wireless Village deployment
- Design principles:
 - Bearer-agnostic
 - OS-independent
 - Based on open standards



Features: Common Features

- Some functionality shared and/or used in more than one feature:
 - **General Search Feature**
 - Currently defined for users and groups
 - Search users by name, e-mail address and groups by name, topic or ID
 - **General Invitation Feature**
 - Enable users to invite one or more other users to e.g. chat session
 - Invitations can include additional explanations
 - All invitations are expected to be either *accepted* or *rejected*
 - **Access Control**
 - Session must be established with the WV server by logging in
 - Actual usage of log-in credentials varies
 - Capability negotiation and “handshake” between the client devices and WV servers

Features: Presence (1/2)

- Broader concept of presence than “traditional” user presence
- Presence attributes can contain information such as:
 - Device capabilities, time zones, geographic location, free text status information, preferred languages, aliases, moods, information links, addresses etc etc.
 - E.g. if geographic location is included:
 - Longitude and latitude are required
 - Altitude and accuracy are optional
- However, top-level “required” presence elements only include:
 - **OnlineStatus**: whether a client is logged in on a WV server or not
 - **UserAvailability**: availability of the user (person) for communication
 - **StatusText**: user-specified text for his or her current state (e.g. “Out to lunch”)

Features: Presence (2/2)

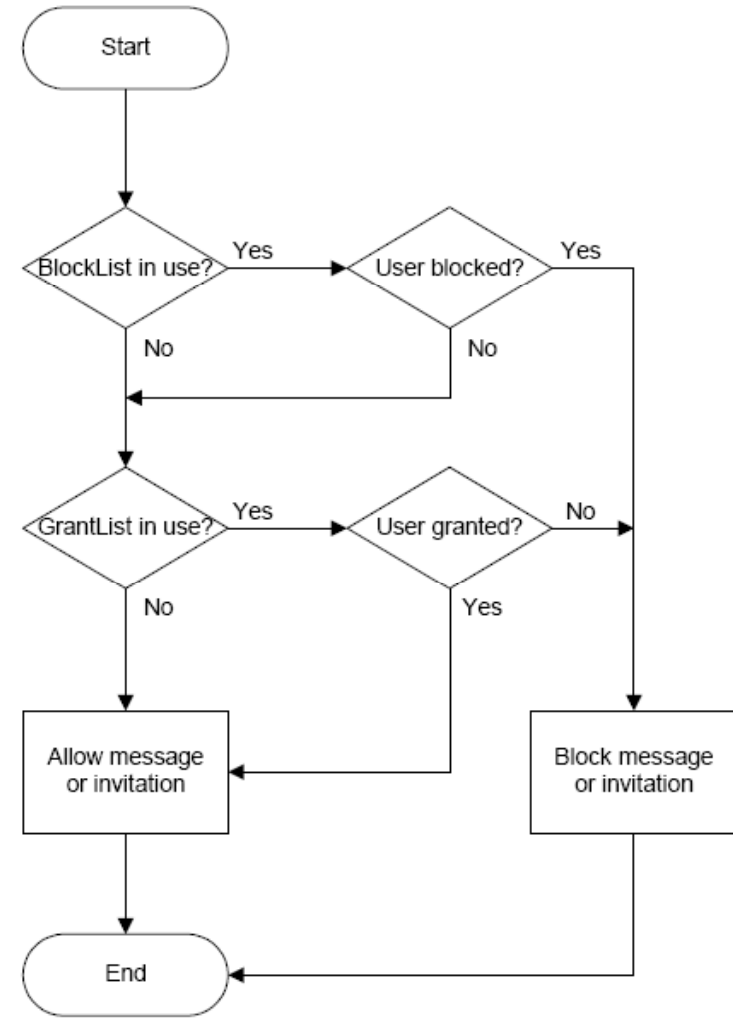
- Two models of authorization to access presence information
 - **Reactive:** users specifically request presence information of another user, who can accept or reject the request
 - **Proactive:** specified presence information is available for people on specific contact lists (multiple lists allowed with different presence visibility; e.g. friends can see geographical location but parents cannot)
- Clients notify the WV Server of their presence changes
- Presence “Watch Lists” maintained by the servers
 - One Watch List for each user
 - Include anyone who have subscribed to presence updates
 - Those on the Watch List with valid subscriptions get notified of presence change
- Publisher of presence information can at any time revoke authorizations

Features: Instant Messaging

- Two delivery types:
 - **Push delivery:**
 - The message itself is directly delivered to the client device
 - Current model for SMS delivery
 - **Notification / pull delivery:**
 - A notification is first delivered, the client then fetches the actual message from the server
 - Users can reject the message when receiving notification
 - Usually used for large messages
 - Current model for MMS delivery
- Target can be a group or an individual
- Access control through white- or blacklisting of message senders

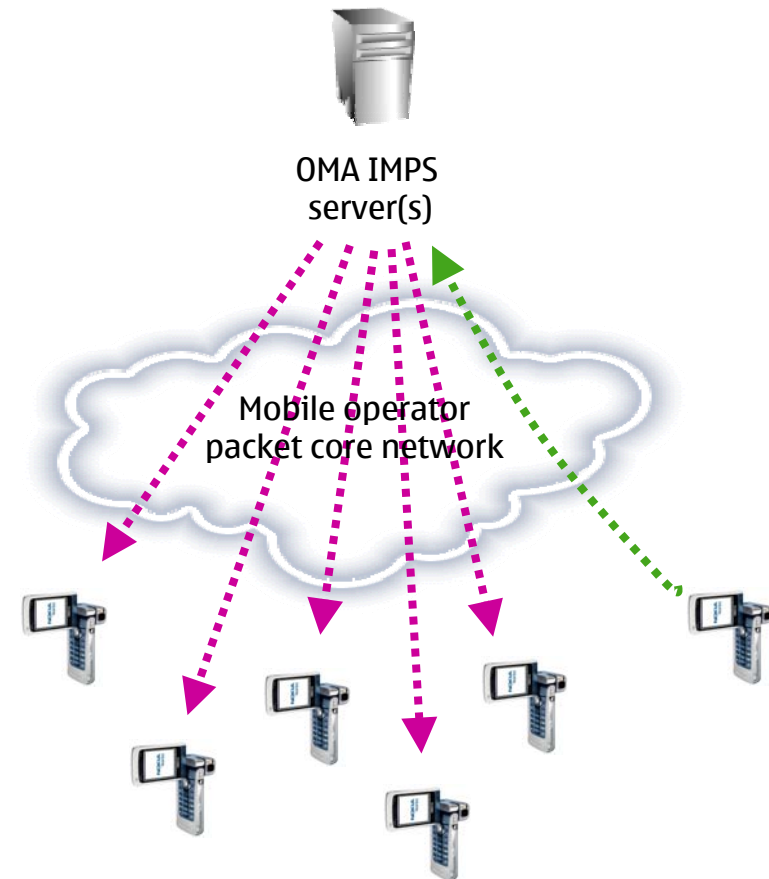
Features: Access Control

- Messages and invitations can be filtered
- Blacklisting & whitelisting possible:
 - Blacklisting = specify users that messages are blocked from
 - Whitelisting = specify users that messages are allowed from
- Filtering done at the WV servers



Features: Groups

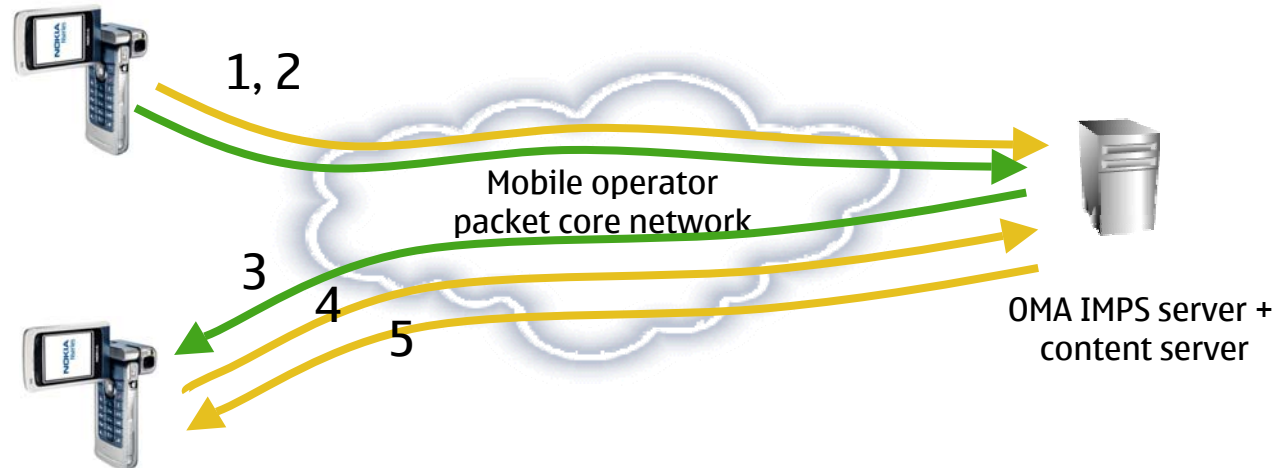
- Basically analogical to IRC channels, complete with optional topics
- Two types of groups:
 - **Public groups:**
 - Set up by the service provider (mobile operator)
 - Open to all
 - **Private groups:**
 - Set up by the users
 - Can be limited to a certain set of users
- Server maintains groups and performs message distribution to clients
- Initial creator has administrative control to the group



Features: Shared Content

- Unlike many other IM systems, even file-sharing is not peer-to-peer
 - Actually makes sense with mobile networks; nodes are not globally addressable between operator networks
- Specification of shared content feature is very light in OMA IMPS v1.2
 - Only specifies that content viewing is initiated by the common invitation feature with sending the URL of the content in the invitation
 - No word on how the content is uploaded, stored or downloaded from the server, when invitations are revoked, how long the content is valid etc
 - Possibility for the service providers to implement the feature in a number of different ways

1. Client uploads shared content to a server
2. An invitation with the URL to the content is sent.
3. The other client receives the invitation.
4. Client initiates fetching of content.
5. Shared content is delivered to the recipient.



Features: Comparison with other IM systems

	OMA IMPS	Other IM Systems
Topology	Purely client-server.	Peer-to-peer connections often utilized at least when in the same subnet.
Protocols	Heavy XML-based. Open standard.	Varies; mostly lighter. Often closed, proprietary.
Content Sharing	Practically unspecified; assumed <i>upload-invite-download-uninvite-cycle</i> .	Usually one or two clicks for sending a photo/file.
Features	Light set of basic IM and presence features.	Often include VoIP, interactive games and other “advanced” features.

Security aspects (1/2)

- OMA IMPS does not dictate or enforce encryption or security models
 - E.g. HTTPS can be deployed, but is not mandatory
 - No end-to-end encryption model specified
- Client authentication/authorization also not strictly mandated
 - Can be userid/password-based
 - Can rely on mobile operator's SIM-based authentication infrastructure
- Most deployments can be assumed:
 - To have client-to-server transport reasonably secure
 - Deployed in closed, “friendly” network
- OMA IMPS Server is a prime location for performing legal (or illegal) interception of the IM traffic

Security aspects (2/2)

- Session IDs potential weak point
 - After authentication, sessions are identified based on server-generated IDs
 - Session keys are up to 50 bytes in length
 - If captured, impersonating another user is fairly easy
 - Capturing does require compromise of client, server or transport
 - May be difficult but not impossible
- Lack of real end-to-end security is a clear drawback:
 - Must trust the service provider to some level
 - Government institutions and corporations may not be willing to do so
- *However:* for the majority of the target group (consumers) security is likely to be “good enough”

Real-life Usage

Case study - Mobile Operators

- In Finland Saunalahti, Sonera, etc
- Providing IMPS services
- Enhanced services like PoC, etc
- Charging
 - For IMPS services or free
 - Revenues from data traffic

Case study – Wireless vendors

- Nokia
 - Series 60 phones comes with IMPS embedded client
 - Over 30 phone models supports at the moment
- Ericsson
- Motorola
- Main contributors while forming the OMA

Case study – IT companies

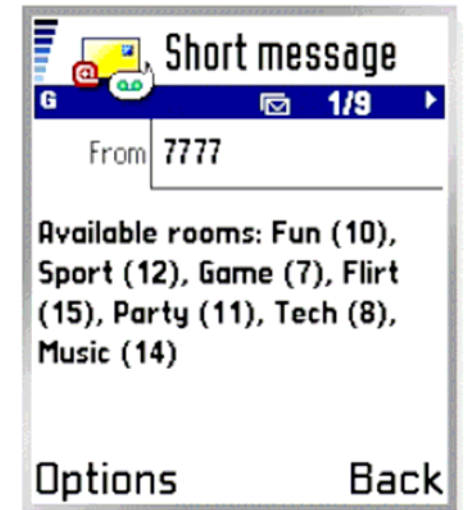
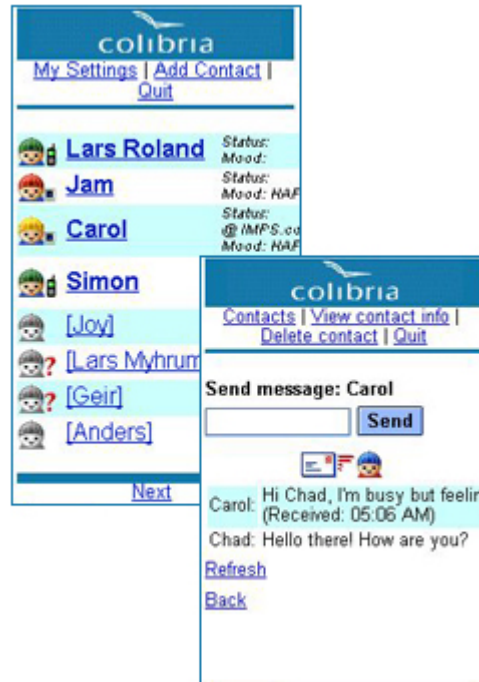
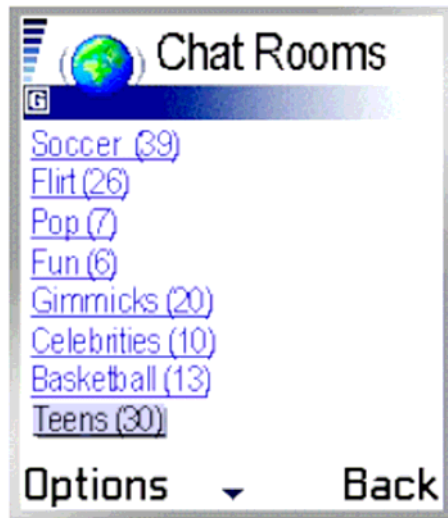
- Colibria
 - OMA member
 - Very active in interoperability testing IOT
 - Provided OMA IMPS solution world wide (Ex. Saunalahti in Finland)
 - <http://www.colibria.com>
- Oz Communications
 - OMA member
 - Partners with significant players
 - <http://oz.com>

Colibria

- IMPS server
 - Support for interoperability
- Variety of clients
 - For PC, Web, WAP and SMS

Colibria – variety of clients

- PC, Web, WAP and SMS Clients



Colibria – presence example

- Shows the status
 - Mobile or PC



Colibria - interoperability

- Clients
 - Symbian, J2ME, HTML, etc
- Colibria Companion instant messaging and presence server
 - Can work with 3GPP and IMS elements
 - Interoperability with other technology
 - Support connecting with other internet IM services like yahoo, AOL, etc

Oz Communications

- Mobile IM Gateway
 - Interoperability
 - Only yahoo, ICQ, AOL and MSN
- Mobile IMPS clients
 - Different platforms
 - Variety – IP, sms
- IMPS server
 - Presence enhanced phone book
 - Interoperable with other technologies (PoC, etc)

Interoperability



Integration of application services

- Access to third party



- Presence enhanced phone book

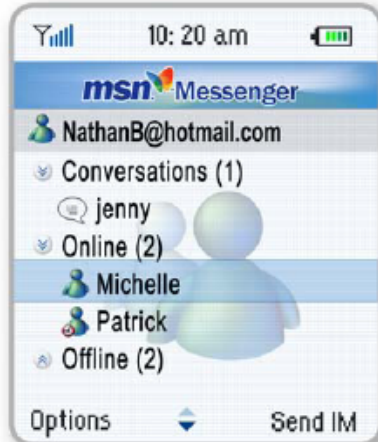


- Presence Enhanced Phonebook (PEP), Push Over Cellular (PoC), etc
- A single address book will emerge

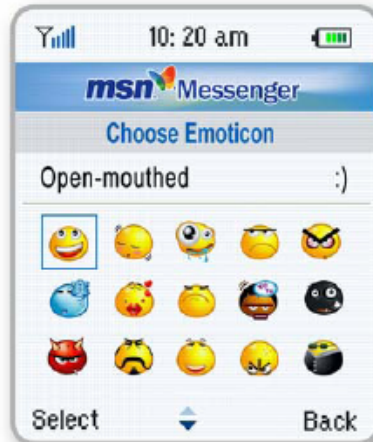


Oz – launched features

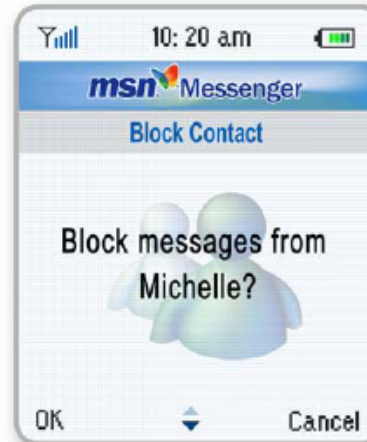
Tree based presence status



Popular Emoticons



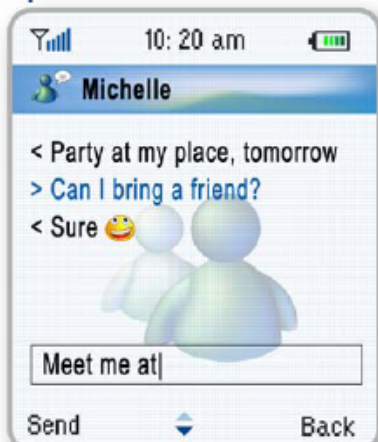
Contact Management



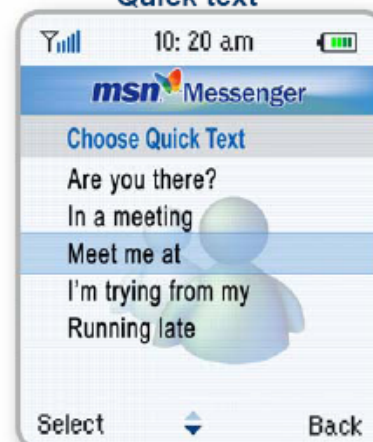
Benefits:

- Instant adoption
- Attract, grow and retains subscriber base and usage

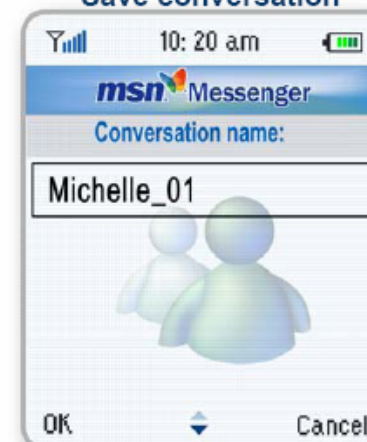
Split-screen Chat interface



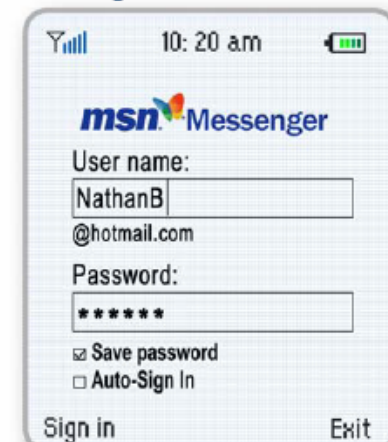
Quick text



Save conversation

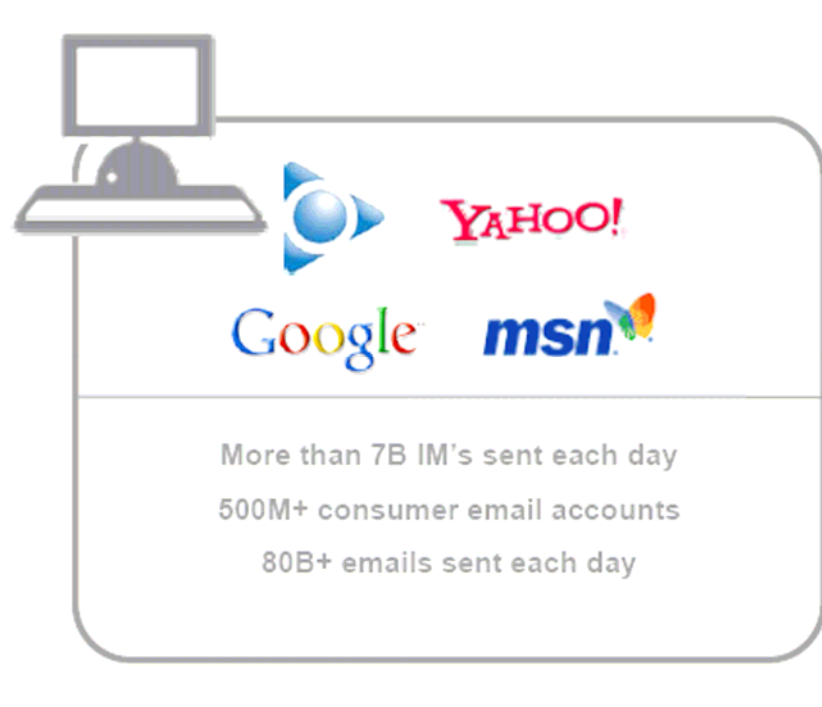


Individual Portal Sign-in credentials



1. Targeting the services and brands already being used

- IMPS services used
 - Yahoo
 - Google
 - MSN
 - AOL



2. Providing PC based user experience

Step 1



Select IM provider and enter existing username and password

Step 2



Sign in with existing username and password

Step 3



Pick an "online" contact from your buddy list

Step 4



Start the live conversation

3. Using mass market devices



✘ cingular
 ..T..Mobile-

Nokia S30/S40
 3595, 3100, 3120,
 3200, 6800, 6010,
 6820



✘ cingular
 SonyEricsson
 T637



✘ cingular
 Samsung
 X427M



..T..Mobile-
 RIM
 7100



..T..Mobile-
 HP iPAQ 6315



✘ cingular



..T..Mobile-
 ✘ cingular



Motorola
 V505, V180,
 V220



Samsung
 C207



Launch TBD
 Sony Ericsson
 P910



Samsung
 X475



Motorola A630



RIM
 7230



Savage OS



Nokia
 3220



Sprint.



Downloadable



..T..Mobile-
 Samsung
 E335



..T..Mobile-
 RIM
 7290



Case study – content provider

- Yamigo
- Free IMPS services on internet
- News Feeds – bbc, formula one, sports, etc
- Service Bots – google, weather,etc
- IMPS embedded client mobile is needed
 - Nokia, Sony Ericsson and Motorola
 - WAP APN (WSP bearer) and internet APN (TCP bearer)
- Took 180 seconds to get the instant message!
- <http://www.yamigo.com>

Conclusions

Conclusion

- **The good:**

- Standard well accepted among device manufacturers
 - E.g. Over 25 phones from Nokia support OMA IMPS
 - Close device integration and pre-installed software makes for an easy user experience
- Explicit support for interoperability with other IM systems
- Overall architecture well suited for mobile operator environments
 - Not necessarily “best” in terms of technical implementation, but suitable in terms of operator business, charging possibilities etc.

- **The bad:**

- Heavy XML-based client-server protocol structure
- No significant take-up or marketing by the mobile operators (yet?)
- Subscriber take-up figures modest so far. Competition already exists on the handsets in the form e.g. Agile Messenger and proprietary messaging solutions.
- Business model remains uncertain for the mobile operators:
 - *Are users willing to pay for the service?*

Thank You!

Questions?

sami@makelainen.com martinpeter.michael@nokia.com