

OMA-MWG-2004-0110R01-MMS-over-3GPP-Interworking-WLANs
Originated by MMSG
19 Aug 2004



LIAISON STATEMENT

Title: Re: MMS over 3GPP Interworking WLANs Public Confidential LS¹
To: 3GPP SA2
Copy: 3GPP SA3, IETF LEMONADE, OMA SEC
Response to: "Tdoc S2-041675", "MMS over 3GPP Interworking WLANs"
Source: MMSG of MWG of the Open Mobile Alliance
Send Replies to: MMSG
Jerry.Weingarten@comverse.com
Contact(s): Randall Gellens, Qualcomm
rg+oma@qualcomm.com,
Attachments: OMA-MMSG-2004-0214R01-Reply-to-3GPP-MMS-over-interworking-WLANs-
Qualcomm-Additional-Information

1 Overview

MMSG is pleased to reply to 3GPP SA2 regarding MMS over 3GPP WLAN Interworking.

2 Proposal

Please see detailed replies in-line with the original LS text below:

TS 23.234 includes the capability for the WLAN User Equipment (UE) to establish IP connectivity with the 3GPP network in order to access certain 3G services. Hence, the WLAN UE can access at least those services that only require IP connectivity. SA WG2 considers the Multimedia Messaging Service (MMS) as such a service, but would like to confirm that this is the case.

OMA MMSG confirms that MMS is such a service, provided that an MM1 is used which requires only IP connectivity.

SA2 has noticed that MMS specifications refer to both a WAP-based and an IP-based implementation of the UE to MMS server interface (MM1), the former relying on OMA protocols and the latter presumably intended to be based on the ongoing work in the IETF LEMONADE working group to optimise protocols such as IMAP for wireless links. SA2 would like to know what is the status of these two implementations and which would be most appropriate for use for UEs connected over WLAN in Release 6.

¹ If the "Confidential LS" box is selected, this liaison statement is intended to be Confidential per agreement by OMA and the addressed organization. Neither side should make this communication available to non-members.

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.

THIS DOCUMENT IS PROVIDED ON AN "AS IS" "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS.

OMA-MWG-2004-0110R01-MMS-over-3GPP-Interworking-WLANs
Originated by MMSG
19 Aug 2004

There are a number of MM1s developed by various groups. The OMA MM1 does use WAP but also has a binding to HTTP. The question is outside of our scope. Please see the attached contribution for more detailed information.

SA2 understands that these implementations assume a secure connection to the IP network, such as that provided by GPRS or equally the capabilities for tunnelled access to external IP networks defined in TS 23.234. SA2 would like to know whether any work is ongoing to specify protocols that would be suitable for use over insecure networks, such as Internet access as provided by the capabilities for Direct IP network access also described in TS23.234.

The question is outside of the scope of OMA MWG MMSG. We invite you to contact the relevant OMA working groups e.g., OMA SEC. Please see the attached contribution for more detailed information.

1. *What is the status of the two MM1 implementations (WAP-based or IP-based) and which would be most appropriate for MMS support over WLAN ?*

Any IP-based MM1 which provides authentication, authorization, and protection for message integrity and privacy may be used to support MMS over WLAN. Please see the attached contribution for more detailed information.

2. *Whether they consider the architecture and procedures described in TS 23.234 enable a WLAN UE to send and receive MMS while connected to a Public Land Mobile Network (Home or Visited) via a-WLAN which supports interworking with a 3GPP system (an Interworking WLAN or I-WLAN) using the procedures for tunnelled access to external IP networks ? Also, whether they see any difference in this respect between the WAP-based and IP-based implementations ?*

The OMA MM1 with http bindings may be used over this secure VPN, provided the authentication and authorization mechanisms are provided by the underlying connection (since these are not part of this MM1).

3. *Whether they foresee any work needed on specifications under their control to enable this, and if so, what timescales are foreseen for the completion of this work ?*

The question is outside of our scope. Please see the attached contribution for more detailed information.

4. *Whether any work is ongoing to allow these protocols to be used over insecure networks, such as the Internet ?*

Any MM1 which includes authentication and authorization mechanisms and protection for message integrity and privacy is suitable for use over open non-secure networks such as the public Internet. We invite you to contact the relevant OMA working groups e.g., OMA SEC. Please see the attached contribution for more detailed information.

3 Requested Action(s)

We hope the supplied information answers your questions. If not, please contact us.

4 Conclusion

OMA MMSG thanks 3GPP SA2 for their interest in MMS.

INPUT CONTRIBUTION

Title: Re: MMS over 3GPP Interworking WLANs Public OMA Confidential
To: 3GPP SA2
Cc: 3GPP2 TSG-X
Source: Randall Gellens, Qualcomm
rg+oma@qualcomm.co
Attachments: n/a Public OMA Confidential
Replaces: n/a

1 Reason for Contribution

Additional reply information to "Tdoc S2-041675", "MMS over 3GPP Interworking WLANs"

2 Summary of Contribution

This contribution answers the questions in "Tdoc S2-041675", "MMS over 3GPP Interworking WLANs" in greater detail than the companion OMA LS. The information provided here is intended as an overview and to answer the questions posed by the original LS, it is not intended to speak for 3GPP2 or IETF.

3 Detailed Proposal

Please see detailed replies in-line with the original LS text below:

SA2 has noticed that MMS specifications refer to both a WAP-based and an IP-based implementation of the UE to MMS server interface (MM1), the former relying on OMA protocols and the latter presumably intended to be based on the ongoing work in the IETF LEMONADE working group to optimise protocols such as IMAP for wireless links. SA2 would like to know what is the status of these two implementations and which would be most appropriate for use for UEs connected over WLAN in Release 6.

There are a number of MM1s developed by various groups. The OMA MM1 does use WAP but also has a binding to HTTP. 3GPP2 has specified two additional MM1s which only require IP, one (called M-IMAP) based on IMAP (3GPP2 X.S0016-311) and one which uses SIP (3GPP2 X.S0016-312). The work of the IETF LEMONADE group is likely to be useful as an alternate, IETF-standard IP-based MM1.

SA2 understands that these implementations assume a secure connection to the IP network, such as that provided by GPRS or equally the capabilities for tunnelled access to external IP networks defined in TS 23.234. SA2 would like to know whether any work is ongoing to specify protocols that would be suitable for use over insecure networks, such as Internet access as provided by the capabilities for Direct IP network access also described in TS23.234.

The IP-based MM1s, including the existing M-IMAP and SIP based ones (above) do include mechanisms for authentication, and can be used over TLS (SSL) to provide for message integrity and privacy protection. The IETF lemonade work incorporates IETF standards which permit a high degree of flexibility in choosing authentication and protection mechanisms, including TLS/SSL and SASL (RFC 2222). As such, any of these protocols would be suitable for use over VPNs, closed private networks, and open non-secure networks.

USE OF THIS DOCUMENT BY NON-OMA MEMBERS IS SUBJECT TO ALL OF THE TERMS AND CONDITIONS OF THE USE AGREEMENT (located at <http://www.openmobilealliance.org/UseAgreement.html>) AND IF YOU HAVE NOT AGREED TO THE TERMS OF THE USE AGREEMENT, YOU DO NOT HAVE THE RIGHT TO USE, COPY OR DISTRIBUTE THIS DOCUMENT.

THIS DOCUMENT IS PROVIDED ON AN "AS IS" "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS.

1. *What is the status of the two MM1 implementations (WAP-based or IP-based) and which would be most appropriate for MMS support over WLAN ?*

There are existing deployments of the OMA MM1 as well as the IP-based M-IMAP MM1 (above). The SIP-based MM1 (above) has been published. The IETF LEMONADE specifications are not yet published. Any IP-based MM1 which provides authentication, authorization, and protection for message integrity and privacy may be used to support MMS over WLAN. The determination as to which is most appropriate may depend on factors such as the desirability of using Internet standards, interworking with other systems, and the flexibility to choose security mechanisms providing the desired cost/benefit ratio as well as authentication/authorization mechanisms which interwork with existing systems.

2. *Whether they consider the architecture and procedures described in TS 23.234 enable a WLAN UE to send and receive MMS while connected to a Public Land Mobile Network (Home or Visited) via a-WLAN which supports interworking with a 3GPP system (an Interworking WLAN or I-WLAN) using the procedures for tunnelled access to external IP networks ? Also, whether they see any difference in this respect between the WAP-based and IP-based implementations ?*

Any of the IP-based MM1s (above) would be suitable for use over the secure VPN connection which TS 23.234 permits. The OMA MM1 with http bindings may also be used over this secure VPN, provided the authentication and authorization mechanisms are provided by the underlying connection (since these are not part of this MM1).

3. *Whether they foresee any work needed on specifications under their control to enable this, and if so, what timescales are foreseen for the completion of this work ?*

The published IP-based MM1s (above) appear to be suitable for use as-is. The IETF LEMONADE work is chartered to be suitable for these uses.

4. *Whether any work is ongoing to allow these protocols to be used over insecure networks, such as the Internet ?*

Any of the published IP-based MM1s (above) which include authentication, authorization, integrity protection, and privacy mechanisms are suitable for use over open non-secure networks such as the public Internet.

4 Intellectual Property Rights

Members and their Affiliates (collectively, "Members") agree to use their reasonable endeavours to inform timely the Open Mobile Alliance of Essential IPR as they become aware that the Essential IPR is related to the prepared or published Specification. This obligation does not imply an obligation on Members to conduct IPR searches. This duty is contained in the Open Mobile Alliance application form to which each Member's attention is drawn. Members shall submit to the General Manager of Operations of OMA the IPR Statement and the IPR Licensing Declaration. These forms are available from OMA or online at the OMA website at www.openmobilealliance.org.

5 Recommendation

We hope the supplied information is helpful. Please contact 3GPP2 and/or IETF for more specific or detailed information on their work. The information provided here is intended as an overview and to answer the questions posed by the original LS, it is not intended to speak for 3GPP2 or IETF.