3GPP TSG SA WG3 Security — S3#30 **S3-030622**
06 - 10 October 2003
Povoa de Varzim, Portugal

MMS TF Doc 204rev.1

First draft of MMS Security Paper

Version 0.1.1

Document Source:	Stefan Andersson, Engineering Support MMS[1] (anderssons@malmo.mail.telia.com,)	
Document Creation Date:	**2003-10-03**	
Document Status:	**For Approval**	
	For Information	**X**
Associated Knowledge Basis:		
Circulation Restricted[2]:	GSM Association	
	Members	**X**
	Associate Members	**X**

[1] Minor revisions between version 0.1.0 and 0.1.1 by Ansgar Bergmann, (ansgar_bergmann@yahoo.co.uk)

[2] **Restricted – Confidential Information**

Access to and distribution of this document is restricted to the persons listed under the heading Circulation Restricted. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those listed under Security Restrictions without the prior written approval of the Association. The GSM MoU Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

© Copyright of the GSM MoU Association 2003

Contents

1 Introduction

The task *MMS Security and Fraud Protection (including Spam)* is Work Area 41.2 of the MMS Task Force (cf. Doc MMS TF 005/03 in its latest revision).

The purpose is to study the security related issues and to produce input to 3GPP SA3, GSMA Security group and OMA that motivates work on countermeasures. It is also a part of the task to suggest countermeasures and security requirements where applicable. The detailed scope is defined in [6].

Security requirements in the current stage 1 document [4] are the baseline for the current security mechanisms in MMS. These requirements are recapitulated below:

> "*The user shall be able to use and access MM in a secure manner. It shall be possible for the contents of MMs to be read only by the intended recipient(s). A Recipient shall be informed of the reliability of the sender in case the sender has authorized his identity to be transmitted.*
>
> *The integrity of MMs during transit shall be assured to the extent of the network capabilities.*
>
> *The MMS shall be intrinsically resistant to attempts of malicious or fraudulent use.*
>
> *The " Security Threats and Requirements" in 22.133 shall not be compromised*"

Section 5.1.29 in the 3GPP2 stage 1 document [1] has some additional requirements:

> "*The MMS shall have the ability to authenticate the user regardless of access technology*
>
> *The MMS shall support data transport in a secure manner between the user and MMS*
>
> *The MMS authentication scheme shall use access specific information.*"

These requirements will be used later in this document as a part of the analysis of threats and countermeasures.

2 References

[1] Multimedia Messaging Services, Stage 1 Requirements. 3GPP2 S.R0064-0 V 1.0
[2] Security in MMS standardization, MMS TF Doc 36/03
[3] Proposed minimum handset security requirements for MMS v2.0, MMS TF Doc 113/03
[4] Multimedia Messaging Service, Stage 1. 3GPP TS 22.140
[5] Multimedia Messaging Service, functional description, stage 2. 3GPP TS 23.140 V6.2.0
[6] Work plan for Work Area 41.2: MMS Security, MMS TF Doc 142/03
[7] RFC 2595 “Using TLS with IMAP, POP3 and ACAP”
[8] RFC 2487 “SMTP service extensions for secure SMTP over TLS”
[9] Open Mobile Alliance; OMA-MMS-CTR-v1_1, Multimedia Messaging Service, Client Transactions, Version 1.1, URL: http://www.openmobilealliance.org/
[10] Open Mobile Alliance; WAP Transport Layer End-To-End Security, WAP-187-TransportE2Esec, URL: http://www.openmobilealliance.org/
[11] WAP Push Security Concerns, Jagjeet Sondh, Vodafone Group Research and Development, Lung Wan Vodafone UK Core Network Development
[12] XML-Signature syntax and processing, W3C Recommendation 12 February 2002, URL: www.w3.org/TR/2002/REC-xmldsig-core/
[12] XML-Encryption syntax and processing, W3C Recommendation 10 December 2002, URL: www.w3.org/TR/2002/REC-xmlenc-core/
[13] “Unsolicited bulk email: Definitions and problems”. Paul Hoffman. Internet mail consortium report: UBE-DEF IMCR-004, October 5, 1997
[14] “Unsolicited bulk email: Mechanisms for control”. Paul Hoffman, Dave Crocker. Internet mail consortium report: UBE-SOL IMCR-008, May 4, 1998
[15] Open Mobile Alliance; WAP-182-ProvArch-20010314, Provisioning Architecture Overview, URL: http://www.openmobilealliance.org/
[16] Open Mobile Alliance; WAP-182-ProvBot-20010314, Provisioning Bootstrap, URL: http://www.openmobilealliance.org/
[17] RFC 2806, ”URLs for telephone calls”
[18] Response to LS from CPWP on MMS read-reply reports, MMS TF 104/03
[19] LS to MMS TF on MMS read-reply reports, MMS TF 181/03
[20] RFC 2368, ”The mailto URL scheme”

3 System architecture

3.1 System overview

Figure 1 below describes the high-level system architecture of the MMS environment. The architecture is fetched from the 3GPP2 stage 1 document [1] since this contains a superset of the 3GPP architecture. The addition in the 3GPP2 document versus its 3GPP counterpart is the possibility to let an independent third party service provide run the MMS. This scenario however is not further dealt with in this report as no such implementations exist.

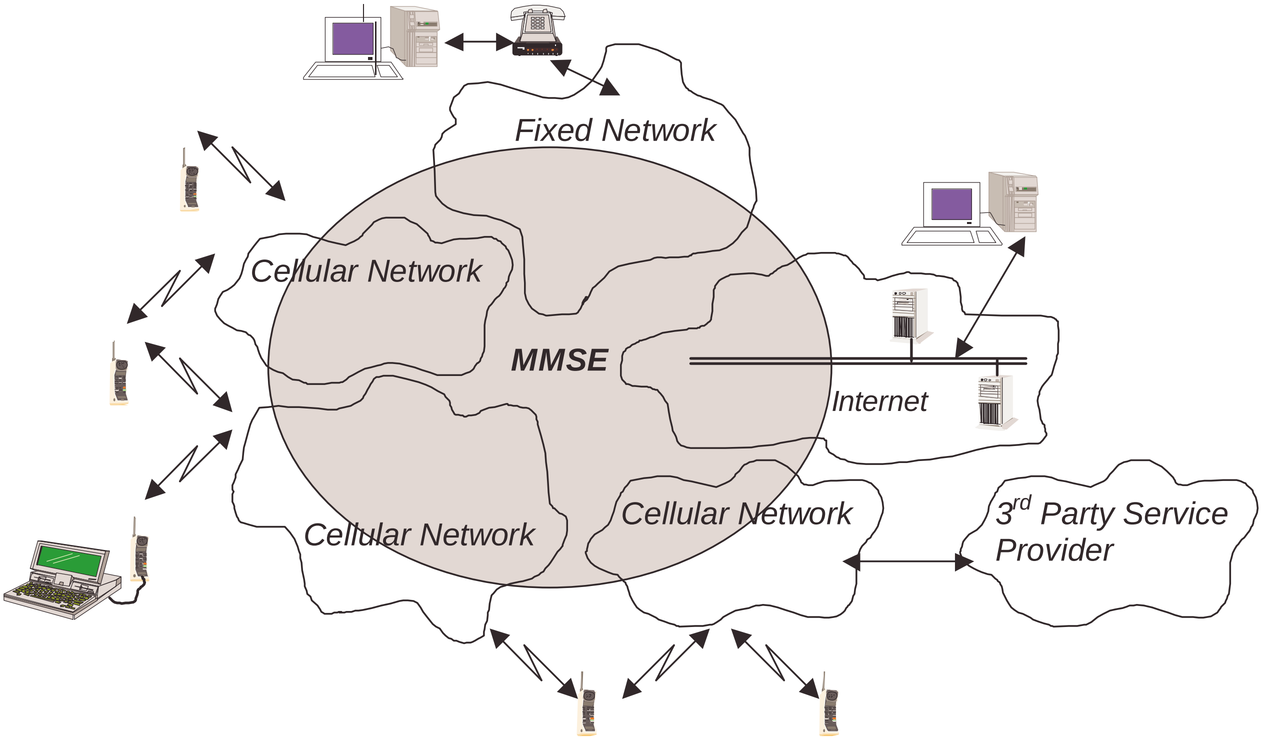

Figure 1 MMS Architecture

From the architecture we derive the more detailed scenarios described in subsequent sections of this document. These scenarios will be used throughout the document as a tool for the security analysis. (Some additional scenarios might be added.)

3.2 Scenario 1

In the first scenario two MMS UAs that reside on different cellular networks communicate. The communication between MMS UAs roughly uses the following path:

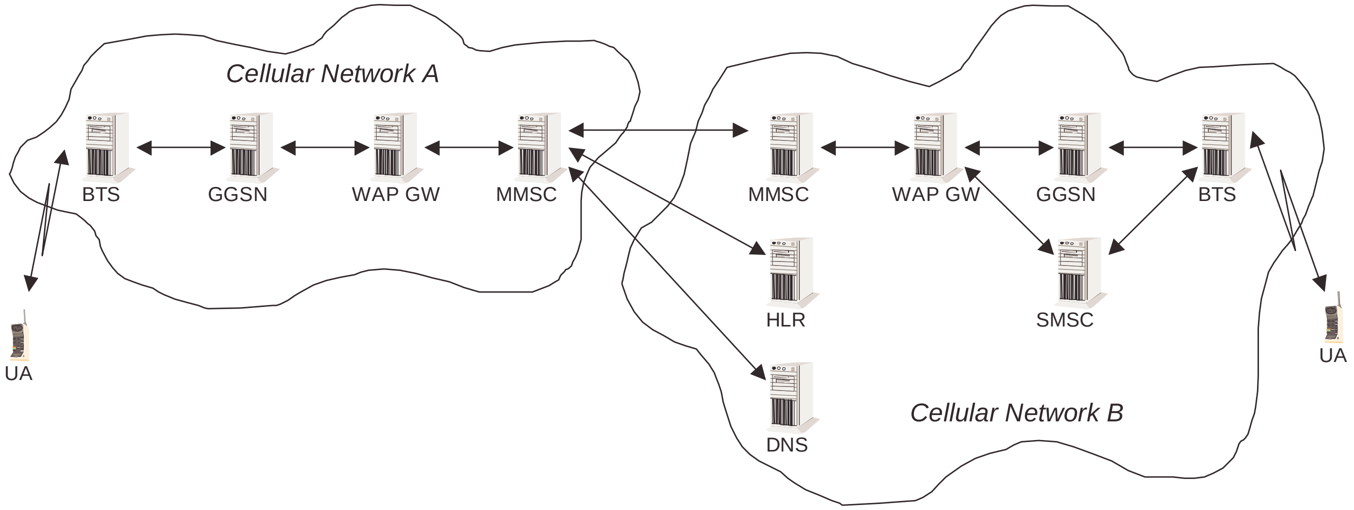

Figure 2 Scenario 1

Explanations to Figure 2:

- When using the WAP 2.0 protocol stack the WAP server might be omitted from the communication path. In this case the communication between the UA and the MMSC would be http-based end to end. However it can be expected that, even with WAP 2.0 terminals, most operators will deploy a WAP GW 2.0 (that is a dual stack proxy being able to relay both WSP and WP-HTTP onto normal HTTP).
- In the figure, between BTS and GGSN, the intermediate nodes in the chain

  BTS – BSC – SGSN – GGSN

  are not shown in order not to overload the figure.
- The originator UA (left) may be roaming. In this case the BTS, BSC and SGSN (on th left) belong to the visited PLMN whereas GGSN, WAP GW and MMSC belong to the HPLMN. In this case, between SGSN (vPLMN) and GGSN (HPLMN), typically GRX is used.
- The recipient UA (right) may be roaming. In this case the BTS, BSC and SGSN (on the right) belong to the visited PLMN whereas GGSN, WAP GW, HLR, SMSC and MMSC belong to the HPLMN. In this case, between GGSN (HPLMN) and SGSN (vPLMN), typically GRX is used.
- The communication between Originator MMSC and Recipient HLR can be performed via an intermediate signalling entity in the Originator PLMN:

oMMSC – intermediate signalling entity - rHLR

- The communication between Originator MMSC and Recipient DNS typically is done via the home DNS:

oMMSC – oDNS - rDNS

We consider the use cases where the UAs reside on the same network as a special case of our first scenario and they will therefore not be described separately.

In scenario 1 we can identify the following existing security measures:

- The communication between UA[3] and SGSN is encrypted and integrity protected
- The interface between MMSCs that reside on different networks, MM4, is SMTP-based and uses typically GRX or similar networks or public IP with IPSec or ‘nailed through connections’ (leased line etc.)
- The communication between the UA and the WAP server may be protected using WTLS. This may provide mutual authentication, integrity protection and confidentiality
- If WAP 2.0 is used the communication between the UA and MMSC may be protected using TLS or SSL. Just as WTLS these protocols may provide mutual authentication, integrity protection and confidentiality
- SSL or TLS may also protect the communication between the WAP server and the MMSC. This may provide mutual authentication, integrity protection and confidentiality
- The communication for SMS (WAP push) is encrypted and integrity protected between the BTS and the UA

3.3 Scenario 2

In our next scenario one of the UAs is replaced with an e-mail client that may reside on a fixed or cellular network. Here the communication path would be as follows:

[3] more exactly: the mobile station. Here and in the following, a distinction within the terminal is not yet made.

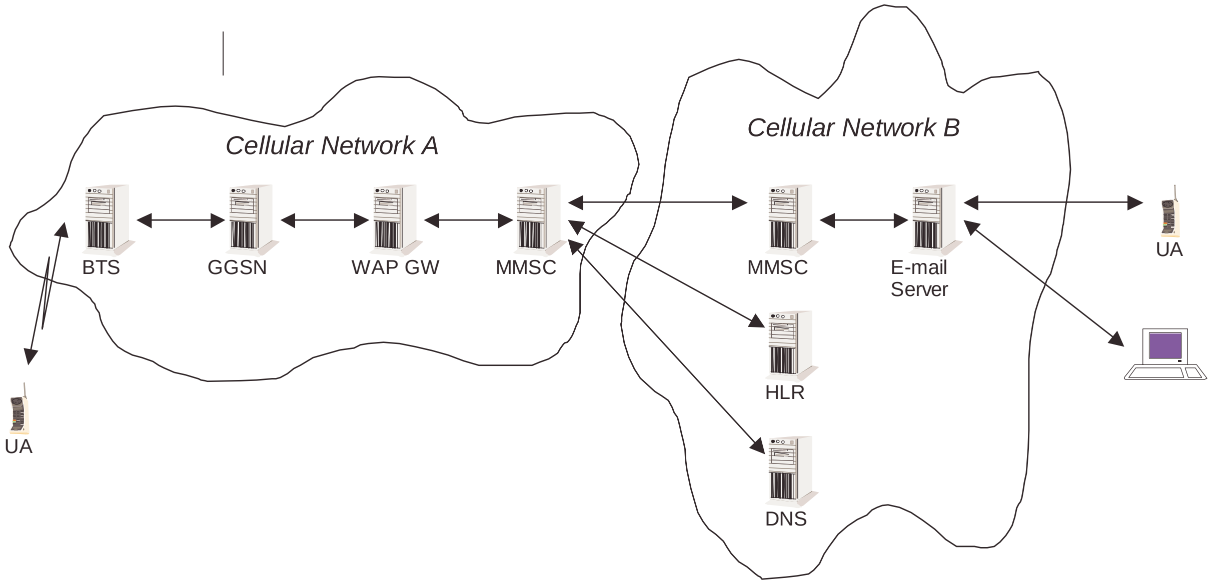

Figure 3 Scenario 2

The same explanations as for figure 2 apply.

In scenario 2 we can identify the following security measure in addition to the ones available in scenario 1:

- TLS or SSL may be used to protect the communication between the recipient UA (right) and the e-mail server as described in [7], [8]

If the e-mail server resides outside cellular network B the interface between it and the MMSC may be protected using the same mechanisms that are used on MM4, i.e. IPSec.

3.4 Scenario 3

In our last scenario, scenario 3, the MMSC is shared between several operators. The figure below elaborates on the architecture.

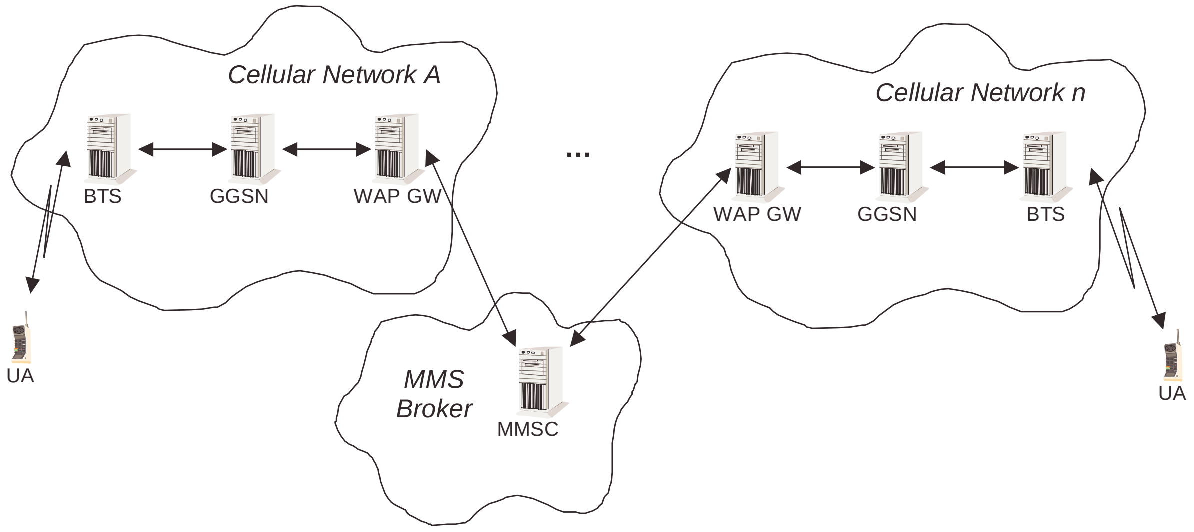

Figure 4 Scenario 3

In this scenario we can utilize the following security mechanisms:

- SSL or TLS may protect the communication between the WAP server and the MMSC. This may provide mutual authentication, integrity protection and confidentiality
- The communication between the WAP server and the MMSC may be protected using IPSec. This may provide mutual authentication, integrity protection and confidentiality

The trust model and the key management scheme must be handled carefully, in a sense this is similar to the establishment of roaming agreements between operators.

4 Threats and countermeasures on the communication path

4.1 Threat categories

To make the threat analysis more systematic we use following the attack definitions described in [2]:

- Protocol attack, an MM is submitted to/retrieved from the MMSC not adhering to the protocol as defined in the standard causing the MMSC or UA to malfunction.

- Data attack, an MM is submitted to the MMSC not adhering to the data format as defined in the standard causing the MMSC or the receiving MMS User Agent to malfunction.

- Service attack, a MM is submitted/retrieved from to the MMSC adhering to all current standards but misusing the service (e.g., unsolicited and spam messages, service theft, identity theft, loss of confidentiality).

We will use these attack definitions when we analyze the interfaces on the communication path in the remainder of this chapter.

4.2 Threats and countermeasures on MM1

4.2.1 Http/WSP

When we analyze the threats that arise from protocol and data attacks the important issue is to determine if such attacks are possible, not to create an extensive list of detailed attack descriptions. It would be impossible to find all attacks and in general that approach would lead us into a never-ending spiral of attacks and countermeasures. Another reason for not choosing this approach is that many attacks will be implementation dependent and they will therefore not have general applicability. We would like to draw this even further by stating that it is enough that an attacker can modify the protocol since it is difficult or even impossible to build a MMSC/UA that can withstand all types of attacks on the signaling protocol. Instead we should require integrity protection on MM1 in scenarios where protocol or data attacks are possible.

Scenario 1 is as secure as the access technology as long as the entire communication path is under operator control. Although there are some recent attacks on 2G security we can conclude that we in all practical cases have a secure system.

If on the other hand one of the communication interfaces between the GGSN, WAP GW or MMSC would be publicly accessible this would make us susceptible to protocol and data attacks. Natural countermeasures are IPSec on the interface between the GGSN and the WAP GW and SSL/TLS on the interface between the WAP GW and MMSC. One potential weakness with this approach is the fact that the communication is in plaintext in the GW. Therefore the physical protection of the WAP GW is quite important. WTLS can be used as an alternative to IPSec but again the communication will be in plaintext in the GW.

Co-locating the WAP GW and the MMSC can reduce this threat. Figure 5 GW navigation flow of events

In a WAP 2.0 architecture end to end TLS would be in use between the UA and the MMSC. This also removes the threat of having plaintext available in the GW.

When using TLS the standards specify that the URI of the server is verified against information in the server certificate. This mechanism is designed to prevent rogue servers from masquerading as legitimate. In wireless clients with limited display capabilities it is even more important since the URI is generally not visible to the user. This mechanism could typically also be used to verify the address of the MMSC in the UA against its server certificate.

There may be a subtle threat to this mechanism that stems from the way the server certificate is verified. The verification will be done against a predefined root certificate on the client. These root certificates may be preconfigured on the UA or on the SIM/WIM and they may even be downloaded by the user. It is this last option that may introduce a threat. If the root of a rogue CA is introduced on the client this CA will be able to issue server certificates that circumvent the URI verification mechanism. The countermeasure would be not to use user downloaded roots for this purpose.

Yet another reason for treating the roots with care is the fact that they define the trust model and control which server a UA can communicate securely with. If these roots can be modified by the user it is he or she that is in control of the trust model and not the operator.

If we look at the portions of the MM protocol that can be protected by TLS we find that TLS or SSL can protect the following PDUs:

- M-Send.req
- M-Send.conf
- M-Retrieve.conf

- M-NotifyResp.ind
- M-Acknoledge.ind
- M-Read-Rec.ind
- M-Forward.req
- M-Forward.conf

A triggering mechanism can be implemented as a configurable parameter in the client or some other means integrated in the protocol. The latter possibility can be compared to how IPSec is triggered from SIP in IPMM.

TLS can also be applied to the retrieval of a MM, triggered by the content location URI in the M-Notification.ind. Here the standards specify the use of the https URI scheme to trigger TLS.

4.2.2 Push

As described in the previous section several parts of the MM protocol can be protected by TLS. Unfortunately this is not as straightforward for the PDUs carried over unconfirmed push:

- M-Notification.ind
- M-Delivery.ind
- M-Read-Orig.ind

In the WAP push architecture, Figure 6 below, push messages are relayed through a push proxy gateway. Service providers and push initiators, access the push proxy gateway using the push access protocol. For MMS the MMSC would act as a push initiator. If the client doesn’t have a WAP session the PPG sends a SMS containing the URI from which the client can download the message.

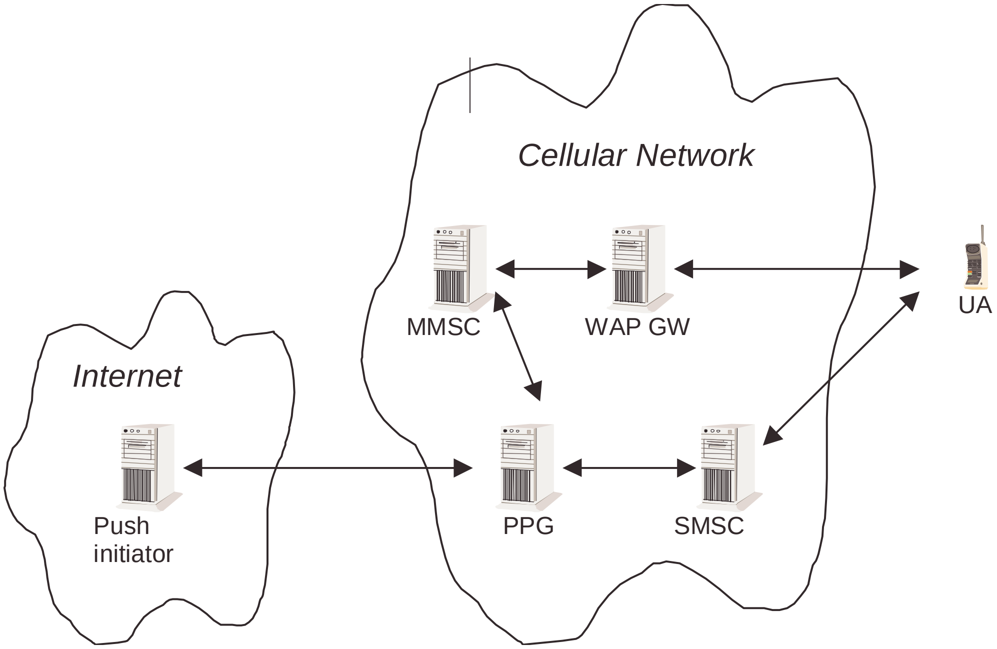

Figure 6 WAP push architecture

Two push mechanisms are defined in OMA:

- Service loading, SL. SMS with URI.
- Service Initiation Request, SIR. SMS with URI and GW address.

Several OMA members have raised security concerns and counter measures for push. The results in [11] are used as a base for much of the remainder of this section. With our notation the attacks related to push would be of the type service attacks.

It should be noted that several of the attacks related to push are generic and not specifically tied to MMS.

The following attacks are identified in [11]:

- With service loading it is possible for an attacker to force the client to download content from the Internet if the WAP GW allows that. If the GW only accepts addresses on the MMSC the request will be rejected and the terminal will prompt “failed” which will also cause inconvenience for the user.

- Using SIR it is possible for an attacker to make the client connect to another gateway instead of the one configured on the client.

A first countermeasure would be to only allow SIR against a predefined set of GWs. Similar mechanisms can protect SL, here the PPG source address would be verified against a predefined set of allowed addresses. The proposed mechanism introduces a white list that holds the details of allowed PPGs. This white list may be stored on the terminal or on the SIM. Solving the generic push security problem through the introduction of a white list mechanism has some deployment difficulties. New fields on the SIM must be specified and introduced or the white lists must be provisioned to the UAs.

There is a simpler solution in the case of MMS based on the configuration information that is already available in the UAs. The idea is to only download messages located at the terminals provisioned MMS server. All control messages (e.g. acknowledgement, reject, etc.) and originate MMS messages are sent from the terminal to a specific URL that are stored in the terminal. If the MMS server stores all messages on locations that start with the correct hostname prefix compared to the URL address that is stored in the terminal, then the terminal could easily check if the MMS message is stored at the MMS server and not somewhere else.

Unfortunately neither of these mechanisms is resistant against SMS spoofing. Therefore work is ongoing in OMA to define more robust push security mechanisms. Currently the push security requirements are being drafted in OMA. At this point it is difficult to guess what security mechanisms will be developed, but it can be concluded that it will take some time before the specifications are ready.

4.2.3 User identification

MM1 assumes that an underlying authentication scheme is used and that the identity information can be retrieved by the MMSC through RADIUS.

In scenarios where the entire MMS is under operator control this is definitely the most efficient and secure approach. Assuming that the underlying authentication mechanism is SIM or USIM based.

This is not true in scenarios where the MMS is not under operator control or where underlying SIM/USIM based authentication is not available, e.g. scenario 2. Here mechanisms in the MMS layer would be preferable, again assuming that they are SIM, USIM or ISIM based. Furthermore it is not obvious that the trust model in scenario 2 is such that the current approach is preferable.

4.3 Threats and countermeasures on MM2

MM2 is not specified by the current MMS release. Therefore the analysis of this interface is very brief. If this interface is publicly accessible, the system is threatened by the same type of attacks as the ones that are possible on MM1. As consequence authentication and integrity protection would be required.

4.4 Threats and countermeasures on MM3

MM3 enables interworking with existing e-mail servers, i.e. scenario 2 described earlier.

Since the MMS protocols are not extended over theMM3 protocol data attacks seem unfeasible on that interface. Unfortunately this is not true for service attacks in general and spam in particular. The main reason for this is that user authentication and charging mechanisms between the e-mail server and the UAs don’t match the mechanisms available in a cellular network. The authentication mechanism is a good example of this mismatch. In a cellular network smart card based mechanisms are used to authenticate the users whereas password based schemes are generally used to authenticate the users towards the e-mail server.

The lack of robust charging and authentication mechanisms opens the possibility to introduce SPAM in MMS through MM3. It should also be noted that SPAM introduced on MM3 would not only affect the operator connected to MM3 but it will spread through MM4 to other operators as well.

Current best practice is not to allow inbound MMs on MM3. This eliminates the SPAM threat. If this is to be changed there is definitely a need to enhance the existing security mechanisms. We will elaborate further on spam later in this document.

4.5 Threats and countermeasures on MM4

MM4 is susceptible to protocol, data and service attacks and it therefore requires relevant security mechanisms. As described earlier there are several mechanisms that can be used, i.e. IPSec etc. Since these mechanism assume direct routing without intermediate MMSCs it is important to architect the networks accordingly

Although MM4 may be the most dangerous interface in MMS it is also the one that is most straightforward to protect using existing technology, IPSec. For IPSec to be effective we must use direct routing between the MMSCs. If SMTP proxies are allowed the use of IPSec will be difficult since IPSec security associations are established hop-by hop on the IP level.

4.6 Threats and countermeasures on MM5

The HLR interface, MM5, may rely on MAP security.

4.7 Threats and countermeasures on MM6

MM6 is another interface that is not specified by the current MMS release. If this interface is publicly accessible, the operator may loose valuable information about his customers.

Furthermore the user privacy aspects of the information should also be taken into careful consideration. As consequence authentication, integrity protection and confidentiality would be required.

4.8 Threats and countermeasures on MM7

On an abstract level MM7 is similar to MM1, where the VAS takes on the role of the UA. In other words the VAS is capable of receiving, sending and forwarding MMs. The two major differences in a security perspective are:

- The VAS communicates with the MMSC over open IP networks

- The VAS is not expected to hold a SIM or USIM for authentication.

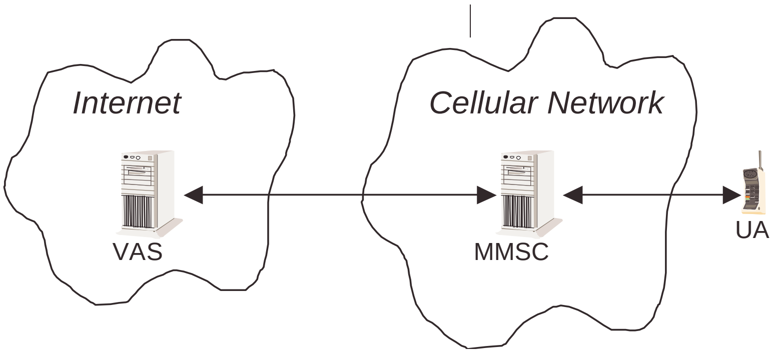

Figure 7 MM7 VAS MMSC interaction

The MMS functional description recommends the use of Http authentication and TLS. In other words it is recommended that we use TLS for integrity protection, confidentiality and server authentication. The VAS authentication will be performed using Http authentication.

A possible weakness with this approach stems from the use of Http authentication. It would be preferable to utilize TLS for client authentication but that would introduce a key management problem. The operator would have to issue TLS client certificates to the VAS provider.

IPSec could also be used to protect MM7 the same way as it can be used to protect MM4. Since IPSec key management generally is considered as cumbersome this approach is most suited for scenarios with rather static operator-VAS relations.

Since MM7 may be SOAP based there is a third alternative, SOAP security. For those not familiar with SOAP security it is based on XML-dsig [12] and XML-encrypt [13]. From a security and key management perspective SOAP security and TLS are quite similar since they are both PKI based. The main difference is that SOAP security is a quite new technology when compared to TLS, which is widely deployed.

Regardless of the choice of security mechanism we must assume close co-operation between the VAS and operator. Basically the operator must be able to trust the VAS. Much of the trust issues can be covered in the business agreement between the VAS and the operator.

If on the other hand the VAS can not be trusted the system will face the following threats:

- Charging abuse as defined in [5]
- The same type of threats introduced by malicious UAs described in section 5.4.

A malicious VAS has many similarities with a malicious UA. We will elaborate further on malicious UAs later in this document and we will leave that discussion for now. Nevertheless a malicious VAS can pose some additional threats since it may abuse the charging mechanisms.

4.9 Threats and countermeasures on MM8

MM8 is the third interface that is not specified by the current MMS release. Even more so than in the case of MM6 the operator is at risk. If this interface is standardized the security aspects and the trust model must be carefully considered.

5 Threats and countermeasures in the UA

5.1 Malicious content

The malicious content attack defined in [2] is directly applicable to threats on the UA. The definition is as follows: a well formatted MM is sent to the MMS but it contains malicious content that will cause harm on the UA.

Since MMS can be considered as both a client and a bearer we have two scenarios related to content rendering. The first is auto rendering of known content types. In this case the MMS UA would automatically render (display, play, execute…) the content from the SMIL presentation. The second is unknown content types, which will not be automatically rendered; instead they may be stored on the UA to be invoked later by the user. This is quite similar to how e-mail is used to carry attachments.

The first scenario is the potentially most dangerous one since it opens up for attacks that can be automated.

Viruses are often defined as malicious software inserted into another application to attack the host and spread to other systems. MMS has the potential of becoming a channel for viruses since:

- MMS supports auto rendering
- MMS supports superdistribution
- MMS may at some point support more dangerous content types such as, script languages, Java etc.

A majority of the supported media types seem to pose no threat when auto rendered. The media types that fall into this category are:

- Text
- Speech
- Audio
- Syntethic audio
- Bitmap graphics
- Video
- Vector graphics

Depending on implementation some of these types may be susceptible to buffer overflow attacks. Currently the majority of handsets are based on closed OS systems built on more or less proprietary hardware. To some extent this act as a protection against buffer overflow attacks that try to execute a malicious application. But it does not protect against buffer overflow attacks targeted at disrupting the UA, e.g. DoS attacks.

The presentation and synchronization formats SMIL and XHTML have some features that could be misused if not implemented correctly.

In SMIL the timing module can potentially be used to perform a denial of service attack against the user. The attack would involve a SMIL presentation with exceptionally long delays between the elements. A MMS UA can easily prevent this attack by always providing the user the option to cancel an ongoing SMIL presentation. This threat can be also be diminished by adding sanity checks to the timing elements of the SMIL presentation.

If the XHTML implementation allows either the: tel, vtel, mailto, smsto or mmsto URI scheme this can be used to commit fraud against the user if the user can be tricked to select one of these links. Things get even worse if the implementation allows automatic interaction with the address book in the UA. This would open the possibility for “I love you” type viruses.

A countermeasure would be to graphically indicate the purpose of a URI. That options seems to be difficult from a usability perspective. A better option is to follow the Java approach and clearly warn the user before initiating a chargeable event. The latter is also the option that is recommended in [17] and [20]. Furthermore [20] also recommends that the “From” address is not set by the URL, instead it should be provided by the mail client.

For MMS, the terminal will to offer more control of the user interface than for other services. For example, the screen may be faked, and the user may be misled to accept actions of the terminal without realizing what he does.

A generic countermeasure is make user the MMS client application visibly distinguishable from system messages and functions. This can be done by only allowing the MMS application to use a portion of the display, the rest would be reserved for system status information, softkeys etc. This would preferably be combined with mechanisms that always allow the user to stop the rendering of a MMS. Technically this can be achieved by giving the MMS application the right priority in the system, i.e. lower than the UI and system threads.

As new media types are added the risk of automatically rendering them must be considered. If MMS end up in the same situation as e-mail is today we face a situation where virus checkers, MMS filters, and firewalls must be introduced at great cost to protect the system.

In the second scenario MMS is merely used as a transport and the rendering client in the UA must handle the threat. This would for example be the case for Java applications distributed using MMS as a bearer.

5.2 Spam and DoS attacks

We derive our definition of MMS spam and the problems it may cause from [13]. The definition of MMS spam would be MMS messages that are sent to a group of recipients who have not requested it.

Spam is so dangerous because the majority of the costs related to the message may passed onto the recipient and the recipient operator. Several such costs can be identified here are some examples:

- Network traffic costs to the destination operator, e.g. bandwidth and MMSC storage capacity
- Time lost deleting unwanted messages
- Loss of revenue due to lowered MMS usage

The thing that makes e-mail spam so devastating is the fact that it is virtually free to send e-mail. This means that nearly all costs are shifted to the recipient. In the case of MMS this is not true as long as MMs are only allowed into the system on channels that support user authentication and charging. So one thing that protects us from spam is the charging model.

Looking at the MMS reference architecture we find four potential entry points for spam, MM1, MM3, MM4 and MM7. As described earlier in this report some configurations of MM1 and MM3 may lack robust authentication and charging mechanisms. This is the kind of environment in which spam can flourish.

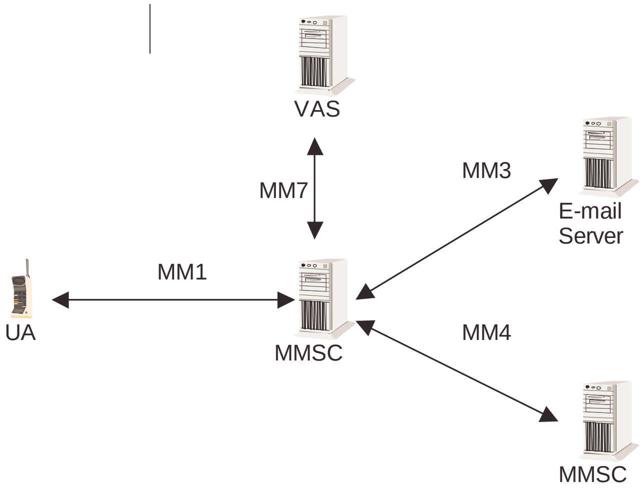

Figure 8 Potential spam entry points

If spam is introduced in the system there are some countermeasures that can be deployed [14]:

- Origin based filtering, at the MMSC or in the UA

- Message based filtering, at the MMSC or in the UA

- Originator accountability

It is assumed that none of these will be able to fully eliminate spam once it is in circulation. It should also be noted that Originator accountability is a prerequisite for robust charging mechanisms.

The potential spam entry points described earlier are also the interfaces most likely to be subject to denial of service attacks. In general the wireless world is inherently less resistant to DOS attacks due to bandwidth limitations, memory and CPU limitations on the clients.

5.3 OTA configuration

OMA defines push based over the air, OTA, configuration mechanisms in [15][16]. The configuration data is a XML document that can contain settings for, the browser, e-mail, MMS etc. The OTA configuration can be performed over several bearers including, SMS, USSD, SIM and cell broadcast. The architecture is further described in Figure 9 below.

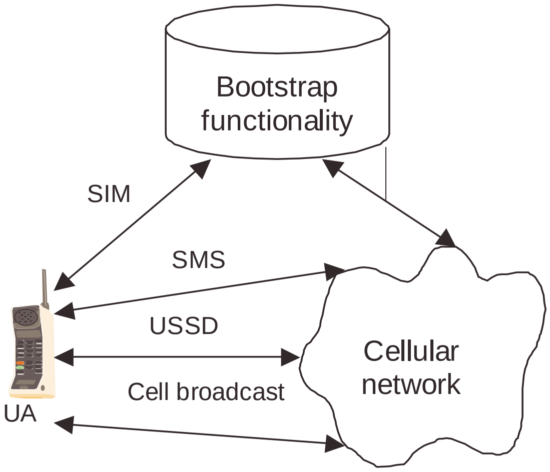

Figure 9 OTA configuration architecture

Adequate security mechanisms are important since OTA configuration easily can be used for malicious purposed. Two methods have been defined to meet the threats:

- Bootstrap security by means of a shared secret

- Bootstrap security by means of an out of band delivery of authentication information.

In the first method the shared secret is used to calculate a SHA-1 based HMAC which integrity protects and authenticates the configuration data. The HMAC value is carried as a parameter to the media type in the content type header. The integrity key can either be a value entered by the user, a value defined by the network or a combination of both. In GSM the IMSI will be used as the network value for the shared secret.

As the name of the second method implies the MAC value is not carried in the OTA message. Instead the MAC is incorporated in a PIN which is delivered to the user by a out of band mechanism. This pin is entered by the user and compared to a value calculated by the UA.

If the security of the OTA configuration mechanism is insufficient it can be used to commit fraud against the users. A possible scenario is that someone creates a fake configuration message where the MMSC address and the access parameters are spoofed. Once the configuration is installed in the client the attacker could send a normal MM which would then make a CSD connection to a malicious MMSC. The MMSC could keep the connection open for monetary fraud or it could launch buffer overflow attacks on the UA.

The robustness of the OTA security mechanisms can be questioned mainly due to limitations in the effective key length of the user entered PIN. This can be compared to the security level that could be achieved if for example the SIM would be used to carry the symmetric key.

5.4 Malicious UAs

Focus in the previous chapters of this paper has been on communication security or threats against the UA. In this section we will elaborate on threats on the system that arise from malicious UAs.

Let’s start by assessing the difficulty to create a malicious UA. The first possibility is that the a phone manufacturer implements a malicious UA. This clearly feasible from a technical perspective but it is definitely prevented by the business environment. If this should ever happen operators can simply decide not to do business with that manufacturer. This trust model is not very different from what is in place concerning the GSM protocols.

A second option is that then MS UA is implemented in Java. This is technically possible since a Java MIDLet can access http and the push inbox.

One way to guarantee that Java untrusted can’t be used to implement a malicious UA is to integrate information in the protocol that can’t be accessed from Java. One such possibility is to include SIM based authentication in the MMS protocol.

It should also be noted that it seems impossible to prevent Java MIDlets from implementing a parallel MMS system outside operator control.

A third possibility for malicious UAs is on open OS terminals based on Symbian OS, Microsoft OS, Linux etc. Here a third party can implement a malicious MMS UA. In this case it is expected that all APIs in the handset are available to the third party provider. Therefore it will be difficult to prevent this type of MMS UA by relying on SIM based authentication.

The conclusion must be that malicious UAs can appear in MMS systems already today.

Assuming that it is possible to implement a malicious UA what will be the consequences? One observation is that the threat is not as dangerous as if MM1 would lack security mechanisms. If there was no user authentication or integrity protection on MM1 any hacker could remotely inject malicious messages. A malicious UA would still need to perform authentication before it can access the MMS. This means that malicious UAs can be detected and blocked from accessing the system.

Although it is possible track malicious UAs the system must still be robust enough to minimize the impact of DoS attacks and fraud.

To prevent DoS attacks from malicious UAs the MMSC must:

- Resist Buffer overflow attacks from UA generated MM1 messages

- Resist DoS attacks where the UA tries to flood the MMSC with MM1 messages.
- Implement mechanisms to resist misuse of the protocol flow, e.g. the UA doesn't send M-Acknowledge.ind in a MMS retrieval transaction with confirmation or it has exceptionally long delays between messages.
- Be robust enough to cope with UAs that modify the MMSC generated transaction identifier in messages such as the M-NotifyResp.Ind and the M- Acknoledge.Ind
- Have sanity checks on the time parameters EarliestDeliveryTime and TimeOfExpiry

A potential source of fraud can be found in the information generated by the UA that may be included in the CDR for a MM. The information we believe have the greatest potential for misuse is:

- ContentInfo, i.e. audio, video, text etc
- MM status, i.e. delivered, rejected etc

Cooperating malicious UAs can circumvent content type based charging by agreeing to use a lower value content type to carry high value content. They can also misuse the MMS status by actively sending error reports even if the content was delivered correctly.

In another type of fraud malicious UAs carry end-to-end information in redundant fields of the MM protocols. This scenario related to read report messages has been studied in [18] and [19]. The read report PDU contains the following information:

- Recipient address
- Originator address
- Message ID
- Date and Time
- Read Status

The transaction flow for the read report is shown in the figure below.

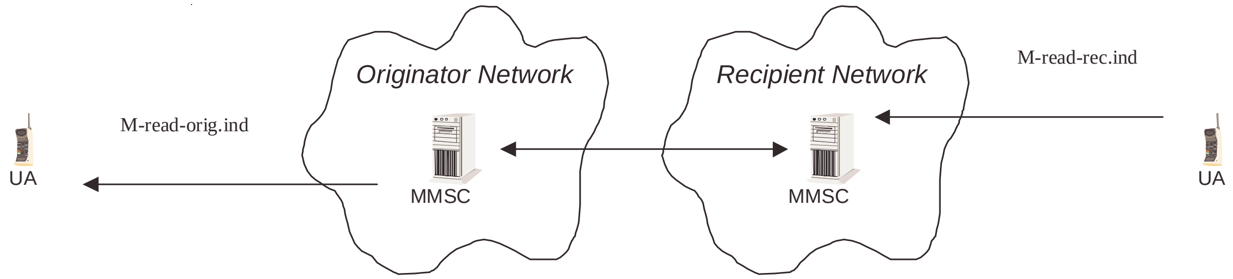

Figure 10 Read report

The potential for fraudulent usage of the fields in the read report PDU is as follows:

- If the recipient MMSC and the originator MMSC accept read-reply report PDUs without verifying them against earlier MM transfer or accept multiple read-reply report requests for the same MM, it is possible to send faked read-reply reports end-to-end.

- If the recipient MMSC and the originator MMSC don’t check the *Recipient address* and *Originator address* then those fields can be used to carry information end-to-end

- The *date and time* and *read status* fields can be used to carry information end-to-end

To prevent misuse the following countermeasures have been identified:

- A read report PDU shall be discarded if the messaged doesn’t match the Message ID of a previous MM where the Read-Reply indicator is activated.

- A read report PDU shall be discarded if a Read-Reply report message with the same Message ID already has been received by the Originator MMSC.

- A read report PDU shall be discarded if the size exceeds a determined amount of bytes.

If these mechanisms are implemented only a few bytes of the read report PDU can be used to carry information end-to-end.

6 Conclusions and proposals for security enhancements

6.1 Conclusions

Our main conclusion is that most aspects of MMS as it is deployed currently seem to be secure with two exceptions, push and OTA configuration. Push seem to face the greatest threat, as it implements virtually no security scheme. OTA configuration is in a better position but the security mechanisms can be improved.

The security and authentication mechanisms in MMS are not sufficient in future configurations such as scenario 2 with incoming email or in scenarios with a MMS operator independent from the radio access operator.

If we compare MMS with IPMM we find that the security mechanisms are quite different. In IPMM authentication and integrity protection are mandatory on the first hop in the IPMM layer. In IPMM the following assumptions, properties, has led to the requirement on integrity protection and authentication:

- signaling protocol in the user-plane
- access independence

MMS already fulfill the first property since the MM messages are relayed form the UA to the MMSC over WAP push or Http.

The second property can be derived from scenario 2 and from the security requirements defined in [1]. To recapitulate the requirement we are referring to: "*The MMS shall have the ability to authenticate the user regardless of access technology*.

6.2 Security enhancements

As concluded in the previous section push security should be improved. The long-term solution is definitely to standardize generic push security mechanisms. With sufficiently generic mechanism this would also improve the situation for OTA configuration. If this can't be achieved we should seek more secure alternatives to the mechanisms defined for OTA configuration. One option is to make the mechanisms based on the shared secret that resides in the SIM, USIM or ISIM.

It is also possible to define a MMS specific short-term solution for the push security issue.

An alignment with IPMM security should be considered. One way to align the solutions would be to:

- Use EAP-AKA in http for MMS

- Run MMS over symmetric key TLS where they keys are derived from AKA.

Furthermore the S3 generic authentication architecture workitem should preferably also take MMS into account when defining the authentication mechanisms.

A sufficiently strong solution authentication and integrity protection solution should be defined for scenario 2 in order to allow incoming email on MM3.

6.3 Final remarks

End-to-end security was not considered in this report since content adaptation was deemed to be an important MMS function, which would not be possible to implement on encrypted messages. This assumption may in the future be reconsidered since transcoding will effectively be prevented by the introduction of DRM in MMS.

7 Open issues

This chapter will be removed when all issues are handled in the report.

Open issues:

- **Error! Reference source not found.** GRX security, are there any ifs in current GRX security

- **Error! Reference source not found.** DNS outside of the operator network, DNS security?

- Push Fraud against the user through SIR, SIR contain phone number if CSD?

- User identification Is SIM authentication or userid/pwd used against the MMS APN?

Threats and countermeasures on MM3, proposals on how to handle incoming email, IMAP, POP3 auth using AKA

- Threats and countermeasures on MM4, Study the security considerations of relevant RFCs

- Malicious content, Elaborate further on threats and countermeasures in [17], [20]

- Malicious content Add gsm-sms URL scheme to the references

- Malicious content Fraud on streaming with malicious URL just as in the push case.

- Spam and DoS attacks, Operator-operator charging for MMS on MM4. Does the sender always handle charging?

- Spam and DoS attacks, DoS attacks on MMS level? Get into the infrastructure (push), spam UA with MM1 messages so they attack MMSC

- Malicious UAs, Verify that the push inbox is accessible in MIDP 2.0

- Malicious UAs Expand to other messages; look for redundant info that can be used as a side channel by a malicious UA. Look at the countermeasures in TF 03 181 and propose others if necessary.

- Malicious UAs If the to field is used to route the read reply message then it may be possible to route the read reply to another user

- Malicious UAs MMSC filtering as described in [14]

- Conclusions and proposals for security enhancements UA threats and countermeasures should be included in chapter 6

- Any reports of MMS fraud?