MMS Interworking Guidelines
Version 3.3
18 December 2006

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction 3
1.1 Overview 3
1.2 Scope 3
1.3 Abbreviations 3
1.4 References 4
2 MMS Roaming and Interworking Scenarios 4
2.1 Interworking 4
2.2 Roaming 6
3 General Requirements of the Inter-PLMN Backbone 8
3.1 IP addressing and routing 8
3.2 Network connection to GRX 8
3.3 Security and Screening 8
3.4 MMS Interworking Provider 9
4 MMS and the Domain Name System – DNS 10
4.1 DNS, MMS Interworking, and GRX 10
4.2 DNS Resource Records 11
5 Addressing Scheme 12
5.1 NAI versus MSISDN 12
5.2 MMS Addressing 13
5.2.1 Direct or Indirect 14
5.2.2 Creating the domain for direct routing 14
5.2.3 Creating the domain for In-direct routing 14
5.3 Address Discovery & Number Portability 14
5.4 Advanced Number Portability using ENUM 17
5.4.1 Separated Databases 17
5.4.2 Central Database 19
6 Conclusion 19
Annex A Document Management 21
A.1 Document History 21
A.2 Other Information 21

1 Introduction

1.1 Overview

This document introduces guidelines for usage of GPRS inter-PLMN connections in MMS environment and requirements for inter-PLMN backbone network caused by MMS.

Throughout this document, GPRS refers to as both GPRS Release '97/98 (i.e. 2.5G) and GPRS Release '99/UMTS (i.e. 3G).

1.2 Scope

This document gives guidance to MMS related issues such as addressing, routing and number portability to ensure interoperable MMS services and networks concerning roaming and interworking cases between different PLMN operators.

The harmonized definitions given in this document are considered as the prerequisites for interoperable MMS roaming and interworking scenarios.

Radio interface, GPRS backbone, MMSC terminal/application connections and billing issues are not in the scope of this document. Aim of this document is not to give an elementary level introduction to MMS, see e.g. GSM Association SE.32 [1] and 3GPP TS 23.140 [2] documents for this purpose.

1.3 Abbreviations

Term	Description
BG	Border Gateway
DNS	Domain Name System
ENUM	Telephone Number Mapping Standard
ESMTP	SMTP Service Extensions
GGSN	Gateway GPRS Support Node
GRX	GPRS Roaming Exchange
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
MM	Multimedia Message
MMS	Multimedia Messaging Service
MMSC	Multimedia Messaging Service Centre
MNP	Mobile Number Portability
MTA	Mail Transfer Agent
NAI	Network Access Identifier
SGSN	Serving GPRS Support Node
SMTP	Simple Mail Transfer Protocol
TLD	Top Level Domain
VPN	Virtual Private Network

1.4 References

Ref	Doc Number	Title
[1]	GSMA PRD SE.32	Multimedia Messaging Service
[2]	3GPP TS 23.140	Multimedia Messaging Service, Stage 2
[3]	GSMA PRD IR.34	Inter-Service Provider IP Backbone Guidelines
[4]	WAP Forum WAP-205	MMS Architecture Overview
[5]	WAP Forum WAP-206	MMS Client Transactions
[6]	WAP Forum WAP-207	MMS Encapsulation Protocol
[7]	ITU Workshop Document WS ENUM-5-E	Version 7 Of The ENUM Supplement, ENUM Tutorial, Geneva, 8 February 2001
[8]	ITU Workshop Document WS ENUM-5-E	Global Implementation Of ENUM: A Tutorial Paper, ENUM Tutorial, Geneva, 8 February 2001
[9]	IETF RFC 2821	Simple Mail Transfer Protocol
[10]	IETF RFC 2916	E.164 Number and DNS
[11]	IETF RFC 2478	SMTP Service Extension for Secure SMTP over TLS
[12]	IETF RFC 2554	SMTP Service Extension for Authentication

2 MMS Roaming and Interworking Scenarios

2.1 Interworking

The following figure describes the MMS interworking. Unlike the SMS scenario the message is sent to the user always via his “home”-MMSC. This implies the necessity of an inter-MMS protocol. This protocol is defined as SMTP in the MMS standard of the 3GPP (23.140 [2]).

SMTP is the standard protocol for email in IP networks, such as Internet. This choice is well within line of MMS standardization aim to utilize existing standards as much as possible instead of creating new ones.

It is crucial to note and understand how much MMS interworking differs from SMS interworking because of this new MMSC-to-MMSC interface, which has no analogy in SMS world. This interface is called MM4 in TS 23.140 [2] and multimedia messages are transported over IP network through it from one MMSC to another. MMS interworking is considerably more complicated than SMS interworking because of increased number of different network elements**.**

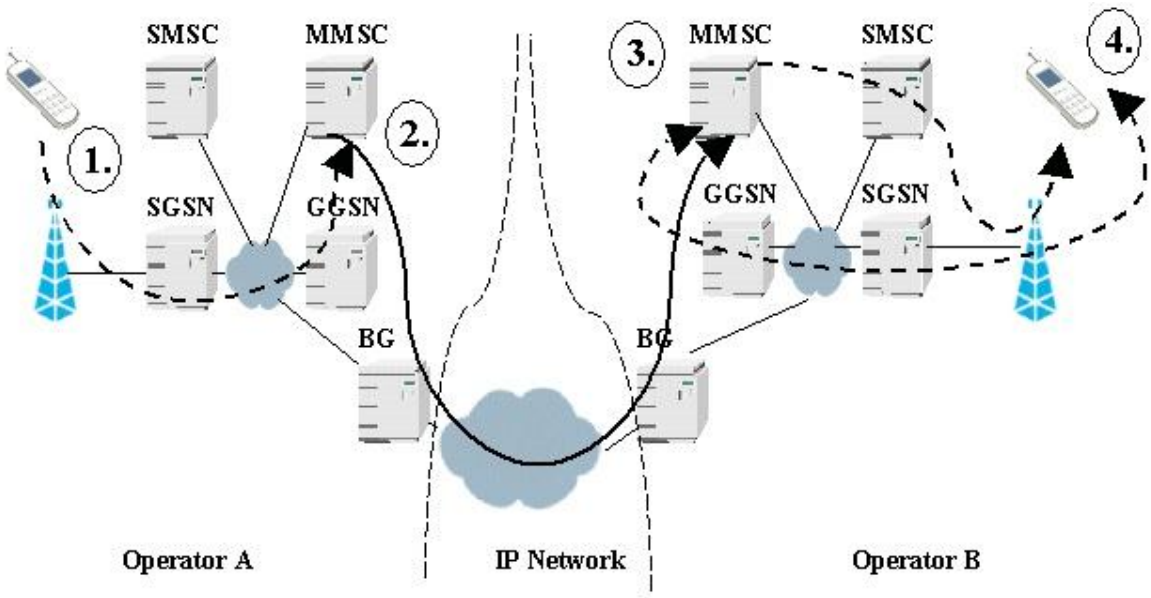

Figure 1: MMS Interworking Case when GPRS is used (Logical Model)

Clarification of Figure 1 (customer of Operator A sends an MM to a customer of Operator B):

1. User A sends an MM addressing it with User B's MSISDN or NAI (RFC 2822), MM is transferred via SGSN/GGSN to MMSC
2. Operator A's MMSC notices based on receiver MSISDN or NAI (RFC 2822) that this MM is addressed to Operator B. It finds the IP address of Operator B's MMSC and sends the MM over IP network via Operator A's own border gateway to inter-PLMN network and Operator B's border gateway. There the MM is routed through Operator B's IP network to MMSC
3. Operator B's MMSC sends notification of new incoming message to User B using WAP Push (SMSC might be used in WAP Push depending on implementation)
4. User B receives notification carrying information such as subject, size and URL of incoming message. Based on that information the terminal fetches the MM by connecting to the MMSC

Note: Figure 1 has been somewhat simplified, for example actual BG probably includes functionality such as firewall and SMTP gateway depending on implementation. Also WAP GW (and Push Proxy GW) can be separated from MMSC.

In order to get MMS service successfully started, interworking between different operators' MMSCs is seen as a major issue. From a technical point of view the required IP network between different operators' MMSCs can be e.g. public internet (with VPN) or direct leased line such as Frame relay or ATM. Another solution, which in many cases could be considered to be the advisable one, is to utilize an existing, proven and reliable inter-operator IP network, i.e. GRX, as specified in IR.34 [3]. This requires some modifications to GRX specifications (allowing SMTP traffic & MX records for DNS), but as a result transferring multimedia messages between different operators is as simple as any normal GPRS roaming traffic. Given this enhancement is done, multimedia messages can be routed as IP based traffic on top of GRX.

Using GRX networks to carry MMS traffic is less onerous than building direct connections between each and every MMSC in the world. Operators should evaluate the physical connect for MM4 and choose the most appropriate. One suggestion would be to use GRX as the default routing choice but where traffic is high (i.e. between national carriers) then a

leased line or IP-VPN may be more cost effective. As the IP routing is separate from the high addressing layers then several physical connections may exist. In practice operators may have several physical interconnect links, leased line for national traffic, IP-VPN for medium volume or non-PLMN and GRX for all others. The DNS system will resolve the MM destination domain to an IP address that will be routed over the appropriate link.

There is no need to build any kind of separate “MMS Roaming Exchange network” only for MMS traffic. Issues such as quality of service, security, control of interworking networks, overall reliability and issuing of new network features such support for ENUM are easier handled inside GRX than when using public internet to relay MMS traffic between operators. This is due to the fact that GRX can be considered to be a closed operator controlled network unlike public Internet, which is totally open for everyone.

Costs might be lower when public internet is used in MM4, but that is not totally free either. Usage of public internet for inter-PLMN network also creates some additional problems and costs, such as message security rules (e.g. unlikely that all operators will use interoperable VPNs), address filtering rules of incoming messages and control of spamming. Note that MMSC is never directly connected to an IP inter-PLMN backbone, but all MMS traffic goes through border gateway, firewall and/or SMTP gateway.

It should be noted that MMS interworking between operators can be problematic if one party has implemented MM4 interface over public internet (with VPN or without it) and another party uses GRX to relay all inter-operator multimedia messages. Connection between these parties might be difficult to implement, for example DNS query made in order to find the receiving MMSC is one of the affected issues, since GRX and public internet have their own DNS hierarchies. Therefore, operators have to agree during inter-operator technical negotiation on the inter-PLMN network to be used for MMS transfer.

Typically adding another inter-operator network interface requires extensive modifications into operator internal IP network structure, such as firewalls, proxies and gateways. Therefore it is recommended that only one network is used to relay messages over MM4 interface in order to reduce the number of options, even though operators can deploy multiple networks if desired because of e.g. cost & capacity reasons.

It is likely that MMS traffic will increase the usage of GRX networks very significantly in the future, if MMS becomes nearly as successful as expected meaning that GRX can be more than just a simple GPRS roaming backbone.

2.2 Roaming

Note that when MMS service is used in a roaming situation the visited network is used only as an access network to the home network’s MMSC, since end-users always use their home MMSC to send and receive multimedia messages also in roaming cases. This means that it is easy for customers to use MMS regardless which network they are using, because there is no need to reconfigure any terminal settings.

The visited network MMSC is used only during the MMS interworking scenario, not in roaming scenario. This means that roaming does not cause any major problems from a technical point of view, since visited network does not need to have any kind of support for MMS. The only required functionality is that receiver must be able to connect to his home MMSC via normal data connection, thus GPRS or CSD must be supported in the visited network in order to MMS roaming to work. If CSD is used then transferring MSISDN from visited PLMN to home MMSC might cause some problems, thus it would be preferred to use GPRS as a MMS bearer.

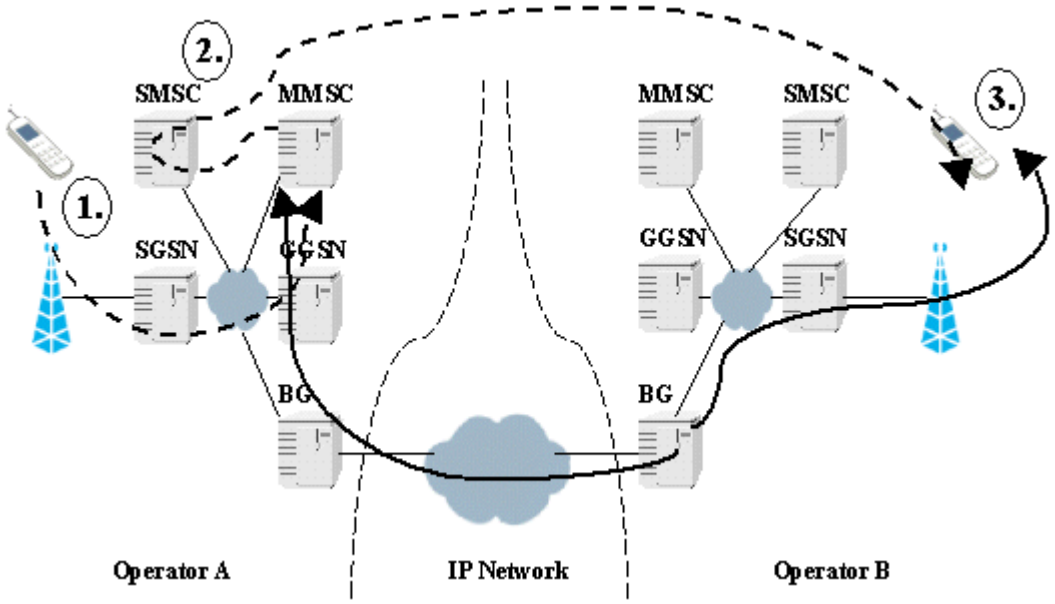

Figure 2: MMS Roaming Case when GPRS is used (Logical Model)

Clarification of Figure 2 (customer of Operator A in Operator A's network sends an MM to another customer of Operator A, who happens to be roaming in Operator B's network):

1. User A sends an MM addressing it with User B's MSISDN or NAI (RFC 2822), MM is transferred via SGSN/GGSN to MMSC
2. Based on receiver MSISDN or NAI (RFC 2822) Operator A's MMSC notices that this MM is addressed to another Operator A's customer, therefore a notification of new incoming message is sent to User B using WAP Push (SMSC might be used in WAP Push depending on implementation)
3. User B receives the notification carrying information such as subject, size and URL of incoming message. Based on that information terminal fetches the MM from home MMSC by connecting to visited SGSN and through Inter-PLMN GPRS roaming network to home GGSN (depending on implementation the MM can also be fetched by connecting to home MMSC from visited GGSN)

Note that Figure 2 has been somewhat simplified, for example actual BG probably includes functionality such as firewall and SMTP gateway depending on implementation. Also WAP GW (and Push Proxy GW) can be separated from MMSC.

If a roaming customer wants to send a MM, he simply connects to his home MMSC via visited SGSN and home GGSN through inter-PLMN network as in any normal GPRS roaming scenario. One point to remember is that roaming customer must be able to receive short messages coming from home SMSC, because notifications for incoming multimedia messages are sent from home MMSC to customers via WAP Push, which utilizes SMS as a bearer. However, WAP Push should use an existing WAP session instead of sending out short messages, if such session exists.

Roaming in MMS case doesn't differ from normal GPRS roaming case due the fact that MMS traffic is transferred inside GTP tunnel.

3 General Requirements of the Inter-PLMN Backbone

General requirements for the inter-PLMN backbone shall be applied from IR.34 [3].

3.1 IP addressing and routing

GRX networks are the preferred way to establish transport of roaming and interworking MMS traffic between inter-PLMN backbones. Public IP addresses should be applied in GPRS backbone networks related to MMS. These public addresses should be invisible to the internet.

3.2 Network connection to GRX

According to IR.34 [3], GPRS backbone is currently connected to GRX networks via BG using G_p Interface to establish transport of roaming traffic between GPRS backbone networks.

To support inter-working MMS, the subnet where the MMSC MM4 interface resides should be connected to GRX networks directly or via MTAs. Operator can decide how to connect the MM4 interface to Border Gateway, directly or via MTA.

Operator should connect its MMS subnet to its existing BG or totally new one:

- Connecting MMS Subnet to operator's existing Border Gateway
  - This option does not need extra connection to GRX networks. Operator should connect its MMSC MM4 interface to its existing BG directly or via MTAs, where the IP addresses of the MMSC MM4 interface or MTAs are made routable to other operators by exchanging the routings with GRX network using BGP4
- Introducing another Border Gateway to connect to GRX networks
  - This option requires operator to setup another BG to connect to GRX networks. The MMSC MM4 interface should be connected to the new BG directly or via MTAs. The IP routings of the MMS subnet would be separated from those of G_n subnet (GPRS backbone)

Note that when introducing new BG it must be run under same AS number than existing BG.

3.3 Security and Screening

In order to maintain proper level of security within the inter-PLMN backbone certain requirements for GPRS operators and Inter-PLMN backbone providers should be taken into account.

It is strongly recommended that operators should implement firewalls adjacent to Border Gateways. Generally operators should allow only routing information (BGP), GTP traffic, signalling, DNS and SMTP traffic. Same security aspects shall be applied as described in IR.34 [3].

Operator should be responsible for the screening the traffic towards its BG. One option is to utilize SMTP GW within operator DMZ network with strict message filtering and screening rules. These rules can be based on incoming and outgoing addresses as well as message content.

Also the screening of MMSC from normal Internet is important, since failure in closing interface between MMS environment and public Internet by one operator can cause e.g. spam problems to each and every operator through inter-PLMN connection.

GRX network as such is just a bearer network, it does not provide any kind of actual security features besides the fact that no outsider should be able to access the GRX network, i.e. security is guaranteed only at a network layer. Therefore there might be a need for some sort of application/service level security functionality such as authentication between MMSCs. This would allow those operators who are security concerned to make sure that they are transferring multimedia messages with certified parties. This means that messages from uncertified parties could be easily discarded, thus increasing the level of security against malicious attempts, such as spam attacks through MM4 interface. One possible solution is listed in Chapter 6.2.

Using a standard firewall system - for example as part of the Border Gateway - could be a way to increase the level of security in the MMS interworking scenario, because it could be set up to ensure that incoming SMTP traffic (as used by MMS in MM4 interface) is accepted only if it comes from a trusted IP address using source IP address checking.

Vendors are strongly recommended to produce such an MMS environment that offers a high level of security by allowing a total network separation, meaning that interfaces for connection to GRX and public internet can be completely separated from each other. This should reduce the number of possible problems in MMS interworking. One major problem related to this issue is that messages can be accidentally routed towards public internet instead of dedicated inter-PLMN network, if separating these networks is too difficult or even impossible. Operators are required to pay special attention to this matter, since this is naturally dependent also on operational procedures and decisions.

Above all, operators should realize that the actual security level of the whole MMS system depends on much more than just securing the transportation between MMSCs. This is done on an operational service level, where it is decided how these services are being used. One example of this is a decision regarding which messages are sent to MM4 interface and which messages are sent to MM3 interface.

3.4 MMS Interworking Provider

Inter-PLMN network can optionally offer an additional element for MMS interworking routing by deploying a separate MMS Interworking Provider functionality (MMS IP) inside the inter-PLMN network. Regardless the number of MMS interworking partners, this would allow operator to make just a single connection from its own MMSC to inter-PLMN network MMS IP, since this MMS IP is then responsible for routing messages towards correct recipient networks. MMS IP will use SMTP over MM4 interface as specified in TS 23.140 [2].

There are basically two role models for MMS IP:

1. Operator A has a commercial relationship with Operator B (MMS IP is used only as the transport mechanism)
2. Operator A has a commercial relationship with MMS IP (MMS IP is used as a broker both for transport and billing purposes)

Regardless of the role model the mobile operator requires a service that provides:

- Visibility of the originating operator to the destination operator. It is recommended that originating operator shall always populate its system-address as defined in TS 23.140 [2] whenever sending a MM4 message, that including both Request and

Response messages, in the Originating-Recipient-Address field (this field is added since 3GPP TS 23.140 version 6.14.0)

- Visibility of all MMS IP's in the path. It is recommended that all MMS IPs in the path shall always populate/append its system-address as defined in TS 23.140 [2] in the MMSIP Address field (this field is added since 3GPP TS 23.140 version 6.14.0) in an orderly manner. The first MMS IP in the path shall add its system address to the MMSIP Address field and the subsequent MMS IP shall append its system address to the MMSIP Address field with "," to separate from the system address populated by the previous MMS IP
- Delivery of acknowledgments

It is possible to have an MMS IP-to-MMS IP connection, i.e. message from originator to recipient can traverse two MMS Interworking Providers. Transparent relay mode of operation will be used for all MMS IP-to-MMS IP connections. Here the term transparent means that the recipient and all intermediate elements are able to see the actual originator and the path (i.e. system addresses) of the message.

If MMS IP forwards the message to a second MMS IP, both must accept responsibility of relaying message delivery acknowledgements towards the originating operator. Symmetric routing of messages (MM4_Forward.REQ and MM4_Forward.RES) should be done, by using X-Mms-Originator-System field to include previous steps in the message route.

Destination address must be resolved to the correct FQDN before MMS IP forwards the message to another MMS IP.

Timers should carefully set in order to minimize unnecessary duplicate messages in MMS interworking interface. Originating MMSC should re-transmit if it has received either a temporary SMTP 4XX series error code (from MMS IP) or MM4_FORWARD.RES indicating a fixable error (from MMS IP or destination MMSC) or no response at all. Any MTA nodes used in operator networks should be MM4 aware, i.e. in case of error MTA should generate MM4_FORWARD.RES instead of SMTP level error.

For more detailed technical information about MMS IP, please see the document "*MMS IP Guideline Document*".

4 MMS and the Domain Name System – DNS

4.1 DNS, MMS Interworking, and GRX

The MMS interworking is based on protocols and mechanism standardised by IETF. The transport protocol over the MM4-reference point is (E) SMTP. Also the MMS-message routing and relaying mechanism is identical to Internet email architecture. DNS is a fundamental part of the Internet email architecture.

The IR.34 [3] specifies in detail how the GRX should utilize the DNS within the GRX. This specification is from pre-MMS era. If the GRX will be used as an interconnection and transmission network for MMS-traffic the DNS functionality must be broader than specified in IR.34 [3]. Thus a number of modifications are required. Also ENUM, which is a part of the MMS and IMS specification, poses new requirements for the GRX DNS. In practice DNS MX-records are needed for SMTP based multimedia message routing and relaying. The selection of used DNS tree hierarchy (Internet or GRX) ultimately depends on the used interconnection network behind the MM4-reference point.

The GRX DNS has the advantage of being separated from the Internet DNS. For example IR.34 [3] defines GRX specific use for DNS root name servers. This separation does not mean that is not possible to resolve names belonging to Internet name space. Functionality of DNS operations origination from opposite direction cannot be guaranteed. The DNS tree hierarchy and administration separation from Internet DNS enables easier and faster integration of new DNS functionality that is required or useful within MMS, such as introduction of ENUM. For example MMS and IMS will benefit from ENUM functionality. Propagating this functionality to GRX DNS should be possible with minor effort. Thus, it is preferred to use both the GRX DNS hierarchy and the GRX transport network in MMS interworking.

ITU-T has done preparing work on specifying how to arrange ENUM DNS tree hierarchy, zone delegation, and management. These guidelines/specifications should be considered closely when building ENUM functionality to GRX. These specifications also state clearly how the DNS zones should be delegated at global level, country level, within a country, and finally among operators. One aim is that an operator is responsible only for her own number space and all possible numbering and administrative changes cause minimal or zero changes to name servers higher in the ENUM DNS tree hierarchy.

The following issues should be considered important when designing the DNS usage within the GRX:

- MMS interworking is based on Internet email architecture, which in larger scale requires DNS MX Resource Records to function. If the GRX is used for MMS interworking then support for MX RRs must be there.
- ENUM is likely to be a part of the MMS specification and in order to avoid local mappings and local routing information GRX is ideal place to enable global ENUM DNS functionality among operators, but operators will need to further explore how best to deploy ENUM functionality.
- ENUM is part of the IMS specification and the signalling traffic between operators will use GRX. Thus GRX is ideal place for enabling global ENUM DNS functionality among operators. IMS also requires SRV Resource Record functionality from DNS, which may also be useful for MMS MNP.
- ENUM may be the answer for MMS MNP. There are several ways to do it utilizing ENUM. For more information see Chapter 5.4
- It is up to operator's policy and administration how much information about operator's internal infrastructure will be visible to global GRX DNS.

As a conclusion in the first phase the only required modification for the GRX DNS is support for MX records. Later when ENUM is being deployed there are additional requirements, but these are not mandatory for the MMS interworking to begin.

4.2 DNS Resource Records

ENUM, email, and IMS require several Resource Records to be functional in the DNS. Email server (E/SMTP server) name resolving and mail routing/relaying needs the MX Resource Record (MX RR – Mail exchange RR). The MX RR describes the names and priorities of the email servers for some domain.

For example MX records for the domain *mms.mnc010.mcc234.gprs* are:

- *mms.mnc010.mcc234.gprs MX 10 mms-smtp1.mnc010.mcc234.gprs.* (relating MMS domain to a mail server - highest priority)
- *mms.mnc010.mcc234.gprs MX 20 mms-smtp0.mnc010.mcc234.gprs.* (relating MMS domain to a mail server - resilient fallback)

- *mms-smtp1.mnc010.mcc234.gprs. 999999 A 161.58.53.160* (Host details of SMTP main server)
- *mms-smtp0.mnc010.mcc234.gprs. 999999 A 209.35.183.204*(Host details of SMTP fallback server)

After resolving the MX RR for some domain the name server can continue resolving the address of the actual mail server. In our example *mms-smtp1.mnc010.mcc234.gprs* will have the IP-address *161.58.53.160*.

ENUM relies on NAPTR Resource Record (RFC2915). The NAPTR RR allows describing and lookup of services for a wide variety of resource names. These resource names include for example URIs and SRV RRs. The NAPTR RR has also a powerful regular expression mechanism building. For example a NAPTR RR for the www.sonera.com might look like:

www.sonera.com
;; order pref flags service regexp replacement
IN NAPTR 100 100 "s" "http+I2R" "" _ _http._tcp.sonera.com

IMS (and especially SIP) requires SRV Resource Records. SRV RRs are used to describe and allow lookup of different resources. The lookup also contains a description of desired service and protocol. To continue the above example a SRV RR for the www.sonera.com might look like:

$ORIGIN sonera.com.
@.... ; many fields follow
; Our web resources over TCP..
_http._tcp SRV 0 1 9 www.server1.sonera.com.
_http._tcp SRV 0 2 9 www.server2.sonera.com.
_http._tcp SRV 0 3 9 www.server3.sonera.com.

A sample DNS configuration is available in IR.34 [3] for more information.

5 Addressing Scheme

5.1 NAI versus MSISDN

In TS 23.140 [2] it is stated that both MSISDN (E.164) and NAI/email (RFC2822) addresses are to be supported in MMS environment. Thus that customer can choose which address he will use when sending the MM and operator's MMS system must support both types of addressing. Both kinds of addresses are likely to be used since end users are probably used to MSISDN due to SMS usage, but email addresses have their advantages, such as support for aliases.

This means that MMSC must be capable of finding out the receiver and sending message successfully in two different scenarios, since mapping of MSISDN to the receiver's MMSC needs more effort than when using email address. It is up to sender MMSC to map non-routable MSISDN address to receiver MMSC, if receiver is a customer of another operator. TS 23.140 [2] defines two options for translating a dialled MSISDN number into the correct MMSC address for a destination operator. ENUM is identified as the long-term solution for MSISDN to MMSC address mapping. In the short term a solution leveraging a MAP query for an IMSI address is defined as a mechanism for manufacturing an MMSC address from a dialled MSISDN number.

In the first phase the preferred way of routing messages is that MSISDN based messages go through dedicated inter-PLMN network such as GRX, while NAI based messages are

routed directly into public internet just like any normal email message. However, it should be possible to route also NAI based messages through GRX e.g. in case of two operators making an interconnection agreement. Note that if you are using the MM3 interface, there are currently no charging mechanisms on this interface. This means that it may not be possible to charge the sending operator for the incoming email traffic received over MM3.

5.2 MMS Addressing

The following section describes a way in which each service provider in the world can have a unique domain address.

In the case where a service provider wishes to use 'friendly name' addressing then they will be required to register a public domain address and specify an MX record to allow routing. This addressing form will be mandatory for all subscribers on MMS service providers that have not been issued a number range directly or indirectly from the ITU. This means that a subscriber on another MMS service provider will address the destination subscriber with a 'friendly' e-mail address. This will require no special MMS functions and normal e-mail routing will occur. As the MM1 interface mandates both SMTP addressing and MSISDN addressing this should not pose a problem. Any terminal manufacturer or service provider that does not support this will not be classed as 3GPP compliant.

In the case of a service provider holding an ITU allocation number range and addressing it's subscribers using only the number then the domain will have obtained from the routing between operators.

One important issue to realize is that IR.34 [3] states that all kinds of traffic, also MMS interworking traffic, should use .gprs TLD in GRX network.

If GRX is used as an inter-PLMN network for MMS, then the following format of FQDN addressing should be used in MMS interworking: *mms.mncXXX.mccYYY.gprs*. Thus, the domain name should begin with the part of "*mms*", because this helps to differentiate IP traffic based on the service used. For example MMS traffic can be very easily separated from IMS traffic because of different domains. In other words, the recipient should be addressed as *+1234567890/TYPE=PLMN@mms.mnc123.mcc456.gprs* in RCPT TO header inside the SMTP message in MM4 interface.

A commonly agreed way reduces the number of options and thus reduces the possibility of problems by simplifying things. Domain *mms.mncXXX.mccYYY.gprs.* could also be utilized as a kind of fallback mechanism, since even if other domains are unknown due to e.g. DNS fault or bug in manually handled host lists, this one commonly agreed domain can be still used to relay messages between operators.

It is important to notice that in order to be able to connect both to public internet and GRX networks, the MMSC must support the use of multiple domain names. Thus, a critical requirement for MMSC is to be able to handle simultaneously for example domain name *mms.operator.com* to be used for e.g. service provider & email server connectivity through public internet, as well as domain name *mms.mnc123.mcc456.gprs.* to be used for interworking connectivity towards other operators through inter-PLMN network. This multiple domain support can be implemented also with other parts of MMS environment than MMSC itself, for example an SMTP GW can be utilized to construct and rewrite a public internet domain for outgoing messages.

The sections below show how a globally unique domain can be created for every PLMN and PSTN operator in the world without having to register them all. The reason for using text

prefixes is that it is possible to have the same actual values in both CC and MCC and even NC and MNC.

5.2.1 Direct or Indirect

Direct addressing refers to the case where the originating service provider derives the domain from the MSISDN or E.164 and takes account of number portability. The originator understands that the receiver will not relay the message if the originator makes a mistake. In the mobile world the number portability issue is usually overcome using the MSISDN.

Indirect addressing refers to the case where the originator derives the domain from the MSISDN or E.164 and does not take into account number portability as the receiver will replace the domain and relay appropriately.

5.2.2 Creating the domain for direct routing

The following section suggests a way in which a domain can be assigned to a MSISDN for direct routing.

Note: lowercase is text and UPPER is replaced with actual data. The MNC and MCC are obtained from the IMSI.

id[/TYPE={PLMN | USER}]@mms.mncMNC.mccMCC.gprs

(e.g.) 447782123456@mms.mnc020.mcc234.gprs

/TYPE=PLMN is optional in 23.140 [2] and as such operators should not expect this to available although it may. If "/TYPE=PLMN" is absent, then MMSC should be able to interpret address as "/TYPE=PLMN", if the address is completely numeric (or includes only +, * and # signs). The IETF proposal (RFC 2303 - /voice=msisdn or /fax=msisdn) does not have tag for mms and as such is a proprietary.

5.2.3 Creating the domain for In-direct routing

In networks that do not have an IMSI or equivalent and have to rely on the MSISDN (E.164) number then the following scheme is proposed.

id[/TYPE={PLMN | USER}]@mms.ncNC.ccCC.gprs

(e.g.) 447782123456@mms.nc7782.cc44.gprs

5.3 Address Discovery & Number Portability

It should be noted that it is the role of the originating operator and its MMSC to handle outgoing interworking related messages accordingly, therefore the recipient operator should not receive messages it cannot forward to addressed recipient(s).

Requirement for number portability support in MMS is concrete, since a number of countries already use MNP for calls and SMS. This means that also MMS systems must be capable of doing this.

One example is when recipient has switched to another operator while retaining his/her original MSISDN, i.e. MNP is in place. Now it is up to originating operator and its MMSC to find out the correct recipient operator via specified address resolution mechanisms before

actually sending the message over inter-PLMN interface. Even though it is specified in TS 23.140 [2] that MMSC should be capable of sending an error message back to sender in case of transfer in MM4 interface fails, it is not mandatory for MMSC to support this feature. Therefore it is beneficial to handle this check even before actually accepting the message from sender to originating MMSC over MM1 interface. In other words the originating MMSC should not accept message from sender's terminal without first checking whether message can be forwarded to recipient operator, meaning that sender would always get noted if message cannot be transferred.

One possible reason for message transfer failure in MM4 interface is the lack of interworking agreement. The recipient MMS environment typically accepts messages only from sources that are its interworking partners. This means that if recipient in an MNP enabled environment has switched to another operator that originating operator does not have MMS interworking agreement with, message typically cannot be routed. Therefore all MMS systems should be able to report sender about transfer failures.

The long-term addressing requirement will likely be met by an ENUM based scheme, but a fall-back IMSI based solution is also required, since ENUM is not deployed yet and it might take some time before that is fully done. While waiting for ENUM to be implemented by MMS capable operators and administrative parties, there likely is a need for IMSI based solution. However, supporting various existing or forthcoming MNP systems with IMSI based solution can be quite difficult. MMSC should probably be capable of doing a number of different MAP look-ups, such as Send_IMSI and SRI_for_SM. In TS 23.140 [2] it is stated that SRI_for_SM is the only mandatory MAP operation for retrieval of the recipient's IMSI, while Send_IMSI is listed as optional for MMSC to support.

Notice that even then it is not certain that all inter-PLMN traffic cases are handled by this solution, for example when HLR does not support these MAP commands or when receiver has denied incoming short messages. This means that there can not be a 100% complete solution using this technique. It should be noted that finding out recipient's MMSC address from IMSI requires a separate internal static mapping table or database, which maintains the associations of MCC + MNC => MMSC FQDN. Furthermore, IMSI based solution is not interoperable with non-GSM operators and their MMS services, unlike ENUM based solution. This is one of reasons that make ENUM the preferred long-term universal way of address resolving. In TS 23.140 [2] it is stated that in case of MMS interworking, when E.164 addressing is used, the mapping for the recipient's address to the recipient's MMSC should use the ENUM protocol. Furthermore, TS 23.140 [2] defines the deployment of ENUM as an operator issue.

The following list describes different ways in order of simplicity to implement address discovery in MMS interworking:

- Static table mapping receiver's MSISDN prefix directly into receiving MMSC IP address (e.g. +35840 <=> 194.251.253.74) will not cope with MNP. Note that this is a non-scalable solution, thus it should really be used only as a quick'n'dirty interim address discovery solution until more advanced solutions are implemented mailto:
- Indirect address where no IMSI lookup is available. (e.g +447782123456 ←→ mms.nc7782.cc44.gprs.) Standard DNS lookup to obtain IP address (194.251.253.74) and SMTP connection to operator that supports indirect routing. Will not cope with MNP at origin but may at destination depending on commercial agreement.
- IMSI based look-up: first get IMSI based on receiver's MSISDN from HLR using MAP query, then resolve MNC + MCC from IMSI, finally use DNS query to resolve the MMSC IP address (e.g. mms.mnc111.mcc222.gprs. <=> 194.251.253.74) supports

MNP, but requires DNS support (can be established within a short period of time if GRX DNS is used).

- ENUM based look-up: please refer to Figure 3. If GRX provider is used, private ENUM can be established within a short period of time. A public ENUM based solution requires more investigation as to whether it is the long term solution for MMS and will probably take several years to be implemented if it chosen

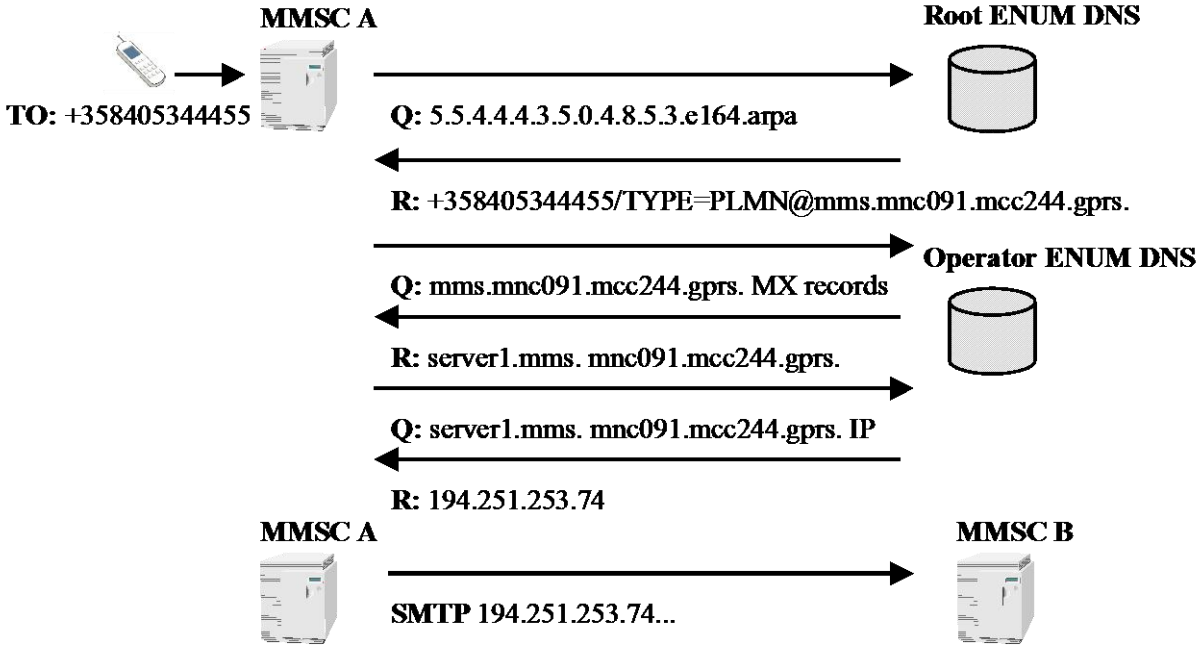

Figure 3: Transfer of multimedia message over inter-PLMN network using ENUM

Figure 3 gives a simplified example of how the sending MMSC finds out the IP address of receiving operator's MMSC using a number of ENUM DNS queries. Note that MX records are not stored in GRX DNS, but rather in administrative domain, i.e. operator DNS system.

In forthcoming MMS specifications from 3GPP both IMSI and ENUM based look-up systems are described. ENUM has already been specified to be used also in other services than MMS, for example the IP Multimedia Subsystem (IMS) utilizes ENUM.

While working on MNP for MMS a general need for Domain Name Portability (DNP) should also considered. The Domain Name Portability has the same scope as MNP and it should be noted that simply forwarding emails and such is not enough, For example service queries and service discovery queries must be able to forward to correct operator regardless of the used Domain Name.

It is not advised to build any kind of "quick'n'dirty" static MMS mapping tables for other than testing purposes, since practice shows that this sort of intermediate hacks will unfortunately remain in service for a quite some time. Static table simply don't scale well enough, since it is expected that a very large number of operators will be offering MMS services and connection to them is a key issue. There still remains a use case for static table in IMSI based look-up, since currently there is no other way of constructing a MMSC domain name

from IMSI. However, supporting number portability with static tables requires much manual work.

5.4 Advanced Number Portability using ENUM

Inasmuch as ENUM can be the way forward in solving the MMS IW addressing discovery problems, operators should further investigate how to actually deploy ENUM in the best possible way. Following sections describe two possible models for ENUM implementation.

When looking at ENUM as a standardized tool for the discovery of IP services like MMS and IMS, the following issues should be taken into account:

- Operator Control: Operators should be in a position to fully control the provisioning of ENUM data for their end-users
- Security: Operators should be in a position to fully define who gets access to their ENUM data on a query by query basis
- Application Specific Query: Applications should be able to query for a specific ENUM record (e.g. MMS, IMS, etc.) in addition to querying for all ENUM records associated with a given MSISDN
- Deployment Flexibility: Operators should have the flexibility to deploy both Tier-2 and Tier-1 ENUM functionality on their own backbone network or outsource this new functionality to GRX operators

5.4.1 Separated Databases

There is an administrative problem and burden with the current ENUM based MNP proposals. The operator who originally gave the user his/her number must provide DNS services for the user even though he/she is currently a customer of other operator. Reserving resources and offering services for other operator's users is not desired. Also the user and his/her new operator may not like the idea that the old operator has knowledge of new operator's services and internal servers.

Following description describes more convenient way of doing MNP using ENUM. We call an operator who gave the original number as an 'Anchor Operator' and operator's DNS as 'Anchor DNS'. For a short description of NAPTR and SRV Resource Records see Chapter 4.2

ENUM DNS hierarchy should be coupled to general GRX DNS hierarchy and delegation mechanisms. In practice this means ENUM DNS root information is located in the same place as the general GRX DNS root information. ENUM DNS root and the rest of ENUM DNS hierarchy should manage delegation in a proper way until final ENUM records located at operator's name servers can be queried.

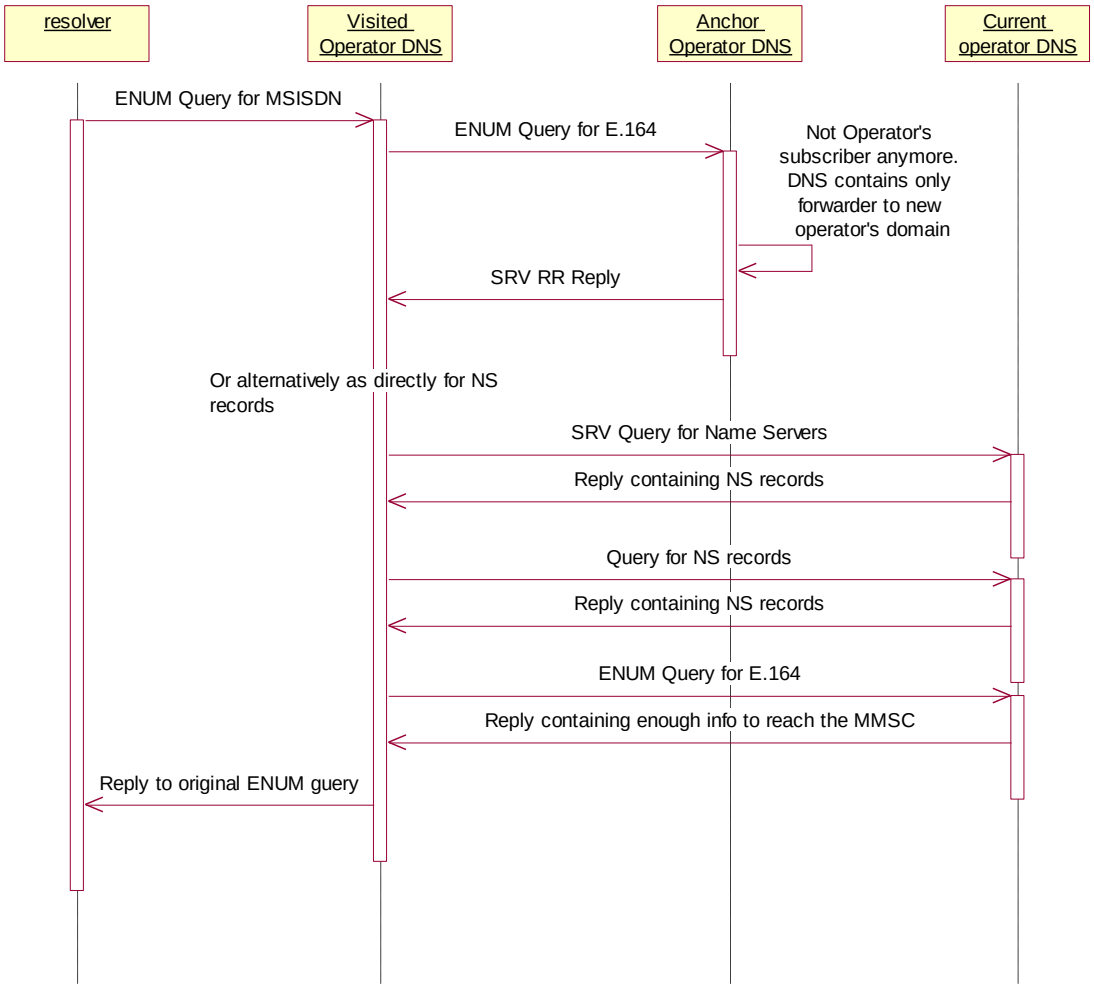

Figure 4: ENUM Query using SRV Resource Records (separated databases)

When the IMS is deployed then also SIP (Session Initiation Protocol) (RFC 2543) systems are deployed. The SIP requires SRV Resource Record (SRV RR) functionality from the DNS. The ENUM is based on NAPTR Resource Record (NAPTR RR), which in turn also specifies mechanism to return referrals to SRV RRs instead of URIs. For example the following NAPTR RR returns an URI:

;; order pref flags service regexp replacement

IN NAPTR 100 10 "u" "E2U+sip" "!^.$!sip:csd@sonera.com!" .*

But the following NAPTR RR will cause the resolver to re-query sonera.com domain for SRV RRs containing names of servers that provide HTTP services over TCP/IP:

;; order pref flags service regexp replacement

IN NAPTR 100 100 "s" "http+I2R" "" _ _http._tcp.sonera.com

Now if the 'Anchor Operator' specifies the 'Anchor DNS' to return a referral to new operator's name servers using SRV RRs instead of ENUM information the administration and resource requirements are minimal for the 'Anchor Operator' (one line per user requiring MNP). At the

time of writing both ENUM and SRV RR functionality is for example included in widely deployed name server Bind v9.

5.4.2 Central Database

On the other hand, there is another possible model for operator controlled ENUM. This requires a central database, where each and every customer of all operators is listed. This model is more simplified and it is positioned to incorporate number portability requirements into the process of cross-operator MMS address discovery. Under an operator controlled ENUM model, the Tier-1 ENUM service becomes responsible for providing a referral to the correct Operator controlled Tier-2 ENUM system even if a number has been ported. The diagram below shows the simplicity of the MMS address discovery in an Operator ENUM infrastructure.

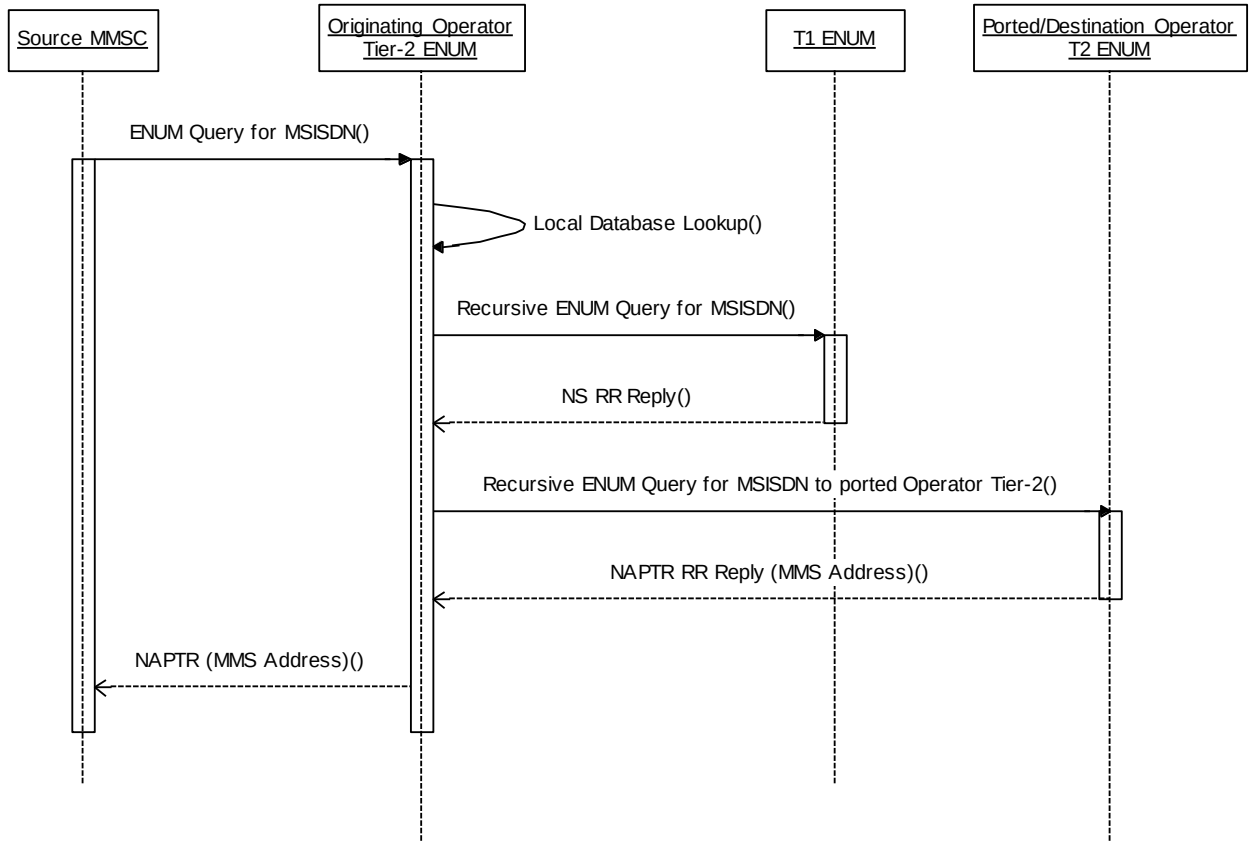

Figure 5: ENUM Query using SRV Resource Records (central database)

6 Conclusion

Successful interworking is crucial for the success of MMS, thus it must be handled as soon as possible. Preferred way is to follow common GSM Association guidelines right from the start rather than try to implement a number of different solutions and later see what solution becomes the de facto standard.

MMS interworking is considerably more complicated than SMS interworking, but it can done via GRX, if certain modifications are made. The GRX DNS has the advantage of being separated from the Internet DNS, thus enabling faster introduction of new functionality. Consequently these facts make GRX the preferred inter-PLMN network also for MMS traffic. If needed, GRX solution can also be combined with other solutions (such as direct connectivity via leased lines or IP-VPN between national carriers).

Preferred actions needed in order to successfully handle the technical aspects of MMS interworking & roaming:

1. Once GRX is technically capable of supporting MMS interworking, it is envisioned that it will eventually become the preferred solution. It should be noted that this does not in any way prevent operators from using also other solutions, such as implementing a leased line for national MMS interworking
2. Make a decision to use GRX DNS as a preferred centralized operator controlled method of MMSC look-up
3. Make modifications to GRX specification to support these requirements (allow SMTP traffic in GRX network & add MX records to GRX DNS)
4. Make sure that both terminals and network equipment support both MSISDN and email addressing
5. Investigate how to actually implement an ENUM based MMSC address look-up solution with MNP support as soon as possible
6. Make sure that roaming partners support SMS MT because of MMS notifications
7. Make sure that GPRS roaming (and/or CSD roaming) has been commercially launched between roaming partners
8. Investigate the MMS backwards compatibility issue
9. Connect MMSC to inter-PLMN network in such manner that when sending messages there are no intermediate servers between MMSC and inter-PLMN network, while when receiving messages there can be such intermediate servers
10. Investigate what kind of capabilities need to be discovered in inter-MMSC traffic and prepare to implement them using e.g. ESMTP extensions

Operators might want to note the following list describing implementation related issues and check whether these are already handled successfully:

1. MMSC should be able to support two separate domain names (by itself or through other parts of MMS environment)
2. MMSC should have interworking domain in the type of *mms.mncxxx.mccyyy.gprs*, if GRX is used as a inter-PLMN network
3. Make sure that MMSC and other MMS environment is capable of network separation, thus MM4 interface can be separated from the public internet
4. Investigate connectivity towards necessary MMS IW partners, what inter-PLMN network they have implemented
5. Check that MMSC is not connected directly to inter-PLMN connection, but protected via BG and DMZ & FW
6. Make sure that connection between MMSC and public internet is well secured and screened in order to prevent e.g. spamming problems

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.0.1	March 4th, 2002	Input paper Packet Doc 036/02 "MMS Interworking Guidelines Proposal"		Tero Jalkanen / TeliaSonera
0.0.2	May 17th, 2002	First draft of PRD document for IREG Packet WP discussion		
0.0.3	June 19th, 2002	Updated based on IREG Packet WP MMS ad hoc meeting discussions		
0.0.4	June 27th, 2002	Updated based on email discussions		
0.0.5	July 17th, 2002	Updated based on email discussions		
0.0.6	August 1st, 2002	Updated based on IREG Packet WP MMS ad hoc meeting discussions		
0.0.7	August 13th, 2002	Updated based on email & conference call discussions		
3.0.0	October 9th, 2002	Approved by EC		
3.1.0	April 8th, 2003	Incorporated IREG Doc 024/03 rev 1 (SCR 001 on IR.52)		
3.1.1	September 19th, 2003	Incorporated IREG Doc 131/03 (NSCR 002 on IR.52)		
3.1.2	March 22nd, 2004	Incorporated IREG Doc 46_069 (NSCR 003 on IR.52)		
3.2	August 29th, 2005	Incorporated IREG Doc 49_031 (NSCR 004 on IR.52) Version number changed to conform with AA.34		
3.3	December 15th, 2006	Incorporated PACKET Doc 27_014 (NSCR 005 on IR.52)		

A.2 Other Information

Type	Description
Document Owner	IREG
Editor / Company	Tero Jalkanen / TeliaSonera

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org

Your comments or suggestions & questions are always welcome.