MMS Interoperability Guidelines

Revision: 3.0

Date: February 5, 2013

Notice to Readers

This document does not contain any confidential material and is therefore not a controlled document. Copies may be made anytime by any service provider or ICV for internal use only. As new versions become available they will be distributed to all involved service providers.

To ensure consistency of the versions and correct distribution this document is managed by CTIA. Any changes to this document should be done with the “track changes” feature of Microsoft Word and submitted to the document manager Jeff Simmons (jsimmons@ctia.org) for consideration by the Messaging Working Group and further distribution.

Definitions and Abbreviations

ASCII – American Standard Code for Information Interchange

CARRIER – any telecommunications carrier as defined in the Communications Act, 47 U.S.C. Section 153(51). A carrier has authority to draw telephone numbers from the NANP, and is subject to FCC oversight with respect to its provision of telecommunications services.

CMRS – Commercial Mobile Radio Service (defined in Section 20.9 of the FCC's rules, 47 C.F.R. 20.9. (http://law.justia.com/cfr/title47/47-2.0.1.1.1.0.1.6.html)

CDMA – Code Division Multiple Access

ESME – External Short Message Entity

GSM – Global Standard for Mobile Communication

ICV – Inter Carrier Vendor – vendors providing connectivity between wireless subscribers, networks, and services

MIN – Mobile Identification Number

MM – Multimedia Message

MMS – Multimedia Messaging Service

MM1 – the protocol between the MMSC and the UA as specified in the 3GPP 23.140 standard

MM3 – the protocol between the MMSC and external servers as specified in the 3GPP 23.140 standard

MM4 – the protocol between the MMSC and another MMSC as specified in the 3GPP 23.140 standard

MMSC – Multimedia Messaging Service Center

MO – Mobile Originated

MS – Mobile Station

MSISDN/MDN – Mobile Subscriber ISDN / Mobile Directory Number

MT – Mobile Terminated

NANP – The North American Numbering Plan is an integrated telephone numbering plan serving 20 North American countries that share its resources. Regulatory authorities in each participating country have plenary authority over numbering resources, but the participating countries share numbering resources cooperatively. The ITU assigned country code "1" to the NANP area and NANP numbers are ten-digit numbers consisting of a three-digit NPA code, followed by a seven-digit local number.

NPA-NXX – represents area code and exchange of the North American Numbering Plan

NON-CMRS – non-carrier service providers

SERVICE PROVIDER – Any entity that makes a messaging service available to consumers through the use of 10-digit telephone numbers included in the North American Numbering Plan. Service providers may include a multitude of companies engaged to provide messaging services including carriers and application providers.

SLA – Service Level Agreement

SME - Short Message Entity

SPAM - the use of messaging systems or services to send unsolicited bulk messages. While e-mail spam is the most widely recognized form of spam, spam includes but is not limited to instant messaging spam, spam text (SMS and MMS), and social networking spam.

TDMA – Time Division Multiple Access

TN – Telephone Number

UA – MMS User Agent (i.e handset/device)

UD – User Data

UDH – User Data Header

UDHI User Data Header Indicator

VENDOR – Intermediary company hired to provide a good or service

VMN – Voice Mail Notification

Table of Contents

1. Introduction

1.1 Version 1.0

The purpose of MMS Interoperability Guidelines is to ensure that carriers can pass Multimedia Messages (MMs) across participating carriers' networks from one peer to another.

The group's objective is to identify and define the involved interfaces, and to agree upon a common feature set that will be supported by all participating carriers.

At the first Inter-Carrier MMS Messaging meeting in Washington, DC on May 11, 2004, all participating carriers agreed that they have the intent to interoperate in inter-carrier MMS messaging. This service enables wireless subscribers to send and receive MMS messages based on their phone number (MSISDN/MDN) to and from any wireless network while in their home markets. Furthermore, they committed to participate in the process to work toward achieving Inter-Carrier MMS Messaging.

1.2 Version 2.0

Version 2.0 of the Inter-Carrier MMS Messaging Guidelines was created to expand the inter-carrier messaging agreement to allow messaging traffic between wireless operators and non-wireless carriers. As a general principle, non-wireless carriers need to follow the inter-carrier messaging guidelines established by wireless carriers.

1.3 Version 3.0

Version 3.0, now renamed "Multimedia Messaging Services (MMS) Interoperability Guidelines" facilitates the entrance of non-CMRS devices and services that use 10-digit Telephone Numbers ("TN's") to exchange MMS messages with CMRS-based wireless devices. In order to protect wireless customers from unwanted messages and spam, as well as combat commercial messages that do not comply with the Telephone Consumer Protection Act ("TCPA")[1] and the CAN SPAM Act,[2] this Version 3.0 addresses the spam risks associated with expanded SMS interoperability.

With the advent of non-CMRS devices and services intended to interoperate via MMS with CMRS-based wireless devices, there are three areas where the spam risks of non-CMRS interoperability are addressed more fully:

1. Clarifications to Sections 3 and 7 of the *CTIA MMS Interoperability Guidelines* of February 5, 2013.
2. Development of guidelines for inter-service provider vendors (ICVs) providing service to non-CMRS entities interoperating with CMRS-based devices.
3. Development of guidelines for non-CMRS entities providing services and devices that interoperate with CMRS-based SMS devices.

The following table illustrates the relationships among CMRS-based messaging and non-network-affiliated messaging for A2P and P2P traffic types.

	CMRS	**Non-CMRS**
Application-to-Person	**Supported via Common**	**Supported via Common**

[1] 47 U.S.C. 227.
[2] 15 U.S.C. 7701, et seq.

	Short Code*	Short Code*
Person-to-Person	**Supported since V1.0**	**Defined in V3.0**

*Information related to Common Short Codes may be found at www.USShortCodes.com

1.4 Mission Statement

Enable phone number addressed MMS messages across participating service providers in the U.S.

2. Interfaces

There are several different options available to interconnect the various carriers and service providers to enable MMS Messaging interoperability.

Three interconnection scenarios have been identified:

1) Every carrier and service provider independently selects an ICV to act as its message transfer point;
2) The participating service providers deploy a hybrid model where they directly connect in some cases and use an ICV in others;
3) Carriers and service providers interconnect their networks directly based on bilateral agreements.

These scenarios are not mutually exclusive. However, since the definition of the interface in case 3) is left to the participating service providers, this document only focuses on cases 1) and 2).

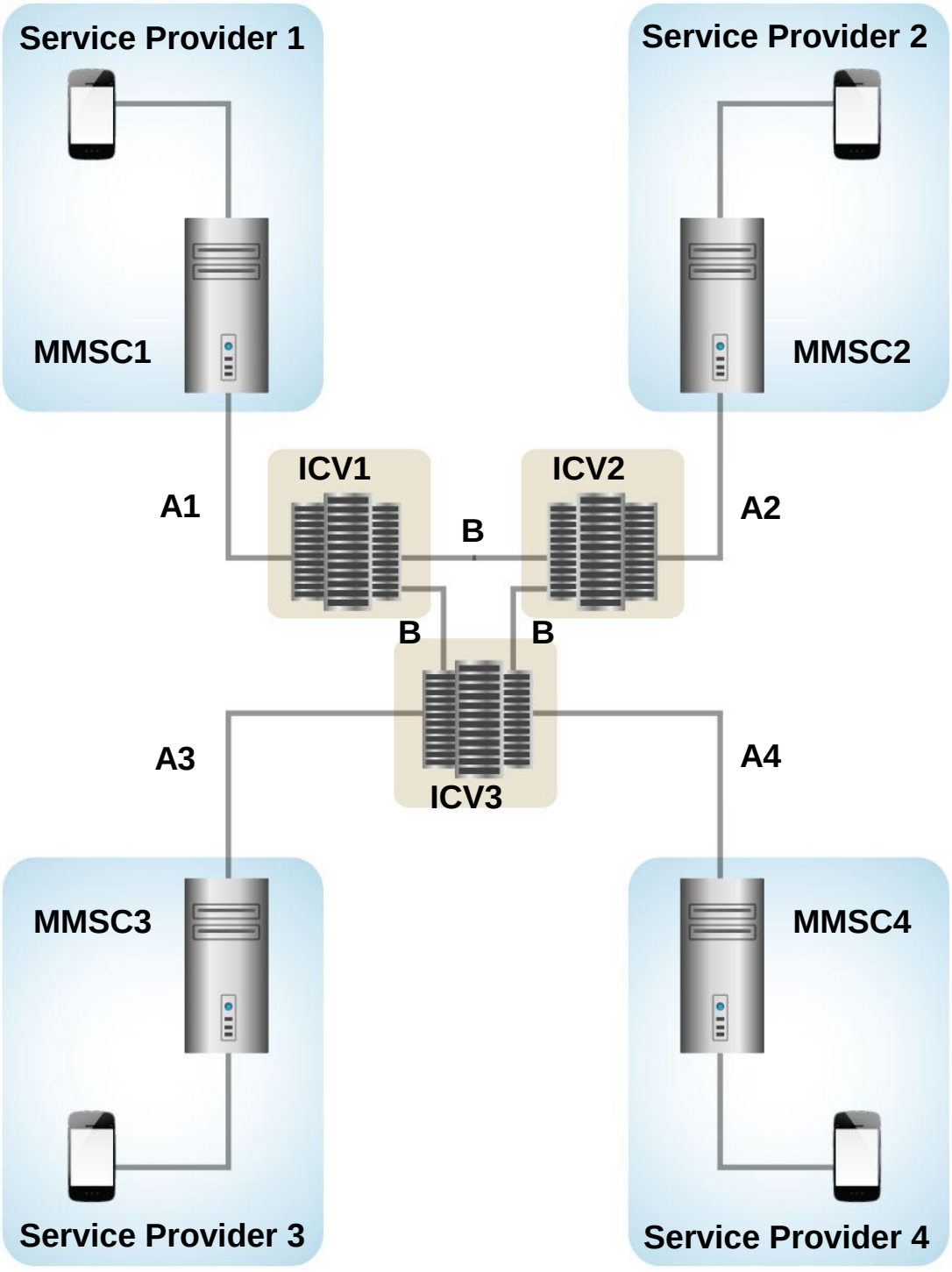
Furthermore this document doesn't discuss any network specific, internal interfaces (e.g. features on the air-interface, etc.) unless they have impact on the available feature-set.

The following diagram shows four different service providers each with a device and a messaging service center MMSC – Multimedia Messaging Service Center) as well as three independent ICVs acting as message transfer gateways.

In general, there are two different main interfaces available. The MM4 interface describes the connection and feature-set between a carrier or service provider and an ICV. Interfaces B describe the connection and feature-set between two ICVs. If there is just one common ICV interface, B is non-existent.

Since each carrier or service provider can have a different feature set between their network and the ICV, they are indexed with the carrier number (MM4-1, MM4-2, MM4-3, MM4-4).

The interface between carriers connecting directly is identified by MM4-5.


Service Provider 1
Service Provider 2
MMSC1
MMSC2
ICV1
ICV2
A1
A2
B
B
B
A3
A4
ICV3
MMSC3
MMSC4
Service Provider 3
Service Provider 4

2.1 MM4 (MMSC to MMSC) or (MMSC to ICV) Interface

This is a standard interface covered in the Definitions and Abbreviations section.

2.2 ICV to ICV interface

This connectivity and protocol support arrangement should be decided among the ICVs. It is recommended to use a MM4 interface between ICVs.

3. General Recommendations

This section identifies the recommended attributes of peer-to-peer (P2P) multimedia messaging service. It is recommended that multimedia messaging services that comply with all of the attributes identified in Sections 3.1 and 3.7, *irrespective of whether the service is offered by a carrier or a non-traditional service provider*, should be able to interoperate with other multimedia messaging services. It is further recommended that multimedia messaging services not complying with *all* of the attributes identified in Sections 3.1 and 3.7 adopt an opt-in mechanism by which users of existing P2P multimedia messaging services as defined herein can be alerted to the differences between their existing P2P services and the service they are considering engaging.

These recommendations apply to regular 10-digit dialable telephone numbers included in the North American Numbering Plan (TNs) and expressly exclude A2P campaigns. It is recommended that A2P traffic utilize messaging channels established to support Common Short Codes (www.USShortCodes.com).

P2P multimedia messaging service is limited to TN-addressed mobile-to-mobile, mobile-to/from-non wireless device/service multimedia messages across service provider networks in the US.

The “highest common denominator” approach as described in Section 3, General Approach of *CTIA SMS Interoperability Guidelines Version 3.2* should be used.

3.1 Attributes of Peer-to-Peer Multimedia Messaging Service

- Privacy

  Messages should originate from a known and identifiable destination, such as a TN. To maintain the trusted nature of messaging service, service providers should adopt and publish privacy policies under which message content is not scanned within the messaging application, used for targeted contextual advertising, or used to profile a user, unless the practice is disclosed to the user or required by law or for SPAM prevention purposes.

- Associated TN

  Users should be associated with a TN that complies with North American Numbering Plan (NANP) requirements. A group of multiple devices within a single household or business may be assigned a single TN. All 10-digit numbers used for messaging purposes should be industry-recognized dialable numbers. If a TN is provisioned for MMS only and has no voice service associated with it, there should be a clearly indicated alternative process available to a message recipient to contact the sender of that message or to contact the service provider from whose platform the message was sent.

  Service should be such that the service provider serving the message recipient has the ability to block or otherwise disable messages from a particular user/account that is associated with abuse. Association of the user/account with a unique, static TN or with another unique identifier and method of presentation recognized through industry processes should be sufficient to satisfy this attribute. Alternatively, service providers may agree to satisfy this attribute by negotiating alternative arrangements, including a

mutually acceptable means for placing the blocking/disabling responsibilities with the service provider serving the message sender.

- Authentication and Registration

  Service providers should have in place methods to authenticate their users and have the means to disable a specific account or TN associated with abuse. Each user should be authenticated by one or more of the following methods: Subscriber Identity Module (SIM); Electronic Serial Number (ESN); verified end customer identification (example: credit check, government issued identification on file) on end customer or family member, relative, personal relationship or employee of the authenticated end customer; and/or association with an industry-recognized dialable TN together with a procedure reasonably designed to confirm the user is an individual.

- Number Portability

  Because users should have the ability to change service providers, numbers used to provide service should support Number Portability/LNP Compliance as defined by the FCC. This includes when numbers port from the originating Service Provider Identification Number (SPID) onto another SPID. This recommendation applies only to TNs that are uniquely assigned to and accessible by end users of the service.

- Single End-User Control

  Device or application for P2P multimedia messaging service should allow only single user, household, or end-user business control to ensure person-to-person communication.

- Person-to-Person Messaging Only

  Application Traffic is note included within the scope of these Guidelines. Application Traffic consists of any automated messaging traffic that is software-generated text, picture, or video messages (such as alerts, advertisements or promotions) or messages that generate premium (billable) charges above and beyond the standard messaging rates. This includes messages being scanned for content/contextual advertisement or that are routed through a system that alters any of the content (multimedia of message, or origination or destination address), unless transcoding is required for device, delivery or routing, or network compatibility reasons. These recommendations apply to regular 10-digit dialable TNs and expressly exclude A2P campaigns. It is recommended that A2P traffic utilize messaging channels established to support Common Short Codes (www.USShortCodes.com).

  Service should not support the automated origination of messages and should have capabilities in place to protect against automating of bulk sending of messages, except that messages may be forwarded from another device or application, individually or in bulk, at the user's specific request or after notice to the user and an opportunity to opt-out. Information (for example, origination address) may be added to messages automatically for the purpose of facilitating forwarding that is consistent with this paragraph.

  Attributes of messages from the service overall should be consistent with typical human operation as follows:

  Throughput

  Throughput from a device or service should be limited by typical human operation and should be comparable to the throughput rates originated on wireless handsets.

Message Volume

Message volume from the device or application should be comparable to message volume generated by typical human operation on wireless handsets.

Quantity of Distinct Recipients

The quantity of distinct recipients of messages from the device or application should be comparable to the quantity of typical human-generated messaging recipients.

Traffic Balance

The balance of traffic between any two TN should be comparable to the balance of traffic observed in human-generated exchanges of messages. TNs having a terminating-to-originating message traffic ratio of at least 3:1 in a calendar month, or more than a 100 percent growth in originating and/or terminating message volume in a month compared to the same month in the preceding year may be inconsistent with typical human operation.[3]

- Governing Law

  Service must comply with all applicable laws. Service providers connecting to the domestic inter-carrier ecosystem using United States TNs should have a legal entity or a registered agent located in the United States and answer to local law in the United States.

- Message Routing

  For routing of messages across networks, each service provider should have a unique, transparent and authenticable identifier associated with all messaging traffic. Except as otherwise agreed by the interconnecting service providers, message routing should be based solely on a Number Portability Administration Center (NPAC) SPID. An NPAC SPID is the Operating Company Number (OCN, synonymous with "Company Code") assigned to a service provider by the National Exchange Carrier Association (NECA). This unique four-character alphanumeric value indicates the service provider for each ported number record in the NPAC. Service providers may have multiple SPIDs. All reference to SPID within this document follows this definition. In general, carriers that manage their TNs in the NPAC for the United States should be entitled to exchange messages without the opt in provisions of Section 3.2 for those TNs associated with their NPAC SPID for which they agree to undertake the responsibilities set forth in this Section 3.1. Carriers that provide TNs for P2P multimedia messaging services should accept the responsibilities set forth in this Section 3.1 for those TNs.[4]

[3] *2011 USF-ICC Transformation Order and Further Notice of Proposed Rulemaking*, FCC 11-161, WC Docket No. 10-90, CC Docket No. 01-92, at App. A (rel. Nov. 18, 2011).

[4] For information on obtaining an NPAC SPID, see https://ncc.neustar.biz/ccs/. To use the NPAC, carriers must demonstrate that they have operating authority. In general, 1) wireline carriers must provide evidence of State operating authority (e.g., Certificate of Public Convenience and Necessity) from the State regulatory agency (e.g. PUC) for one State in each NPAC/SMS Service Area for which NPAC/SMS service is desired, 2) wireless carriers must provide evidence of an FCC radio license in one location in each NPAC/SMS Service Area for which NPAC/SMS service is desired, and Class 1 Interconnected VoIP providers must provide evidence of eligibility to receive numbering resources directly from NANPA and the PA (e.g., an FCC order). The entities must also execute NPAC user agreements. Note that service providers may have multiple separate services.

3.2 Opt-In/Opt-Out

Those multimedia messaging services that do not conform to all of the attributes identified in Sections 3.1 and 3.7 should provide the opt-in/opt-out mechanism described in this section so that users of P2P multimedia messaging services with the attributes recommended in Sections 3.1 and 3.7 can be alerted to the differences between their service and the service they are considering engaging. Adoption of an opt-in/opt-out mechanism does not relieve a service provider of the obligation to ensure that all P2P traffic is person-to-person in nature, as set forth in Section 3.1 above. Services that comply with all of attributes set forth in Sections 3.1 and 3.7 may at their option adopt an opt-in/opt-out mechanism, but there is no recommendation that opt-in/opt-out mechanism be required of such compliant services.

- Opt-In

  Carrier, service provider or ICV acting on behalf of either a carrier or a service provider should operate an opt-in/opt-out process for service providers' users as described in Section 7 for ICVs. With this process, a user can consent to receive messages from the service by replying with the word "START" or other agreed-upon keywords, to opt-in and start receiving messages from a service provider. Opt-in should be per service and should allow traffic from all TNs associated with the service.

  Except as described in section 3.3 "Initial Invitation," messages to users who have not opted-in should not be allowed, protecting customers from unwanted messages and SPAM.

  Bulk provisioning for users who have already accepted an existing service may be provided, so such users are not requested to opt-in to the same program. After that time, new users will need to initiate the interaction by sending a MMS message from their device with the word "START".

- Opt-Out

  A user must be able to revoke consent and stop receiving messages from any service to which consent had previously been given by sending a "STOP" command to the TN used for that service.

  If multiple TNs are associated with the service, a "STOP" command should terminate traffic from all TNs associated with the service.

  Service provider may send a one-time confirmation message before terminating traffic.

- Help command

  The TN being used for messaging should respond to HELP messages and provide the name of the program, offer opt-out commands, and a customer support number within the message body.

- Compliance with industry best practices

  To encourage the use of familiar and established vocabulary for commands, procedures used to join, modify or quit a service should be those stated in the current version of the Mobile Marketing Association's *Consumer Best Practices*, as relevant. Compliance includes obtaining and retaining appropriate opt-in notifications and honoring all opt-out notifications. Users must always be permitted to opt-out of any group or message service at their discretion.

3.3 Group Messaging Applications

Group Messaging Applications are subject to the following additional guidelines:

- Group size

  The maximum recommended group size per TN is sixty (60).

- "Pyramid" or Recursive Groups

  "Pyramid," "recursive," or "nesting" structure, in which a group could be made a member of one or more additional groups, is not recommended. Note, however that a single TN may be a member of more than one group.

- Initial Invitation

  Generally, it is acceptable that group messaging applications send one unsolicited initial invitation to recipients being asked to join a group. Invitations sent by an individual initiating a group via a group messaging application should be limited to a single message to any invitation recipient with a single informed acceptance (valid for an indefinite duration and number of messages) required by the invitation recipient prior to any subsequent messaging.

- Opt-out

  Group messaging applications should provide group members the ability to unsubscribe from any group at any time. Use of the mechanisms described in Section 3.2 is suggested for this purpose.

- Group Messaging—Number Transparency

  Group Messaging services should allow the recipients of group messages to identify all recipients of the group message directly on their devices (i.e., recipients should not have to consult a web site associated with the group messaging service to identify group members) and should provide recipients a clear indication of who will receive their reply.

3.4 Reply-All (Group Messaging)

Reply-All feature provides customers a way to send messages to multiple recipients in a way that will enable recipients with capable devices to reply to entire list.

It is recommended that group messaging be supported over MM4 (refer 23.140 3GPP release 6). Messages exchanged between the same groups of participants should be supported. Conversation participants should be identified by addresses in From, To, Cc and Bcc headers in MM4 forward.req message.

Service providers and their associated aggregators should persist the From, To and Cc fields in the message headers as sent from the originator device to allow conversation participants to identify distribution list and reply to all conversation participants.

3.5 Location Object Shared Across in Message

It is recommended that Location Message be sent as an MMS and include a location attachment in the following format:

- Location messages should be supported over MM4 interface (refer 23.140 3GPP release 6).
- Location object should be included in vCard 3.0 envelope.
- Location message should include message header and Location body parts as described below. At a minimum, it should include the location vCard object.
- To be recognized as Location object vCard MUST include the following fields:
  - GEO tag, containing LAT/LON location
  - Extension tag X-LOCATION-OBJ to identify the vCard as location object.
  - A Name or Address field to indentify the location.
- Location Message may include the following vCard fields:
  - URL filed with a link pointing to a mapping tool (such as Google Maps) that may be available to the receiver of the object to view location information.
  - Additional attributes as available, for example, name field with POI/contact name, address (may be from reverse geo-code), phone number for a POI/contact.
  - Any other vCard field that is relevant to describe the location information.

    An MMS message containing location information may include a static image of the map attached to the message. This will show as a separate mime body part in the same message. A map attachment will be referred to in the location vCard with an extension attribute X-LOC-MAP-IMG. The value shall include the file name attached to the message.

Only one location object should be allowed per message. This does not include any geo-coded objects that user may have included as part of the message. All geo-coded objects should default as OFF unless turned ON by subscriber.

3.6 GeoTagging Information

- Any geo-tagging metadata present in the multi-media should be preserved.

3.7 Spam and Anti-Abuse

- Permitted Message Sources and Addresses

  To help contain the degradation of the customer experience by spam, phishing and other abusive or unwanted messages, it is recommended that the messaging service be limited to messages across wireless carrier networks using NANP numbers as the address.

  Messages should only be allowed from/to devices with TN's within the NPA-NXX range of any participating carrier or service provider.

  Messages from other sources should not be permitted. This includes any 3rd party application provider being connected to any carrier's SMSC (*e.g*. ring tone and picture messaging provider, business applications etc.), any other messaging web interface (http), wireless Internet gateway (email) or any other type of device that does not comply with the recommendations stated in Section 3.1.

  With the exception of SMPP interfaces, all messages passed over an inter-carrier, inter-service-provider interface, or IP-based subscriber interface should include, and any receiving system should require, the use of an Internet domain in all destination mobile device addresses (e.g., 12223334444@example.com, not 12223334444).

- Controls

  To address increased spam risks associated with expanded MMS interoperability, carriers and service providers, or a vendor hired on their behalf, should implement rapid, robust controls to protect consumers from inter-carrier and inter-service-provider abusive or unwanted messages such as spam.

  ICVs should be capable of providing mechanisms to control message flow per carrier / user and also allow blacklisting of certain MSISDN/MIN, TN or NPA-NXX ranges at a carrier or service provider's request.

- Automated System for in-Network Abuse Report Collection

  Each carrier and service provider should establish and maintain an automated system to collect user reports of abusive messaging. The system should be accessible to that service provider's or carrier's users.

  The goal of this system is to rapidly and efficiently collect accurate information identifying abuse, facilitating its containment. An example of such a system is the GSM Association's SMS Spam Reporting Service, which allows users to report spam by forwarding unwanted messages to short code 7726, which has been adopted by many North American MNOs. While generally usable by the collecting service provider or carrier, there may be legal restrictions that prevent sharing some or all of the collected information between service providers and/or carriers. Specific requirements for **sending** collected information to other carriers and/or service providers, while helpful in containing abuse, are outside the scope of this document.

- Inter-Carrier/Inter-Service-Provider Abuse Communication

  Each carrier and service provider should establish and maintain a process and/or system for **accepting**, from all other participating carriers and service providers, reports of abusive messaging. Both a routine submission process (*e.g.*, form, phone number, email address) and a responsive human point of contact for escalations should be documented and made available to all participating carriers and service providers.

- Process for Abuse Identification and Containment

  Each participant should establish and follow a process to identify and contain abuse. The goal of this process is to mitigate messaging threats, protecting end users and networks from spam and other unwanted messages, as well as combat commercial messages that do not comply with the Telephone Consumer Protection Act ("TCPA") and/or the CAN SPAM Act.

- Anti-Spoofing

  Recognizing that it is possible for users to send unsolicited commercial and other unwanted messages to other parties, service providers should ensure that all messages clearly identify a calling party TN; users who send unsolicited or unwelcome messages should be contactable regarding their activities and unsolicited messaging and when justified, be subject to repercussions up to and including disconnection, and actions pursuant to law seeking money damages and injunctive relief where appropriate.

Each carrier and service provider should implement and maintain technical measures sufficient to ensure that any message passed over an inter-carrier or inter-service-provider interface and which was originated inside their network is associated with an authenticated calling party and uses as the calling party ID a TN that is assigned to the originating carrier or service provider.

4. File Types

Each participating service provider should handle inbound MMS messaging traffic with their own network capabilities and feature sets. Message types and feature sets are defined later in this document.

The following media types should be supported (at a minimum) by the participating service providers. Support does not imply device or service capability, but rather infrastructure support (i.e., transcoding can be performed at the terminating network).

IMAGES	
JPEG (same as JPG	BMP
PNG	87a GIF (same as GIF)

TEXT	
SMIL	AMR

AUDIO		
3gpp	mp3	wav
3gpp2	mpeg	x-wav
amr	qcelp	mid
evrc	sp-mid (same as sp-midi)	ogg
midi	vnd.qcelp (same as QCELP)	

VIDEO		
3gpp	3g2	h264
3gp	h263-2000	mp4
egpp2	h263	mp4v-es

It is recommended that all service providers support H.264 media type.

5. Inter-Working between Inter-Service Provider Vendors

5.1 Maximum number of Interworking ICVs

To ensure maximum reliability and transparency for all parties, it is recommended that no more than two ICVs be involved in the end-to-end delivery chain. In an effort to maximize consumer satisfaction, each ICV should be compliant with all terms of these guidelines.

5.2 Defining responsibilities via SLAs

In the case of more than one Inter-Service Provider Vendor (ICV) being involved in the end-to-end delivery chain, it is desirable to define clear responsibilities for all involved parties to clarify accountability in case of problems.

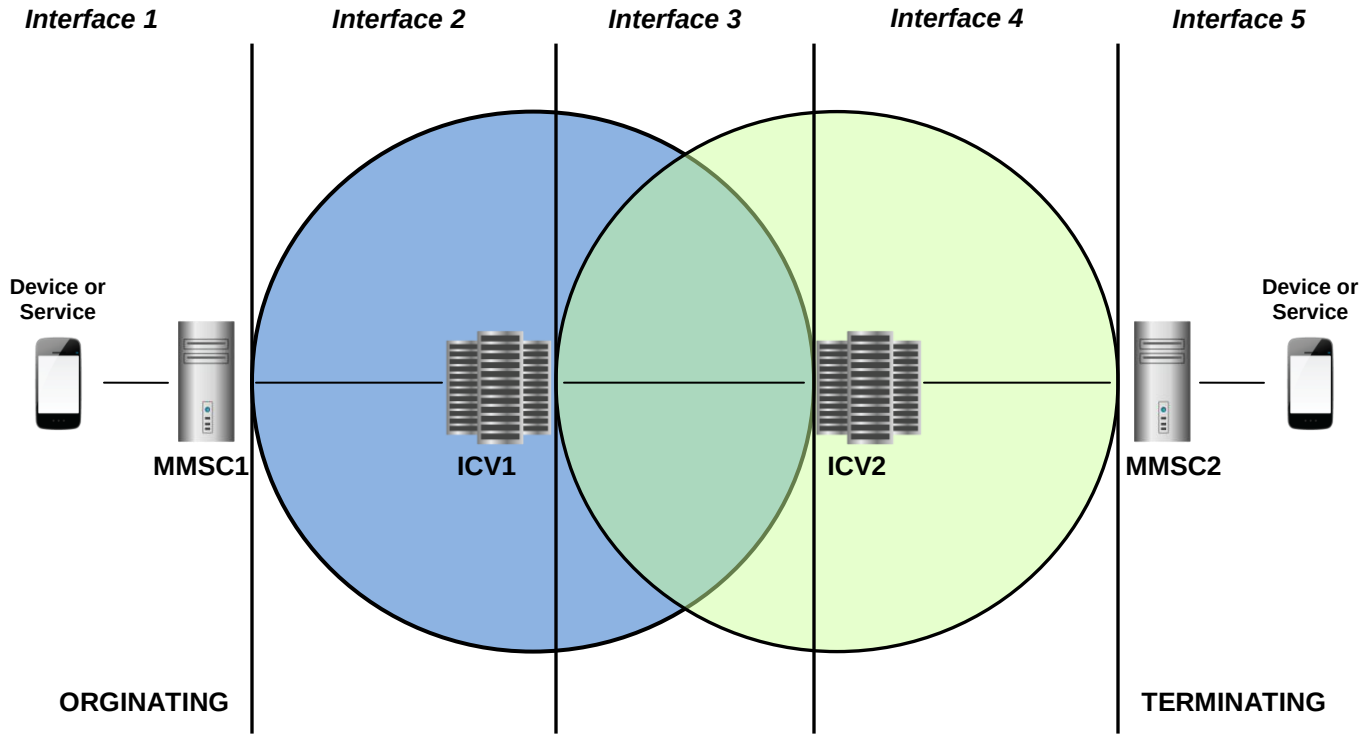
The delivery chain (with two ICVs) can be divided into 5 different interfaces:

1. Carrier-originated device to Carrier-originated MMSC (Originator device to Originator MMSC) (MM1)
2. Carrier-originated MMSC to Originating Carrier inter-service provider vendor (Originator MMSC to ICV) (MM4)
3. Originating Carrier inter-service provider vendor to Terminating Carrier inter-service provider vendor (ICV to ICV) (not defined)
4. Terminating Carrier inter-service provider vendor to Terminating Carrier MMSC (ICV to Recipient MMSC) (MM4)
5. Terminating Carrier MMSC to Terminating carrier device (Recipient MMSC to Recipient device) (MM1)

For illustrative purposes these delivery chains presents a carrier-to-carrier arrangement; however service providers could be substituted at either end of the diagram.

Interfaces 1, 2, 4, and 5 are fully in control by the originating and terminating service providers and their relationships with their ICVs. SLAs between the parties ensure a defined level of availability.

In case of interface 3, the ICVs should deliver all compliant messages across their interfaces. Therefore it is recommended that an SLA between a service provider and an ICV include as the ICV's obligation the responsibility for any ICV-to-ICV connections, but leave to each ICV the decision to subcontract that obligation to someone else (*e.g*. the other ICV). Under this scenario, the ICV's collectively should be responsible for supporting interconnecting links that meet or exceed the SLA requirements. The figure below depicts this relationship.


Interface 1
Interface 2
Interface 3
Interface 4
Interface 5
Device or Service
MMSC1
ICV1
ICV2
MMSC2
Device or Service
ORGINATING
TERMINATING

6. Transcoding Responsibility

It is recommended that transcoding responsibility rest with the terminating service provider's network, either in the service provider's MMSC or through a third party contracted by the terminating network (i.e, an ICV). The content types in Section 4 of this document are the supported types for Interoperable MMS Messaging. The current list of supported content will be updated on an "as-needed" basis and the Working Group will continue to meet in order to update these guidelines.

The originating service provider that sends an unsupported media type not listed in Section 3 of this document understands that the terminating service provider may not be able to support the delivery of the message. Carriers and service providers may choose different methods to handle unsupported media types.

7. Interworking between carriers and service providers

It is the responsibility of the terminating carrier or service provider to handle the MMS delivery to the non-CMRS device.

7.1 Delivery of MMS to non-wireless and verified devices and applications

The ability of non-CMRS TNs to receive or send SMS messages is still developing. This uncertainty around the MMS capabilities of non-CMRS devices and services potentially presents a problem when only a small number of MMS messages addressed to non-CMRS TNs can be successfully delivered.

Carriers and service providers may choose different approaches to deal with the above-mentioned challenge. Some may decide to follow the approach implemented today in the wireless ecosystem, in which case the existing wireless inter-carrier infrastructure would be used. Based on this approach, the message destination is determined at the carrier level during the message routing procedure and there is no verification of MMS capability of the terminating device. Wireless carriers may select this approach for several reasons including: relying on the expectation that non-wireless carriers will deliver all messages, even to customers with non-MMS capable devices by some alternative means; or because it provides a simple implementation option.

Where no verification of the MMS capability of the terminating device is obtained, the message will follow one of two different scenarios.

1) In some cases, the message with be converted from text to voice and delivered to the terminating device as a voice message.
2) In other cases, the message is simply dropped when it cannot be delivered to the terminating device.

7.2 Additional SLA Recommendations for ICVs

Additional SLA recommendations for ICVs directed at containing spam and fraud should be considered with the entry of participants into the ecosystem. ICVs offering services to MMS service providers should comply with the following guidelines:

- Compliance with Section 3.1 of these Guidelines

ICVs should insure that each provider meets or exceed the recommendations in Section 3 of the *Guidelines* and document how their customers meet these recommendations.

- SPAM identification and containment

ICVs should monitor throughput using accepted anti-SPAM methods used for all messaging. If abuse of these recommendations is found, then the ICV should block the offending messages and where appropriate, seek legal recourse against the originator of the message. ICVs should also utilize existing reporting structures to notify the industry of customers sending Spam messages.

- Opt-in and Opt-out

Where indicated, ICV acting on behalf of its carrier or service provider customer should operate an Opt-In/Opt-Out process for service providers' subscribers as described in Section 3.2 if the carrier or service provider is not compliant with Sections 3.1 and 3.7.

- Unique/transparent identity

ICVs should confirm that all service providers are uniquely and transparently identified in all reporting and messaging tracking that is visible to any other service provider. Currently, in some cases, the higher level CLEC name is shown rather than the end-customer (non-CMRS). ICVs should verify that they can identify and if necessary block traffic from individual service providers. Carriers may reasonably require ICVs to identify and block certain service providers and services that are sending unacceptable amounts of spam and unwanted messages to their customers.

- International

It is recommended that ICV's may connect international service providers into the ecosystem, to interoperate with US service providers as long as the international service provider complies with all the recommendations set forth in these guidelines. Likewise, the reverse is true: +1 non-CMRS providers may connect with non +1 carriers, as long as the +1 non-CMRS provider complies with all of the recommendations herein.

- Traffic binds

Inter-carrier traffic binds should not be leveraged or used to carry traffic for which they were not originally intended. This includes all non-CMRS providers, long codes, 500 code numbers (e.g. details below) or any other traffic not routed between two CMRS entities which is being routed by ICV. Traffic not intended as traditional inter-carrier traffic may be subject to an additional agreement between the participating entities and be carried via separate connections/binds. Absent the specific agreement of both service providers, messaging traffic between Non-CMRS and CMRS service providers should not be intermingled with intercarrier traffic.

Area codes 500, 522, 533, 544, 566, 577, 588 are non-geographical area codes reserved for Personal Communication Services. These are special purpose telephone numbers with a set of capabilities that allow service profile management.
www.nanpa.com/number_resource_info/500_codes.html

- Traffic differentiation

For routing of messages across networks, each service provider must have a unique, transparent and authenticatable identifier associated with all messaging traffic.

- Traffic routing

Message traffic destined to a particular CMRS carrier should contain MSISDN's/MDN's that reside on the carrier's network. Message traffic should not be delivered to a CMRS carrier to be passed through to another CMRS carrier without the specific agreement of both service providers.

- Source Address Validation

  ICVs should validate the source MSISDN against the source service provider. This helps ensure the source MSISDN is not being used by other sources for sending non-authorized traffic.

8. Delivery Reports and Read Replies

8.1 Delivery Reports

If an agreement exists between operators, the originating MMSC may request a Delivery Report, on MM4, regardless of whether the originating device requested the Delivery Report. Then, if the originating MMSC requests a Delivery Report, the terminating MMSC shall generate a Delivery Report for each MM for which a Delivery Report has been requested.

Note: This requirement is covered in 23.140 3GPP release 6 (i.e. v6.5.0, 2004-03)

If a Delivery Report has been requested by the originating device but the recipient device denies the Delivery Report confirmation, the participating networks should adhere to the standards referenced above.

When using MM4, the originating MMSC shall route an MM forward to the terminating MMSC using the MM4_forward.REQ, which contains MMS control information and the MM content.

The terminating MMSC shall respond with a MM4_forward.RES, which provides the status of the request if an MM4_forward.RES was requested.

Support for MM4_forward.REQ and MM4_forward.RES is mandatory for the MMS Relay/Server.

The participating carriers will make best efforts to deploy the following optional feature in the 23.140 3GPP standard their networks and their vendors' networks. For failure conditions, the terminating MMSC shall respond with a MM4_forward.RES, which includes a status code that indicates the reason the MM was not accepted, e.g., no subscription, bad address, network not reachable, etc., if an MM4_forward.RES was requested.

8.2 Read Reply Reports

Read Reply Reports may be supported over MM4, but this feature is optional and may not be supported by all participants. If a request comes in to a network that does not support the option, the message should still be delivered but the Read Reply Report may not be delivered back to the originating subscriber. Read Reply Report may be considered and routed back to the client that requested the report as a new MM type Read Report (same functionality as for Read Reply Reports over MM1).

MMS Read Receipt: SMS notification sent back to the originator when the MMS message has been read. It serves as validation that the MMS message has been read on the targeted device. It includes (READ_ACK_REQ) or SMS Read Acknowledgment Message.

9. Minimum/Maximum Message Size

If the originating network sends a message that is larger than the agreed upon size, the terminating service provider may not be able to support the delivery of the message. The minimum/maximum size of the message will be variable depending on the media type being sent.

The following message sizes should be supported at a minimum:

Images: up to 100kb

Audio: up to 100kb

Video: up to 100kb

It is recommended that participants support:

Images: up to 5MB

Audio: up to 5MB

Video: up to 5MB

The purpose of including these message size recommendations is to provide a goal toward which each service provider should strive to support.

The industry recognizes that it will take time for service providers to enhance their network to support 5MB file sizes or to adapt the attachments down to a size that is supportable by the participating networks.

10. Throttling over MM4

The Working Group recommends having both end-to-end and point-to-point throttling capabilities. This is especially desirable in an outage environment where a network element has been “offline” and suddenly floods the other connected networks when it comes back online.

Throttling is defined as flow control – the sender is notified of the ability to begin sending when the receiving network becomes available. The sender is notified of the ability of the receiving network to stop sending the messages.

11. Legacy Support

Definition

"**Legacy Customer**" means a subscriber who cannot send or receive a MM, but can receive a text message.

Requirements

In the event that the intended recipient of an MM is a Legacy Customer, then the terminating service provider should promptly store the MM upon receipt and send to the Legacy Customer a non-MM text message notifying the Legacy Customer of an inbound MM and directing them to a web site (Legacy Site) to view the MM. This non-MM text message may include, the originating customer's telephone number populated in the message header field commonly referred to as the "From" field, the URL from which the MM may be viewed/accessed, and any associated message ID and/or password. The recipient customer should be able to reply to this non-MM SMS message as a text message (assuming that their device or service capabilities and provisioning allow for device originated SMS).

The terminating service provider should ensure that the non-MM SMS notification message is prioritized and follows the same delivery and retry schedule of the terminating service provider's intra-service provider non-MM SMS notification messages.

The recipient operator may elect to outsource this functionality.

In addition, with the understanding that the purpose of Inter-Service Provider MMS Messaging is to facilitate the exchange of MMS messages between subscribers of different service providers, and recognizing that not all subscribers will have MMS-capable devices or services, service provider should not block replies to an MM from a Legacy site, if a service provider elects to offer this functionality to its Legacy Customers. This reply message may be transmitted via Text or MMS, depending on the service provider's capabilities and business model. Such messages will have the original recipient's telephone number in the "From" field and shall be considered as originating from a device, as the intent is to reply to a message that was sent to a device.

Service providers should make every effort to ensure that Legacy Customers who reply to MMS messages from a Legacy Web site cannot abuse the capability and initiate SPAM-type messaging. For example, the "Reply" functionality should be limited only to the sender of the MMS.

12. Unsupported Media Type Treatment

Service providers receiving unsupported media types should make best effort to deliver the content to the destination subscriber.

Examples include the delivery of a video file to the non-capable MMS device.

The Working Group will continue to evaluate support of different media types and will update these guidelines accordingly.

13. Digital Rights Management (DRM)

It is recommended that all participating service providers support DRM. On a forward-going basis, the responsibility of maintaining the integrity of the content (DRM) should be on the originating provider's network (this includes the devices as well). This applies to DRM as specified in the MMS standard (TS23.140). It is agreed that if the originating provider is effective in managing the digital content, then the sender will not be able to send the protected content.

14. Service Level Agreement

In addition to the recommendations in this document, a service provider may opt to establish Service Level Agreements (SLA) individually with each peer MMSC/ICV connection. The service provider has ultimate accountability for defining roles of responsibilities for performance, maintenance and levels of support. It is also understood that provisioning and enforcement of an SLA is typically at the sole discretion of the service provider.

15. Message Bundling and Unbundling

The goal of service providers is to deliver the messages, with multiple recipients, as efficiently as possible while maintaining the integrity of the address list and enable the “reply all” capability. Section 3 provides additional details regarding Group Messaging or message bundling.

16. Testing

Testing will be the responsibility of each participating service provider and ongoing testing will be encouraged.