

SMS Interoperability Guidelines

Version 3.2.1

Effective Date: February 5, 2013

NOTICE TO READERS

This document does not contain any confidential material. Copies may be made anytime by any carrier, service provider or Inter Carrier Vendor (ICV) for internal use only. As new versions become available they will be distributed to all involved.

To ensure consistency of the versions and correct distribution this document is managed by CTIA. Any proposed 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 review, approval, and further distribution.

Table of Contents

1 INTRODUCTION 4

1.1 VERSION 1.0 4
1.2 VERSION 2.0 4
1.3 VERSION 3.0 5
1.4 VERSION 3.1 5
1.5 VERSION 3.2 7

2 INTERFACES 7

3 GENERAL APPROACH 10

3.1 COMMON FEATURE SET 10
3.2 CARRIER INTEGRATION 12
3.3 PROCESSING TELEPHONE NUMBER DEACTIVATIONS 12

4 GENERAL RECOMMENDATIONS 12

4.1 ATTRIBUTES OF PEER-TO-PEER TEXT MESSAGING SERVICE 13
4.1.1 Privacy 13
4.1.2 Associated TN 13
4.1.3 Authentication and Registration 13
4.1.4 Number Portability 14
4.1.5 Single End-User Control 14
4.1.6 Person-to-Person Messaging Only 14
4.1.7 Governing Law 15
4.1.8 Message Routing 15
4.2 OPT-IN/OPT-OUT 15
4.2.1 Opt-In 16
4.2.2 Opt-Out 16
4.2.3 Help command 16
4.2.4 Compliance with industry best practices 16
4.3 GROUP MESSAGING APPLICATIONS 17
4.3.1 Group size 17
4.3.2 "Pyramid" or Recursive Groups 17
4.3.3 Initial Invitation 17
4.3.4 Opt-out 17
4.3.5 Group Messaging—Number Transparency 17
4.4 8XX TELEPHONE NUMBERS PROVISIONED FOR SMS 17
4.4.1 Permitted Traffic 18
4.4.2 Initiation of a Messaging Session between Consumer and 8XX Telephone Number 18
4.4.3 Authority to Text-Enable 8XX Telephone Numbers 18
4.4.4 Anti-Spoofing and Authority to Originate and Relay Messages from 8XX Telephone Number 19
4.4.5 Status of 8XX Telephone Number in SMS/800 Registry 19
4.4.6 Spam Containment for Text-Enabled 8XX Telephone Numbers 19
4.4.7 Processing Telephone Number De-Activations 19
4.5 SPAM AND ANTI-ABUSE 19
4.5.1 Permitted Message Sources and Addresses 19
4.5.2 Controls 20
4.5.3 Automated System for in-Network Abuse Report Collection 20
4.5.4 Inter-Carrier/Inter-Service-Provider Abuse Communication 20
4.5.5 Process for Abuse Identification and Containment 21
4.5.6 Anti-Spoofing 21
4.6 PROTOCOLS 21
4.7 CHARACTER SET 22
4.8 MESSAGE ADDRESSING 22
4.9 MESSAGES LENGTH / CONCATENATED MESSAGES 22

4.10 DISTRIBUTION LIST 22
4.11 VALIDITY PERIOD 22
4.12 REPLY ADDRESS 23
4.13 CALL BACK NUMBER 23
4.14 BINARY DATA OR SPECIAL USER DATA 23
4.15 PRIORITY 23
4.16 DELETE/REPLACE IN SMSC 23
4.17 DELIVERY RECEIPT / ERROR MESSAGES / STATUS REPORTS 23
4.18 GENERAL SMPP CAPABILITIES 24

5 INTERWORKING BETWEEN INTER-CARRIER VENDORS 28

5.1 MAXIMUM NUMBER OF INTERWORKING ICVS 28
5.2 DEFINING RESPONSIBILITIES VIA SLAS 28

6 INTERWORKING BETWEEN CARRIERS AND SERVICE PROVIDERS 30

6.1 DELIVERY OF SMS TO NON-WIRELESS AND VERIFIED DEVICES AND APPLICATIONS. 30
6.2 ADDITIONAL SLA RECOMMENDATIONS FOR ICVS 30
6.2.1 Compliance with Section 4 of these Guidelines 30
6.2.2 SPAM identification and containment 30
6.2.3 Opt-in and Opt-out 31
6.2.4 Unique/transparent identity 31
6.2.5 International 31
6.2.6 Traffic binds 31
6.2.7 Traffic differentiation 31
6.2.8 Traffic routing 31

7 SERVICE LEVEL AGREEMENT 32

8 TESTING 32

9 APPENDIX A: SUPPORTED FEATURES ON A INTERFACES 33

9.1 AT&T 33
9.2 LEAP 34
9.3 SPRINT NEXTEL 34
9.3.1 Handset Capabilities 34
9.3.2 Subscriber Capabilities 34
9.3.3 Preferred Interface 34
9.3.4 Character Set 34
9.3.5 Message Length 34
9.3.6 Concatenated Messages 34
9.3.7 Distribution Lists 34
9.3.8 Validity 34
9.3.9 Message priority features 34
9.3.10 Reply Path 34
9.4 US CELLULAR 35
9.5 VERIZON WIRELESS 35
9.6 T-MOBILE USA 35
9.6.1 Handset capabilities: 35
9.6.2 Subscriber capabilities 35
9.6.3 SMSC vendor / preferred interface 35
9.6.4 Message addressing 36
9.6.5 Character Set: 36
9.6.6 Message length 39
9.6.7 Concatenated messages 39
9.6.8 Distribution list 39
9.6.9 Validity Period 39
9.6.10 Message priority features 39

9.6.11 Reply Path 39
9.6.12 Message types 40
9.6.13 Status report / delivery receipt 40
9.6.14 Deferred delivery 40
10 APPENDIX B: FEATURE TABLE 42
11 APPENDIX C: ASCII/GSM CHARACTER SET MAPPING TABLE 43
12 ABBREVIATIONS AND DEFINITIONS 47

1 Introduction

1.1 Version 1.0

At the first inter-carrier messaging meeting in Las Vegas on October, 25th 2001 all participating carriers indicated their intent to support inter-carrier messaging. This service enables wireless subscribers to send and receive messages using their phone number (MSISDN/MIN) to and from any wireless network.

Furthermore the participating carriers announced their commitment to participate in the process to work toward achieving inter-carrier messaging.

The following Mission Statement of Inter-carrier messaging service was agreed upon:

Allow phone number addressed mobile-to-mobile text messages across wireless carrier networks in the US.

To achieve this goal, subgroups were formed to address technical implementation options and a commonly defined feature-set based on the definition of the available interfaces.

The objective of the interface and feature-set subgroup was to:

Identify and define the involved interfaces and agree upon as well as specify the supported common feature-set.

1.2 Version 2.0

Inter-carrier Messaging Guidelines Version 2.0 was created to expand inter-carrier messaging by enabling messaging traffic between wireless carriers and non-wireless carriers on SMS-capable devices. As a general principal, non-wireless carriers need to follow the inter-carrier messaging guidelines established by wireless carriers to insure interoperability. However, several unique provisions/recommendations were added to the document to reflect the differences between wireless and non-wireless carriers from the messaging perspective.

The initial Mission Statement was revised to reflect the agreed changes in the scope of the Inter-carrier Messaging Guidelines:

Enable phone number addressed text messages
across participating wireless and non-wireless carrier networks in the US

It was expected that only a relatively small number of devices in non-wireless carrier networks initially would be SMS-capable and wireless and non-wireless carriers could develop alternative methods and capabilities for delivering messages to their customers (for example, using text-to-speech conversion).

The focus of this document is on the inter-carrier exchange of SMS messages. The alternative methods can be pursued at any time and fall outside the scope this agreement.

1.3 Version 3.0

Version 3.0 is created to facilitate the entrance of non-CMRS devices and services that use 10-digit Telephone Numbers ("TN's") to exchange SMS 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 SMS 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 4 and 6 of the *CTIA Inter Carrier Messaging* document of January 29, 2009.
2. Development of guidelines for inter-carrier 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 Short Code***	**Supported via Common 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 Version 3.1

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

Version 3.1 identifies the attributes of original carrier-provided text messaging services and provides a path for text messaging services with differing business models to interoperate, while also ensuring that consumers have the opportunity to understand the different business models used by text messaging services.

When first introduced to consumers, text messaging was available only from wireless carriers, which offered texting services alongside voice telephone service. Consumers have expected that, although text messaging and voice are quite different, text messaging services offered by wireless carriers will be subject to and protected by the same strict privacy practices that have historically governed the provision of telephone voice services by carriers.

The popularity of text messaging has led to the development of internet-based text messaging services that, just like carrier-offered text messaging, use ten-digit telephone numbers to send and receive text messages. (Many also offer voice capabilities, which are not the subject of these Guidelines.) A wide variety of these non-traditional services exist, and the enterprises that provide these services utilize an equally-wide variety of business models and privacy policies. In some cases, these services are ad-supported and provided free of charge to the user. Some service providers scan the content of text messages to refine their marketing messages. Some will append targeted advertising messages to the content of text messages exchanged among users.

All responsible service providers will ensure that their business models and privacy policies are disclosed to and accepted by users who enroll for their services. However, because these non-traditional services employ 10-digit telephone numbers that are indistinguishable from 10-digit telephone numbers issued to wireless subscribers, wireless subscribers who exchange text messages with users of these non-traditional services currently have no way to assess the business model and privacy policies of the service used by their new text messaging correspondent. Lacking any way to distinguish between a text message sent from a traditional carrier-provided service and a text message sent from an internet-based service, wireless customers may incorrectly assume that the same privacy policies that have historically governed carrier-provided text messaging apply to all text messaging services.

To ensure consumer awareness of the various privacy practices in the evolving text messaging ecosystem, Version 3.1 recommends that all users of text messaging services based on 10-digit telephone numbers be provided information about the privacy or business policies of any messaging service that operates under different policies and practices from those of the original carrier-provided text messaging services. Based on this information, a user of any text messaging service should have the right to decline any traffic exchange with non-traditional services whose privacy or business policies are not acceptable to the user.

Version 3.1 identifies the attributes of traditional carrier-provided text messaging service to which wireless customers have become accustomed. It is recommended that any text messaging service that complies with all of the identified attributes, *irrespective of whether it is offered by a carrier or a non-traditional service provider*, be allowed to interoperate without additional notifications. It is further recommended that text messaging services not complying with one or more of the identified attributes adopt a mechanism by which users of traditional text messaging services can be made aware of where their service differs.

Version 3.1 also refines recommendations for protecting consumers from unwanted messaging including spam, phishing and other exploitive and abusive traffic, reinforcing the importance of robust spam detection, prevention and reporting across all parties involved in interoperable SMS messaging.

1.5 Version 3.2

Version 3.2 further broadens the definition of peer-to-peer (P2P) text messaging services, and recommends that text messaging services that comply with all of the attributes of P2P text messaging be able to interoperate with other text messaging services. Additionally, Version 3.2 refines recommendations for group messaging and containment of abusive messaging such as spam, phishing, etc. Version 3.2.1 of September 2014 incorporates guidelines for text-enabling toll-free voice telephone numbers, developed in conjunction with SMS/800, the U.S. registrar for toll-free telephone numbers.

2 Interfaces

There are several different options available to interconnect the various carriers and service providers to enable the 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) all carriers and service providers select a single ICV or industry association to provide interoperability;
3) carriers and service providers interconnect their networks directly based on bilateral agreements.

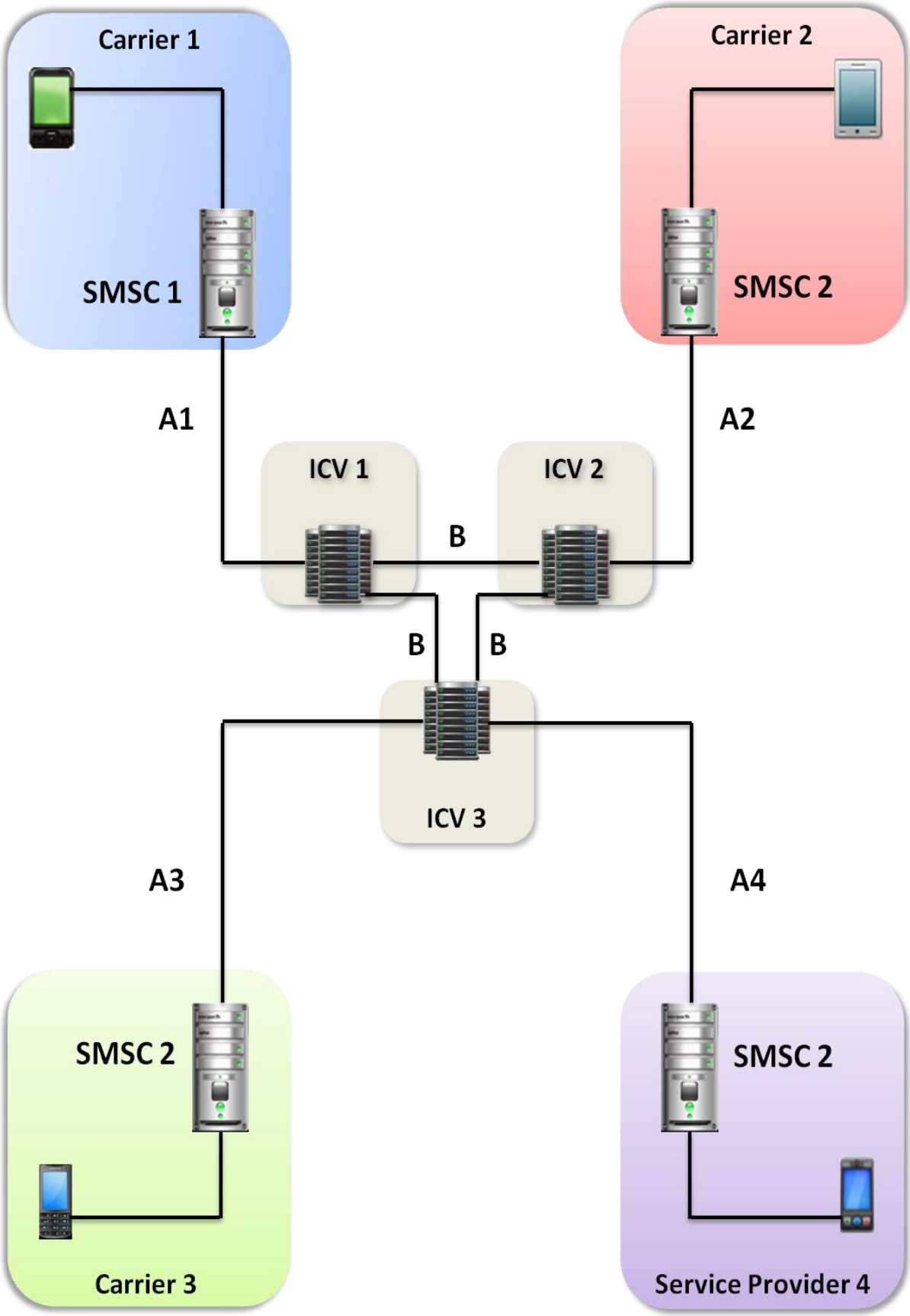
These scenarios are not mutually exclusive. However, since the definition of the interface in case 3) is left to the participating service providers, this document only focuses on cases 1) and 2).

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

The following diagram shows four different carriers and service providers each with a device and a messaging service center (SMSC – Short Message Service Center) as well as three independent ICVs acting as message transfer gateways.

In general, there are two different main interfaces available. The A interfaces describe 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 different numbers (A1, A2, A3 and A4).


Carrier 1
SMSC 1
Carrier 2
SMSC 2
A1
A2
ICV 1
ICV 2
B
B
B
ICV 3
A3
A4
SMSC 2
Carrier 3
SMSC 2
Service Provider 4

3 General Approach

3.1 Common Feature Set

In general, there are two different approaches to define the common feature set for the inter carrier messaging service:

a.) Define the lowest common denominator among all carriers and service providers;
b.) Define the feature set for each carrier and service provider and messaging limits based on the Originating and Terminating carrier and service provider relationship (A1 to A2, A2 to A3 and A1 to A3)

The following illustration illustrates the differences between those approaches as well as their pros and cons.

Each carrier and service provider supports a unique, defined feature-set A (A1, A2 or A3).

In case a.) (lowest common denominator) the feature-set would be limited to the cut set of all involved carriers and service providers. This would relate to the white area B below.

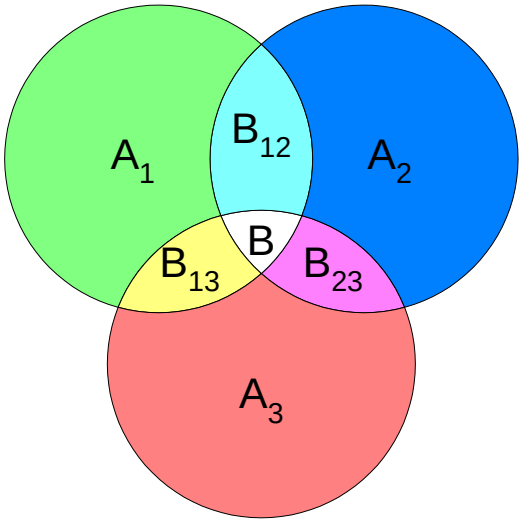
In this approach the ICV has to support the minimal feature-set on interface B and the carrier or service provider-specific feature set on interface A. The limitation of the feature-set would occur at the ICV of the originating side.

With this prerequisite, any ICV that supports any of the A interfaces is able to support interoperability.

In case b.) the feature-set would be limited to the cut set of the Originating and Terminating carrier or service providers. This feature set is reflected in the white area B plus one of the colored areas B12, B13 or B23 depending on the involved parties.

In this approach, the ICV has to support an overall feature-set of any carrier or service provider on the interface B. The limitation of the feature-set would take place at the ICV of the terminating side.

This scenario allows only ICVs supporting all A interfaces to support inter-carrier messaging.



The lowest common denominator approach (a) has the following pros and cons:

Pros:

+ Higher number of ICVs available
+ Additional joining carriers and service providers only have to fulfill interface B recommendations

Cons:

- all carriers and service providers are restricted to the limited feature set
- limited user experience
- Any ICV can enter the business without supporting all carrier and service provider features

The highest common denominator approach (b) has the following pros and cons

Pros:

+ Originating carrier and service provider is only restricted to the feature-set of the receiving carrier and service provider
+ Optimal feature set for a richer user experience
+ Only ICVs that can comply with all carrier and service providers features can participate

Cons:

- Additional joining carriers and service providers can't introduce new features that are not supported by the participating ICVs
- Number of available ICVs is probably lower

In case of more than one ICV being involved in the end-to-end delivery path, all carriers and service providers are interested in maintaining an agreed minimum set of features for the B interfaces.

To provide maximum flexibility for all service providers, it is possible to extend the feature set for specific bilateral scenarios. This ensures the best available user experience.

In every case as much information/features as possible should be included along the delivery path and the terminating ICV should then modify the message according to the capabilities of the receiving network.

3.2 Carrier Integration

Carrier may offer a direct integration to service provider or may hire a third party to handle the connection with 10-digit Service Provider. To insure impartiality, to be able to serve as a 10-digit aggregator, it is recommended that vendor be restricted from providing 10-digit services.

3.3 Processing Telephone Number Deactivations

All text messaging service providers should process TN deactivation information and share Deactivation TN Lists. Receiving Deactivation Lists may require individual agreements among service providers to preserve confidentiality.

Deactivations should be processed as soon as possible, but in no event more than twenty-four (24) hours after delivery of the Deactivation Notification, Service Providers should update their systems to bar all deactivated TN's listed in the Deactivation Notification from being sent Messages. Additionally, the status of all deactivated TN's listed on the Deactivation Notification should be changed from "Subscriber" to "Deactivated."

4 General Recommendations

This section identifies the recommended attributes of peer-to-peer (P2P) text messaging service. It is recommended that text messaging services that comply with all of the attributes identified in Sections 4.1 and 4.5, *irrespective of whether the service is offered by a carrier or a non-traditional service provider*, should be able to interoperate with other text messaging services. It is further recommended that text messaging services not complying with *all* of the attributes identified in Sections 4.1 and 4.5 adopt an opt-in mechanism by which users of existing P2P text 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 text messaging service is limited to TN-addressed mobile-to-mobile, mobile-to/from-non wireless device/service text messages across service provider networks in the US.

The "highest common denominator" approach (as described in Section 3, General Approach) should be used.

4.1 Attributes of Peer-to-Peer Text Messaging Service

4.1.1 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.

4.1.2 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 SMS 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.

4.1.3 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.

4.1.4 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.

4.1.5 Single End-User Control

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

4.1.6 Person-to-Person Messaging Only

Application Traffic is not 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 (text 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:

4.1.6.1 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.

4.1.6.2 Message Volume

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

4.1.6.3 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.

4.1.6.4 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]

4.1.7 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.

4.1.8 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 4.2 for those TNs associated with their NPAC SPID for which they agree to undertake the responsibilities set forth in this Section 4.1. Carriers that provide TNs for P2P text messaging services should accept the responsibilities set forth in this Section 4.1 for those TNs.[4]

4.2 Opt-In/Opt-Out

Those text messaging services that do not conform to all of the attributes identified in Sections 4.1 and 4.5 should provide the opt-in/opt-out mechanism described in this section so that users of P2P text messaging services with the attributes recommended in Sections 4.1 and 4.5 can be alerted to the differences between

---

[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.

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 4.1.6 above. Services that comply with all of attributes set forth in Sections 4.1 and 4.5 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.

4.2.1 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 6 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 4.3.3, 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 SMS message from their device with the word "START".

4.2.2 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.

4.2.3 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.

4.2.4 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.

4.3 Group Messaging Applications

Group Messaging Applications are subject to the following additional guidelines:

4.3.1 Group size

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

4.3.2 "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.

4.3.3 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.

4.3.4 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 4.2.2 is suggested for this purpose.

4.3.5 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.

4.4 8XX Telephone Numbers Provisioned for SMS

For this document, "8XX" refers to telephone numbers utilizing the Numbering Plan Area Codes (NPAs) reserved in the North American Numbering Plan for toll-free voice service. Current active NPAs assigned to toll-free voice are 800, 888, 877, 866, 855 and 844. Cloud-based telephony services enable toll-free voice telephone numbers to be provisioned for messaging services that can interoperate with traditional mobile-device-based SMS. The ability to exchange SMS messages with a toll-free voice telephone number provides new convenience and increases the value of telephone-number-based messaging services to consumers. Because 8XX toll-free voice telephone numbers are commonly commercial in nature, recommendations for provisioning 8XX telephone numbers for messaging seek to protect consumers from unwanted or

abusive messages, consistent with the legal requirements of the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227.

The guidelines in this section 4.4 have been jointly developed with SMS/800, Inc., which operates SMS/800, a centralized system that performs Toll Free number management. All Toll Free Service Providers that assign Toll Free numbers for use within the North American Numbering Plan (NANP) must use SMS/800 to verify the availability of specific numbers, reserve them, create Customer Records, and download records to Service Control Points (SCPs) to facilitate call processing. SMS/800 administers Functions Tariff F.C.C. No. 1, available at: http://www.sms800.com/Controls/NAC/Tariff.aspx#.

4.4.1 Permitted Traffic

To protect consumers from unwanted and abusive messages, traffic involving text-enabled 8XX telephone numbers must strictly comply with the Telephone Consumer Protection Act. Generally, traffic should be restricted to "transactional" messages, which facilitate an already agreed-upon transaction or update a customer about an ongoing transaction. Unsolicited commercial content messaging, which advertises or promotes a commercial product or service, is not supported.

4.4.2 Initiation of a Messaging Session between Consumer and 8XX Telephone Number

Text messaging interaction between an 8XX telephone number and a consumer should be initiated solely at the specific request of a consumer.

4.4.3 Authority to Text-Enable 8XX Telephone Numbers

The authority to control voice telecommunications services and/or information services (*e.g.*, SMS, MMS or future services) associated with an 8XX Telephone Number resides with the subscriber who is the holder of record of the toll-free voice Telephone Number ("holder"). To facilitate coordination with voice service on a given 8XX telephone number, it is recommended that only the SMS/800 Responsible Organization (RespOrg) selected by the holder of that 8XX telephone number have the authority to text-enable 8XX Telephone Numbers solely at the direction of the holder of the 8XX telephone number. Any person, company, or organization that can demonstrate the required skills and financial responsibility for managing Toll Free numbers can apply to become a RespOrg in SMS/800. A list of RespOrgs in good standing is available from the SMS/800, Inc., web site at http://www.sms800.com/Controls/NAC/Serviceprovider.aspx.

At present, the SMS/800 registry associates only one RespOrg with any 8XX telephone number. It is acknowledged, though, that the holder of any 8XX telephone number may wish to utilize one RespOrg for voice services ("Controlling RespOrg") and a different RespOrg ("Non-controlling RespOrg") for text messaging services. In this case, the Non-controlling RespOrg should secure a Letter of Authorization ("LOA") from the Controlling RespOrg, memorializing the Controlling RespOrg's acknowledgement of the Non-Controlling RespOrg's intention to text-enable the 8XX telephone number

controlled by the Controlling RespOrg. For such purposes, the Controlling RespOrg is the RespOrg of record in the SMS/800 Registry.

It is anticipated that the SMS/800 registry will be supplemented with new functionality so that additional RespOrgs can be identified for each additional service associated with a particular 8XX telephone number (e.g., a RespOrg for text messaging, a RespOrg for video calling, etc.) At such time, the RespOrg identified as the messaging RespOrg in the SMS/800 registry would have the authority to text-enable an 8XX telephone number unilaterally.

4.4.4 Anti-Spoofing and Authority to Originate and Relay Messages from 8XX Telephone Number

It is recommended that only the service provider identified as the RespOrg for a specific 8XX number's text messaging service may submit a text message from that 8XX number to a service provider for relay to the inter-service-provider SMS network. Service providers that provide interconnect service to 8XX number holders should verify that all messages received from an 8XX number holder for relay to other service providers correctly identify the sending 8XX number.

4.4.5 Status of 8XX Telephone Number in SMS/800 Registry

It is recommended that only 8XX telephone numbers identified as being in either "Reserved" or "Working" status in the SMS/800 registry be text enabled.

4.4.6 Spam Containment for Text-Enabled 8XX Telephone Numbers

Service Providers for 8XX telephone numbers should provide robust anti-spam and anti-abuse controls consistent with the recommendations in Section 4.5, Spam and Anti-Abuse. As a general guideline, the introduction of 8XX messaging traffic and associated anti-spam controls should not disrupt the effectiveness of existing anti-spam controls in use by service providers, nor require any changes for existing anti-spam controls to effectively protect consumers from spam.

4.4.7 Processing Telephone Number De-Activations

As noted in Section 3.3 of these Guidelines, all service providers should process TN deactivation information and share Deactivation TN Lists. Receiving Deactivation Lists may require individual agreements among service providers to preserve confidentiality.

4.5 Spam and Anti-Abuse

4.5.1 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 4.1.

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).

4.5.2 Controls

To address increased spam risks associated with expanded SMS 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.

4.5.3 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.

4.5.4 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.

4.5.5 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.

4.5.6 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.

4.6 Protocols

There are various protocol types used in the industry for messaging application and for interfacing between different messaging entities.
Most commonly used are:

- SMPP (Logica)
  http://www.smsforum.net

- EMI/UCP (CMG)
  http://madism.org/~madcoder/tmp/EMI-UCP4.6.pdf

- SMS2000/OIS (Sema)
  http://www.kannel.org/download/1.4.0/userguide-1.4.0/userguide.html

- SNPP
  http://www.faqs.org/rfcs/rfc1861.html

Depending on the service providers' network infrastructure and technology a certain protocol might be preferred.

All participating carriers agreed for SMPP to be preferred protocol for the inter-carrier messaging service. SMPP version 3.4 should be supported as a minimum recommendation. Future versions of SMPP are allowed as long as they are backwards compatible to SMPP version 3.4.

4.7 Character set

Different network technologies and service centers might use different character sets. The ICV should be capable of matching one set to another to ensure a readable message.
The supported character sets are ASCII and GSM 7-bit (according to GSM 03.40). Carrier-originated messages can be sent in either of the character-sets. The terminating ICV reformats the message accordingly to match the supported character-set of the receiving carrier. Not supported characters should be presented as an underscore "_".

The table in Appendix C should be used for mapping ASCII to GSM 7-bit.

4.8 Message addressing

The destination and origination address is available in different formats depending on the carrier. Supported formats are 10-, 11-, or international E.164 format. To ensure correct routing and reply mechanisms the ICV on the terminating side should adapt the format accordingly.

4.9 Messages length / Concatenated messages

The maximum message length varies by the service provider network [and user device]. Segmentation might be necessary to adapt message length according to the networks' capabilities.
Each service provider can determine the format of a segmented message separately. It is recommended to append an identifier or order reference to the message.
The terminating entity is responsible to segment the incoming message if the terminating carrier is limited in message length. Concatenated messages on the originating side should be put into a single SMPP message by the originating entity.
The transmission of any message between an originating carrier and its ICV as well as between ICV's should always be done as one message.

4.10 Distribution list

In case the originating service provider supports distribution lists it is the responsibility of the originating entity to separate the originated message into individual messages with a single recipient.
In case of more than one ICV in the delivery chain, only messages that can be delivered from a specific ICV are allowed to be forwarded to that ICV, e.g. a message from AT&T to recipients in T-Mobile and Verizon has to be split up by AT&T's ICV if T-Mobile and Verizon aren't connected to the same ICV.

4.11 Validity period

The validity period for the inter-carrier messaging service should be at least 72 hours in the terminating SMSC. The validity period for all involved ICV's should be also at least 72 hours. The maximum validity period can be determined by each store and forward entity.

4.12 Reply address

The reply address of an incoming message should be automatically set to the originating address of the original message by the terminating ICV. The number format should be formatted according to the address formats specified in "Message Addressing"

4.13 Call Back number

The Call Back number feature, which allows the recipient to place a voice call to the originator of the message, varies by network and device, and therefore this feature is optional. Thus, if the originating carrier populates the specific parameter there is no recommendation for the terminating carrier to pass that information to the end user. The originating carrier might choose to include the call-back number as a part of the text message itself.

4.14 Binary Data or special User Data

The initial effort focuses on text messaging only. Therefore the originating entity is only allowed to send messages containing human readable text.

4.15 Priority

The priority feature is defined differently for most messaging services. Therefore a matching of the available levels has to be performed by the terminating ICV. Even if all priority levels might be allowed / possible on the originating network, there is no guarantee that it is supported on the terminating network. The formatting / matching of priority levels between the originating network and terminating network is the responsibility of the terminating entity.

4.16 Delete/Replace in SMSC

This feature, which allows the originator to replace or delete previously sent messages that haven't yet been delivered to the final destination, is not supported.

4.17 Delivery receipt / Error Messages / Status reports

If the same SMSC is not used for origination and termination, network implemented delivery and status reports may not be supportable by all carriers. Furthermore additional error messages must be supported and be capable of delivery to the end-user.

The high level recommendation for the inter-carrier messaging service is to ensure availability of an end-to-end delivery receipt mechanism, so that the originating subscriber and carrier can be informed when and if the message has been transmitted successfully to the receiving device. This includes the case where more than one ICV is involved in the delivery chain. Furthermore the delivery report might be required for billing purposes.

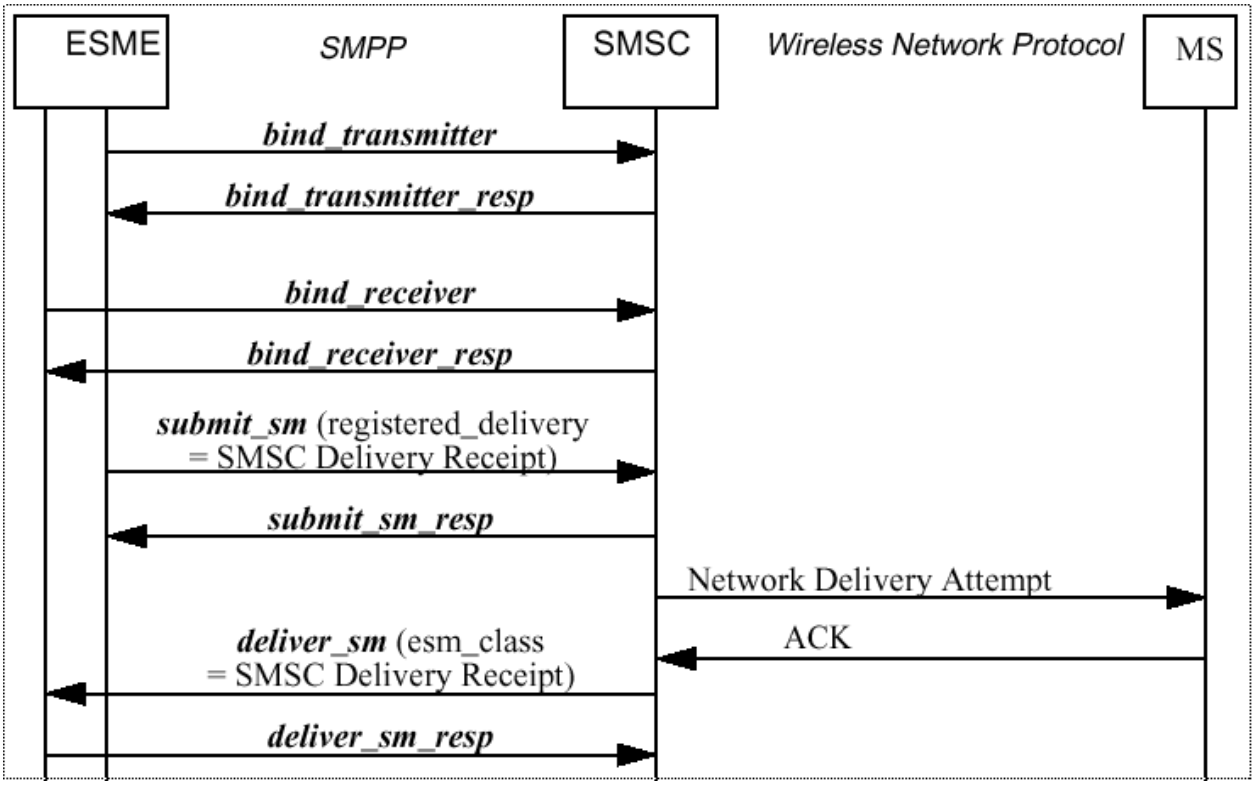
Different technical restrictions bring up some barriers for an end-to-end delivery receipt. Therefore the support for SMSC Delivery Receipt and SME Delivery Acknowledgment is optional for all involved service providers and ICVs.

The remaining part of the chapter describes the implementation of a delivery receipt on a general level.

4.18 General SMPP capabilities

The SMPP protocol specification describes the following scenarios:

In general, SMPP protocols support three message modes, of which two work with some kind of receipt (acknowledgement of final delivery). These are the “Store and Forward Message Mode” and the “Transaction Message Mode”. Both scenarios describe a mobile terminated message coming from the ESME being connected via SMPP to an SMSC.
It is assumed that only the “Store and Forward Message Mode” is used for the inter-carrier messaging service.



Typical SMPP sequence for a registered store and forward message (from SMPP 3.4, Version 1.2 page 31)

The standard doesn’t describe the carrier-originating scenario specifically and it might look different for different network types. It is basically the reverse path with differences in the delivery receipt handling (see example for GSM in T-Mobile’s section in Appendix A)

Furthermore three specific message types are defined for Delivery receipts, notifications and acknowledgements. Not all of them are supported on all network types or SMSC implementations.
See below for quote from SMPP specification 3.4, Version 1.2 pages 34/35

_____Start quote_____

SMPP Specification 3.4. – Message Types Quote

In addition to "normal" short messages, special messages can be transferred between ESME and the SMSC in a ***submit_sm, deliver_sm*** or a ***data_sm*** operation. The message type is defined in the *esm_class* parameter of the above SMPP operations.
The following message types are supported in SMPP:

SMSC Delivery Receipt
This message type is used to carry an SMSC delivery receipt. The SMSC, on detecting the final state of a registered message stored in the SMSC, should generate a receipt message addressed to the originator of the message. The SMSC Delivery Receipt is carried as the user data payload in the SMPP ***deliver_sm*** or ***data_sm*** operation.
The following fields are relevant in the ***deliver_sm*** and ***data_sm*** operations when used for transmitting delivery receipts.

- source address (i.e. *source_addr_ton, source_addr_npi, source_addr*)
  The source address will be taken from the destination address of the original short message which generated the delivery receipt.
- destination address (i.e. *dest_addr_ton, dest_addr_npi, destination_addr*)
- The destination address will be taken from the source address of the original short message which generated the delivery receipt.
- *esm_class*
- *message_state*
- *network_error_code*
- *receipted_message_id*

Intermediate Notification
An intermediate notification is a special form of message that the SMSC may send to an ESME for a device terminated message delivery. It provides an intermediate status of a message delivery attempt.
Typical uses are

- to provide a "memory capacity exceeded" notification to a Voice Mail System.
- to report the outcome of the first delivery attempt that has failed but the message is still held in the SMSC for further delivery attempts.

Support for Intermediate Notification functionality is specific to the SMSC implementation and the SMSC Service Provider and is beyond the scope of this specification.

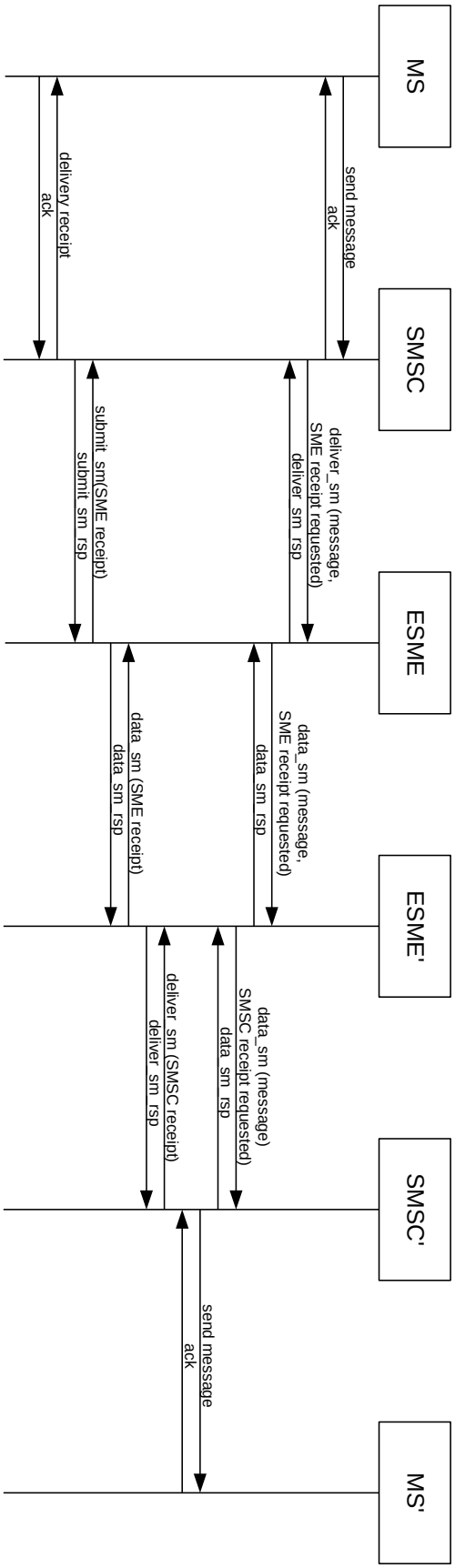
SME Delivery Acknowledgement
Despite its name, an SME Delivery Acknowledgement is not an indication that the short message has arrived at the SME, but rather an indication from the recipient SME that the user has read the short message. For a device-based SME, an SME Delivery Acknowledgement is sent when the user or device application has read the message from the SMS storage unit (e.g. SIM card).
Note: The SME Delivery Acknowledgement function may not be supported on all network types.

_____end quote_____

The request and delivery of a receipt, notification or acknowledgement is controlled with the parameters "esm_class", "registered_delivery" and contains additional information in the fields "network_error_code", "message_state" and "receipted_message_id".

Based on those features and commands an end-to-end delivery notification can be achieved. However this is contingent on all involved ESMEs and SMSCs supporting the request and generation of the SME Delivery Acknowledgement or SMSC Delivery receipts as well as the mapping of messages IDs between the different SMPP links by the ICV.

The figure on the next pages shows the general call flow based on SMPP for an originating to terminating service provider message via 2 ESMEs.


MS
SMSC
ESME
ESME'
SMSC'
MS'
send message
ack
delivery receipt
ack
deliver_sm (message,
SME receipt requested)
deliver_sm_rsp
submit_sm(SME receipt)
submit_sm_rsp
data_sm (message,
SME receipt requested)
data_sm_rsp
data_sm (SME receipt)
data_sm_rsp
data_sm (message)
SMSC receipt requested)
data_sm_rsp
deliver_sm (SMSC receipt)
deliver_sm_rsp
send message
ack

5 Interworking between inter-carrier 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 must be compliant with all terms of these guidelines.

5.2 Defining responsibilities via SLAs

In the case of more than one ICV being involved in the end-to-end delivery chain, it is desirable to define clear responsibilities for all involved parties to establish an efficient problem resolution process.

The delivery chain (with two ICVs) can be divided into 5 different areas.

1. Carrier-originated device to Carrier-originated SMSC
2. Carrier-originated SMSC to Originating Carrier ICV
3. Originating Carrier ICV to Terminating Carrier ICV
4. Terminating Carrier ICV to Terminating Carrier SMSC
5. Terminating Carrier SMSC to Terminating Carrier device

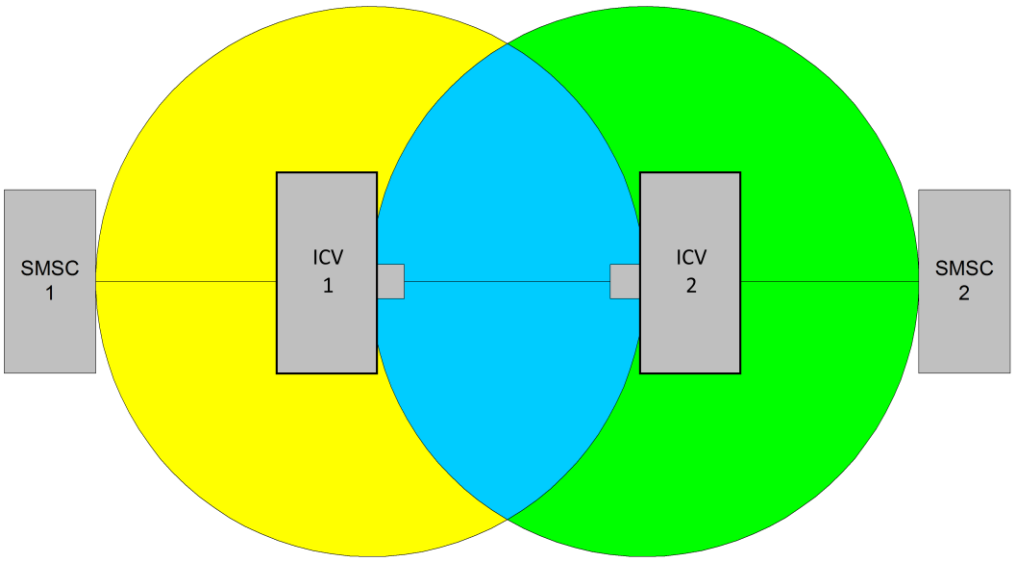
For illustrative purposes these delivery chains presents a carrier-to-carrier arrangement; however there are circumstances when service providers could be substituted to either end of the diagram.

Areas 1, 2, 4, 5 are fully in control by the originating and terminating carrier and their relationship to their ICV's. SLAs between them 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. Figure 5.1 depicts this relationship.

Figure 5.1

Circles depict extension of SLAs to include ICV-to-ICV Links



6 Interworking between carriers and service providers

6.1 Delivery of SMS to non-wireless and verified devices and applications.

While essentially 100% of CMRS handsets can receive and send SMS messages, the ability of non-CMRS TNs to receive or send SMS messages is still developing. This uncertainty around the SMS capabilities of non-CMRS devices and services potentially presents a problem when only a small number of SMS 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 SMS 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-SMS capable devices by some alternative means; or because it provides a simple implementation option.

Where no verification of the SMS 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.

6.2 Additional SLA Recommendations for ICVs

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

6.2.1 Compliance with Section 4 of these Guidelines

ICVs should insure that each non-CMRS provider meet or exceed all of the recommendations in Section 4 of the *Guidelines* and document how their non-CMRS customers meet these recommendations.

6.2.2 SPAM identification and containment

ICVs should monitor throughput using accepted anti-SPAM methods used for all P2P 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.

6.2.3 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 4.2.

6.2.4 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.

6.2.5 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.

6.2.6 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.)

6.2.7 Traffic differentiation

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

6.2.8 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.

7 Service Level Agreement

In addition to the recommendations in this document, a service provider may opt to establish Service Level Agreements (SLA) with another service provider / ICV. Each 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 carrier.

8 Testing

In order to maintain a certain service level for the end-to-end service testing should be completed whenever a new service provider joins the inter-carrier messaging community. Each carrier/ICV should be responsible for their testing. The testing of each new carrier should include end-to-end testing to the other carriers as well as internal tests on the system level between the carrier and his ICV.

In general, each service provider is responsible for level 1 and 2 testing as well as troubleshooting together with its ICV. Any remaining issues have to be resolved by the "new" carrier with the terminating carrier and the involved ICVs.

Testing results or problem solutions that might affect QOS and thus be valuable to other carriers or ICV's should be disclosed to interested service providers. Each service provider, working with their selected ICV, is responsible for determining which test results or problem solutions will be disclosed.

9 Appendix A: Supported Features on A interfaces

This section lists each carriers supported feature-set as it was provided by the carrier.

9.1 AT&T

Note : This table applies to SMPP formats, encoding, and parameters for traffic between ICVs. Connections to non-ESMEs may have different capabilities.

Item	Subject	GSM Supports
1	Message Type	Text only
2	Subscribers Provisioned for 2 Way	Customers may opt out of SMS
3	Handsets Support 2 Way	All handsets support 2 way messaging
	SMPP Version	3.4
	SMPP PDUs allowed	Submit_sm, deliver_sm, bind_transmitter, bind_receiver, enquire_link and responses
4	SMSC Provided by	Multiple vendors
5	Character Set	ISO 8859-1 (Latin1) for ICV/ESMEs. SMSC maps to 7 bit GSM + extension characters. UCS2 is allowed and passed through to the Device. Mapping provided on request.
6	Message Header	Not supported
7	Message Length	160 7 bit characters or 70 USC2 characters
8	Concatenated Messages	Not supported
9	Addressing Convention for Mobile to Mobile	11 & E164 digit address for MO & MT
10	Validity Period	5 minutes up to 3 days
11	Message Indicators for Message Types	Not supported
12	Delete/Replace in SMSC	Not supported
13	Short Message Urgent Flag and Auto Display	Not supported
14	Error Message	Not supported
15	Differing Error Messages on SMSC	SMSC will return temporary or permanent errors to ICV in the submit_sm_resp
16	SMSC Status Reports	Not supported.
17	Confirmation Delivery	Not supported.
18	Reply Service	A reply to an incoming message is automatically addressed to the Originating address of the initial message. No user input is necessary.
19	Allow for Callbacks	Optional parameters are not allowed from ICVs, so the callback_num is stripped. Most handsets provide an option to call the originator.
20	User Data (UD, UDH, UDHI)	Not supported
21	Group Distribution List	Not supportedl
22	Distribution lists within SMSC	Not Supported
23	Priority Delivery - queuing	Not supported
24	Deferred Delivery	Not supported
25	Message Throttling	MT throttling rates are negotiated with ICV. No MO throttling.
26	Spamming	Currently controlled for Wireless e-mail
27	Black/White List	Supported if AT&T destination is Smart Limits subscriber.

9.2 Leap

See feature table

9.3 Sprint Nextel

9.3.1 Handset Capabilities

All existing handsets support 2-way SMS.

9.3.2 Subscriber Capabilities

90+% of Sprint Nextel subscribers are 2-way messaging capable.

9.3.3 Preferred Interface

Sprint follows 3GPP SMS messaging standards. Preferred interface is SMPP.

9.3.4 Character Set

Sprint Nextel supports the ASCII character set as a set of emoticons. Sprint Nextel is willing to translate all icons into ASCII as needed, including 7 bit ASCII, 8 bit Latin, and 16 bit UCS.

9.3.5 Message Length

Sprint Nextel's SMS text messaging product has a 160 character limit at this time. Most of the devices support up to 1000 characters with some legacy devices supporting 160 characters.

9.3.6 Concatenated Messages

Is not an issue given the 1000 character limit. Sprint does support on outbound but not widely on the inbound messages. Currently have a small amount of devices launching shortly that will support on inbound.

9.3.7 Distribution Lists

Sprint Nextel will support messages being sent to multiple recipients; however they will be originated as separate messages.

9.3.8 Validity

Messages are retried for 72 hours. 100 messages can be held for retry for 72 hours.

9.3.9 Message priority features

Sprint Nextel does not support message priority at this time. Some handsets support but Sprint does not support in the network.

9.3.10 Reply Path

A reply to an incoming message is automatically addressed to the originating address of the initial message. No user input is necessary.

9.4 US Cellular

See feature table in appendix

9.5 Verizon Wireless

1. Delivery Receipts
   The delivery receipt feature allows customers to keep track of when a message is successfully delivered to the recipient.
   Refer section 2.11 in SMPP 3.4 for delivery receipts
2. Supported Character Set in SMS and EMS
   a. 7-bit ASCII
   b. IA5 Character Set
   c. Latin 1 (ISO-8859-1)
   d. GSM 7-bit (Refer to 3G TS 23.038 V.3.0 (2000-01) for GSM Character Alphabets and Language)
   e. GSM 8-bit (Refer to 3gpp TS 23.038 and 23.040)
   f. Unicode/UCS-2 (16 bit). This feature allows customers to send/receive multilingual messages.

   The messages will be garbled on the handset for all other Character Sets
3. SMS: Max Message length of 140 bytes
4. Enhanced Messaging Service (EMS)
   a. Handset can send a text message of at least 7 segments
   b. Handset can receive a text message of at least 20 segments
5. Priority: Normal and Urgent (refer the section 4.5.9 in SMPP 3.4). Other categories are not supported
6. Deferred delivery up to 5 days
7. Support 10 digit Mobile telephone number addressing only
8. Support Call Back number - used as number to call back
9. Messages to multiple destinations. All group text messages sent as MMS.
   - Handsets support sending messages up to 20 destinations

9.6 T-Mobile USA

9.6.1 Handset capabilities:

All existing T-Mobile handsets do support full 2-way messaging based on the GSM standard 03.40. Depending on the handset manufacturer the user interface and options might vary slightly, but usually go along GSM 03.40 as well.

9.6.2 Subscriber capabilities

100% of existing T-Mobile subscribers is provisioned for 2-way messaging.

9.6.3 SMSC vendor / preferred interface

The SMSC (Short Message Service Center) is provided by CMG. Today the preferred interface to an ICV is SMPP Version 3.4. T-Mobile sees some value in going towards an SS7-based implementation in the future.

9.6.4 Message addressing

The three following addressing schemes are supported: 10-digit, 11-digit, international E.164 format. The destination address can be entered either as 425 444 2835, 1 425 444 2835 or +1 425 444 2835. The originating address is usually displayed in international E.164 format.

9.6.5 Character Set:

T-Mobile uses the standard GSM 7-bit character set according to GSM 03.38. Below the GSM character table and extension table is shown.

Start: From GMS 03.38 (Version 7.2.0, chapter 6.2.1)

Character table:

				b7	0	0	0	0	1	1	1	1
				b6	0	0	1	1	0	0	1	1
				b5	0	1	0	1	0	1	0	1
b4	b3	b2	b1		0	1	2	3	4	5	6	7
0	0	0	0	0	@	Δ	SP	0	¡	P	¿	p
0	0	0	1	1	£	_	!	1	A	Q	a	q
0	0	1	0	2	$	Φ	"	2	B	R	b	r
0	0	1	1	3	¥	Γ	#	3	C	S	c	s
0	1	0	0	4	è	Λ	¤	4	D	T	d	t
0	1	0	1	5	é	Ω	%	5	E	U	e	u
0	1	1	0	6	ù	Π	&	6	F	V	f	v
0	1	1	1	7	ì	Ψ	'	7	G	W	g	w
1	0	0	0	8	ò	Σ	(	8	H	X	h	x
1	0	0	1	9	Ç	Θ	)	9	I	Y	i	y
1	0	1	0	10	LF	Ξ	*	:	J	Z	j	z
1	0	1	1	11	Ø	1)	+	;	K	Ä	k	ä

1	1	0	0	12	ø	Æ	,	<	L	Ö	l	ö
1	1	0	1	13	CR	æ	-	=	M	Ñ	m	ñ
1	1	1	0	14	Å	ß	.	>	N	Ü	n	ü
1	1	1	1	15	å	É	/	?	O	§	o	à

1) This code is an escape to an extension of the 7 bit default alphabet table. A receiving entity which does not understand the meaning of this escape mechanism should display it as a space character.

GSM 7bit default alphabet extension table

				b7	0	0	0	0	1	1	1	1
				b6	0	0	1	1	0	0	1	1
				b5	0	1	0	1	0	1	0	1
B4	b3	b2	b1		0	1	2	3	4	5	6	7
0	0	0	0	0					|			
0	0	0	1	1								
0	0	1	0	2								
0	0	1	1	3								
0	1	0	0	4		^						
0	1	0	1	5							2)	
0	1	1	0	6								
0	1	1	1	7								
1	0	0	0	8			{					
1	0	0	1	9			}					
1	0	1	0	10	3)							
1	0	1	1	11		1)						
1	1	0	0	12				[				
1	1	0	1	13				~				
1	1	1	0	14				]				
1	1	1	1	15			\					

In the event that an MS receives a code where a symbol is not represented in the above table then the MS should display the character shown in the main default 7 bit alphabet table in section 6.2.1

1) This code value is reserved for the extension to another extension table. On receipt of this code, a receiving entity should display a space until another extension table is defined.

2) This code represents the EURO currency symbol. The code value is that used for the character ‘e’. Therefore a receiving entity which is incapable of displaying the EURO currency symbol will display the character ‘e’ instead.

3) This code is defined as a Page Break character and may be used for example in compressed CBS messages. Any mobile which does not understand the 7 bit default alphabet table extension mechanism will treat this character as Line Feed

End: From GMS 03.38 (Version 7.2.0, chapter 6.2.1)

9.6.6 Message length

A single Short Message in GSM is limited to 140 bytes of user data translating to 160 characters based on a 7-bit character set. Different service indicator bits allow to include binary data or extended header information within the user data field. See below for more information.

9.6.7 Concatenated messages

The GSM 03.40 standard in general allows up to 255 messages with 153 characters each. However this feature is handset dependent. Only handset supporting concatenated messages are able to send longer messages and also display them correctly on the receiving end. If a concatenated message is sent to a non-supporting phone, the user will see 3 cryptic characters in front of each single message part.

9.6.8 Distribution list

In general distribution list are supported by the SMSC. Messages to multiple recipients however would be originated as separate messages

9.6.9 Validity Period

The relating field can contain a validity period ranging from 5 minute to a maximum of 63 weeks according to the standards. T-Mobile however limits the range from 1 hour to 168 hours with a default of 72 hours.

9.6.10 Message priority features

Class 0 / Auto Display message allows forcing the message to be displayed on the handset screen upon arrival. No user interaction is required. The message is not stored on the phone/SIM card.
Priority messages will be attempted to deliver irrespective of whether or not the handset has been identified as temporarily absent or having no free memory capacity.
SMSC priority allows moving a message to the top of the queue for a particular subscriber in case there are other messages stored in the SMSC waiting for delivery.

9.6.11 Reply Path

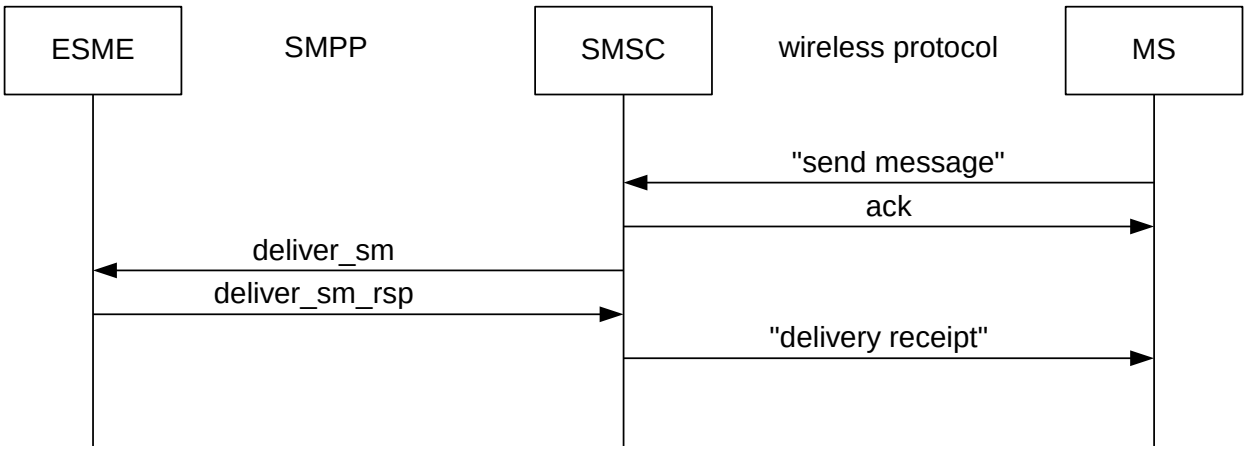
A reply to an incoming message is automatically addressed to the originating address of the initial message. No user input is necessary.
Furthermore according to GSM specification a handset is allowed to indicate in a MO message that the recipient may use the originators SMSC for his reply message.
This feature wouldn’t work for inter carrier messaging.

9.6.12 Message types

The message header includes flags for different types of messages (e.g. voicemail, notifications/receipts, and binary data). Depending on those flags the message might get treated differently in the MS. Even more advanced messaging features can be included by extending the message header to the user data field and indicating that within the message header. Some proprietary implementations as well as EMS (enhanced messaging service) standards make use of that feature.

9.6.13 Status report / delivery receipt

In case of a GSM MO to GSM MT message there is a full end-to-end delivery report available.
As soon as the message gets delivered to the receiving handsets a delivery receipt is generated (if requested) and sent back to the origination handset.
In case of a message being delivered to an ESME (external short message entity) this receipt gets generated as soon as the ESME has acknowledged the message with the submit_sm_rsp reply, even if that doesn't mean that the message has been delivered to the final destination.
Below is an example of the call/signaling flow for the GSM case.



In case the receiving entity (MS or EMSE) is not reachable the message gets stored in the SMSC and a status report with error code/reason is issued to the originating MS. Once the validity period is reached and the message couldn't be delivered in the meantime it gets deleted and a new status report with error code/reason is sent to the originating MS.

9.6.14 Deferred delivery

Based on SMSC functionality a message delivery can be scheduled to happen at a certain time or with a certain delay. It would get stored in the meantime in the SMSC.

10 Appendix B: Feature Table

	AT&T (GSM)	Leap	Sprint	Nextel	Verizon Wireless	T-Mobile	US Cellular CDMA	US Cellular TDMA
2-way handsets (in %)	100	95%	100 (via wireless web)			100	10	50
2-way subscribers	100	95%	90 + (via wireless web)			100	confidential	confidential
SMSC	multiple vendors	Schlumberger Sema				CMG	ADC	Logica
SMPP	yes 3.4	yes 3.4	yes			yes	yes	yes
Addressing	11, E164	10, 11,E164		number@messaging.nextel.com	10	10,11,E164	10,11,E164	10,11,E164
Character set	7-bit GSM, 8-bit GSM UCS2 supported	7-bit ASCII, 8-bit ASCII	ASCII, emoticons		7-bit ASCII	7-bit GSM	7-bit ASCII	7-bit ASCII
Message length	160	160	1000	500	160	160	150	150
Concatenated message	no	no	N/A			yes, depending onhandset	No	No
Distribution list	no	yes	yes, will be sent as separate message			yes, will be sent as different messages	No	No
Validity period	yes, 5 min minimum to 72 hours maximum	variable, 5 minutes to 7 days	72 hours	7days	absolute and realitve up to 5 days	variable, 1-168 hours, default 72 hours	7 days	7 days
Priorities	no	bulk, normal, urgent, very urgent	no		normal, urgent	Auto Display, move to top of queue	Urgent, normal	Urgent, normal
Reply (subscriber DA)	yes	yes	yes		yes, OOA	yes, E164	yes	yes
Call back	not supported	yes			yes	yes	yes	yes
Delivery reciept	not supported	yes (status/delivery)		yes (status/delivery)	yes	yes (status/delivery), if requested and supported by handset)	Yes	Yes
Deferred delivery	no	no			yes up to five days	yes	No	No
Message types	text only	custom text message, voice mail notification						
Delete/replace in SMSC	not supported (not on user level)	yes		canned message	message cancelation		No	No

11 Appendix C: ASCII/GSM character set mapping table

exact match
proposed alternative
no close match

In GSM the ESC character is used to give access to the extension table. In order to avoid any misinterpretation the ESC character in ASCII should be mapped to a "_" instead of the ESC character in GSM. In the case of mapping from GSM to ASCII the ICV has to detect the ESC sequence an replace the whole sequence with the matching character in ASCII.

GSM to ASCII

GSM	Character	ASCII (7-bit)	proposed Character	Mapped ASCII
0	@	64	@	64
1	£		L	76
2	$	36	$	36
3	¥		Y	89
4	è		e	101
5	é		e	101
6	ù		u	117
7	ì		i	105
8	ò		o	111
9	Ç		C	67
10	LF	10	LF	10
11	Ø		O	79
12	ø		o	111
13	CR	13	CR	13
14	Å		A	65
15	å		a	97
16	□		_	95
17	_	95	_	95
18	□		_	95
19	□		_	95
20	□		_	95
21	□		_	95

ASCII to GSM

ASCII	Character	proposed Character	Mapped GSM
0	NUL	_	17
1	SOH	_	17
2	STX	_	17
3	ETX	_	17
4	EOT	_	17
5	ENQ	_	17
6	ACK	_	17
7	BEL	_	17
8	BS	_	17
9	HT	SP	32
10	LF	LF	10
11	VT	_	17
12	FF	page brk	E10
13	CR	CR	13
14	SO	_	17
15	SI	_	17
16	DLW	_	17
17	DC1	_	17
18	DC2	_	17
19	DC3	_	17
20	DC4	_	17
21	NAK	_	17

22	□		_	95	22	SYN	_	17
23	□		_	95	23	ETB	_	17
24	□		_	95	24	CAN	_	17
25	□		_	95	25	EM	_	17
26	□		_	95	26	SUB	_	17
27	ESC	indicates use of GSM extension table			27	ESC	_	17
28	Æ		A	65	28	FS	_	17
29	æ		a	97	29	GS	_	17
30	ß		s	115	30	RS	_	17
31	É		E	69	31	US	_	17
32	SP	32	SP	32	32	SP	SP	32
33	!	33	!	33	33	!	!	33
34	"	34	"	34	34	"	"	34
35	#	35	#	35	35	#	#	35
36	¤		_	95	36	$	$	2
37	%	37	%	37	37	%	%	37
38	&	38	&	38	38	&	&	38
39	'	39	'	39	39	'	'	39
40	(	40	(	40	40	(	(	40
41	)	41	)	41	41	)	)	41
42	*	42	*	42	42	*	*	42
43	+	43	+	43	43	+	+	43
44	,	44	,	44	44	,	,	44
45	-	45	-	45	45	-	-	45
46	.	46	.	46	46	.	.	46
47	/	47	/	47	47	/	/	47
48	0	48	0	48	48	0	0	48
49	1	49	1	49	49	1	1	49
50	2	50	2	50	50	2	2	50
51	3	51	3	51	51	3	3	51
52	4	52	4	52	52	4	4	52
53	5	53	5	53	53	5	5	53
54	6	54	6	54	54	6	6	54
55	7	55	7	55	55	7	7	55
56	8	56	8	56	56	8	8	56
57	9	57	9	57	57	9	9	57
58	:	58	:	58	58	:	:	58
59	;	59	;	59	59	;	;	59
60	<	60	<	60	60	<	<	60

61	=	61	=	61	61	=	=	61
62	>	62	>	62	62	>	>	62
63	?	63	?	63	63	?	?	63
64	¡		!	33	64	@	@	0
65	A	65	A	65	65	A	A	65
66	B	66	B	66	66	B	B	66
67	C	67	C	67	67	C	C	67
68	D	68	D	68	68	D	D	68
69	E	69	E	69	69	E	E	69
70	F	70	F	70	70	F	F	70
71	G	71	G	71	71	G	G	71
72	H	72	H	72	72	H	H	72
73	I	73	I	73	73	I	I	73
74	J	74	J	74	74	J	J	74
75	K	75	K	75	75	K	K	75
76	L	76	L	76	76	L	L	76
77	M	77	M	77	77	M	M	77
78	N	78	N	78	78	N	N	78
79	O	79	O	79	79	O	O	79
80	P	80	P	80	80	P	P	80
81	Q	81	Q	81	81	Q	Q	81
82	R	82	R	82	82	R	R	82
83	S	83	S	83	83	S	S	83
84	T	84	T	84	84	T	T	84
85	U	85	U	85	85	U	U	85
86	V	86	V	86	86	V	V	86
87	W	87	W	87	87	W	W	87
88	X	88	X	88	88	X	X	88
89	Y	89	Y	89	89	Y	Y	89
90	Z	90	Z	90	90	Z	Z	90
91	Ä		A	65	91	[	[	E60
92	Ö		O	79	92	\	\	E47
93	Ñ		N	78	93	]	]	E62
94	Ü		U	85	94	^	^	E20
95	§		_	95	95	_	_	17
96	¿		?	63	96	`	'	39
97	a	97	a	97	97	a	a	97
98	b	98	b	98	98	b	b	98
99	c	99	c	99	99	c	c	99

100	d	100	d	100	100	d	d	100
101	e	101	e	101	101	e	e	101
102	f	102	f	102	102	f	f	102
103	g	103	g	103	103	g	g	103
104	h	104	h	104	104	h	h	104
105	i	105	i	105	105	i	i	105
106	j	106	j	106	106	j	j	106
107	k	107	k	107	107	k	k	107
108	l	108	l	108	108	l	l	108
109	m	109	m	109	109	m	m	109
110	n	110	n	110	110	n	n	110
111	o	111	o	111	111	o	o	111
112	p	112	p	112	112	p	p	112
113	q	113	q	113	113	q	q	113
114	r	114	r	114	114	r	r	114
115	s	115	s	115	115	s	s	115
116	t	116	t	116	116	t	t	116
117	u	117	u	117	117	u	u	117
118	v	118	v	118	118	v	v	118
119	w	119	w	119	119	w	w	119
120	x	120	x	120	120	x	x	120
121	y	121	y	121	121	y	y	121
122	z	122	z	122	122	z	z	122
123	ä		a	97	123	{	{	E40
124	ö		o	111	124	|	|	E64
125	ñ		n	110	125	}	}	E41
126	ü		u	117	126	~	~	E61
127	à		a	97	127	DEL	_	17
Ext. tbl								
E10	Pg brk		FF	12				
E20	^	94	^	94				
E40	{	123	{	123				
E41	}	125	}	125				
E47	\	92	\	92				
E60	[	91	[	91				
E61	~	126	~	126				
E62	]	93	]	93				
E64	|	124	|	124				
E165	Є		e	101				

12 Abbreviations and Definitions

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
CTM – Custom Text Message
ESME – External Short Message Entity
GSM – Global Standard for Mobile Communication
ICV – Inter Carrier Vendor – vendors providing connectivity between wireless subscribers, networks, and services. For clarity and continuity, the historical term "***Carrier"*** is used, but ICVs provide their services to all service providers.
MIN – Mobile Identification Number
MO – Mobile Originated
MS – Mobile Station
MSISDN – Mobile Station ISDN 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
SMPP – Short Message Peer-to-Peer Protocol
SMS – Short Message Service
SMSC – Short Message Service Center
TDMA – Time Division Multiple Access
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