OPEN CONNECTIVTY SMS HUBBING ARCHITECTURE

2.0

26 February 2009

This is a non-binding permanent reference document of the GSM Association.

Security Classification Category (see next page)	
Unrestricted	

Security Information - UNRESTRICTED

Copyright Notice

Document History

Version	Date	Brief Description
0.1	26 July 2006	Rev1 version. MNP is only defined for SS7, and not for SMPP, and remains an optional item for the SMS Hubbing Trial.
0.2	26 July 2006	MNP is now defined more completely. Roaming for SS7 remains an issue.
0.3	2 August 2006	Final architecture for SMSHTI Trial presented in SMSHTI5
0.4	31 August 2006	Mostly clarification changes. First revision since baseline at SMSHTI5. This version was approved at SMSHTI#6 31 August 2006.
0.5	11 September 2006	The revisions are mainly from discussions results of SMSHTI6 including MNP now part of the defined architecture, and contributions from Tyntec.
0.6	19 October 2006	Main changes are to include roaming and deliver reporting in inter-standard inter-working case.
0.7	22 December 2006	A number of changes made primarily on MAP private extensions, error mapping and MAP version negotiation
1.0	09 March 2007	First IREG approved PRD release
2.0	26 February 2009	Change of security classification to unrestricted
Changes Since Last Version 1. Change of security classification to unrestricted 2. Change in company name of editor		

Other Information

Type	Description
Document Owner	IREG
Revision Control	To be determined as required
Document editor/company	Paolo Villaflores, SMART Communications, Inc.

Feedback

This document is intended for use by the members of GSMA and in particular those involved in Open Connectivity based SMS Hubbing. It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at mailto:prd@gsm.org. Your comments or suggestions are always welcome.

Table of Contents

1 OVERVIEW

1.1 Audience

This document is targeted at the following audiences:

- Hub providers who will participate in GSMA Open Connectivity SMS Hubbing
- Client Operators who will participate in GSMA Open Connectivity SMS Hubbing

1.2 References

1.2.1 Normative References

The following are referenced in the body of the text in this permanent reference document (PRD):

[1] 3GPP TS 23.40: “Technical realization of the Short Message Service (SMS) Point-to-Point (PP)”, Version 6.7.0 or higher
[2] 3GPP TS 29.002: “Mobile Application Part (MAP) specification”, Version 7.4.0 or higher
[3] 3GPP TS 123.066: “Universal Mobile Telecommunications System (UMTS); Support of GSM Mobile Number Portability (MNP)”, Version 6.0.0 or higher
[4] IR.70: “SMS SS7 Fraud”, Version 3.1 or higher
[5] IR.71: “SMS SS7 Fraud Prevention”, Version 3.1 or higher
[6] AA.50: “SMS Fraud Criteria”, Version 3.1 or higher
[7] AA.19: “Addendum to the International GSM Roaming Agreement: SMS Interworking Agreement”, Version 11.0 or higher
[8] AA.71: “Agreement for International SMS Hubbing Services”
[9] OC 6_004 and 8_004: “High Level Requirements for Open Connectivity”
[10] “Short Message Peer to Peer”, Version 3.4, dated 12-Oct-1999 Issue 1.2
[11] “Short Message Peer to Peer”, Version 5.0
[12] 3GPP TR 23.840: “3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Study into routeing of MT-SMs via the HPLMN”, Version 1.0.0 or higher
[13] IR.67: “DNS Guidelines for Operators”, Version 1.3 (9 August 2006) or higher
[14] RFC 4355: “IANA Registration for Enumservices email, fax, mms, ems, and sms”

2 GLOSSARY OF TERMS

The following terms are used in this document:

Term	Definition
Fraud	Technical methods to fraudulently send SMS traffic to an operator (defined in GSMA PRD IR.71 [4])
FSM or MT_FSM	SS7 MAP Forward short message for SMS MT
GT	(SS7) Global Title

IO-MMS	Inter-Operator MMS
IO-SMS	Inter-Operator SMS
IP	Internet Protocol
IREG	International Roaming Expert Group (GSMA)
IWG	Inter-Working Group (GSMA)
MAP	Mobile Application Part: MAP is a protocol that typically runs on top of the SS7 protocol. It is associated with non-call signalling and designed to support (in a distributed environment) interactive mobile applications such as short messaging, paging, etc…
MNO	Mobile Network Operator
MNP	Mobile Number Portability
MNP DB	Mobile Number Portability Database
MS	Mobile Station.
OC Project	Open Connectivity Project
RN	Stands for Routing Number which is used in SS7 MNP. An RN is utilized to route an SRI from MNO2 to MNO3.
SM	Short Message
SM-MO	Defined by 3GPP as a message submitted by an MS to an SMSC.
SM-MT	Defined by 3GPP as a message delivered by an SMSC to an MS.
SMS	Short Message Service
SMSC	Short Message Service Centre: function responsible for the relaying and store and forwarding of a short message.
Solution Provider	For SMS Inter-working this refers to the provider of the SMS Hubbing service.
Spam	Unsolicited SMS traffic sent to an operator, using fraudulent or genuine methods
SRI or SRI-SM	Send Routing Information for SM
SS7	Signalling System 7
TADIG	Transferred Account Data Interchange Group (GSMA)
TCP/IP	Transport Control Protocol over IP

3 GSMA ANTI-TRUST COMPLIANCE

All work on the Open Connectivity project will be carried out STRICTLY in accordance to the GSMA Anti-Trust Compliance policy. All individuals contributing to the project must familiarise themselves with this policy before commencing on the project.

The GSMA Anti-trust compliance manual can be found at the following location:

https://infocentre.gsm.org/cgi-bin/securenonprddownload.cgi/gsma_compliance_manual_ic_120095.doc?120095&doc

4 BACKGROUND

The OC project completed an open SMS Hubbing proof of concept in February 2006 where two hub providers interconnected to enable delivery of SMS between networks.

The OC Project also has successfully completed a full-scale Open SMS Hubbing trial involving more major Client Operators and hub providers. The trial had a wider scope than the proof-of-concept, namely:

- It included all hubs and all regions (NA, Europe, Africa and Asia)
- It tested whether all OC high level requirements are feasible and can be met by participants

The IREG and IWG GSMA working groups have also contributed to the trials by generating documentation to enable SMS Hubbing to co-exist with bi-lateral solutions:

- SMS Hubbing Agreement Template
- SMS Hubbing Testing Recommendations
- SMS Hubbing Handbook

Now that the trials are complete, it is expected that operators and hub providers are looking into preparations leading up to actual implementations.

4.1 Current Situation and the Problem

Roaming and Inter-working are at the core of the GSM success story. 3GSM subscribers now expect to access the same set of services at home and abroad. They expect to be able to share all 3GSM services with any other subscriber on any network.

The bi-lateral relationship on which this success has been based, however, is now becoming a limiting factor to future success. With over 600 operator members of the GSMA, diversification of services and an increasing number of access technologies, it is unlikely that the current paradigm of bilateral relationships between networks will meet the expectations of operators going forward.

The overall cost of establishing bi-lateral relationships is preventing some operators from opening new roaming and Inter-working agreements. Often when a new roaming relationship is taken individually, the venture represents insufficient additional value for an operator that is already established with other roaming partners in the region or when the volume potential is low. With the introduction of more new services the problem will become more evident and the overall costs greater.

This is a particular concern for the newer GSM networks—those networks that are late entries into the market and finding it difficult to set-up roaming relations with the more established operators.

At the same time, the problem is arising for many established operators who already have voice roaming open but are facing low return on investment for new 2.5/3G roaming relationships and SMS Inter-working ventures.

This document derives from the Open Connectivity Project of the GSMA.

Open Connectivity is defined as the following:

- For all roaming services, to ensure that an operator is able to allow its customers to roam on the network of any other GSMA member.
- For Inter-working, in the short-term to ensure that the customers of all 3GSM networks can send and receive services between themselves. In the long-term to ensure that the customers of all 3GSM networks can send and receive services between themselves and customers of non-GSM networks.

Open Connectivity is needed so that:

- For Inter-working full global coverage is achieved to enable end-customer satisfaction
- For roaming the continued growth of GSM is ensured and all GSMA members can access the full advantages of 3GSM Roaming
- Operators can optimise costs involved in establishing and maintaining roaming & Inter-working agreements

The aim of the document is to publish the SMS Hubbing architecture seen as essential for a successful Open Connectivity solution for SMS inter-working.

5 DOCUMENT SCOPE

This document describes specific aspects of the technical architecture that has been used to conduct the SMS hubbing trials during September 2006, and shall also guide post-trial SMS Hub commercial implementations.

The document establishes the technical requirements for participating hubs and then details the following SMS hubbing scenarios:

- SMS inter-working using SS7 hubbing
- SMS inter-working using IP hubbing
- SMS inter-working using Hybrid (SS7/IP) hubbing

5.1 Out of Scope

- This document currently does not cover scenarios in which the Client Operator is not a GSM operator.
- Although the GSMA recognizes that some operators connect to hubs using different IP-based protocols, this document does not cover IP-based protocols other than SMPP over TCP/IP.

6 APPROACH

6.1 Use of SS7 or IP-based connectivity

The GSMA does not recommend the use of a particular technology. MAP over SS7 offers advantages in terms of reliable delivery reporting, whereas SMPP over IP offers cost benefits. This document covers the use of both technologies in all SS7, all IP and in hybrid environments.

Hubs shall support as a minimum, both pure SS7 (or SS7 over IP via SIGTRAN) and SMPP over IP as detailed in this hubbing architecture document. In cases where the originating and destination Client Operator have the same SMS protocol, the intermediate hubs shall carry the transaction end-to-end using the same original protocol. In cases where there is a need to convert because the destination protocol is different, such a conversion shall be carried out at the last possible point by the destination hub in its interface to the destination Client Operator. At this point, hubs may be required to perform character conversion or message segmentation, or other processing, as necessitated by the interface to their attached Client Operator. For instance, it may be necessary for the destination hub to break up the message should the length of the original message exceed the maximum length dictated by the data coding scheme utilized by the destination Client Operator's SMS protocol. Hubs should not need to perform any aggregation of messages, however.

Operators may opt to consider the use of other SMS messaging protocols in their private interface with the hub (such as UCP instead of SMPP), and this is alright, as long as the OC High Level Requirements are not violated in any way. The minimum baseline and what is expected to be common to all nodes in the hub network however remains only SS7 and SMPP. In the case where it is necessary to choose between SS7 or SMPP because the originating interface is something else (e.g. UCP), then the choice shall be made based on whether the original protocol is using cascaded signaling or store-and-forward method. The cascaded signalling method maps to SS7 and store-and-forward maps to SMPP.

6.2 Technical Implementation Guidelines for Operators

Operators looking at getting into SMS Hubbing should find it easy to get into SMS Hubbing. That is the main objective of this document. This document sets out the technical requirements on hubs so that the hub network functions smoothly for the benefit of the operator.

Hubs shall provide appropriate guidance to prospective operator clients, and this document shall be among those essential documents that will form baseline reference in any initial implementation and configuration discussion. Hubs shall also provide sufficient primer material and resources in order to prepare and orient operators for SMS Hubbing.

This architecture document has been deliberately designed with the objective of minimizing the impact on operators as much as possible, in terms of the transition to hubbing. Where there are impact considerations to make, these have been summarized in section 7.13.

Upon implementation, it is recommended that the operator and hub walk-through the requirement and architecture items discussed within this document in order to confirm that all applicable specifications are properly applied.

This document goes into details of the solution approach for Open Connectivity-based SMS Hubbing, and provides guidance on alternative methods or options where multiple solution approaches apply.

Further detail can also be found in the several other referenced specifications. If there are discrepancies between the description of the services in this document and the referenced specifications, what is stated in the referenced specifications shall prevail.

6.2.1 Connectivity to the Hub

6.2.1.1 Type of Connectivity

A Client Operator can choose to connect to the OC-SMS Hubbing Solution Provider using either SS7 MAP-based interface or IP-based SMPP interface. Operator must determine which of the connectivity methods is chosen for implementation. Typically, the capabilities of the Operator’s network nodes will determine this choice. The level of performance of the connectivity between the Client Operator and the Hubbing Solution Provider shall be covered by an SLA, relevant to said connectivity.

6.2.1.2 Dimensioning of Connectivity

Appropriate capacity and performance engineering must be carried out to dimension the connections in respect of both SS7-based and IP-based connectivity.

6.2.1.3 Basic Testing of Connectivity

Basic testing must be performed at Physical, Data link and Network (MTP3) layers to verify/validate the quality and performance of the connectivity between Client Operator and Solution Provider. This basic testing will ensure that Operator is able to exchange data at network level with the Solution Provider.

6.2.2 SMS Hubbing Information

The Client Operator would be required to provide both the technical information (network-level and product/system-level) as well as administrative information to the SMS Hubbing Solution Provider. The Client Operator must establish suitable interface mechanisms to either notify the Solution Provider or to provision/configure such information themselves in a secured, automated way. The Client Operator should provide the following information to the Hub:

6.2.2.1 Operator Contact Information

This would include the following information:

- Company/Operator Name
- Company/Operator Address
- Company/Operator Time Zone
- Complete contact details for multiple Business Contacts, SMS Technical Contacts, SMSC Vendor Technical Contacts

6.2.2.2 Operator Profile Information

This would include the following information:

- Primary Hub Selected
- Secondary Hub Selected (if any, in case of multiple Hubs used by the Operator)
- Technology Environment (GSM/CDMA/TDMA/iDEN)
- MCC-MNC
- Type of Connectivity (SS7 or SMPP)
- MNP Applicable or Not
    - If yes, type of MNP implementation (Central/Distributed Database, onward-forwarding, etc.—for more info see section 8.6)
- Outbound Roaming SMS MT Applicable Solution Approach—for more information, see also section 8.7

6.2.2.3 SMS Technical Information

For SS7, this would include the following information:

- GSM MAP version
- E.212 MCC-MNC
- E.214 CC-NC
- E.164 CC-NDC
- E.164 Nodes
- E.164 MSISDN Range(s)
- Retry Frequency (on SS7).

For SMPP, this would include the following information:

- SMPP Version
- VPN Device Type
- SMSC Format Information
- Tunnel End-Point (Public IP Address except the address blocks 10.0.0.0–10.255.255.255.255,172.16.0.0–172.31.255.255, 192.168.0.0–192.168.255.255)
- SMSC Host IP Address (Public IP Address except the address blocks 10.0.0.0–10.255.255.255.255,172.16.0.0–172.31.255.255, 192.168.0.0–192.168.255.255)
- SMSC Port
- System ID
- VPN Parameters
- MSISDN Range(s)
- (Honest) Delivery Reports Supported
- Retry Frequency (on IP)
- Store & Forward (on IP)

6.2.3 Signalling Routing

Client Operator will route all signalling pertaining to desired OC-SMS Hubbing Inter-working relationships to the Solution Provider.

6.2.3.1 SS7-based Connections

The OC-SMS Hubbing model is based on Cascaded signalling flow. The Client Operator's SMSC therefore shall route the SS7 signalling messages to the SMS Hub's Global Title address using multiple intermediary Signalling Providers. How the Client Operator chooses to do this is implementation specific. There are different ways the Client Operator can accomplish this routing definition:

- By using SS7 protocol stack level intermediate translations
- By using SCCP and MAP level address translations for OA and DA mapping on the SMSC
- By using a SCCP International Gateway Provider to provide such translation based on source and destination.

Alternatively, Signalling Gateways/ITPs can be deployed in the Client Operator's premises and the Hub can establish SIGTRAN connections to the Signalling Gateway.

6.2.3.1.1 Response Timers

Several SMS Command/Response Timers have been defined in 3GPP TS 29.002 [2] for GSM-MAP.

s = from 3 seconds to 10 seconds;
m = from 15 seconds to 30 seconds;
ml = from 1 minute to 10 minutes;
l = from 28 hours to 38 hours.

The Timer for SRI_SM is m (medium), and for FSM, it is ml (medium-long). The Client Operator must define proper setting of these SS7 timers.

6.2.3.2 IP-based Connections

IP-based hubbing uses the SMPP client/server protocol over TCP/IP. The connections between Client Operators and hubs can be TCP/IP tunnels which are generally more cost-efficient than SS7 connections and do not necessarily involve per-message pricing structures.

It is recommended that the Hub shall bind to the operator i.e. the Hub acts as the SMPP Client (ESME) and the Operator acts as the SMPP Server (SMSC). The operator may still however request a different setup. Based on the SMPP specifications, there is a strict association between bind direction and the use of Submit_SM or Deliver_SM.

The Client Operator must specify whether it can support Stored-and-Forward mechanism or it requires such support from the SMS Hub.

6.2.4 Co-existence of Different Models

6.2.4.1 Co-existence of Bilateral & Hubbing Models

The Client Operator may choose to have bilateral SMS Inter-working relationships also co-existing for many other Inter-working partners. The Client Operator will thus manage the separation of the signalling as it pertains to OC-SMS Hub managed Inter-working relationships versus bilateral Inter-working relationships. The Operator may also be able to enlist the support of the SCCP International Gateway Provider towards this end.

6.2.5 Co-existence of Multiple Hubbing Solution Providers

The Client Operator may choose to have multiple OC-SMS Hubbing Solution Providers for various reasons (redundancy, diversity, cost, etc.). The Client Operator will thus manage the separation of the signalling as it pertains to Inter-working relationships managed by one Hub versus another.

6.2.6 OC-SMS Hubbing Agreement

GSMA IWG has defined a new OC-SMS Hubbing Agreement template in the GSMA PRD AA.71 [8]. This Agreement is to be signed between the Client Operator and the Hubbing Solution Provider. The most recent copy of the PRD AA.71 [8] can be downloaded from the following URL (subject to GSMA access restrictions): https://infocentre.gsm.org/cgi-bin/prddets.cgi?237089.

6.2.7 Other Operator Preferences

The Client Operator may also choose to deploy/use certain capabilities, such as:

- Ability to aggregate multiple concatenated messages received
- Contract Opt-in or Opt-out for SMS Inter-working partners
- SMSC Black-listing preferences for messages received from
- MSISDN Black-listing for messages sent or received
- Binary Message Content filtering in their capacity as Recipient Operator
- Restrictions for allowed minimum and maximum length of Destination MSISDNs in its capacity as Recipient Operator.

The Client Operator shall notify its SMS Hubbing Solution Provider(s) accordingly to provision/configure appropriate information.

6.3 Examples

This document illustrates inter-working SMS relationships between two Client Operators by detailed examples that are based around 1 or 2 hubs.

6.4 Hub and operator labelling conventions

At various points in this document, it becomes necessary to reference specific operators and hubs as they pertain to a certain SMS message scenario. For ease of describing SMS message scenarios, the following convention is used, unless specified otherwise:

MNO1 – refers to operator where the SMS message is originated
MNO2 – refers to operator where the SMS message is terminated
HUB1 – originating hub - MNO1's SMS hub
HUB2 – terminating hub - MNO2's SMS hub

Of course, there is nothing preventing MNO1 being the same as MNO2 or HUB1 being the same as HUB2. In the most general case, they can be distinct entities.

6.5 Qualification on SMS Reply Handling

Using mechanisms in which any reply to the received SMS is to be sent from the handset directly to the Hub Global Title instead of the subscriber's operator SMSC are not compliant with OC SMS Hubbing. Solutions such as using reply-path are considered unnecessary in view of the capabilities provided within the current OC SMS Hubbing model.

7 TECHNICAL REQUIREMENTS FOR HUBS

7.1 SS7 Compliance

Hubs, as part of their offering SS7 connectivity to their operator customers, must offer emulated HLR and MSC/VLR functionality when receiving information from the originating Client Operator and virtual SMSC functionality when receiving information from the terminating Client Operator. In this document the following terms are used:

- vHLR: Virtual (or emulated) HLR
- vMSC: Virtual (or emulated) MSC/VLR
- vSMSC: Virtual (or emulated) SMSC

Moreover, it has been agreed that when both the originating and terminating operators are connected to a hub through SS7, the intermediate hubs will also connect through SS7.

7.2 Cascading Signal Flow

In order to guarantee “honest” delivery reports in a MAP/SS7 environment, a cascading signal flow from source to destination and back to source will be used. Moreover, addresses will be manipulated at each step of the signal flow. In particular, at any stage of the flow, the SCCP and MAP address will relate to the sender of the signal and also relate to the entity to be charged within the cascade-billing model. This does imply, on the down-side, that the full delivery path is not known to the receiving and sending parties.

7.3 SM Store and Forward and Error Management

The implementation of store-and-forward logic will be optional (except where the destination is SS7 in inter-standard SMS) for hubs. This document describes both the scenarios whereby hubs implement this functionality as well as scenarios where this functionality remains with the originating SMSC (in this case, the role of the hub is that of a proxy-server facilitating signal transit between Client Operators and other hubs).

7.4 Fraud Detection and Management

Hubs will be expected to comply with the relevant IR.70 [4] mechanisms for fraud detection. In particular, they should check the source and verify that the SCCP and MAP addresses are consistent. Further, the hub should consider any other relevant provisions in IR.70 [4], IR.71 [5] and AA.50 [6] in their implementations of fraud prevention, anti-spoofing, and anti-spamming

7.5 Address Manipulation

The following three levels of addresses are included in an SM:

- SCCP Calling and Called Global Titles
- MAP SM-OA or SM-DA
- Calling Number address (MSISDN) within the SM

7.5.1 Modification of sender information

These addresses play an important part in the fraud detection and management procedures that are the object of IR.70 [4]. In order not to disrupt these procedures, it is important that the SCCP and MAP addresses remain consistent. Namely, they must belong to the same operator and should be able to be seen by entities readily as belonging to the same entity. Sometimes hubs provide Global Titles that relate to a geographical region different to their own in order to access a local MNP DB. In these cases, the MAP and SCCP addresses should still remain consistent.

The Calling Number should not be changed – the originating MSISDN should be visible to the terminating hub and Client Operator.

7.5.2 Segmentation

Address length increase due to MAP or SCCP address manipulation could lead to additional TCAP segmentation as per 3GPP TS 29.002 [2], Section 23, provided by the hub.

7.5.3 Transparency

It is a goal of the SMS hubbing architecture to provide message transparency meaning that the receiving Client Operator is able to identify the sending Client Operator regardless of how many hubs the message may have transited through. To this end, we propose the following manipulation rules:

For SS7:

- At the signalling SCCP layer, hubs will replace incoming the GT with their own (for instance, the first hub in a message sending chain will replace the originating operator's GT with its own).
- At the MAP layer, hubs will replace the incoming GT with the first part of the hub's GT + 6 digits identifying the originating operator in a unique fashion (details are discussed in section 8.2.3). It has been agreed that for SMS hubbing, the unique operator identifier will consist of the operator's MCC/MNC information.

A more detailed example of the address manipulations that take place during hub-based SMS inter-working is provided in section 8.2.3, SS7 Transparency - Address Manipulation.

For IP:

- The `source_subaddress` parameter will be utilized to identify the source operator that is associated with the MSISDN issuing the SMS message.
- The `dest_subaddress` parameter will be utilized to identify the destination operator that is associated with the MSISDN receiving the SMS message. `dest_subaddress` shall only be utilized in the context of MNP.
- For Operator Identification, a 6 digit MCC+MNC value will represent the source or destination operator. For CDMA operators, an MNC value of 000 shall be used unless; further discussions have taken place with the MNC authority to get specific allocation. It is recommended that CDMA operators, who don't have specific allocation, make an application to obtain one.

Further details are discussed in section 8.3.5, SMPP Transparency.

Transparency is a crucial requirement of the SMS Hubbing architecture and it is quite important that the approach taken is consistent and standard for all Hubs. For the long term implementation of SMS Hubbing, this requirement is considered mandatory.

7.5.4 TCAP Negotiation

TCAP negotiation (hand-shaking) can be used now and will help to provide for a trusted environment. It is recommended that TCAP negotiation be used for authentication purposes throughout SMS Hubbing implementations.

7.6 Time Synchronization

It is important to be able to assess message latency for various purposes, and in particular, during the trial, this is part of the actual tests. To assure proper timing is used, it is mandatory that NTP synchronization (or similar functionality and timing accuracy) be applied by all nodes participating in the trial.

7.7 Black and White listing

It is important for the hub to be able to apply black lists and white lists for filtering messages. Among the possible applications foreseen are:

1. Filtering for presence of the inter-working contractual relationship. SS7 error code should be “Unknown subscriber” for SRI and ”Unexpected Data Value” for MT_FSM. The SMPP error shall be ESME Receiver Reject Message Error.

   For the case where MNO2 has MNP in-place, HUB1 shall not block messages unless it has certainty of the destination subscriber’s operator identity. In this case, if HUB1 is uncertain it can relay filtering responsibility to HUB2.

2. Black-listing of a Client Operator from sending any message (for SS7, this applies to SRI and MT-FSM origination). Hub shall be able to black-list any Client Operator such that it is not possible for that Client Operator to originate any SMS to its Client Operators or to another Hub via it. SS7 error code shall be “Unknown subscriber” for SRI and “Unexpected Data Value” for MT_FSM. The SMPP error shall be ESME Receiver Reject Message Error.

   For the case where MNO1 has MNP in-place, HUB1 shall not block messages unless it has certainty of the destination subscriber’s operator identity. In this case, if HUB1 is uncertain it can relay blacklisting responsibility to HUB2.

3. Black-listing of a Client Operator from receiving any message (for SS7, this applies to SRI and MT-FSM termination). Hubs shall be able to black-list any Client Operator such that it is not possible for that Client Operator to receive any SMS from its Client Operators or from another Hub via it. SS7 error code shall be “Unknown subscriber” for SRI and “Unexpected Data Value” for MT_FSM. The SMPP error shall be ESME Receiver Reject Message Error.

For the case where MNO2 has MNP in-place, HUB1 shall not block messages unless it has certainty of the destination subscriber's operator identity. In this case, if HUB1 is uncertain it can relay blacklisting responsibility to HUB2.

4. Black-listing of an MSISDN from sending any message (for SS7, this applies to SRI and MT-FSM origination). Hub shall be able to black-list any MSISDN whether or not the Client Operator, to which the MSISDN belongs is connected to it, such that it is not possible for that MSISDN to originate any SMS via the Hub. The Hub should apply this black-listing treatment for MSISDNs on a per recipient Client Operator basis. This is an optional requirement on hubs. SS7 error code shall be "Illegal Equipment". The SMPP error shall be ESME Receiver Reject Message Error.

5. Black-listing of an MSISDN from receiving any message (for SS7, this applies to SRI and MT-FSM termination). Hub shall be able to black-list any MSISDN whether or not the Client Operator, to which the MSISDN belongs is connected to it, such that it is not possible for that MSISDN to receive any SMS via the Hub. The Hub should apply this black-listing treatment for MSISDNs on a per-sending Client Operator basis. This item shall be optional for the Hub provider, and is mainly conditioned upon the request of the terminating operator. This is an optional requirement on hubs. SS7 error code shall be "Illegal Equipment". The SMPP error shall be ESME Receiver Reject Message Error.

6. Black-listing Service Centre Addresses. The hub shall be able to black-list any Service Centre GT address to receive incoming SRI or MT-FSM messages from. The Hub should apply this black-listing treatment for SC addresses on a per recipient Client Operator basis. SS7 error Code shall be "Unknown subscriber" for SRI and "Unexpected Data Value" for MT_FSM. In actual implementation, this function shall be achieved by combination of black and white listing, allowing only authorized Service Centre GT addresses to pass.

7. Black-listing on MSISDN length. The Hub shall be able to define restrictions for allowed minimum and maximum length of destination MSISDNs of incoming SRI or MT-FSM messages. The Hub should apply this restriction on a per recipient Client Operator basis. This is an optional requirement on hubs. SS7 error Code shall be "Unknown subscriber" for SRI and "Unexpected Data Value" for MT_FSM. The SMPP error shall be ESME Receiver Reject Message Error.

8. Binary Message Content Filtering. The Hub shall be able to apply binary message content filtering on a per recipient Client Operator basis. This is an optional requirement on hubs.

9. Blocking SS7 Messages from Unknown Operator/Hub. The Hub shall only accept SS7 MAP SRI_SM and MT_FSM messages from known provisioned Operators or Hubs.

10. Blocking SMPP Binds from Unknown Operator/Hub. The Hub shall only accept incoming SMPP Bind requests from known provisioned Operators or Hubs.

11. Blocking in the case where the roaming is not allowed. In the case where the roaming between the VPLMN (MNO3) and HPLMN (MNO2), it is the responsibility of HUB2 to check this and block it. In SS7, the SRI error shall be “Call barred”.

These scenarios should be supported by hubs. The SS7 error codes have been chosen from the list of SRI and MT_FSM applicable permanent error codes in 3GPP TS 29.002 [2]. Where MT_FSM specific error (such as “Illegal Equipment”) cannot be used because the error is for SRI, then “Unexpected Data Value” can be used. The list of available errors based on the MAP specifications (3GPP TS 29.002 [2]) is only very short and is cited here for reference only. For MAP_SRI_For_SM:

- Unknown subscriber
- Call Barred
- Teleservice Not Provisioned
- Absent Subscriber_SM
- Facility Not Supported
- System failure
- Unexpected Data Value
- Data missing

The errors that can be returned in the MAP_MT_Forward_SM operation are:

- Unidentified subscriber
- Absent Subscriber_SM
- Subscriber busy for MT SMS
- Facility Not Supported
- Illegal Subscriber indicates that delivery of the mobile terminated short message failed because the mobile station failed authentication
- Illegal equipment indicates that delivery of the mobile terminated short message failed because an IMEI check failed, i.e. the IMEI was blacklisted or not white-listed
- System Failure
- SM Delivery Failure
  - The reason of the SM Delivery Failure can be one of the following in the mobile terminated SM:
    - memory capacity exceeded in the mobile equipment
    - protocol error
    - mobile equipment does not support the mobile terminated short message service.
- Unexpected Data Value;
- Data Missing.

Hubs shall make the error values for all blocking and blacklisting cases configurable for flexibility, but the standard values are as they are specified here.

For avoidance of doubt, SMPP errors shall be returned in the Submit_SM_Resp or Deliver_SM_Resp that corresponds to the initial message sending. It is not to be conveyed through the deliver report messages.

Blocking of SS7 messages should normally occur at the SRI message, and blocking of MT_FSM should be avoided.

7.8 Concatenated messages

The Hub shall be able to support concatenation of multiple Short Messages sent to the same MS only as required by the destination operator's SMS inter-working protocol. Hubs may need to segment messages; however, it is normally unnecessary to perform any aggregation of messages.

The only exception would be, if the receiving SMSC is known to be unable to support concatenated messages, then the responsibility to adapt the message so that it does successfully terminate falls on the hub. This may involve aggregation of the SMS before terminating to the recipient operator.

7.9 Service Troubleshooting

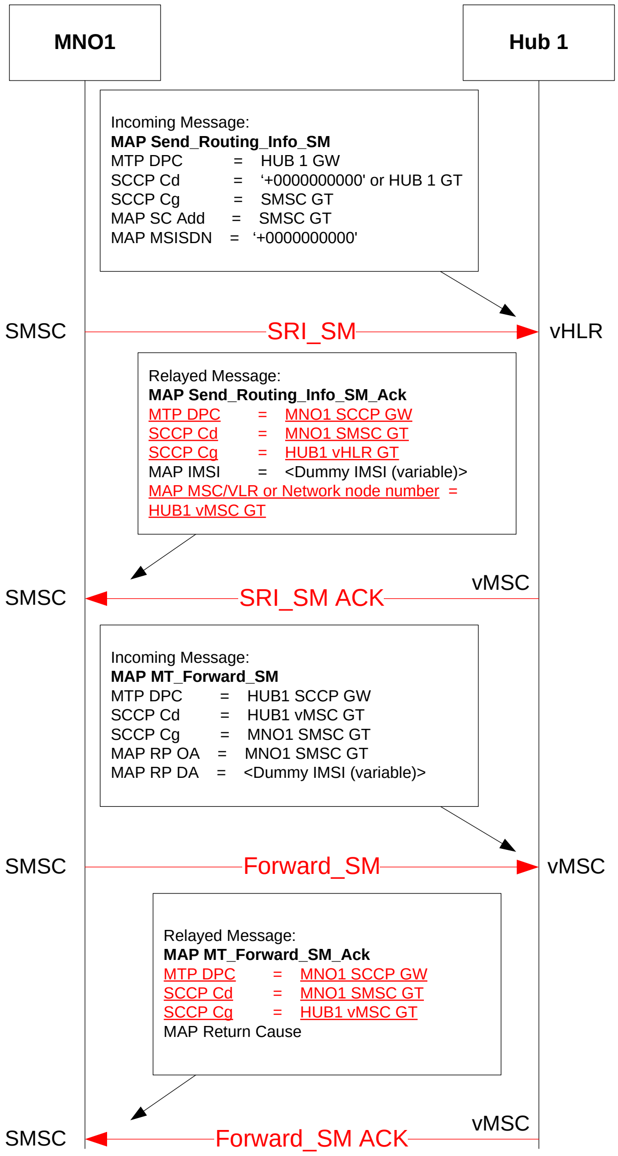
The Hub shall be able to provide visibility into message routing, and actual connections utilized by any specific message for troubleshooting purposes.

7.10 Loopback Destination Address

The destination address +0000000000 shall be recognized by all hubs as a loopback destination. When it is received the hub shall generate an internal acknowledgement to any message received bearing this destination address without forwarding the message or accessing the egress interface.

End-to-end KPI assessment normally involves Client Operator to Hub to Client-Operator testing. Such a destination address can be useful for performing Client Operator to Hub stand-alone KPI assessments.

Illustration for SS7 case:



7.11 Usage & Performance Reporting

The Hub shall be able to provide usage and performance reports to its Client Operator. Usage Reports will be Summary reports on per Connection-type basis and also on a per-Client Operator basis for different Connection types. Reports from the Hub shall include:

1. Outgoing message count
2. Incoming message count for SRI, FSM and SMPP
3. Incoming and outgoing delivery report successful percentage.
4. Throughput per connection (minimum, average and maximum transactions processed per second in a 10 minute period).
5. Audit and reconciliation report. The format can be specific to each hub, but the basic purpose of this report is to say that transactions received by the hub is equal

to the transactions that have come out of the hub, and can be utilized as an effective audit of the completeness of the hubs processing. A sample report is attached here.

C:\OC\smshtig\
sample audit and reco

7.12 High Availability

The Hub shall provision its network in such a way that it is resistant to single-points of failure issues, and shall have 99.999% availability over a year.

7.13 Operator Considerations

7.13.1 Wholesale Billing for Inter-operator SMS

The technical changes brought about by the SMS Hubbing Architecture are mostly straightforward and transparent from the point of view of the Client Operator. Perhaps the main thing to consider is being ready for Inter-Operator SMS billing or wholesale settlements. The transit and termination fees involved in SMS Hubbing will be covered by AA.71 [8] which replaces the AA.19 [7] agreement for bilateral SMS Hubbing.

Inter-operator billing or accounting for SMS is typically event-based, accounting only successful SMS sending/receive events. The only challenging part might be if the Hub requires the SRI charged (or per signalling event charge). This is already up to operator and Hub negotiations. Such signalling events are typically not captured by the operator in the normal course of inter-operator billing unless SS7 probes are in-place for this purpose.

In which case, hub shall account these signalling events for the operator in full detail with monthly and daily breakdown possible.

7.13.2 Retry attempts frequency

A high frequency of SS7 retry attempts could generate SS7 signalling without the actual SMS message data being relayed, and this could generate spurious signalling traffic on the SMS Hubbing network. A similar scenario may also apply to SMPP IP inter-working.

Thus, it is recommended by the SMS Hubbing Architecture, to limit the frequency of retry attempts through the hub. The actual value is to be agreed between the Client Operator and their hub.

7.13.3 Mobile Operator and Hub Technical parameter exchange

The relevant technical information will be gathered by the hub from their Client Operator using standard template document deviations which are agreed between the Parties and will typically contain the following:

- Participating Client Operator IR.21
- Contact information
- IP or SS7 connectivity details
- Test numbers and SIM cards information
- Any relevant handset configuration

Mobile Operator will provide two test numbers to Hub for testing. With these numbers from the Mobile Operator, the Hub is able to facilitate testing as each of the other Participating Client Operators is connected via the Hub with the Mobile Operator. The hub has to collect the information identified in the subsequent section 7.14 also, so that it can share the information to other hubs as required.

7.14 Hub to Hub Technical parameter exchange

In order to assure maximum inter-operability among SMS hubs, hubs need to share their current list of SMS Hub clients with each other and the following client operator technical parameters:

1) Routing info: operator MSISDN range, MCC+MNC, MAP version
2) Presence of MNP at the client operator, and the chosen MNP solution approach if applicable.
3) Client operator is on SS7 or SMPP
4) If Client operator is on SMPP, do they support honest deliver reports
5) SS7/SMPP response timers
6) Chosen solution approach for roaming termination
7) The hub's MAP version negotiation approach as discussed in section 7.15
8) Client operator's primary hub and any secondary or alternate hubs designations

7.15 MAP Version Negotiation

There are 3 possible approaches: end-to-end MAP version negotiation, per-hop MAP version negotiation, and a third method which is a sort of in-between case whereby only HUB2 is performing MAP version decoupling only when necessary. The 3 methods are expected to be able to inter-work successfully, so any one can be applied however the full set of implications has to be considered.

The three approaches are believed to be able to inter-work successfully, and hubs can include in their technical parameter exchange which MAP version negotiation strategy it is that they apply.

7.15.1 End-to-end MAP version negotiation

This is the simplest approach where the MAP version is dictated by the lowest of the MAP versions among the involved nodes/end-operators. If a hub employs this strategy, they may need to explain to their operator how it is they handle sending of large SMS Messages (noted in #5 below), and Roaming SMS MT solution approach 2, and SS7 MNP. Quite possibly, the hub is taking exception of the end-to-end MAP version handling only for these cases.

1. This approach may quickly fall back to using MAP v1 very often in SS7 dialogues. If a single GT address is used by the hub provider towards the originating operator, it is likely that the originating SMSC would fall back to MAP v1 operation quickly and so be without the features of the higher MAP versions. Operators' equipments may have a MAP version learning function which may add to the problem of being at MAP v1.
2. Falling back to MAP v1 has several implications. TCAP handshake cannot be applied hub-to-hub. Private extensions also cannot be used.

3. Without TCAP handshake, the security of inter hub communication may be compromised.
4. There may be issues with sending large messages, if a hub is implementing FSM-Relay, as the destination address for an MT_FSM message may not yet be known within the first TCAP segment. The dialogue portion goes in the initial begin message, with the component portion in the subsequent TCAP continue message. The IMSI is normally contained in the component portion. With a large message, the component portion will arrive in the subsequent TCAP Continue from the originator
5. Impacts delivery of large messages. MT_FSM for large messages may not contain sufficient information to identify the destination of the message and particularly the preceding SRI based on the IMSI, as the initial MSU may contain only the dialogue portion (sans the content portion). Hubs using end-to-end MAP version negotiation can work around this by retaining a large range of GT addresses which can be inserted/suffixed into the MAP MSC-VLR address of the initial SRI response. The hub then extracts the information from the SCCP CdPA of the MT_FSM message, which is derived from/equivalent to the SRI response MAP MSC-VLR address.

7.15.2 Per-hop MAP version negotiation

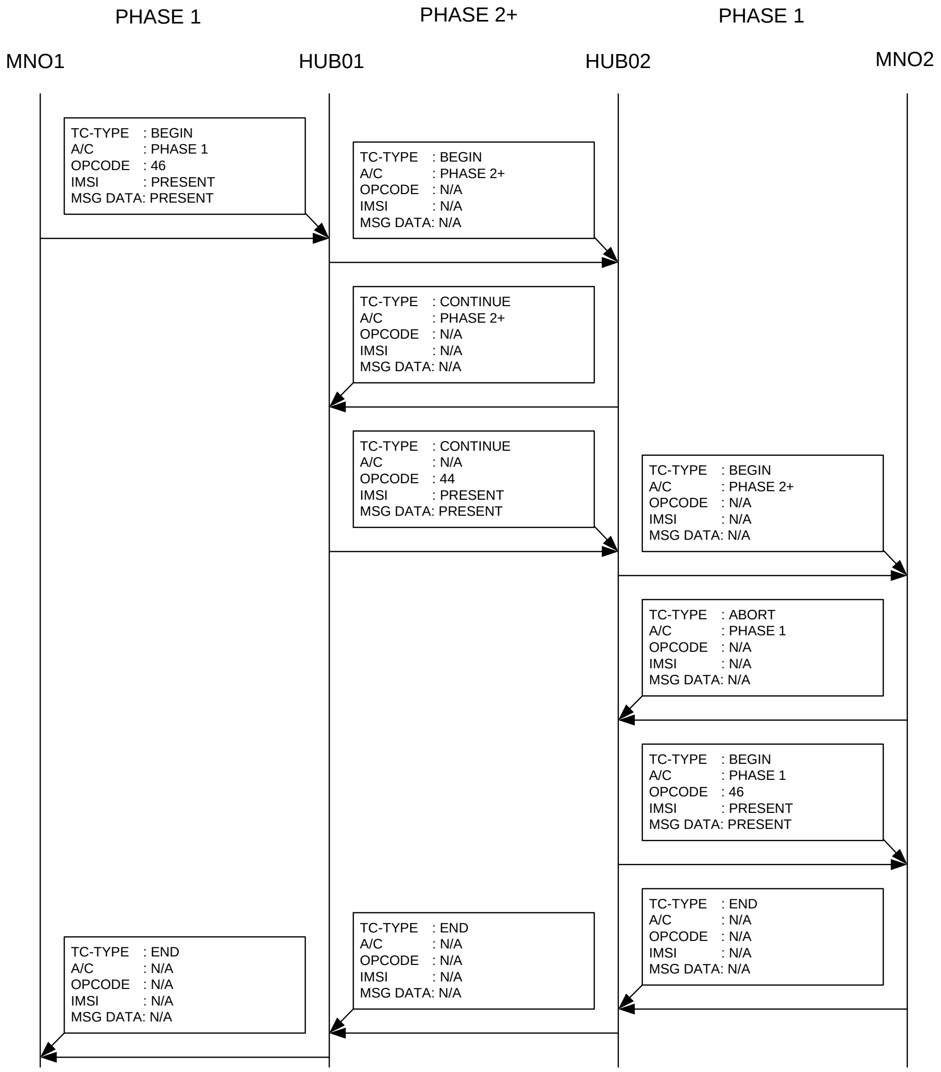
This is the most flexible approach in terms of decoupling the MAP version negotiation between hubs and ensures hubs are communicating at the best MAP version possible.

1. This approach allows TCAP handshake to be consistently applied hub-to-hub
2. This approach allows private extensions which require MAP v2 or MAP v3 to be applied hub-to-hub, especially for SS7 MNP or SS7 SMT MT for Roaming solution approach 2.
3. It is recommended for hubs to implement a fairly recent version of MAP and this can only be consistently effective if the hub is using a per-hop MAP negotiation.
4. In a case such as RSDS_SIM_FULL error which is not available to MAPv1 needs to be returned, a similar type error can be used. Specific care may need to be taken to ensure that the error mapping is appropriate.
5. This approach involves some extra signalling and additional latency which is potentially minor.

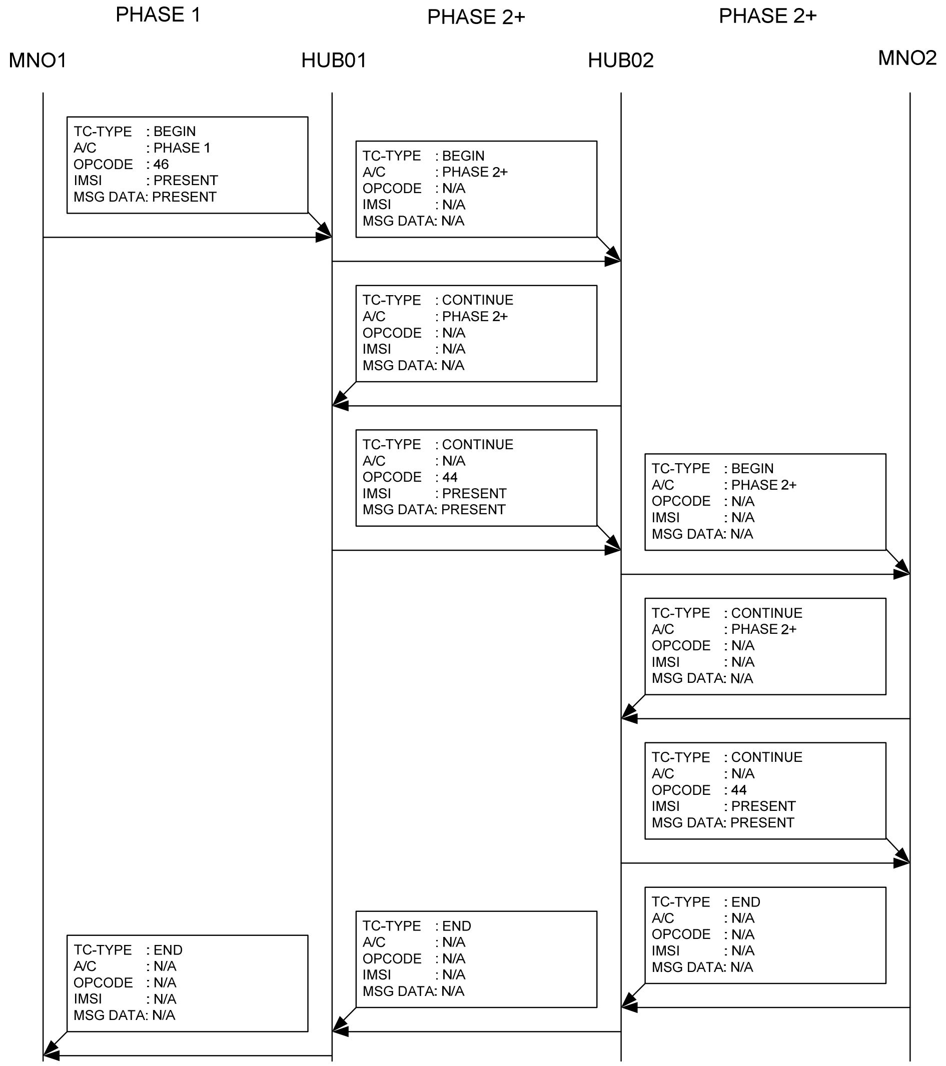
7.15.2.1 Per-hop MAP version negotiation solution diagram detail

The solution approach is diagrammed in detail below. 4 combinations are considered, and MAP version 2 and 3 are taken together and simplified as equivalent to MAP version 3.
If the message is large, the MAP version/phase between the hubs has to be MAP version 2 or 3 (or phase 2+). At MAP version 2 or 3, the component and dialogue portions will not fit in a single MSU, so the dialogue portion goes in the BEGIN, with the component portion in the subsequent CONTINUE.

7.15.2.1.1 MAP version/phase 1-3-1



7.15.2.1.2 MAP version/phase 1-3-3



TC-TYPE : BEGIN
A/C : PHASE 1
OPCODE : 46
IMSI : PRESENT
MSG DATA: PRESENT

TC-TYPE : BEGIN
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : CONTINUE
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : CONTINUE
A/C : N/A
OPCODE : 44
IMSI : PRESENT
MSG DATA: PRESENT

TC-TYPE : BEGIN
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : CONTINUE
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

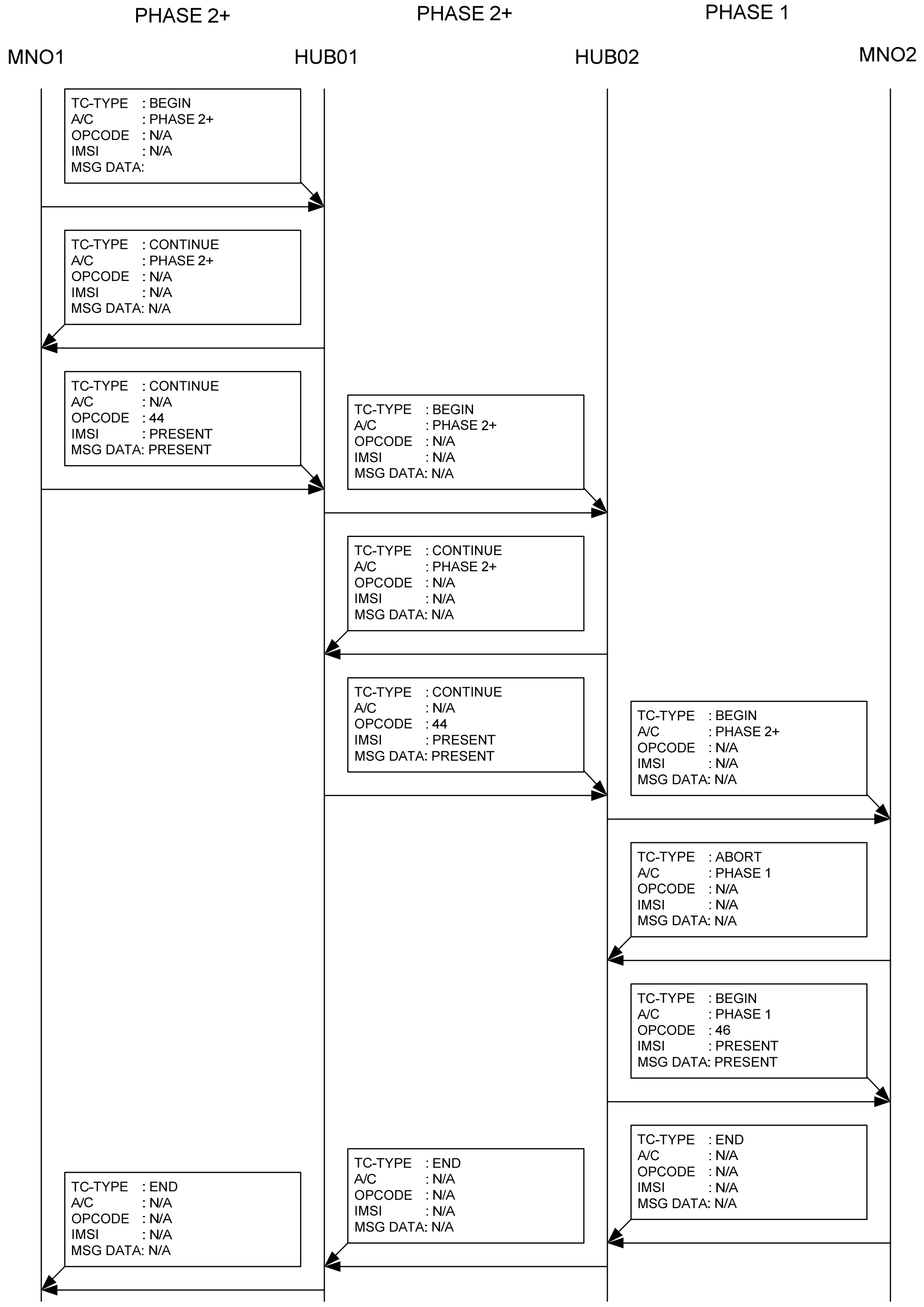
TC-TYPE : CONTINUE
A/C : N/A
OPCODE : 44
IMSI : PRESENT
MSG DATA: PRESENT

TC-TYPE : END
A/C : N/A
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

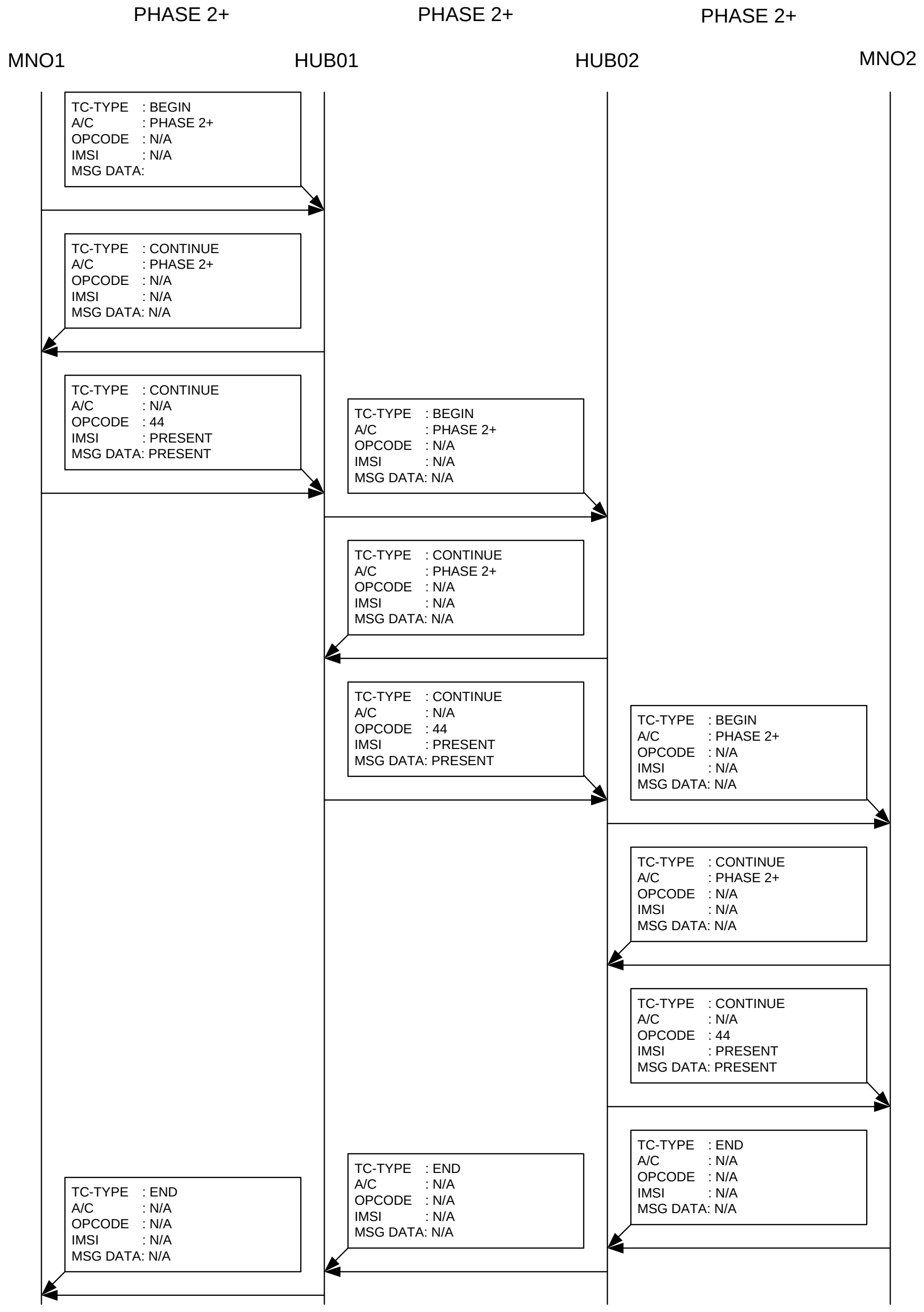
TC-TYPE : END
A/C : N/A
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : END
A/C : N/A
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

7.15.2.1.3 MAP version/phase 3-3-1



7.15.2.1.4 MAP version/phase 3-3-3



7.15.3 HUB2 is performing MAP version decoupling only when necessary

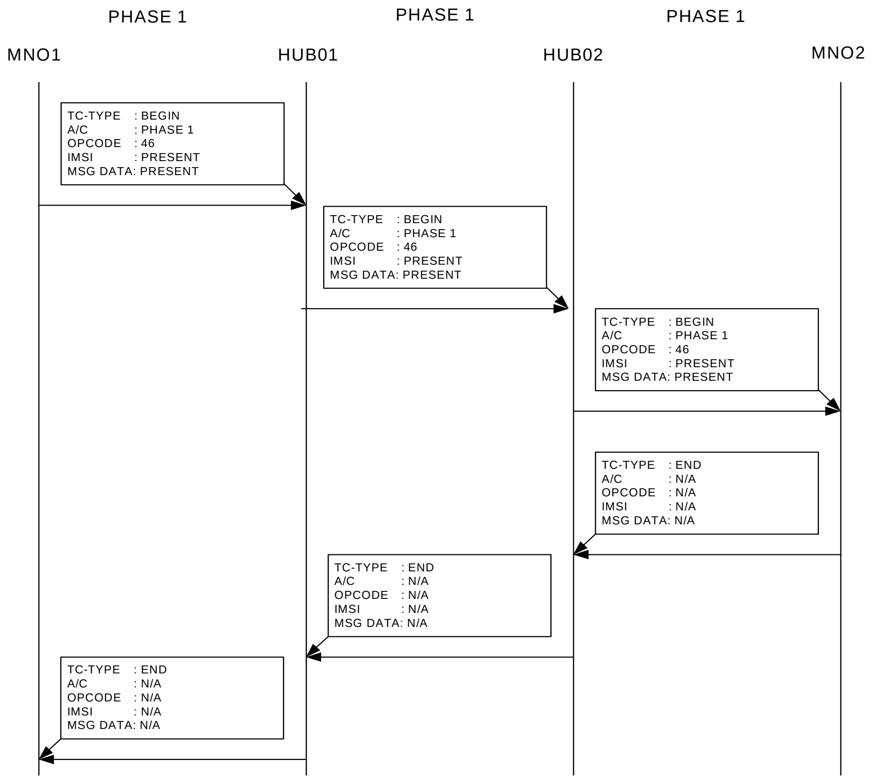
In this approach, it is HUB2 that is decoupling the MAP version negotiation only when it is necessary. The MAP version is retained in its original version based on MNO1's MAP version and the MAP version is decoupled only by HUB2 to accommodate the version at MNO2. If a hub employs this strategy, they may need to explain to their operator how it is they handle sending of large SMS messages, and Roaming SMS MT solution approach 2, and SS7 MNP. Quite possibly, the hub is taking exception of the MAP version handling only for these cases, when the need arises.

1. The MAP version management is somewhat more simplified, as it is clear from this approach that only HUB2 is handling MAP version decoupling, and it is clear that the responsibility falls on HUB2 only.
2. MAP version decoupling is minimized as much as possible in this approach. The original MAP level is retained as long as possible (end-to-end if possible).
3. If the message is not segmented when arriving at a hub, and needs to be segmented for sending out, the hub may do so, but without changing the MAP AC version. An MT_FSM on MAPv1 always completely fits in one TCAP message.

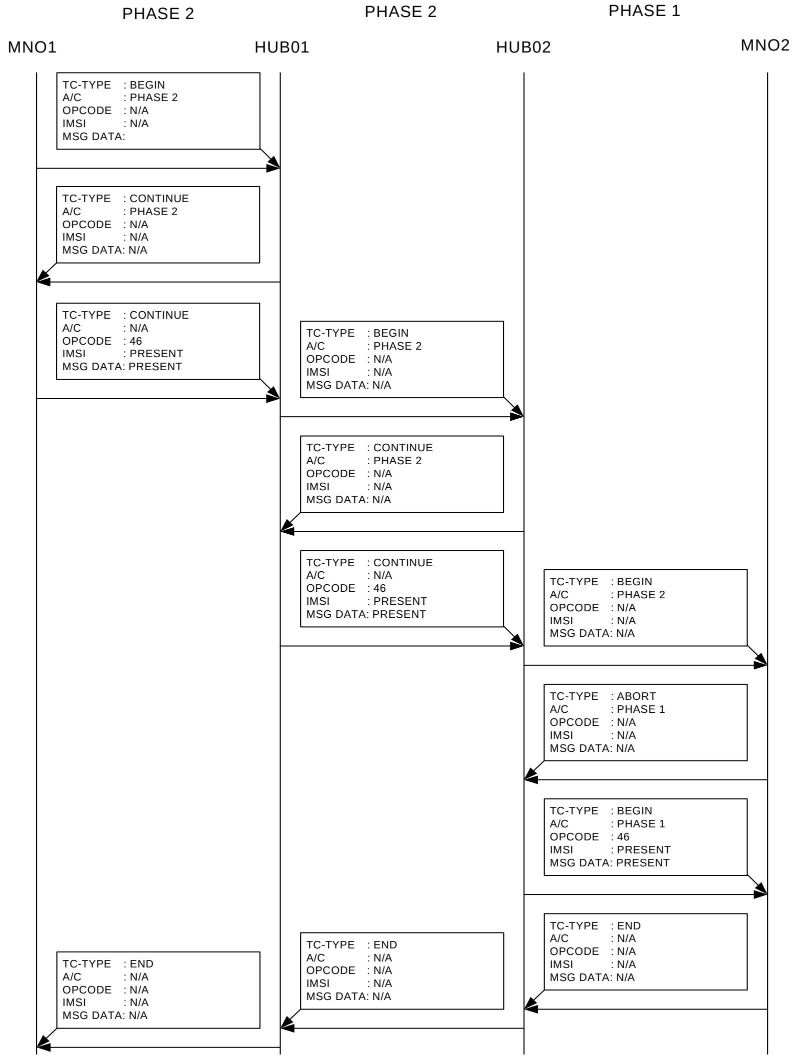
7.15.3.1 Solution diagram detail

The solution approach is diagrammed in detail below. 4 combinations out of the 9 possible are considered, which are the cases 1, 2, 3 and 6 of the corresponding example cases from section 7.15.4.

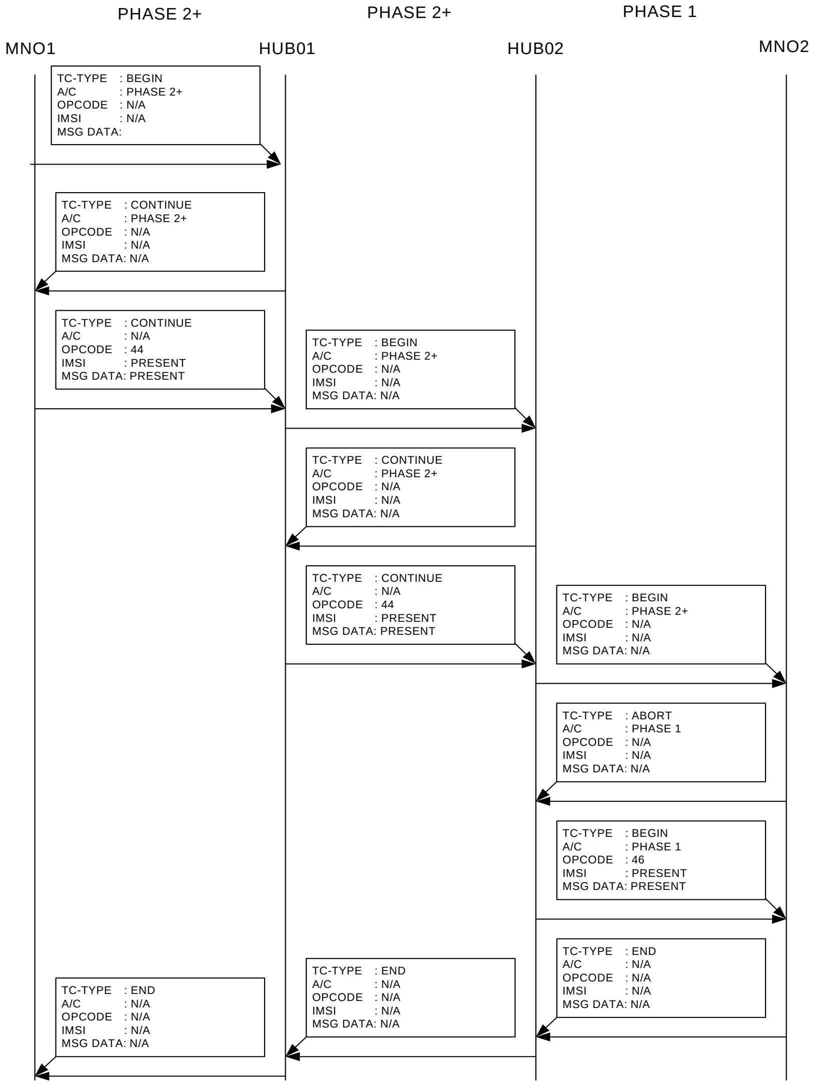
7.15.3.1.1 Case 1



7.15.3.1.2 Case 2



7.15.3.1.3 Case 3



TC-TYPE : BEGIN
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA:

TC-TYPE : CONTINUE
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : CONTINUE
A/C : N/A
OPCODE : 44
IMSI : PRESENT
MSG DATA: PRESENT

TC-TYPE : BEGIN
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : CONTINUE
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : CONTINUE
A/C : N/A
OPCODE : 44
IMSI : PRESENT
MSG DATA: PRESENT

TC-TYPE : BEGIN
A/C : PHASE 2+
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : ABORT
A/C : PHASE 1
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

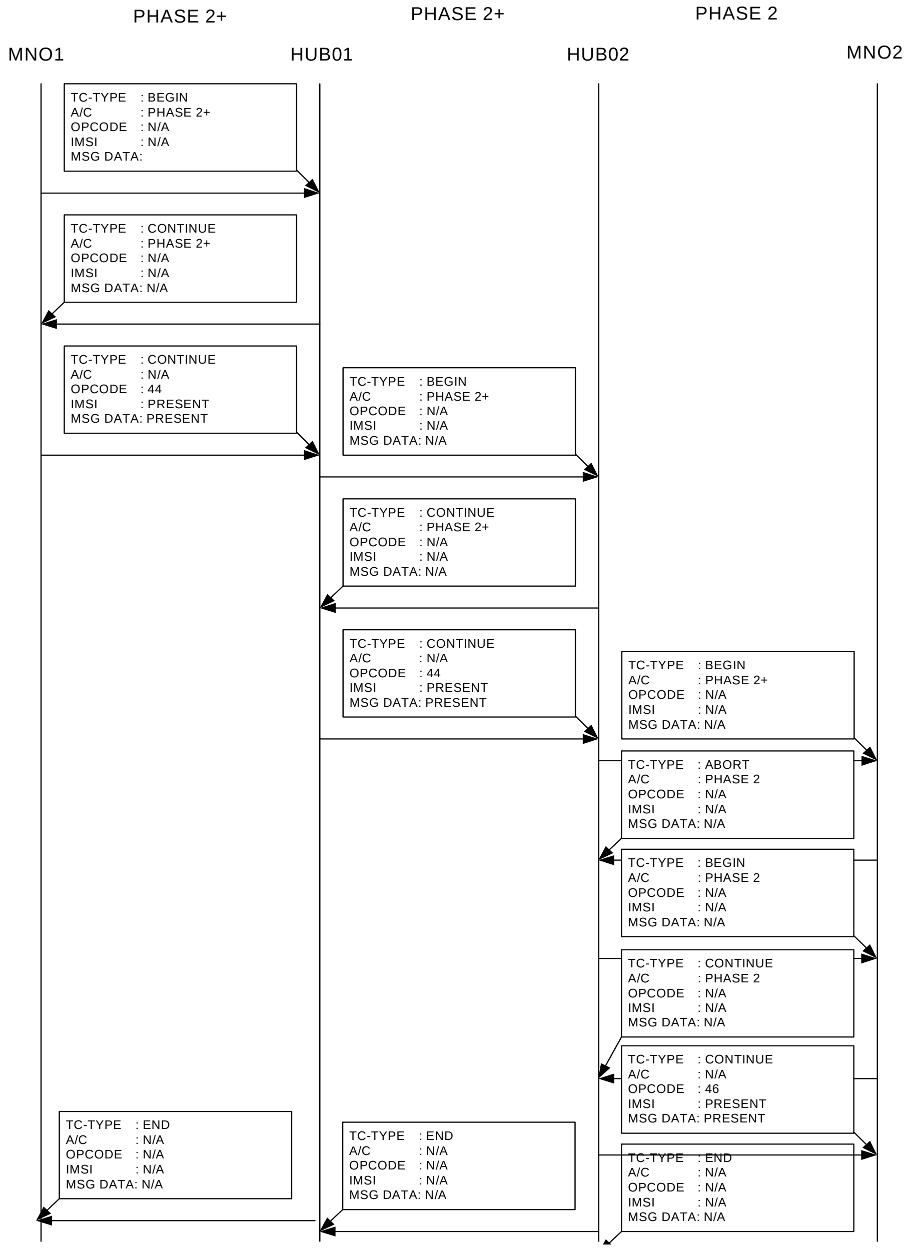
TC-TYPE : BEGIN
A/C : PHASE 1
OPCODE : 46
IMSI : PRESENT
MSG DATA: PRESENT

TC-TYPE : END
A/C : N/A
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : END
A/C : N/A
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

TC-TYPE : END
A/C : N/A
OPCODE : N/A
IMSI : N/A
MSG DATA: N/A

7.15.3.1.4 Case 6



7.15.4 Examples

The tables below provide an example in various example cases of actual MAP versions and the resulting effective MAP version.
For end-to-end MAP negotiation:

	Actual MAP versions				Effective MAP Version		
	MNO1	HUB1	HUB2	MNO2	MNO1 to HUB1	HUB1 to HUB2	HUB2 to MNO2
Case 1	1	3	3	3	1	1	1
Case 2	3	3	2	1	1	1	1

Case 3	2	1	3	3	1	1	1
Case 4	3	3	3	2	2	2	2

It should be noted that Case 3 should normally never happen though since hubs must always be of the most recent MAP version capability level.

For per-hop MAP version negotiation:

	Actual MAP versions				Effective MAP Version		
	MNO1	HUB1	HUB2	MNO2	MNO1 to HUB1	HUB1 to HUB2	HUB2 to MNO2
Case 1	1	3	3	3	1	3	3
Case 2	3	3	2	1	3	2	1
Case 3	2	1	3	3	1	1	3
Case 4	3	3	3	2	3	3	2

It can be noted again that case 3 should normally not occur.

For the third approach where HUB2 performing the MAP version decoupling:

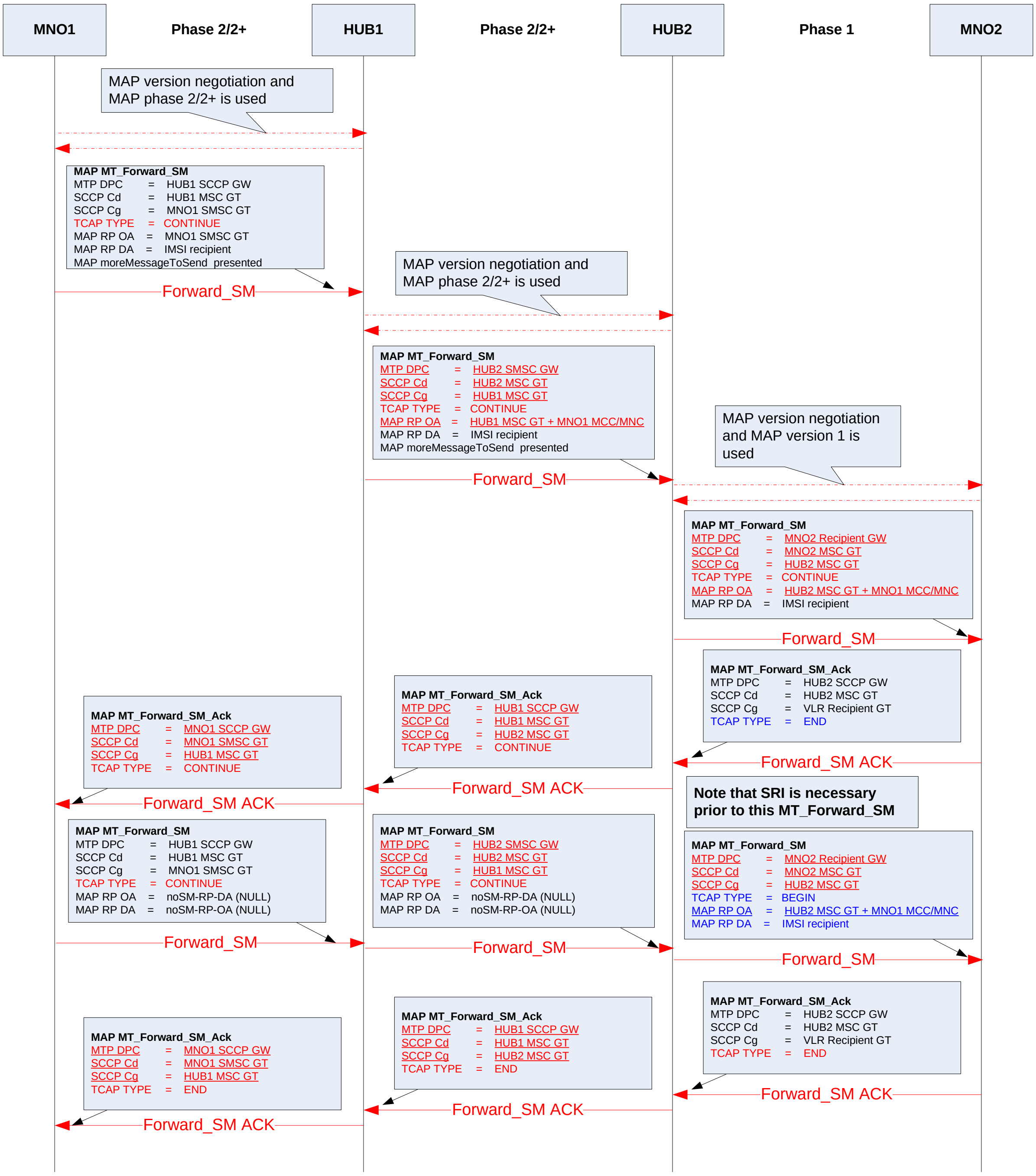
	Actual MAP versions				Effective MAP Version		
	MNO1	HUB1	HUB2	MNO2	MNO1 to HUB1	HUB1 to HUB2	HUB2 to MNO2
Case 1	1	3	3	1	1	1	1
Case 2	2	3	3	1	2	2	1
Case 3	3	3	3	1	3	3	1
Case 4	1	3	3	2	1	1	1
Case 5	2	3	3	2	2	2	2
Case 6	3	3	3	2	3	3	2
Case 7	1	3	3	3	1	1	1
Case 8	2	3	3	3	2	2	2
Case 9	3	3	3	3	3	3	3

Take note in the above sample cases that the hubs are assumed to have the highest capability, and all possible combinations of MAP versions between MNO1 and MNO2 are considered. The cases where there is MAP version decoupling occurring are the ones highlighted in bold. Illustration of these particular cases is provided in section 7.15.3.1

7.15.5 More message to send and MAP version negotiation

In a multiple short message transfer using the more message to send (also unfortunately referred to as "MMS") capability, the FSM can be used several times within a single TCAP transaction as illustrated below. If HUB2 is decoupling the MAP version and MNO2 is on MAP v1, it maybe necessary for HUB2 to issue a new SRI between HUB2 and MNO2 when MNO2 terminates a transaction via TCAP END response. A new SRI is needed before each subsequent FSM between HUB2 and MNO2.

MAP v1 has no support for the more message to send capability, which is inefficient from a signalling point of view (because every FSM message requires a preceding SRI), and also from an air interface point of view (because the MSC needs to re-page the handset for each message, whereas with more message to send capability, the MSC keeps the air interface open).


MNO1
Phase 2/2+
HUB1
Phase 2/2+
HUB2
Phase 1
MNO2
MAP version negotiation and MAP phase 2/2+ is used
Forward_SM
MAP version negotiation and MAP phase 2/2+ is used
Forward_SM
MAP version negotiation and MAP version 1 is used
Forward_SM
Forward_SM ACK
Forward_SM ACK
Forward_SM ACK
Note that SRI is necessary prior to this MT_Forward_SM
Forward_SM
Forward_SM
Forward_SM
Forward_SM ACK
Forward_SM ACK
Forward_SM ACK

MAP MT_Forward_SM
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = MNO1 SMSC GT
TCAP TYPE = CONTINUE
MAP RP OA = MNO1 SMSC GT
MAP RP DA = IMSI recipient
MAP moreMessageToSend presented

MAP MT_Forward_SM
MTP DPC = HUB2 SMSC GW
SCCP Cd = HUB2 MSC GT
SCCP Cg = HUB1 MSC GT
TCAP TYPE = CONTINUE
MAP RP OA = HUB1 MSC GT + MNO1 MCC/MNC
MAP RP DA = IMSI recipient
MAP moreMessageToSend presented

MAP MT_Forward_SM
MTP DPC = MNO2 Recipient GW
SCCP Cd = MNO2 MSC GT
SCCP Cg = HUB2 MSC GT
TCAP TYPE = CONTINUE
MAP RP OA = HUB2 MSC GT + MNO1 MCC/MNC
MAP RP DA = IMSI recipient

MAP MT_Forward_SM_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 MSC GT
SCCP Cg = VLR Recipient GT
TCAP TYPE = END

MAP MT_Forward_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = HUB2 MSC GT
TCAP TYPE = CONTINUE

MAP MT_Forward_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 MSC GT
TCAP TYPE = CONTINUE

MAP MT_Forward_SM
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = MNO1 SMSC GT
TCAP TYPE = CONTINUE
MAP RP OA = noSM-RP-DA (NULL)
MAP RP DA = noSM-RP-OA (NULL)

MAP MT_Forward_SM
MTP DPC = HUB2 SMSC GW
SCCP Cd = HUB2 MSC GT
SCCP Cg = HUB1 MSC GT
TCAP TYPE = CONTINUE
MAP RP OA = noSM-RP-DA (NULL)
MAP RP DA = noSM-RP-OA (NULL)

MAP MT_Forward_SM
MTP DPC = MNO2 Recipient GW
SCCP Cd = MNO2 MSC GT
SCCP Cg = HUB2 MSC GT
TCAP TYPE = BEGIN
MAP RP OA = HUB2 MSC GT + MNO1 MCC/MNC
MAP RP DA = IMSI recipient

MAP MT_Forward_SM_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 MSC GT
SCCP Cg = VLR Recipient GT
TCAP TYPE = END

MAP MT_Forward_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = HUB2 MSC GT
TCAP TYPE = END

MAP MT_Forward_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 MSC GT
TCAP TYPE = END

7.16 Security Requirements

GSMA’s Security Group has considered the proposed architecture and recommends the use of TCAP SEC where appropriate. The operations and maintenance access control policies outlined in SG.14 should be adhered to. Additionally, SG has identified the following requirements:

7.16.1 IGP Filtering

The Hub Provider should implement filtering of authorized operators in the IGP at SCCP level thereby creating a white list of operators allowed to send SMS traffic to other operator networks and the parameters used to create this white list should be described. Additionally, the Hub Provider should describe the process to create and modify the white list and should describe the methods and parameters/thresholds to detect spam and SS7 fraud (faking).

7.16.2 ISMS-G Filtering

The Hub Provider should describe the filtering of incoming messages (e.g. based on SMSC global Title, etc.) and the barring possibilities. The technical methods used to detect fraudulent activity should be described and these could include parameters such as inconsistency between MAP and SCCP Calling party addresses, imbalance between SendRequestInformationForShortMessage and ForwardShortMessage, and other possible parameters like those described in the GSMA document.

7.16.3 SMS-G Anti-spamming

The Hub Provider should describe the technical methods to detect, block and report the SMS spamming activity.

7.16.4 Security Controls

The Hub Provider should explain how read and write access to the filtering rules to staff is authorized and controlled i.e. who has access, who controls the authorizations, available logs, restrictions on local or remote access to the equipment, etc.). The Hub Provider should have implemented adequate controls (staff and infrastructure) and should be compliant with the security standard BS7799/ISO27001.

7.16.5 Reporting

The Hub Provider should describe the level and nature of reporting provided to customers on SMS activity and SMS fraudulent activity (barred operators, number of SMS rejected, etc…). Reporting should be provided monthly and on the occasion of a flagged incident.

7.16.6 Audit

The Hub Provider should authorize network operators, or their appointed agents, to perform a security audit to verify the means implemented by the Hub Provider to protect networks from spam and fraudulent traffic from other operators.

7.16.7 Traces

The Hub Provider should be able to provide technical traces (MAP, SCCP…) when requested to provide these by operators in order to provide evidence of fraudulent activity. In case of an incident, the traces should be provided to operator within 24 hours.

7.16.8 Penetration Testing

Operators may request the hub to perform penetration testing to verify that the Hub Provider has deployed adequate security measures.

7.16.9 SS7 SMS and SRI preceding MT_FSM Requirement

An SRI shall always precede the MT_FSM in SS7 SMS. This is an important requirement for security purposes because it allows the GT address of the originating node to be validated before any MT_FSM is allowed to originate. This is a definite mandatory requirement. All hubs shall consistently apply this check at all interfaces: operator-to-hub, hub-to-hub and hub-to-operator.

The only exception to this rule is the case of termination of SMS in a valid porting or roaming case where this architecture document describes a mechanism for performing a direct MT_FSM.

Please note that there is a detailed error value that can be returned in case MAP private extensions are used in the event that this criterion is violated.

The hub may provide an option for the operator to have an SRI result cache with a short timeout (between 2 to 5 minutes). This SRI result cache allows the operator to send an FSM without a preceding SRI if a recent previous SRI result is already available, as this results in an efficiency gain. This option can apply differently on the originating and receiving side interface of the operator.

On the receiving side, if the MNO2 requires strict SRI at all times, then HUB2 has to mediate and insert the necessary SRI if it was not sent by MNO1. Hub-to-hub it can be between hubs to agree how to handle this, but the most general case is that a hub will send to another hub a combination of SRI and FSM-sans-SRI based on SRI cache. It will have to be up to the HUB2 to insert SRI as necessary. The important thing is that hubs must have validated the GT address of the originator on a recent basis at all times. 2 to 5 minutes is the required interval.

8 HUBBING ARCHITECTURE

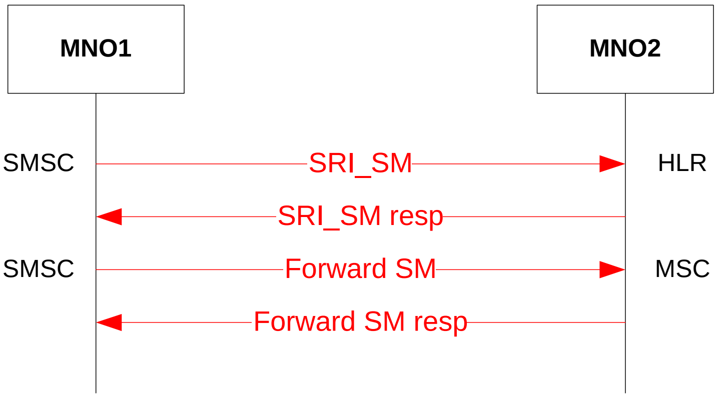
8.1 Current bi-lateral Client Operator to Client Operator architecture

This section illustrates the current technical connectivity architecture that is used between operators operating with MAP protocol over SS7.

Hubbing and bi-lateral connections are compatible concepts. Operators can and will most likely continue to maintain bi-lateral connections of this nature. It is likewise feasible within the architecture for operators to use any number of hubs, and one of those hubs simply has to be designated primary for the operator in terms of destination routing of incoming messages.

8.1.1 Process Flow

- o Operators will continue to maintain bi-lateral connections through standard MAP procedures over SS7 networks.
- o No changes if operators choose to maintain bi-lateral agreements



Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing tables to define which HLR to request route from.
1	SMSC sends an SRI-SM to MNO2 HLR.
2	MNO2 HLR responds with MSC/VLR location of subscriber for delivery of SM-MT.
3	SMSC delivers SM-MT to subscriber via specified MSC/VLR.
4	(optional) Delivery report generated.

8.1.2 Error management and retry logic

The following table lists error codes that may be returned on attempted delivery of an SM-MT (from SMSC to Client Operator).

An error code can either be Permanent (status P) or Temporary (status T). A permanent error means the SMSC will discard the message and take no further action. A temporary error will trigger re-try logic which is specific to each operator. A typical re-try process could be

- Retry 3 times at 30 second intervals
- Wait 2 hours and retry 3 times at 30 second intervals
- After 3 days, discard message.
- Optionally, send MS delivery failure report.

Error indication	Status	Meaning
Unknown subscriber	P	No allocated IMSI or directory number for the mobile subscriber in the HLR.
Teleservice not provisioned	P	Recipient MS has no SMS subscription
Call barred	T	MS barred
Facility not supported	T	SMS not provisioned in VPLMN
Absent subscriber	T	▪ there was no response via the SGSN, MSC or both ▪ the MS is subject to roaming restrictions ▪ The HLR does not have an MSC, SGSN or both numbers stored for the target MS ▪ Unidentified subscriber ▪ MS purged
MS busy for MT SMS	T	Congestion encountered at the visited MSC or the SGSN.
SMS lower layers capabilities not provisioned	T	MS not able to support the Short Message Service.
Error in MS	T	Error occurring within the MS at reception of short message, e.g. lack of free memory capacity or protocol error.
Illegal Subscriber	P	MS authentication failure
Illegal Equipment	P	IMEI of the MS black-listed in the EIR
System failure	T	Network or protocol failure others than those listed above. Please review the note under section 8.4.2 about this error as well.
Memory Capacity Exceeded	T	Short message rejected by MS because no memory capacity available to store the message

The table above has been sourced directly from 3GPP TS 23.40 [1].

There are several cases where a hub needs to reject a message being passed through it by an attached Client Operator. For instance, when an inter-working contractual relationship does not exist between MNO1 and MNO2 and a hub observes a message being sent from MNO1 to MNO2, that message has to be rejected. A permanent error code shall be returned and this is now specified to be the error code “Unknown subscriber” for SRI and “Unexpected Data Value” for MT_FSM.

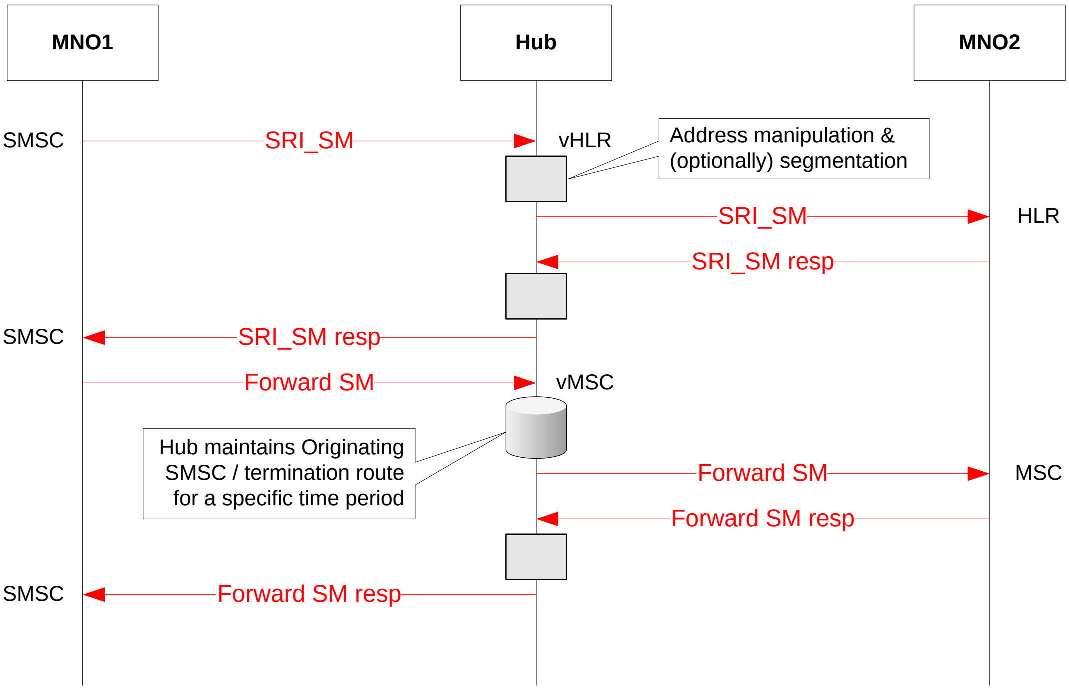
8.2 SS7 based Hubbing

8.2.1 Overview

This section describes SS7-based hubbing where the connectivity is entirely over SS7. This architecture has the advantage (over entirely SMPP/IP architectures and hybrid MAP/SS7-SMPP/IP architectures) of enabling reliable delivery reports.

8.2.2 Successful Outcome

The following flow-chart illustrates the successful SS7 hub based SMS inter-working scenario between MNO1 and MNO2.


MNO1
Hub
MNO2
SMSC
SRI_SM
vHLR
Address manipulation & (optionally) segmentation
SRI_SM
HLR
SRI_SM resp
SMSC
SRI_SM resp
Forward SM
vMSC
Hub maintains Originating SMSC / termination route for a specific time period
Forward SM
MSC
Forward SM resp
SMSC
Forward SM resp

Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing tables to define which HLR to request route from.
1	SMSC sends an SRI-SM to the vHLR located on the hub.
2	The hub modifies addressing information in a way that keeps MAP and SCCP addresses consistent (see section 7.1). The SRI request is then cascaded to the terminating operator (it could also be routed to a second hub).
3	The terminating operator receives the request from the hub and returns an error message or the necessary routing information (MSC location of the terminating subscriber).
4	The hub manipulates the address information replacing the terminating Client Operator’s MAP and SCCP address information with its own and forwards the error message or routing info back to the originating Client

	Operator.
5	The originating SMSC forwards the SM to the route that it has received. In this case, the route is to the hub's vMSC.
6	The hub has maintained the "Originating SMSC" / "Termination Route" relationship and now addresses the SM to the MNO2's MSC/VLR
7	The MNO2 responds to the hub with a delivery confirmation
8	The hub relays the delivery confirmation to the initiating Client Operator.
9	(Optional) the initiating subscriber receives a delivery report.

8.2.3 SS7 Transparency - Address Manipulation

The following diagram illustrates address manipulation by describing the message contents in the above example. The principles are the same for address manipulation for all the scenarios listed in this document and therefore subsequent process-flow diagrams do not go into message content details:

The address manipulation recommended involves appending the MCC+MNC to the MAP address. It is recommended that a 6 digit MCC+MNC be used in the translation to assure compatibility with North America, while observing that the maximum length of the address field is 15. CDMA operators may be assigned an MNC of 000 unless; further discussions have taken place with the MNC authority to get specific allocation. It is recommended that CDMA operators, who don't have specific allocation, make an application to obtain one.

The coding scheme needs to support three digit MNCs, for North America For elsewhere in the world, the two digit MNCs are suffixed with a 0 (Zero). Hence the use of six digits becomes standard.

8.2.3.1 Hub E.164 Address and MCC+MNC Translation Cases

8.2.3.1.1 Case 1.

When the Hub E.164 address (typically of similar length to the SCCP Global Title address) is short (less than or equal to 9 digits), the Hub shall append the MCC+MNC without over-writing any of the hub GT address information.

8.2.3.1.2 Case 2.

When the Hub E.164 address already exceeds 9 digits, appending the six digits for MCC+MNC would exceed the 15 digit limit of the MAP address / OA address. It is expected that the Hub will use a combination of appending and overwriting to prevent the 15 digits limit being exceeded, and maximize the use of the 15 digit allocated space.

In both cases none of the vital CC+NDC information in the Hub GT address prefix is expected to be over-written or lost.

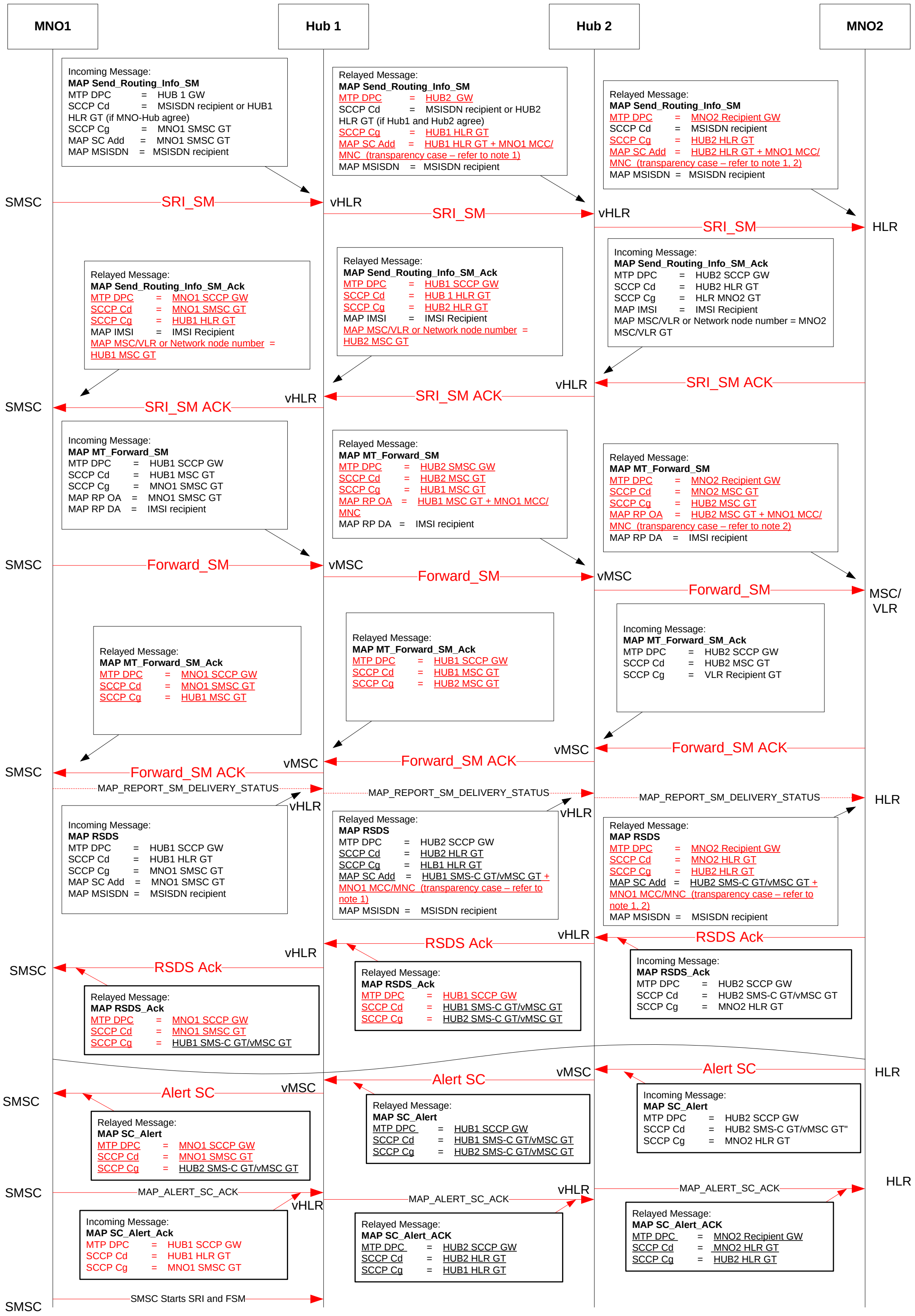
Given a 15-digit MAP SC Address field, this is expected to be achieved in the following way:

9 digits (SMSC GT address prefix of the last HUB) + 6 digits (originating MNO's MCC+MNC)

8.2.3.2 Hub E.164 Address and MCC+MNC Database

In light of the cases detailed previously, Hub operators must disclose to GSMA their translated E.164+MCC+MNC data, and GSMA for the trial, will establish a central file table or database.

8.2.3.3 Detailed diagram of the message flow



Incoming Message:
MAP Send_Routing_Info_SM
MTP DPC = HUB 1 GW
SCCP Cd = MSISDN recipient or HUB1 HLR GT (if MNO-Hub agree)
SCCP Cg = MNO1 SMSC GT
MAP SC Add = MNO1 SMSC GT
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = HUB2 GW
SCCP Cd = MSISDN recipient or HUB2 HLR GT (if Hub1 and Hub2 agree)
SCCP Cg = HUB1 HLR GT
MAP SC Add = HUB1 HLR GT + MNO1 MCC/ MNC (transparency case – refer to note 1)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = MNO2 Recipient GW
SCCP Cd = MSISDN recipient
SCCP Cg = HUB2 HLR GT
MAP SC Add = HUB2 HLR GT + MNO1 MCC/ MNC (transparency case – refer to note 1, 2)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = HUB1 MSC GT

Relayed Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB 1 HLR GT
SCCP Cg = HUB2 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = HUB2 MSC GT

Incoming Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 HLR GT
SCCP Cg = HLR MNO2 GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = MNO2 MSC/VLR GT

Incoming Message:
MAP MT_Forward_SM
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = MNO1 SMSC GT
MAP RP OA = MNO1 SMSC GT
MAP RP DA = IMSI recipient

Relayed Message:
MAP MT_Forward_SM
MTP DPC = HUB2 SMSC GW
SCCP Cd = HUB2 MSC GT
SCCP Cg = HUB1 MSC GT
MAP RP OA = HUB1 MSC GT + MNO1 MCC/ MNC
MAP RP DA = IMSI recipient

Relayed Message:
MAP MT_Forward_SM
MTP DPC = MNO2 Recipient GW
SCCP Cd = MNO2 MSC GT
SCCP Cg = HUB2 MSC GT
MAP RP OA = HUB2 MSC GT + MNO1 MCC/ MNC (transparency case – refer to note 2)
MAP RP DA = IMSI recipient

Relayed Message:
MAP MT_Forward_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 MSC GT

Relayed Message:
MAP MT_Forward_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = HUB2 MSC GT

Incoming Message:
MAP MT_Forward_SM_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 MSC GT
SCCP Cg = VLR Recipient GT

Incoming Message:
MAP RSDS
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 HLR GT
SCCP Cg = MNO1 SMSC GT
MAP SC Add = MNO1 SMSC GT
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP RSDS
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 HLR GT
SCCP Cg = HLB1 HLR GT
MAP SC Add = HUB1 SMS-C GT/vMSC GT + MNO1 MCC/MNC (transparency case – refer to note 1)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP RSDS
MTP DPC = MNO2 Recipient GW
SCCP Cd = MNO2 HLR GT
SCCP Cg = HUB2 HLR GT
MAP SC Add = HUB2 SMS-C GT/vMSC GT + MNO1 MCC/MNC (transparency case – refer to note 1, 2)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP RSDS_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 SMS-C GT/vMSC GT

Relayed Message:
MAP RSDS_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 SMS-C GT/vMSC GT
SCCP Cg = HUB2 SMS-C GT/vMSC GT

Incoming Message:
MAP RSDS_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 SMS-C GT/vMSC GT
SCCP Cg = MNO2 HLR GT

Relayed Message:
MAP SC_Alert
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB2 SMS-C GT/vMSC GT

Relayed Message:
MAP SC_Alert
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 SMS-C GT/vMSC GT
SCCP Cg = HUB2 SMS-C GT/vMSC GT

Incoming Message:
MAP SC_Alert
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 SMS-C GT/vMSC GT"
SCCP Cg = MNO2 HLR GT

Incoming Message:
MAP SC_Alert_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 HLR GT
SCCP Cg = MNO1 SMSC GT

Relayed Message:
MAP SC_Alert_ACK
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 HLR GT
SCCP Cg = HUB1 HLR GT

Relayed Message:
MAP SC_Alert_ACK
MTP DPC = MNO2 Recipient GW
SCCP Cd = MNO2 HLR GT
SCCP Cg = HUB2 HLR GT

Take note that the SCCP Cd address in the SRI_SM is the MSISDN of the recipient, which implies that the hub must be capable of ad hoc routing for SS7 messages based on the originating entity. The parties involved may also opt to use SCCP Cd address based on next node address, in order to accommodate hubs that are not SCCP providers.

The transparency information is mandatory in the MT_FSM.

The section diagrammed above for RSDS (MAP_REPORT_SM_DELIVERY_STATUS) applies for cases of an error.

The hub-to-operator interface is considered private and therefore it does not necessarily have to strictly follow what is diagrammed, although what is depicted is the best and recommended approach. The hub and operator may still achieve their interworking in a different way, and the approach remains valid as long as transparency and the OC High Level Requirements are maintained. The hub-to-hub interface however is considered public and therefore this needs to strictly follow the message flow inter-working diagram.

In a multiple short message transfer using the more message to send capability, the FSM can be used several times within a single TCAP transaction. As defined in 3GPP TS 29.002 [2], the parameter SM-RP-DA and SM-RP-OA shall be omitted in the subsequent FSM's. On the other hand, if the originating party becomes a different operator in a series of messages, then the next message needs to be in a different TCAP dialog, as the transparency originating network ID becomes different.

Notes:
Note 1: Transparency is optional on SRI on the hub-to-operator interface, and considered mandatory on the hub-to-hub interface, where it is crucial to enable hubs to verify the originator of the message. Transparency is optional on RSDS on the hub-to-operator interface and on the hub-to-hub interface. The transparency being optional on the hub-to-operator interface is to circumvent a potential issue in ALERT_SC handling which could generate a return message to the Hub GT address + MCC/MNC. This may not be routable on SCCP. In any case the terminating hub (HUB2) is responsible for ALERT_SC, if required, is sent to the GT of the originating hub (HUB1) as SCCP Cd PA. The conditions surrounding this are best discussed by the hub and operator and between hubs to come up with an approach that is workable.

Notes 2: Transparency may be requested by the operator not to be included, e.g. for instance if the operator is concerned about the change impact vis-à-vis their wholesale billing application. The hub can place their GT address in the MAP SC Address field to suppress transparency. On the other hand, if the operator explicitly requires it then the hub shall provide transparency.

MAP Specification References:
For reference only, the following excerpts from 3GPP TS 29.002 [2] (version 7.15.0 Release 1998) are included.

From page 731:

- if no MSC identity is stored for the mobile subscriber or the "MSC Area Restricted Flag" is set or the "MS purged for non GPRS" flag is set, i.e. the MS is not reachable, the MSISDN-Alert and the SC address are included in the MWD (if possible), the flag MNRF is set and the "Absent Subscriber_SM" error is returned with the appropriate absent subscriber diagnostic indication, i.e. 'Deregistered in HLR for non GPRS ', 'Roaming Restricted' or 'MS-Purged for non GPRS '.

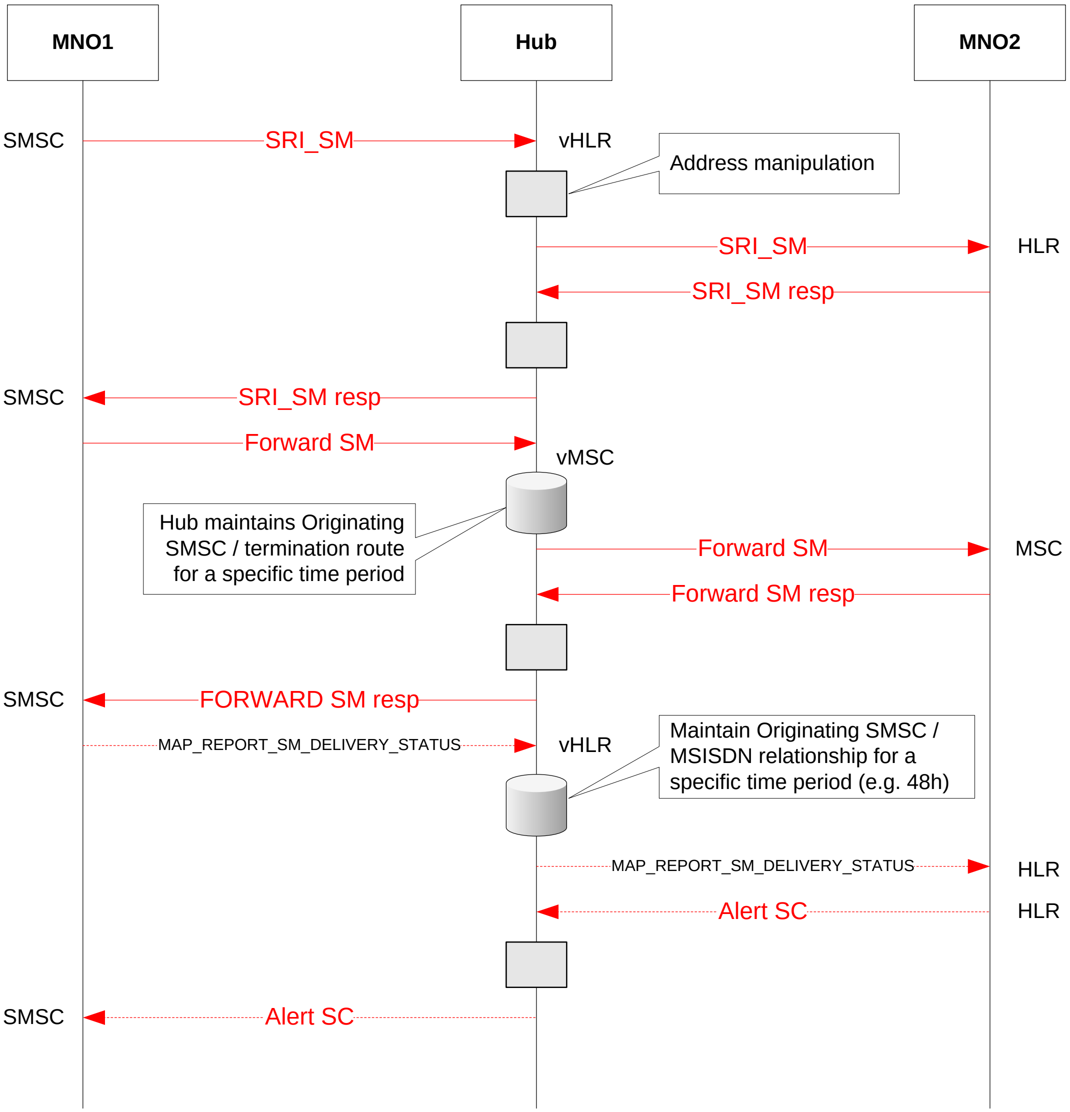
From page 90:

7.6.8.3 MWD status

This parameter indicates whether or not the address of the originator service centre is already contained in the Message Waiting Data file. In addition, it contains the status of the Memory Capacity Exceeded Flag (MCEF), the status of the Mobile subscriber Not Reachable Flag (MNRF) and the status of the Mobile station Not Reachable for GPRS flag (MNRG).
MS not reachable flag (MNRF)

8.2.4 Error management and retry logic

Error code and re-try management should be analogous to the Client Operator-Client Operator scenario described in 8.1. The following process-flow illustrates an SS7-based hubbing scenario where the terminating Client Operator returns a non-delivery reason code back to the hub as a response to the Forward_SM request. This is a common scenario and could indicate, for instance, the subscriber has his/her mobile temporarily switched off.


MNO1
Hub
MNO2
SMSC
SRI_SM
vHLR
Address manipulation
SRI_SM
HLR
SRI_SM resp
SMSC
SRI_SM resp
Forward SM
vMSC
Hub maintains Originating SMSC / termination route for a specific time period
Forward SM
MSC
Forward SM resp
SMSC
FORWARD SM resp
MAP_REPORT_SM_DELIVERY_STATUS
vHLR
Maintain Originating SMSC / MSISDN relationship for a specific time period (e.g. 48h)
MAP_REPORT_SM_DELIVERY_STATUS
HLR
Alert SC
HLR
SMSC
Alert SC

Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing

	tables to define which HLR to request route from.
1	SMSC sends an SRI-SM to the vHLR located on the hub.
2	The hub modifies addressing information in a way that keeps MAP and SCCP addresses consistent (see section 7.1). The SRI request is then cascaded to the terminating operator (it could also be routed to a second hub).
3	The terminating operator receives the request from the hub and returns an error message or the necessary routing information (MSC location of the terminating subscriber). In this case, the return code is an error code with error reason of type “T” (Temporary) and with reason code “Absent Subscriber”:
4	The hub manipulates the address information replacing the terminating Client Operator’s MAP and SCCP address information with its own and forwards the error message back to the originating Client Operator.
5	The originating SMSC forwards a MAP_REPORT_SM_DELIVERY_STATUS request to the vHLR. The hub must store the relationship between the originating SMSC and the terminating MSISDN and forward the alert request to the MNO2 HLR.
6	When the subscriber next becomes active, the HLR will send an alert to the hub, informing of delivery status
7	The hub relays the alert to the originating SMSC. The SMSC can then repeat the SRI request to re-send the message if necessary.
8	After a successful transfer an SMS-C may issue a Report Short Message Delivery Status with the code "successful transfer" to the HLR of the terminating network. This should also be handled transparently through the Hub.

8.3 IP-based Hubbing

8.3.1 Overview

IP-based hubbing uses the SMPP client/server protocol over TCP/IP. The connections between Client Operators and hubs can be TCP/IP tunnels which are generally more cost-efficient than SS7 connections and do not necessarily involve per-message pricing structures.

The SMPP does support delivery reporting although this is not generally effective in practice, as the destination operator usually does not support it.

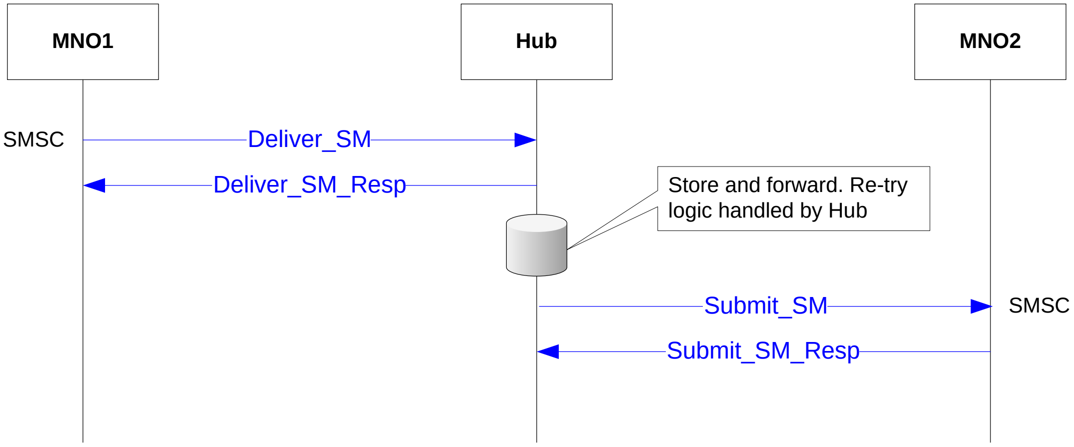
The SMPP hub can optionally handle SM store & forward; however it is necessary when the destination is using SS7 inter-working. We describe both cases in the following sections:

8.3.2 SMPP General Requirements

1. Protocols – SMPP v3.4 as the default
2. Character set – 7 bit ASCII and 7 bit GSM
3. Source and destination numbers will be passed in E.164 international format
4. Messages shall have the parameter TON = 1 (International) and NPI=1 (ISDN (E163/E164)).
5. Messages length / Concatenated messages – No maximum message length, the hub will handle the segmentation if necessary
6. Binary Data or special User Data – still for assessment on the extent of support. At the very least GSM binary user data should be fully supported since it is a well known service, which for example could contain v-cards, picture or ring tones. This is further supported from the architecture requirement of maintaining the user message data untouched when the end-points are using the same SMS inter-working protocol. Any binary content in such a scenario should remain intact.
7. The `submit_multi` operation may be used to submit an SMPP message for delivery to multiple recipients or to one or more Distribution Lists. The `submit_multi` PDU does not support the transaction message mode. In case SMPP is used for SMS interworking, it is recommended that `submit_multi` not be implemented in order to reduce technical and commercial complexity. Also, `submit_multi` in SMPP has only one message ID. It is thus unclear what SMS in a `submit_multi` are delivered to the customer’s handset when a delivery receipt is generated. It is common practice in big distribution lists that messages are submitted one by one, so that a unique message id is registered.
8. SMPP Bind Direction
   - Operator to Hub – it is recommended that the Hub shall bind to the operator—i.e., the Hub is the client (ESME) and MNO is the server (SMSC). The operator may still however request a different setup. The diagrams presented in the succeeding sections illustrate the recommended bind setup, but does not rule out a different bind direction.
   - Hub to Hub - Hubs shall support both client and server mode to be flexible. The diagrams presented in the succeeding sections illustrate the recommended bind setup, but does not rule out a different bind direction.

8.3.3 Hub implements store-and-forward

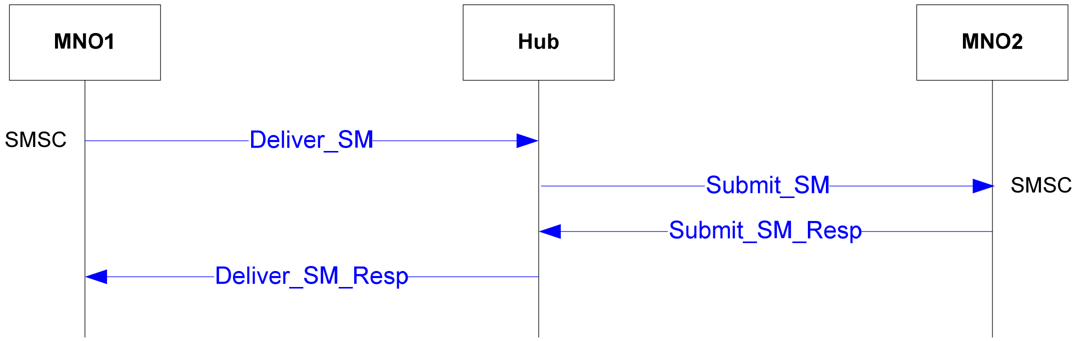
This is the default implementation.



Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing tables to decide which routing strategy to apply.
1	SMSC sends a deliver SM request to the hub.
2	The hub stores the request and responds with a “message sent” acknowledgement. This is not reliable as the hub has in reality not yet forwarded the message to its destination.
3	The hub forwards the message to the terminating Client Operator, and converts the message to a SUBMIT_SM.
4	The terminating Client Operator responds with an error message or an acknowledgment.

8.3.4 Hub acts as proxy

This is an alternative implementation, which should work fine if IP is applied end-to-end. It is not feasible when the end-point is on SS7. SMPP error codes do not support temporary errors that can be generated by the SS7 destination, unless a new temporary error code is introduced on SMPP.



Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing tables to decide which routing strategy to apply.
1	SMSC sends a deliver SM request to the hub.
2	The hub forwards the message to the terminating MNO2.
3	MNO2 responds to hub
4	The hub forwards the response to MNO1

8.3.5 SMPP Transparency

This section the parameters within SMPP standards that are to be utilized to pass operator identification information that is necessary to satisfy the transparency requirement. There are 2 SMPP parameters to be utilized: `source_subaddress` and `dest_subaddress`.

The possibility of using `source_network_id` and `dest_network_id` parameters defined in SMPP v5.0 has been considered as well. There is close similarity in the definition of these parameters and the way that SMS Hubbing transparency uses MCC+MNC. However, there is also substantial difference in actual semantics. The SMS Hubbing definition of transparency consistently uses 6-digit MCC+MNC for all types of operators; and the SMPP version 5.0 definition for `source_network_id` and `dest_network_id` does not. For the moment, the long-held transparency definition is not going to be changed, and perhaps appropriate liaison with SMPP forum can be made in the future.

8.3.5.1 Source_subaddress

The `source_subaddress` will be utilized to identify the source operator that is associated with the MSISDN issuing the SMS message.

- Parameter Tag
    - Size 2 Octets
    - Type Integer
- Length
    - Size 2 Octets
    - Type Integer
    - Description Length value part in octets
- Value
    - Size Var, 2-23
    - Type Octet, String
    - Description The first octet of the data field is a type of subaddress tag and indicates the type of subaddressing information included, and implies the type of length of subaddressing information which can accompany this tag value in the data field.
      The value tag to be used is:
      10100000 – User Specified
      The remaining octets contain the source operator identification value. The value to be used shall be the 6 digit MCC + MNC for GSM operators. CDMA operators shall use an MNC of 000 unless; further discussions have taken place with the MNC authority to get specific allocation.

Example

0202	Src_Subaddr_Tag
0007	Src_Subaddr_Len
a0	Src_Subaddr_Contents type (user defined)
333130333830	Src_Subaddr_Contents value (310380)

```
00 00 00 5d 00 00 00 04 00 00 00 00 a0 9b 67 46  | ...]..........gF
00 01 01 31 38 31 32 32 31 32 30 30 30 31 00 01  | ...18122120001..
01 31 38 31 33 32 31 33 30 30 30 31 00 00 00 00  | .18132130001....
00 00 00 00 00 00 10 31 20 6b 65 6e 79 40 73 6b  | .......1 keny@sk
79 70 65 2e 6e 65 74 02 02 00 07 a0 33 31 30 33  | ype.net.....3103
31 30 02 03 00 07 a0 33 31 30 33 38 30              | 10.....310380
```

8.3.5.2 Dest_subaddress

The `dest_subaddress` will be utilized to identify the destination operator that is associated with the MSISDN receiving the SMS message. This parameter is utilized only in the context of MNP, and when it is present it indicates that an MNP dip has been performed.

- Parameter Tag
  - o Size 2 Octets
  - o Type Integer
- Length
  - o Size 2 Octets
  - o Type Integer
  - o Description Length value part in octets
- Value
  - o Size Var, 2-23
  - o Type Octet, String
  - o Description The first octet of the data field is a type of subaddress tag and indicates the type of subaddressing information included, and implies the type of length of subaddressing information which can accompany this tag value in the data field.
    The value tag to be used is:
    10100000 – User Specified
    The remaining octets contain the destination operator identification value. . The value to be used shall be the 6 digit MCC + MNC for GSM operators. CDMA operators shall use an MNC of 000 unless; further discussions have taken place with the MNC authority to get specific allocation. It is recommended that CDMA operators look into obtaining their own MCC + MNC allocation.
    .

Example

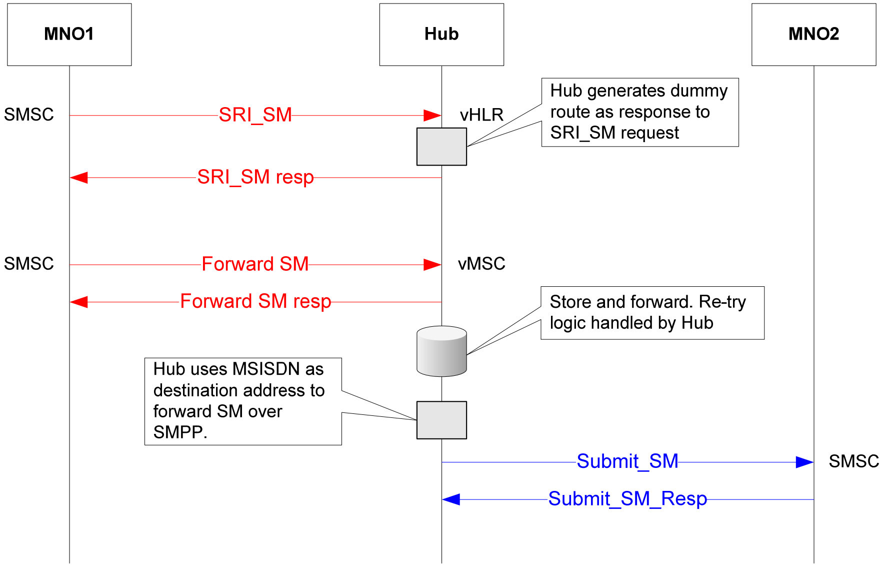
0203	Dst_Subaddr_Tag
0007	Dst_Subaddr_Len
a0	Dst_Subaddr_Contents type (user defined)
333130333130	Dst_Subaddr_Contents value (310380)

```
00 00 00 5d 00 00 00 04 00 00 00 00 a0 9b 67 46  | ...].........gF
00 01 01 31 38 31 32 32 31 32 30 30 30 31 00 01  | ...18122120001..
01 31 38 31 33 32 31 33 30 30 30 31 00 00 00 00  | .18132130001....
00 00 00 00 00 00 10 31 20 6b 65 6e 79 40 73 6b  | .......1 keny@sk
79 70 65 2e 6e 65 74 02 02 00 07 a0 33 31 30 33  | ype.net.....3103
31 30 02 03 00 07 a0 33 31 30 33 38 30           | 10.....310380
```

8.4 Hybrid Scenarios – inter-standard inter-working

8.4.1 SS7 to IP with store and forward

When the destination is IP, the store-and-forward works equally as well as the opposite case (Section 8.4.2)

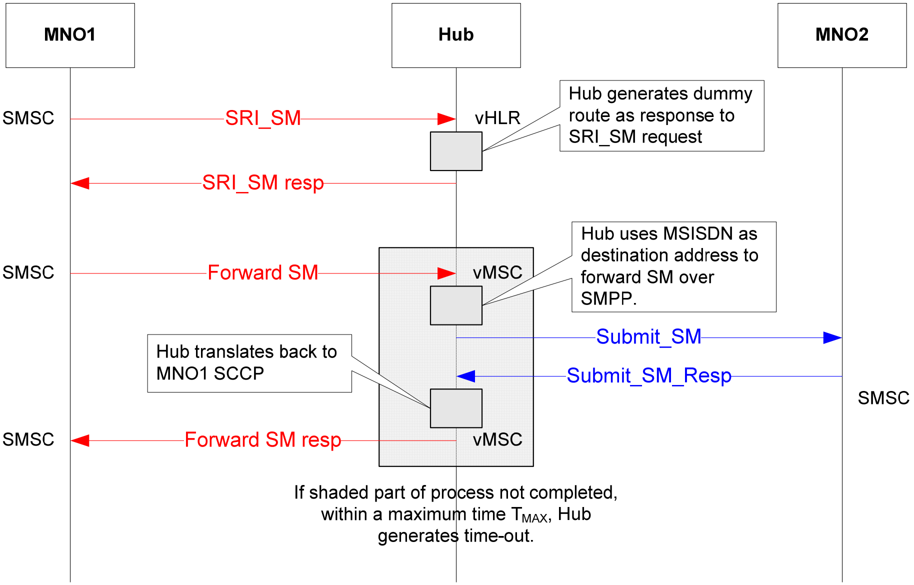

MNO1
Hub
MNO2
SMSC
SRI_SM
vHLR
Hub generates dummy route as response to SRI_SM request
SRI_SM resp
SMSC
Forward SM
vMSC
Forward SM resp
Store and forward. Re-try logic handled by Hub
Hub uses MSISDN as destination address to forward SM over SMPP.
Submit_SM
SMSC
Submit_SM_Resp

Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing tables to decide which routing strategy to apply.
1	MNO1 SMSC sends an SRI request to the hub.
2	The hub generates a dummy SRI response to MNO1. The MAP IMSI prefix of the SRI response shall be consistent with the MCC+MNC of MNO2, and the MAP VLR address shall be the Hub vMSC GT address.
3	MNO1 SMSC send an MT_FSM to the hub
4	The hub generates an MT_FSM response.

5	The hub forwards the message to the terminating MNO2 and converts the message to a SUBMIT_SM.
6	MNO2 responds to hub

8.4.2 SS7 to IP (no store and forward)

When the destination is IP, this case, no store-and-forward works equally as well as the opposite case (Section 8.4.1)


MNO1
Hub
MNO2
SMSC
SRI_SM
vHLR
Hub generates dummy route as response to SRI_SM request
SRI_SM resp
SMSC
Forward SM
vMSC
Hub uses MSISDN as destination address to forward SM over SMPP.
Submit_SM
Hub translates back to MNO1 SCCP
Submit_SM_Resp
SMSC
SMSC
Forward SM resp
vMSC
If shaded part of process not completed, within a maximum time T_{MAX}, Hub generates time-out.

Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing tables to define which HLR to request route from.
1	SMSC sends an SRI-SM to the vHLR located on the hub.
2	The hub responds immediately providing MNO1with the route to its vMSC. The MAP IMSI prefix of the SRI response shall be consistent with the MCC+MNC of MNO2, and the MAP VLR address shall be the Hub vMSC GT address.
3	MNO1 forwards the SM to the hub’s vMSC. The hub needs to communicate this SM to MNO2 via SMPP. However, as the hub will need to respond to MNO1 via SS7, the originating SMSC and destination MSISDN relationship must be maintained at this point. The SMPP communications must be completed within a given period (T_{MAX}) or the hub should return a time-out to MNO1. In SMPP a Response Timer is defined. This timer specifies the time lapse allowed between a SMPP request and the corresponding SMPP response. SMPP Response Timer in the Hub has to be lower than the timer for MT_Forward_SM and MNO2 is supposed to reply within the SMPP Response Timer. This is to prevent a potential double sending of the message, whereby MNO2 is still sending the message while the hub already has assumed the timeout state. This timeout condition should normally never occur. If it does, it may indicate that either SMPP or SS7

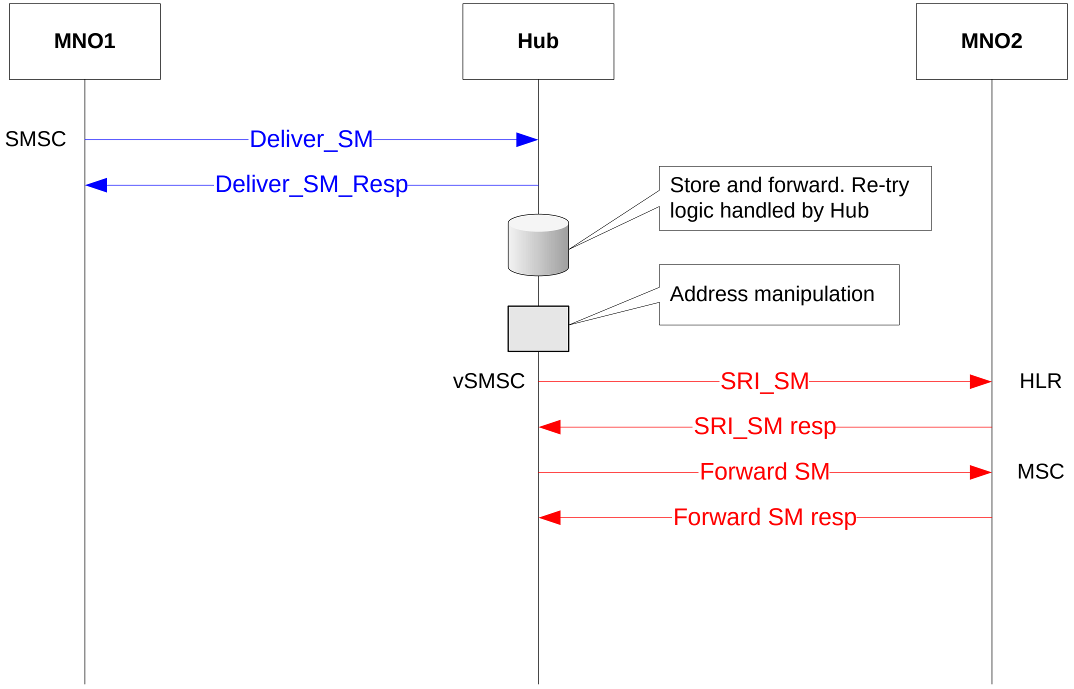
	response timer is not properly set.
4	The hub forwards the SM to MNO2 via SMPP SUBMIT_SM.
5	MNO2 responds to the forward with a delivery response.
6	The hub translates the response back to SS7, replacing the MAP and SCCP addresses to its own and relays the response to the originating MNO1.

In the general 2 hub case and in the event of a permanent error at the MNO2 side, HUB2 shall only be able to block at the MT_FSM message coming from HUB1. Since the MT_FSM is occurring after a successful SRI, it is possible that the MNO1 SMSC may retry. As much as possible, blocking on MT_FSM should be avoided; however in this case the error codes “System failure”, “Unexpected Data Value”, “Data missing”, “Illegal Subscriber” or “Illegal equipment” can be used and this may minimize the retry mechanism—and “System failure” shall be considered the default value. In the event that the retry mechanism from the MNO1 SMSC cannot be avoided, then the Hubs should be able to handle and block the SRI from any further retry attempts—i.e., by recognizing that destination MSISDN is the same. Effectively hubs have a cache of recent MSISDNs that have returned with permanent error failures that may be used to immediately block SMS; however such a cache shall not have retention of longer than 10 minutes per destination MSISDN, in the absence of fresh information. This has to be selectively applied per client operator of the hub rather than making it a globally applied mechanism.

3GPP TS 23.40 [1] defines the “System Failure” error as temporary, but this is now confirmed to be a permanent error based from authoritative sources. Therefore, it is now believed that 3GPP TS 23.40 [1] is merely in error and needs correction.

8.4.3 IP to SS7 store and forward

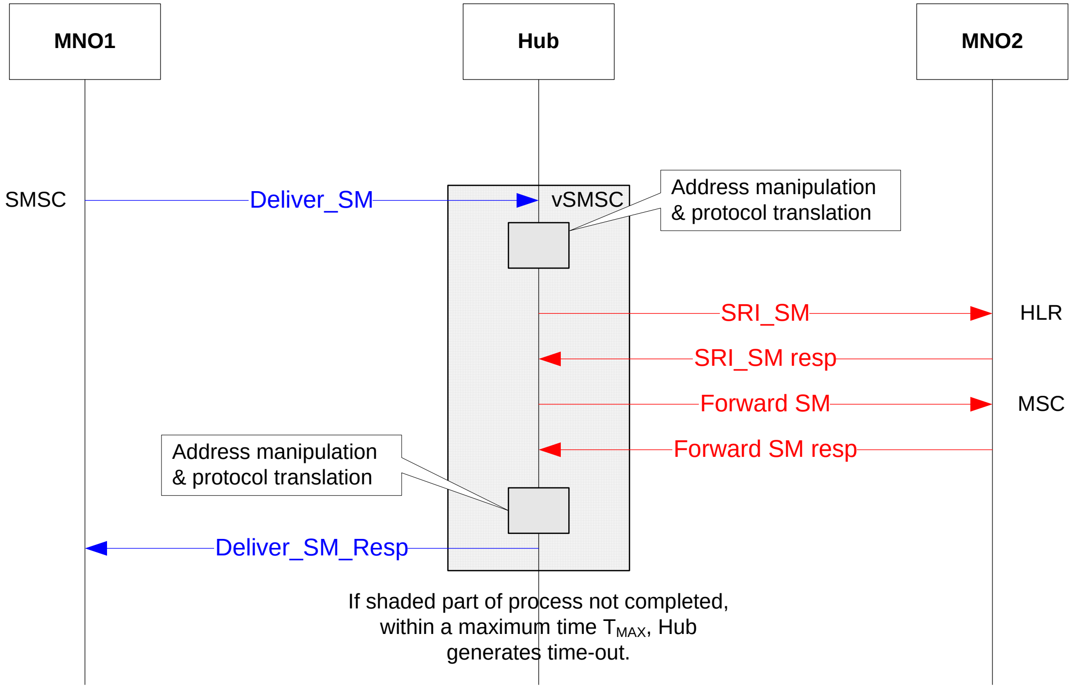
This is the recommended default implementation.



Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing tables to decide which routing strategy to apply.
1	SMSC sends a deliver SM request to the hub.
2	The hub stores the request and responds with a “message sent” acknowledgement. This is not reliable as the hub has in reality not yet forwarded the message to its destination. The hub can create an internal message ID.
3	The hub generates an SRI request to MNO2 using the hub’s SCCP and MAP addresses.
4	The terminating operator receives the request from the hub and returns an error message or the necessary routing information to the hub’s vSMSC.
5	The hub forwards the SM to the route that it has received.
6	The MNO2 responds to the hub with a delivery confirmation

8.4.4 IP to SS7 (no store and forward)

This implementation is not feasible when the end-point is on SS7. SMPP error codes do not support temporary errors that can be generated by the SS7 destination, unless a new temporary error code is introduced on SMPP.


MNO1
Hub
MNO2
SMSC
Deliver_SM
vSMSC
Address manipulation & protocol translation
SRI_SM
HLR
SRI_SM resp
Forward SM
MSC
Forward SM resp
Address manipulation & protocol translation
Deliver_SM_Resp
If shaded part of process not completed, within a maximum time T_{MAX}, Hub generates time-out.

Stage	Description
0	Subscriber generates SM. SMSC receives SM-MO and consults routing tables to decide which routing strategy to apply.

1	SMSC sends a deliver SM request to the hub.
2	The hub generates an SRI request to MNO2 using the hub's SCCP and MAP addresses.
3	The terminating operator receives the request from the hub and returns an error message or the necessary routing information to the hub's vSMSC. The hub needs to communicate this SM to MNO2 via SS7. The SS7 communications must be completed within a given period (TMAX) or the hub should return a time-out to MNO1. In SS7 a Response Timer is defined MT_Forward_SM is a medium long range timer (from 1m to 10m). This timer specifies the time lapse allowed between a SMPP request and the corresponding SMPP response. SMPP Response Timer in the Hub has to be lower than the timer for MT_Forward_SM and MNO2 is supposed to reply within the SMPP Response Timer. This is to prevent a potential double sending of the message, whereby MNO2 is still sending the message while the hub already has assumed the timeout state.
4	The hub forwards the SM to the route that it has received.
5	The MNO2 responds to the hub with a delivery Confirmation
6	The hub has maintained the originating SMSC/terminating MSISDN combination and can relay the delivery confirmation to the initiating MNO1 via SMPP.

8.4.5 Inter-standard inter-working and extending the response time on the ingress interface of the destination hub

There is value in extending the time taken to respond for as long as possible on the ingress part of the destination hub (HUB2) who is handling the inter-standard conversion. For instance, in the IP to SS7 scenario shown in section 8.4.3, the Deliver_SM response does not need to be returned immediately upon receipt of the Deliver_SM. The destination hub can allow some time to pass in order to provide opportunity for MNO2 to return information about the state of the recipient subscriber. For instance, the SS7 recipient MNO2 may return "unknown subscriber" state which can be relayed to the ingress interface.

Therefore, HUB2 returns a response either when the response to the egress interface is received, or if the ingress interface timer should expire. This handling is most relevant in permanent error conditions

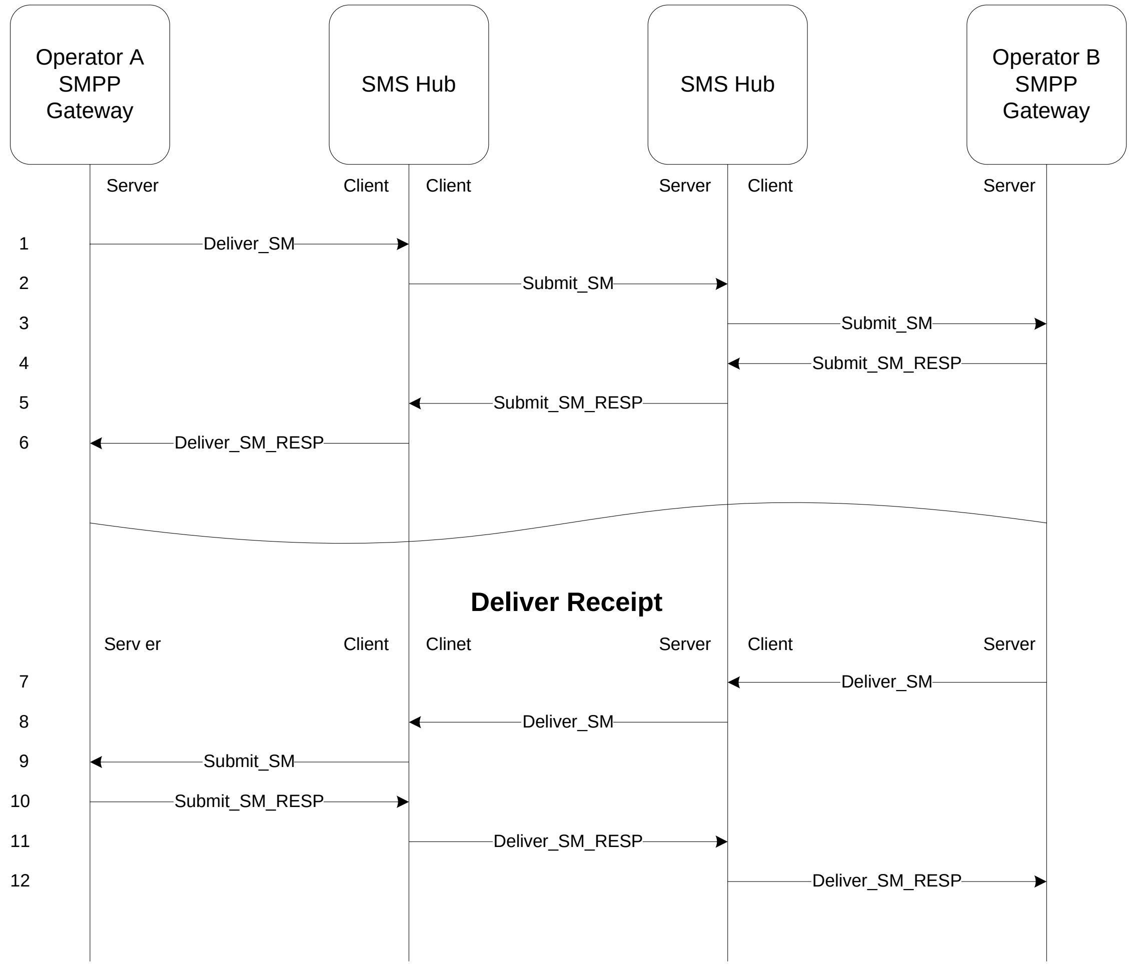
8.5 Delivery Reporting on SMPP

Honest delivery is not usually guaranteed in an SMPP environment. Operators for whom the SMS delivery service is important are recommended to use MAP/SS7. This is the recommended implementation for delivery reporting in SMPP. The accuracy of the result remains dependent on whether the destination operator supports the facility. The status as to whether operators using SMPP also support honest delivery reports should be collected by Hub providers so that they can cascade the information to other client operators.

The materials presented in this section will be of most benefit to operator using SMPP who also do have support for honest delivery reports. If the SMPP operator does not support honest delivery reports, then any implementation is consequently ineffective as well in terms of the delivery reporting.

8.5.1 Originating and Destination Client Operator is SMPP

If the originating operator requires an additional delivery confirmation they will be required to request a delivery receipt.



1) The source operator issues a Deliver_SM to its SMS Hub with a registered delivery request. The source SMS Hub emulates an SMPP client when receiving the message from the source operator. The initial Deliver_SM can also be a Submit_SM if it is agreed between the operator and the hub, such as for the purpose of having a message ID relayed to the operator, and which could be later associated to the deliver receipt.
2) The source SMS Hub issues a Submit_SM to the destination SMS Hub with the registered delivery flag set. The source SMS Hub emulates an SMPP client and the destination SMS Hub emulates an SMPP server.

3) The destination SMS Hub issues a Submit_SM to the destination operator. The destination SMS Hub emulates an SMPP client when issuing the message to the destination operator.
4) The destination operator responds to the destination SMS Hub with a Submit_SM_Resp.
5) The destination SMS Hub responds to the source SMS Hub with a Submit_SM_Resp. The source SMS Hub emulates an SMPP client and the destination SMS Hub emulates an SMSC.
6) The source SMS Hub responds to the source operator with a Deliver_SM_Resp. The source SMS Hub emulates an SMPP client.
7) After some time has passed the destination MS receives the message and the destination operator issues the acknowledgement that the MS has received the message. The destination operator issues a Deliver_SM to the destination SMS Hub. The destination SMS Hub emulates an SMPP client.
8) The destination SMS Hub issues a Deliver_SM to the source SMS Hub. The destination SMS Hub emulates an SMPP server when issuing the message to the source SMS Hub.
9) The source SMS Hub issues a Submit_SM to the source operator. The source SMS Hub emulates an SMPP client.
10) The source operator responds to the source SMS Hub with a Submit_SM_Resp.
11) The source SMS Hub responds to the destination SMS Hub with a Deliver_SM_Resp
12) The destination SMS Hub responds to the destination operator with a Deliver_SM_Resp.

8.5.2 Use of Submit_SM instead of Deliver_SM in the originating operator to hub interface

Many arguments have been raised why this interface should use Submit_SM instead of Deliver_SM. The purpose of this section is simply to summarize them. Item 8 in section 8.3.4 specifies that the bind direction in this interface can be either way depending on the operator preference. Based on the SMPP specifications, there is a strict association between bind direction and the use of Submit_SM or Deliver_SM, and this shall have to be closely followed still.

Reasons for the use of Submit_SM:

1) The operation performed is a submission operation to the Hub (and either Submit_SM or Data_SM is to be used according to the SMPP specifications) and not a delivery operation to a Short Message Entity (Deliver_SM)
2) The SMS-MO received by the SMSC has been entered in the originating MNO store-and-forward message database and is to be submitted to another SMSC/Hub
3) Some SMSCs may have a problem in using the Deliver_SM command to send an SMS to be forwarded, and some will not be able to properly handle the errors that may occur, and could not set Deliver_SM options (such as expiry time).
4) No message ID can be supplied by the first SMS Hub since SMPP V3.4 explicitly states that the message-ID field in Deliver_SM_Resp has to be set to NULL.
5) Better Service Troubleshooting. A message can be isolated easily to determine the cause why it could not be submitted or delivered. Trying to identify a message by the originator or destination number may result in multiple

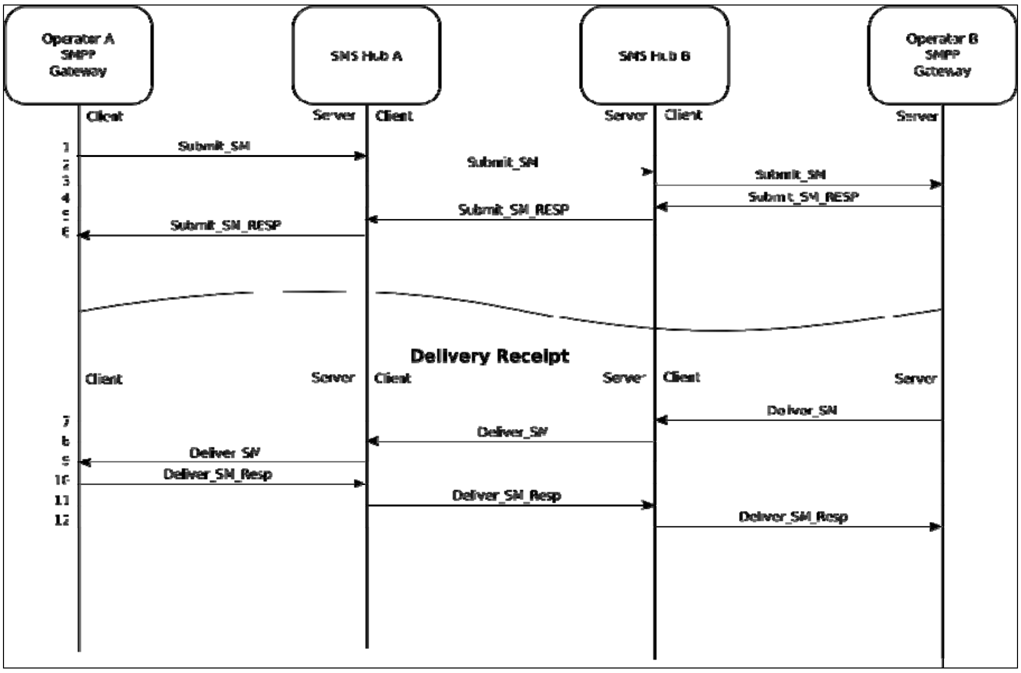
messages, and could make it harder to determine an error cause that is specific to a single message.

6) The delivery receipt can be uniquely matched against the message that was submitted. This is especially useful when multiple messages have been sent from the originator to the destination; for example with a concatenated SMS.
7) Being able to match delivery receipts against sent messages results in easier monitoring of delivery quality.

In the deliver receipt, a Deliver_SM is to be used:

1) Chapter 2.11 (Message Types) of the SMPP V3.4 specification states that a delivery receipt has to be sent either through a Deliver_SM or Data_SM.
2) Chapter 5.2.12 (esm_class) of the SMPP V3.4 specification allows the bits to identify the delivery receipt type only for Deliver_SM and Data_SM to be set.

This alternative deliver report handling in SMPP is fully compatible with the SMS Hubbing Architecture, and is diagrammed as follows:



1) The source operator “Operator A” sends a Submit_SM request to SMS Hub A with the “registered delivery” flag.
2) SMS Hub A forwards the Submit_SM request to SMS Hub B
3) SMS Hub B then forwards the Submit_SM request to the destination operator “Operator B”
4) Operator B responds with a Submit_SM_Resp to SMS Hub B. This Response contains a message id for the submitted message.
5) SMS Hub B forwards the Submit_SM_Resp to SMS Hub A
6) SMS Hub A again forwards the Submit_SM_Resp to the source operator “Operator A”
7) When the message reaches a certain state Operator B sends a Delivery Receipt by means of a Deliver_SM PDU to SMS Hub B. This Delivery Receipt contains

the same message id in the optional field “receipted_message_id” that was contained in the Submit_SM_Resp in step 4.

8) SMS Hub B forwards the Deliver_SM to SMS Hub A
9) SMS Hub A finally sends the Deliver_SM to the source operator “Operator A”.
10) Operator A can now match the message id in the Delivery Receipt from step 9 against the one in the Submit_SM_Resp in step 6. He then responds with a Deliver_SM_Resp
11) SMS Hub A forwards the Deliver_SM_Resp to SMS Hub B
12) SMS Hub B again forwards the Deliver_SM_Resp to Operator B

This alternative SMPP deliver report handing will require 2 binds as minimum standard in order for the originating operator to handle reply messages via the hub using Submit_SM coming from the hub.

8.5.3 2 Binds in the hub-to-hub interface

Because there is a strict association between the use of Submit_SM or Deliver_SM and the bind direction in the SMPP specifications, there is a need for 2 binds in the hub-to-hub interface. This is to allow the hubs to handle messages properly in either direction. Each hub has to be able to perform both Submit_SM and Deliver_SM towards their partner hubs according to what is required.

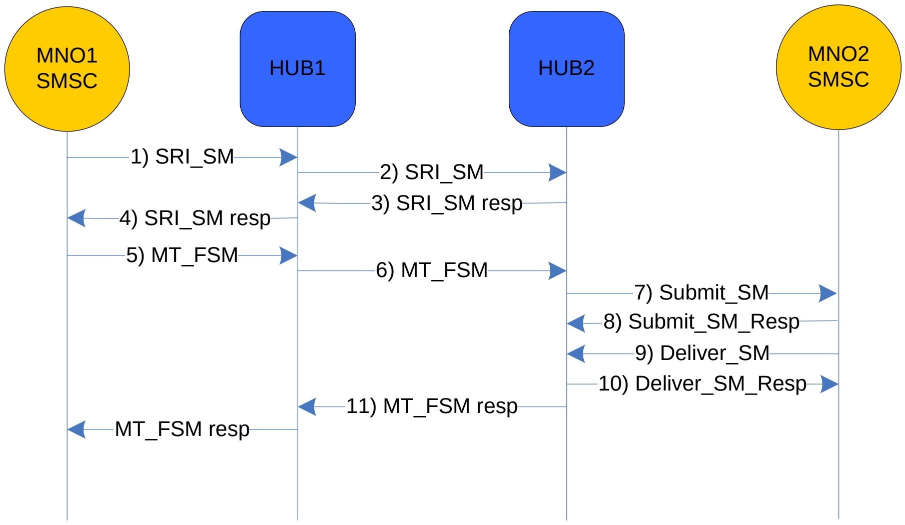
This is necessary in case a deliver receipt is requested where SUBMIT_SM must be used in the initial message delivery to establish a message ID.

This is the minimum standard base configuration that hubs shall provide; however, in the event that hubs agree that the equivalent capability is sufficiently addressed using only one bind then they are not restricted from pursuing an alternative configuration, and shall equally support deliver receipts.

8.5.4 SS7 Originating Operator to SMPP Destination Operator Deliver Reports

Deliver reporting currently mainly does not work for the specific case of SS7 to SMPP because the destination operator does not support deliver reports. This is most particularly the case when the destination operator is in North America and using CDMA.

Assuming MNO2 supports honest delivery reports; deliver reporting shall work in the following way:



1) MNO1 sends SRI to HUB1
2) HUB1 sends SRI to HUB2
3) HUB2 knows the destination is on SMPP, so it must return a dummy SRI response to obtain the message payload. HUB2 generates dummy SRI response to HUB1
4) HUB1 forwards SRI response to MNO1
5) MNO1 sends MT_FSM to HUB1
6) HUB1 forwards MT_FSM to HUB2
7) HUB2 converts to SMPP the message payload and sends Submit_SM to MNO1 and requests delivery report
8) MNO1 sends Submit_SM_Resp
9) HUB2 waits until either:
    a) MT_FSM timer expires, or
    b) Deliver_SM for the final deliver receipt from MNO1 is received
10) In case b, HUB2 generates Deliver_SM_Resp to MNO1 and sends a positive MT_FSM response to HUB1
11) HUB1 forwards MT_FSM response to MNO1

In case a of step 9, HUB2 shall subsequently return a temporary error to HUB1 and this is then forwarded to MNO1. There are 2 possibilities again from this point. Either MNO1 retries sending the MT_FSM or MNO1 sends an RSDS.

In the event that MNO1 retries the MT_FSM, the message will be relayed by HUB1 to HUB2, and HUB2 shall reply with a temporary error until HUB2 has received the final deliver report from MNO2. HUB2 should be able to isolate the MT_FSM retries that pertains to the original SRI (step 2) and MT_FSM (step 6) based on fields such as originating address, service centre and destination MAP IMSI address. 3GPP TS 23.40 [1] states in section 6.2, “SC functional requirements” that:

- To identify each SMS DELIVER sent to an MS in a unique way, a time stamp value is included in the field TP Service Centre Time Stamp, TP SCTS, of the SMS DELIVER. The time stamp gives the time when the message arrived at the SC with the accuracy of a second. If two or more messages to the same MS arrive at the SC within one second, the SC shall modify the time stamp of those messages in such a way that:
- all messages to the MS contain different time stamps;
- the modification of the time stamps is kept to a minimum.

- The SC is only allowed to have one outstanding SMS DELIVER (i.e. a message for which a report has not been received) to a specific MS at a given time.
- The SC shall be able to initiate overwriting of short messages previously received by the SC if requested by the same originating address (MS or any other source) by use of the same message type.

In the alternative event that the MNO1 triggers an RSDS (instead of MT_FSM retries), HUB2 must store this fact (simulating HLR behavior for RSDS), and HUB2 must send an ALERT_SC towards HUB1 / MNO1 when the final deliver report is received from MNO2. MNO1 will subsequently start doing SRI and then MT_FSM. HUB2 must acknowledge positively the 2nd round of SRI+MT_FSM messages towards HUB1 but it must not itself forward them again to MNO2 otherwise that would be double sending. It should be not a problem to isolate the second round of SRI and MT_FSM, based on what has been cited previously from 3GPP TS 23.40 [1].

The MAP Specifications 3GPP TS 29.002 [2] provides the value of several SMS command timers:

s = from 3 seconds to 10 seconds;
m = from 15 seconds to 30 seconds;
ml = from 1 minute to 10 minutes;
l = from 28 hours to 38 hours.

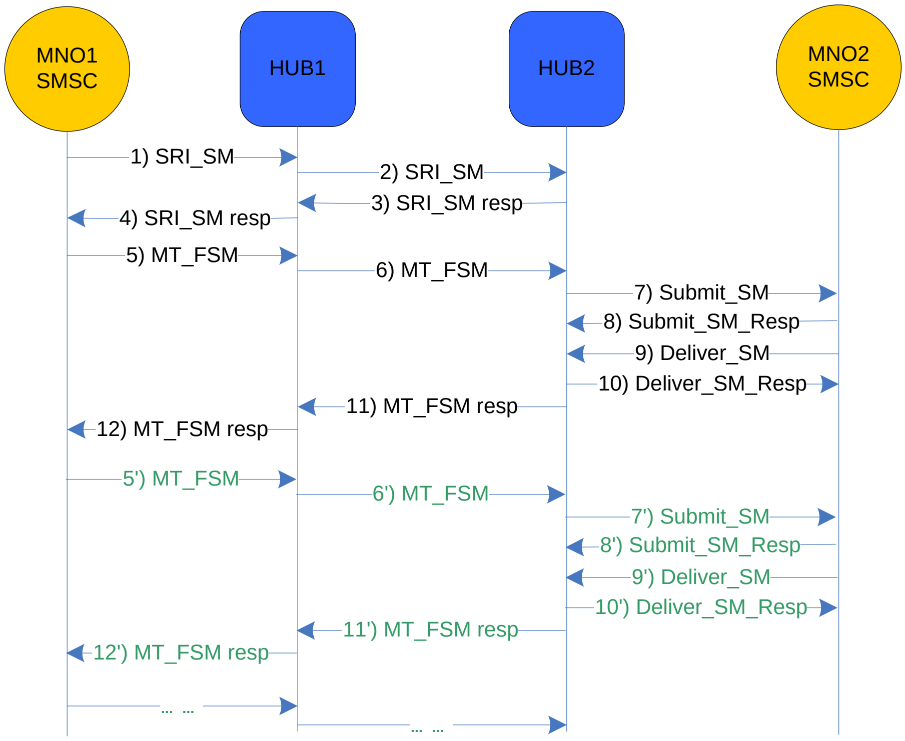
The Timer for SRI is m (medium), and for FSM it is ml (medium long). Since the timer for MT_FSM is quite long, it may be possible that often the Deliver_SM response (step 9 b) will be received in time. Although, this will have to be proven from actual data.

The proper setting of consistent SS7 timers from MNO1 to HUB2 is crucial for this solution to work. This deliver reporting capability from SS7 to SMPP is already broken in the current situation. SMS Hubbing is therefore not creating a new problem. This is merely an attempt to resolve the issue.

In a real-life scenario, perhaps this is not going to solve the issue in all cases (especially if the parties involved are not closely complying with 3GPP specifications such as in the SS7 response timers, or in respect to having only one SMS Deliver outstanding per destination). It however helps in explaining the problem to those parties who are interested in a solution to the problem. If the parties involved are keen and interested in implementing a solution, then it is quite possible that the solution approach presented will work, and it is the best solution available so far.

8.5.4.1 Deliver reporting issue for concatenated SMS and More Message to Send

The resulting flow for supporting Concatenated Messages and More Message to send case may be diagrammed as follows:



The ideal behavior is for the Deliver_SM to be returned in timely fashion for each MT_FSM by MNO2 to HUB2, without waiting for all parts of the concatenated message to be collected. If the MNO2 SMSC waits for all parts of the concatenated messages, then the message flow would be quite different and honest deliver reporting would not work. This would be an SMSC issue.

SAR (Segmentation And Reassembly) is an SMPP feature to allow passing of fragments between two peers without having to encode using UDH or any other technology-specific format. This is defined exclusively using TLVs (`sar_msg_ref_num`, `sar_total_segments`, `sar_segment_seqnum`) which will indicate the same detail as a normal UDH message would use.

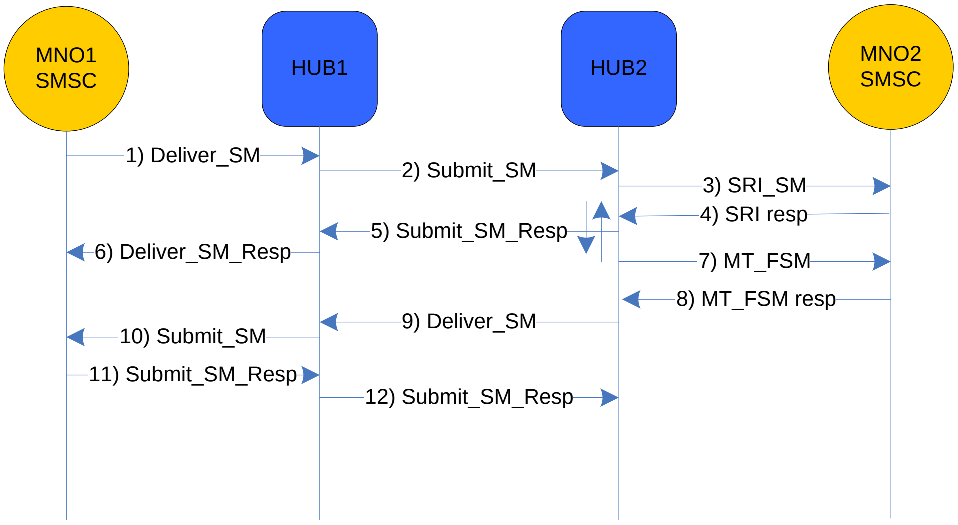
SMPP-based platforms are expected to honor deliver reports per fragment if requested per fragment.

8.5.5 SMPP Originating Operator to SS7 Destination Operator Deliver Reports

There are 2 cases to consider. Either a deliver report is requested or not by MNO1. If it is not requested, then deliver reporting is not relevant.

8.5.5.1 Deliver Report Requested

This will work with store and forward. None store and forward or proxy mode is problematic for this scenario as that results in problems relaying a temporary SS7 error backwards towards SMPP.



Deliver reporting shall work in the following way:

1) MNO1 sends Deliver_SM to HUB1
2) HUB1 sends Submit_SM to HUB2
3) HUB2 sends SRI_SM to MNO2
4) MNO2 returns SRI_response to HUB2
5) HUB2 returns at this point or earlier or later a Submit_SM_resp to HUB1. If store and forward is closely followed, this step will have occurred earlier (ahead of step 3). This step could occur later if HUB2 has allowed extra time to permit permanent errors to filter down from MNO2.
6) HUB1 returns Deliver_SM_Resp to MNO1
7) HUB2 sends MT_FSM to MNO2
8) MNO2 returns MT_FSM response. This confirms that the message has in fact been delivered to the subscriber.
9) HUB2 initiates Deliver_SM for final deliver report to HUB1.
10) HUB1 sends Submit_SM to MNO1
11) MNO1 sends Submit_SM_Resp to HUB1
12) HUB1 sends Deliver_SM_Resp to HUB2

In the event that MNO2 should return a temporary error, HUB2 shall trigger RSDS as appropriate and return a Deliver_SM for final deliver report to HUB1 only when .the MT_FSM is positively acknowledged by MNO2

8.6 Number portability

For this discussion, we use the following definitions:

HUB1 – refers to the originating hub

HUB2 – refers to the number range holder hub

HUB3 – refers to the terminating hub or ported subscriber hub

Similarly,

MNO1 – refers to the originating operator

MNO2 – refers to the number range holder operator

MNO3 – refers to the terminating or ported subscriber operator

The MNP lookup and message forwarding can be achieved in any of 4 methods:

a. HUB1 starts with a normal SM sending initiation, and then HUB1 receives a positive ported flag response including MNP information, and HUB1 handles the message forwarding (to a HUB3).
b. HUB1 starts with an explicit MNP dip, and when HUB1 receives a positive ported response, HUB1 handles the message forwarding
c. HUB1 starts with a normal SM sending initiation, and then HUB2 decides to handle the forwarding for the ported destination.
d. HUB1 starts with a normal SM sending initiation, HUB2 relays to MNO2 and MNO2 decides to handle the forwarding for the ported destination.

All of these methods are considered as available alternatives for MNP implementation and they apply equally to SS7 and SMPP.

The MNP lookup implementation can be different for each MNP domain; however, this only affects the way the in-MNP-domain MNP lookup (or MNP dip) itself is performed. Some domains may have an MNP database. Such a database shall be considered internal to the MNP domain, and the interface to it is out of scope (private to the MNP domain). The SMS Hubbing architecture defines a hub-to-hub interface for MNP lookup which includes:

1. SS7 SRI lookup and routing using CdPA = hub GT or MSISDN hub-to-operator, RN (nationally) MNO-to-MNO and MAP private extensions in MT_FSM when forwarding to another hub
2. ENUM-based lookup
3. SMPP 5.0-based Number Portability

The matrix below summarizes all the possible combinations of MNP handling that are in consideration:

MNP Lookup	Applies to	As a
1	a	Hub to hub interface
1	c	Internal MNP domain resolution
2	b	Hub to hub interface
2	c	Internal MNP domain resolution
3	a	Hub to hub interface
3	c	Internal MNP domain resolution and MNP result pass-back mechanism

Strictly speaking there is no MNP lookup with respect to method d, but there maybe SMPP 5.0 destination information pass-back, similar to scenario 3c. This can be referred to as MNP scenario d3. A case of no information pass-back will be referred to as MNP scenario d0.

The options enumerated are the ones that are seen to be technically feasible, and lists all the possible combinations that are seen to be possible. The business models that surround the application of these solutions however still deserve further analysis, and that specific area shall be out-of-scope for the architecture document.

Where the HUB2, does not support forwarding of the message (as in method c), or elects not to do so, it is mandatory for them to expose the appropriate Number portability hub-to-hub interface (either, or combinations, of methods 1 to 3 above).

A specific error for the case where a message is forwarded to a hub or Client Operator but it does not belong due to porting may be necessary. These errors should only be returned when the hub is neither the number range holder hub nor the ported subscriber destination hub.

For SS7, the error code shall be "Unknown Subscriber" for SRI_SM and "Unidentified Subscriber" for Forward_SM. However, typically for SRI_SM, the message should be handled by sending a SRI_ACK positive response including the IMSI and MNO3 VLR (or hub GT) address, as outlined in section 8.6.1.

For SMPP, the error code shall be InvalidDestinationAddress. Considering the number portability capability detailed in section 8.6.2 and 8.6.6, it should normally be unnecessary to return an error.

Since there are several MNP solution approaches, hubs will have to maintain a list of destinations and their chosen MNP termination approach. The MNP scenarios are (as they are noted above):

1) a1
2) a3
3) b2
4) c1
5) c2
6) c3
7) d3
8) d0

If there should be any conflict or doubt about the correct approach, it shall be the MNO2's chosen preference that should prevail. In the absence of information on how to route a message, it should be safe to route the message to HUB2 which is the hub of the number range holder operator, and the HUB2 should be capable of handling the message termination via an appropriate MNP termination strategy (which could be any of the scenarios discussed). Responsibility logically falls on HUB2, as part of it entering into a service with a client operator who belongs to an MNP domain.

8.6.1 MNP scenario a1 on SS7 (method a, hub interface 1 – a1; HUB1 delivers using SS7 based MNP)

For the detailed description of this MNP scenario, please refer to the Annexes section 10.1.1

8.6.1.1.1 MAP extension private container

This solution approach requires MAP version 2 or higher. Private extension containers are not available at MAP version 1.

The MAP protocol allows the definition of private extension parameters to carry extensions or additional field information defined outside of the MAP specification. Such extensions are perfectly suited to carry SMS Hubbing private parameters between SMS Hubs.

Please note the encoding of such extensions vary according the MAP Application Context (AC) version:

- For AC of V2, the private extensions follow the extension marker and are tagged using PRIVATE up to and including 29.
- For AC of V3 and higher, the private extensions are included only in the Private Extension Container; using an OID beginning with the GSM Association allocated private OID (see also section 8.9) suffixed by the same numeric assignments as with the V2 private extensions.

Up to 10 extensions could be encoded in the ASN.1 extensionContainer as follows:

```
extensionContainer SEQUENCE {
    privateExtensionList [0] IMPLICIT SEQUENCE (SIZE( 1 .. 10 ) ) OF
    SEQUENCE {
        extId MAP-EXTENSION .&extensionId ( {
            ,
            ...} ),
        extType MAP-EXTENSION .&ExtensionType ( {
            ,
            ...} { @extId } ) OPTIONAL} OPTIONAL,
        pcs-Extensions [1] IMPLICIT SEQUENCE {
            ... } OPTIONAL,
    ... } OPTIONAL
}
```

The following private extensions shall be defined:

Private extensions	Description
smshub-recipientMSC-VLR	Used in SS7 MNP or Roaming SMS MT termination solution approach 2.
smshub-senderMSC	Optional parameter for providing transparency of the originating operator node GT
smshub-smppError	Used to convey the actual SMPP error to allow a more transparent pass-back of SMPP errors. Optional.
smshub-recipientIMSI	Can be used in a case where intermediate hubs return a dummy IMSI in the case of hybrid SMS interworking, or MNP dip results in IMSI or MCC/MNC information only sans the MSC-VLR GT. Optional.
smshub-senderIMSI	May be used to convey the sender IMSI. Optional.
smshub-detailedError	Used to convey more detailed error information. Optional.
smshub-applicationContext	Can be used to convey the MAP AC version of the originating node forward in the message flow. Optional.
smshub-donotretry	Can be used to convey to a previous hub or node that the error case is permanent and no further retry attempt should be made. Optional. Value of 1 means the flag is set.
smshub-HUB1-GT	GT of HUB1 which may be used for transparency of routing. Optional. This can be used in the case that the recipient operator wishes to have routing transparency. This may also be used in the case of roaming or MNP where three hubs could be involved. So, for instance in a HUB1->HUB2->HUB3 case, HUB2 can use this field to inform HUB3 of the route taken by the message.

smshub-HUB2-GT	GT of HUB2 which may be used for transparency of routing. Optional. See also description above for smshub-HUB1-GT.

For MAP v2, the extensions are conveyed using MAP private extensions and are defined as follows:

```
smshub-recipientMSC-VLR [PRIVATE 20] ISDN-AddressString OPTIONAL
smshub-senderMSC [PRIVATE 21] ISDN-AddressString OPTIONAL
smshub-smppError [PRIVATE 22] INTEGER OPTIONAL
smshub-recipientIMSI [PRIVATE 23] IMSI OPTIONAL
smshub-senderIMSI [PRIVATE 24] IMSI OPTIONAL
smshub-detailedError [PRIVATE 25] INTEGER OPTIONAL
smshub-applicationContext [PRIVATE 26] INTEGER OPTIONAL
smshub-donotretry [PRIVATE 27] INTEGER OPTIONAL
smshub-HUB1-GT [PRIVATE 28] ISDN-AddressString OPTIONAL
smshub-HUB2-GT [PRIVATE 29] ISDN-AddressString OPTIONAL
```

For MAP v3, the extensions are conveyed using the MAP extensionContainer structure. All SMS Hubbing extension containers use object identifiers (OID) allocated under the GSM Association OID (see also section 8.9).

```
    smshub-ExtData ::= SEQUENCE {
        extId MAP-EXTENSION.&extensionId {{smshub-ExtDataSet}),
        extType MAP-EXTENSION.&ExtensionType {{smshub-ExtDataSet}{@extId})
        OPTIONAL
    }

    smshub-ExtDataSet MAP-EXTENSION ::= {
        smshub-recipientMSC-VLR |
        smshub-senderMSC |
        smshub-smppError |
        smshub-recipientIMSI |
        smshub-senderImsi |
        smshub-detailedError |
        smshub-applicationContext |
        smshub-donotretry |
        smshub-HUB1-GT |
        smshub-HUB2-GT
        -- smsHub-ExtDataSet is the set of all defined private
        -- extensions for the MAP commands used by SMS Hubbing
    }

    smshub-recipientMSC-VLR MAP-EXTENSION ::= {
        &ExtensionType ISDN-AddressString,
        &extensionId { 0 4 0 127 0 9 20 }
    }

    smshub-senderMSC MAP-EXTENSION ::= {
        &ExtensionType ISDN-AddressString,
        &extensionId { 0 4 0 127 0 9 21 }
    }

    smshub-smppError MAP-EXTENSION ::= {
        &ExtensionType INTEGER,
        &extensionId { 0 4 0 127 0 9 22 }
    }

    smshub-recipientIMSI MAP-EXTENSION ::= {
        &ExtensionType IMSI,
        &extensionId { 0 4 0 127 0 9 23 }
    }

    smshub-senderIMSI MAP-EXTENSION ::= {
        &ExtensionType IMSI,
        &extensionId { 0 4 0 127 0 9 24 }
    }

    smshub-detailedError MAP-EXTENSION ::= {
        &ExtensionType INTEGER,
        &extensionId { 0 4 0 127 0 9 25 }
    }

    smshub-applicationContext MAP-EXTENSION ::= {
        &ExtensionType INTEGER,
        &extensionId { 0 4 0 127 0 9 26 }
    }

    smshub-donotretry MAP-EXTENSION ::= {
        &ExtensionType INTEGER,
        &extensionId { 0 4 0 127 0 9 27 }
    }

    smshub-HUB1-GT MAP-EXTENSION ::= {
        &ExtensionType ISDN-AddressString,
        &extensionId { 0 4 0 127 0 9 28 }
    }

    smshub-HUB2-GT MAP-EXTENSION ::= {
        &ExtensionType ISDN-AddressString,
        &extensionId { 0 4 0 127 0 9 29 }
    }
```

Values for smshub-detailedError:

1) Hub internal timer for recipient has timed out, and hub has generated timeout condition.
2) Hub has generated an immediate MT_FSM response without assurance of actual delivery.
3) Hub has received a message for a destination which is potentially ported and NP ported location has been provided but NP resolution location result is wrong/invalid.
4) The hub cannot resolve MNP.
5) The hub cannot find a suitable route to the destination.
6) The recipient subscriber happens to be roaming and HUB2 reverts the message to HUB1 for HUB1 to route to the destination.
7) The recipient subscriber happens to be ported and HUB2 reverts the message to HUB1 for HUB1 to route to the destination.
8) Interworking relationship with the recipient is absent.
9) Interworking relationship with the originator is absent.
10) Interworking relationship is absent.
11) Recipient operator is not valid/blacklisted.
12) Originating operator is not valid/blacklisted.
13) Recipient subscriber is blacklisted.
14) Originating subscriber is blacklisted.
15) Destination GT is blacklisted/not allowed.
16) Originating GT is blacklisted/not allowed.
17) Destination MSISDN length is invalid.
18) Binary content is invalid.
19) MT_FSM without preceding SRI.
20) Incorrect format/use of a direct MT_FSM
21) Mandatory transparency of originating network has not been provided by the previous hub
22) Origin network transparency information is invalid.
23) The destination is not on the hub network.

8.6.2 MNP scenario a3 on SMPP using SMPP 5.0 parameters (method a, hub interface 3 – scenario a3: HUB1 delivers using SMPP based MNP)

Scenario a3 means it is HUB1 that handles the message delivery, and using SMPP 5.0 message parameters.

8.6.2.1 New Message Parameters for SUBMIT_SM, DELIVER_SM, DATA_SM

SMPP 5.0 extensions provide number portability information results moving forward from HUB1 or HUB2 to HUB3. The optional parameter will only be used with the following message types:

- SUBMIT_SM
- DELIVER_SM
- DATA_SM

These parameters are optional, in the sense that the `dest_subaddress` parameters are available for conveying essentially the same information.
The Number portability optional parameter will contain the following parameters:

Parameter	Description
`dest_addr_np_resolution`	Indication if the query has been performed to identify if the number has been ported.
`dest_addr_np_information`	Data specific to the NP Type.
`dest_addr_np_country`	County code of the operator

NP Resolution consists of the parameters as described below:

Tag	Value	Wireless Network Technology
`dest_addr_np_resolution`		Generic

Field	Size octets	Type	Description
Parameter Tag	2	Integer	`dest_addr_np_resolution`
Length	2	Integer	Length of value part in octets
Value	1	Integer	0 = query has not been performed 1 = query has been performed, number not ported 2 = query has been performed, number ported

Rules to be applied based on dest_addr_np_resolution value.

`dest_addr_np_resolution`	**`dest_addr_np_information`**	`dest_addr_np_country`
0	Not Required	Not Required
1	Not Required	Not Required
2	Required	Required

NP Information consists of the parameters as described below:

Tag	Value	Wireless Network Technology
`dest_addr_np_information`		Generic

Field	Size octets	Type	Description
Parameter Tag	2	Integer	`dest_addr_np_information`
Length	2	Integer	Length of value part in octets
Value	Variable	Integer	Routing information

Rules to be applied based on NP Resolution value.

NP Resolution	NP Information	NP Country
0	Not Required	Not Required
1	Not Required	Not Required
2	Required	Required

When the Number Portability parameters are used within the US the information contained with the NP Information will be the Location Routing Number (LRN).

A LRN is a 10-digit number, in the format NPA-NXX-XXXX, that uniquely identifies a switch or point interconnection (POI). The NPA-NXX portion of the LRN is used to route calls to numbers that have been ported.

The following is a listing of references for Local Number Portability in the US. Other than the US, operators are expected not to need the LRN and instead utilize the `dest_subaddress` parameter.

Title	Source
Location Routing Number Assignment Practices	ATIS – INC 98-0713-021
Wireless Number Portability Phase I	TIA/EIA/IS - 756
Wireless Number Portability Phase II	TIA/EIA/IS – 756 - A
Wireless Number Portability Phase III	TIA/EIA/IS - 841
Wireless Features Descriptions	TIA/EIA/IS – 664 - A
First Report & Order and Further Notice of Proposed Rulemaking	FCC 96-286
Second Report & Order	FCC 97-074

`dest_addr_np_country` consists of the parameters as described below:

Tag	Value	Wireless Network Technology
`dest_addr_np_country`		Generic

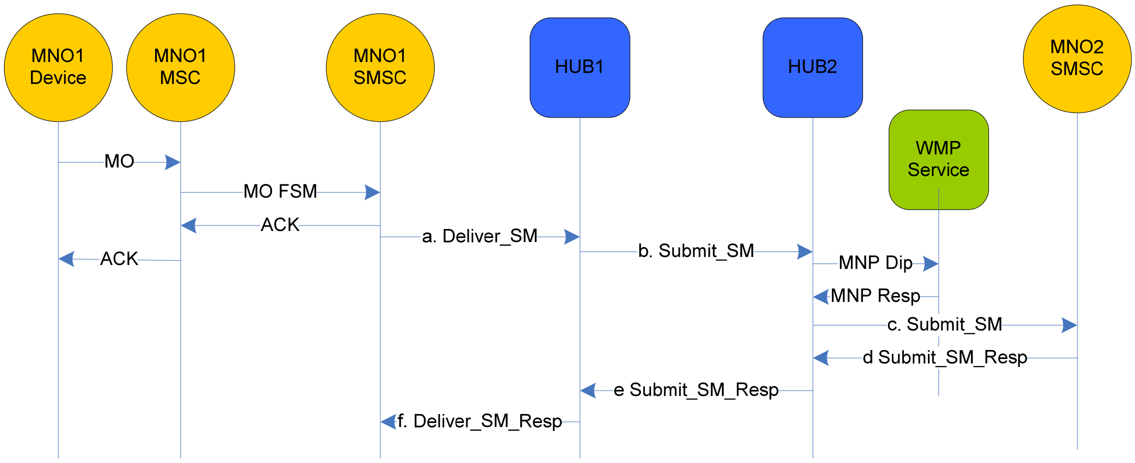
Field	Size octets	Type	Description
Parameter Tag	2	Integer	`dest_addr_np_country`
Length	2	Integer	Length of value part in octets
Value	Variable 1 - 5	Integer	Country code of the origination operator (E.164 Region Code)

Rules to be applied based on dest_addr_np_resolution value.

`dest_addr_np_resolution`	`dest_addr_np_information`	`dest_addr_np_country`
0	Not Required	Not Required
1	Not Required	Not Required
2	Required	Required

8.6.2.2 Message flows

Destination has been dipped but has not been ported:



a. MNO1 sends a Submit_SM to HUB1 with no porting information supplied.

b. HUB1 performs an internal lookup to determine if the destination MSISDN is associated with a customer of HUB1. When the lookup is performed it is determined that destination MSISDN is associated with MNO2 connected to HUB2. A Submit_SM is constructed and MNO1 is identified in the `source_subaddress` optional parameter. `dest_subaddress` is not populated. When `dest_subaddress` is not present, it means MNP resolution has not been performed. HUB1 sends the Submit_SM to HUB2.

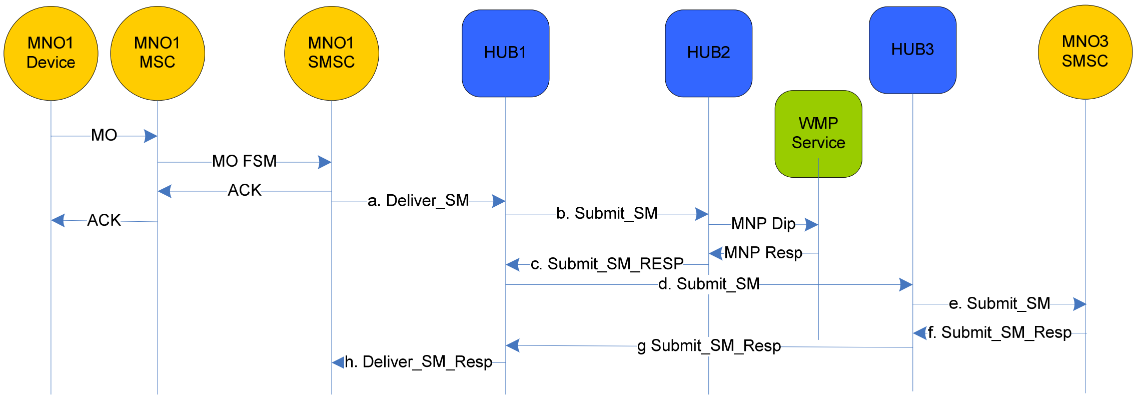
c. HUB2 receives the message, and recognizes the destination as belonging to its client operator. Since HUB2 belongs to an MNP domain, an MNP lookup must be performed, and HUB2 sees that `dest_subaddress` is absent and realizes that the HUB1 did not perform an MNP lookup. HUB2 performs an MNP dip to determine if the destination number has been ported. The response from the dip indicates that the number has not been ported. HUB2 sends a Submit_SM to MNO2 with `source_subadress` = MNO1 MCC+MNC.

d. MNO2 responds with Submit_SM_Resp to HUB2

e. HUB2 returns a Submit_SM_Resp to HUB1 with `dest_subaddress` = blank/null. When `dest_subaddress` = blank/null it means that the destination MNO has been checked for number portability and has been found to be not ported.

f. HUB1 responds with Deliver_SM_Resp to MNO1 with `dest_subaddress =` blank/null.

Destination has been dipped and has been ported:



a. MNO1 sends a Submit_SM to HUB1 with no porting information supplied.

b. HUB1 performs an internal lookup to determine if the destination MSISDN is associated with a customer of HUB1. When the lookup is performed it is determined that destination MSISDN is associated with MNO2 connected to HUB2. A Submit_SM is constructed and MNO1 is identified in the `source_subaddress` optional parameter. `dest_subaddress` is not populated. When `dest_subaddress` is not present, it means MNP resolution has not been performed. HUB1 sends the Submit_SM to HUB2.

c. HUB2 receives the message, and recognizes the destination as belonging to its client operator. Since HUB2 belongs to an MNP domain, an MNP lookup must be performed, and HUB2 sees that `dest_subaddress` is absent and realizes that the HUB1 did not perform an MNP lookup. HUB2 performs an MNP dip to determine if the destination number has been ported. The response from the dip indicates that the number has been ported. However, HUB2 does not have connectivity or elects not to forward, so it returns a Submit_SM_Resp to HUB1 with error code = 0x00000402 (HUB_WNPOK_ROUTEFAIL), `dest_subaddress` = MNO3 MCC+MNC.

d. HUB1 realizes that the destination number is ported, and that HUB2 elected not to deliver. So, HUB1 sends a Submit_SM to HUB3 with `source_subaddress` = MNO1 MCC+MNC, `dest_subaddress` = MNO3 MCC+MNC and optionally provides also `dest_addr_np_resolution` = 2, `dest_addr_np_information` and `dest_addr_np_country`.

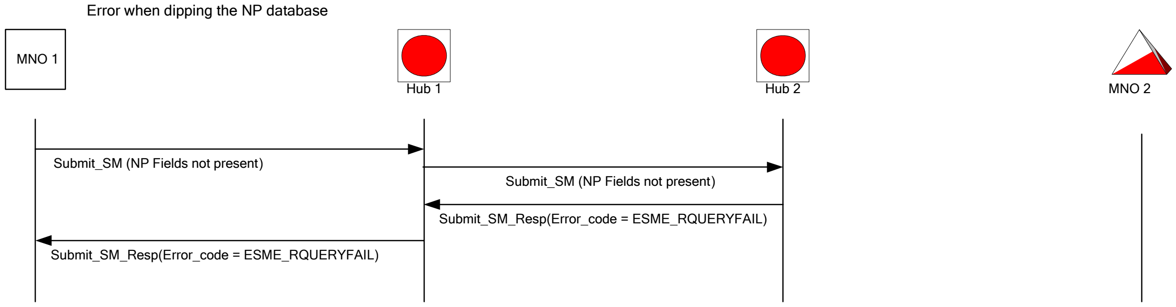
e. HUB3 receives the message, and with `dest_addr_np_resolution` present realizes that the HUB1 is cascading MNP dip results. HUB3 recognizes the destination as belonging to its client operator, based on `dest_subaddress`. HUB3 at its discretion may perform a second MNP dip to be certain that the MNP information has not changed. HUB3, either relying on the original MNP information or finding the MNP information has not changed, relays the Submit_SM to MNO3 with `source_subadress` = MNO1 MCC+MNC.

f. MNO3 responds with Submit_SM_Resp to HUB3

g. HUB3 responds with Submit_SM_Resp to HUB1

h. HUB1 responds with Deliver_SM_Resp to MNO1 with `dest_subaddress =` MNO3 MCC+MNC.

Error when dipping the NP Database:


Error when dipping the NP database
MNO 1
Hub 1
Hub 2
MNO 2
Submit_SM (NP Fields not present)
Submit_SM (NP Fields not present)
Submit_SM_Resp(Error_code = ESME_RQUERYFAIL)
Submit_SM_Resp(Error_code = ESME_RQUERYFAIL)

a. MNO1 sends a Submit_SM to HUB1 with no porting information supplied.

b. HUB1 forwards the Submit_SM to HUB2.

c. HUB2 performs an MNP dip to determine if the destination number has been ported. The MNP dip is unable to identify if the number has been ported. HUB2 responds with Submit_SM_Resp to HUB1 with the Error_code set to ESME_RQUERYFAIL.

d. HUB1 responds with Deliver_SM_Resp to MNO1 with the Error_code set to ESME_RQUERYFAIL.

8.6.3 MNP scenario b2 on SMPP (method b, hub interface 2 – scenario b2: HUB1 delivers using ENUM based MNP)

In IO-MMS both an MAP SRI_SM/SS7 and ENUM based number addressing solution has been defined. Consequently, it is recommended that IO-SMS inherit the same ENUM infrastructure. MNP handling based on ENUM is described here.

In MNP method b, the originating hub (HUB1) shall be responsible for MNP resolution, and should forward the message to the appropriate next hop destination. Double MNP dipping can be avoided by using `dest_subaddress` in SMPP to carry the MNC/MCC of the destination operator when a message is sent to the next hop. Hubs are not prevented however from performing a second MNP dip, if they deem this to be appropriate. The type of sub-address tag shall be “10100000 – user specified”, and the value shall be 6 octets long <mnc><mcc>.

For example: 02030007a0123456

To fulfill transparency, `source_subaddress` in SMPP shall be used to carry the MNC/MCC of the originating operator. The type of Subaddress tag shall be “10100000 – user specified”. The value shall be 6 octets long <mnc><mcc>.

For example: 02030007a0001002

For MNP domains that utilize method b, the SMS Hubs in that domain shall be required to expose the appropriate ENUM service for other hubs, unless there is a separate ENUM authority providing this specific service to SMS Hubs.

For information on the basic models or architecture options for Operator ENUM, please refer to IR.67 [13], under the section for “DNS Structure and ENUM Delegation Models”. The operator ENUM domain is e164enum.net and is available only in the IPX network. Therefore SMS hubs must connect to the IPX network to gain access to the ENUM service.

8.6.3.1 Scope

<u>In-scope</u>

- Define network interface between SMS Hub and MNP Gateway
- SMPP interface between two peering SMS Hubs

<u>Out-of-scope</u>

- The access method from MNP Gateway to country MNP database
- The implementation details of the MNP Gateway

8.6.3.2 ENUM DNS Server Implementation

1) This ENUM DNS Server is not necessarily a full-blown operator managed ENUM server. It can be an MNP Gateway for converting an external third MNP solution to a standard MNP solution to be queried by SMS Hub.
2) The ENUM DNS Server can be provided by
   a. Option 1: SMS Hub itself
   b. Option 2: Another 3rd party (such as an ENUM authority)
3) If the ENUM DNS Server is to support SMS, it can return the following value upon a NAPTR query:
   ```
   IN NAPTR 100 10 "u" "sms+e2u"
   "!^.*$!SMS:+1234567890@sms.mnc123.mcc456.3gppnetwork.org!"
   ```

The network name in the resulting NAPTR is for illustration only. For guidelines on domain naming, please refer to the guidelines in IR.67 [13].

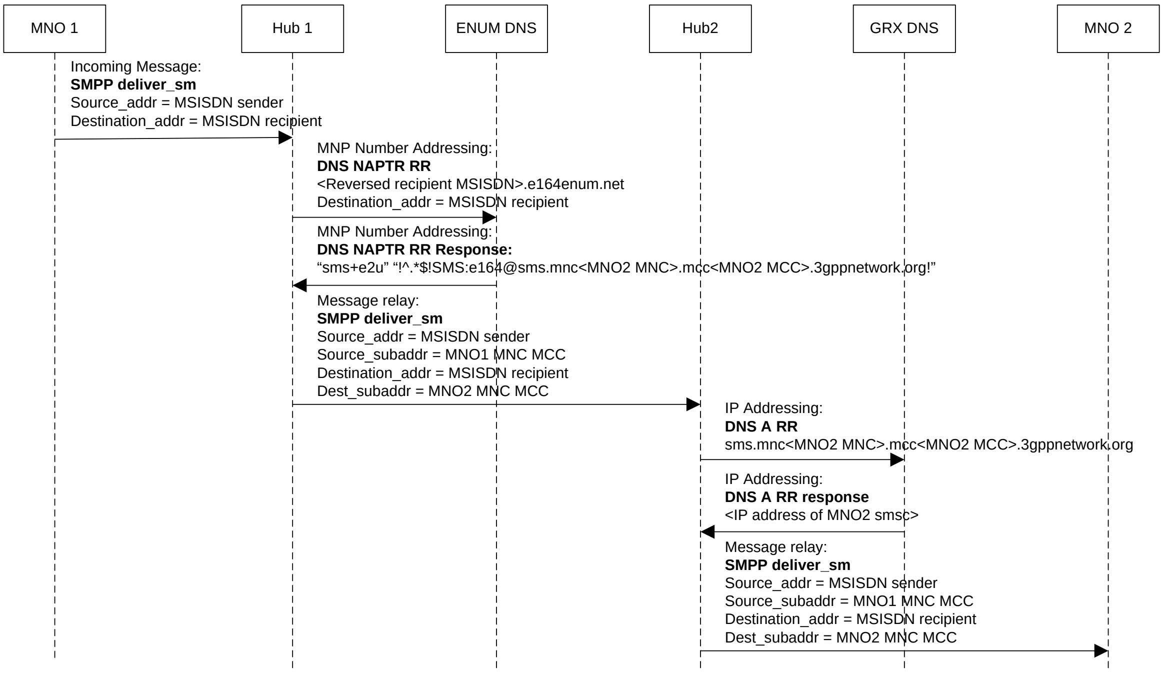
It may not be such a big concern to see that there is a specific key assigned to SMS as illustrated above “sms+e2u”. Any NAPTR record may well fit the requirement as long as the recipient network is already identified. The hub shall be expected to be capable of routing the SMS message as soon as the identity of the recipient network is known via any NAPTR result, or NS redirect. In this sense, the only objective of this discussion is to resolve number portability by identifying the ported-into network. For further treatment on routing and name resolution IR.67 [3] section 4.6.1, “Solving Number Portability in ENUM,” can be referenced.

RFC 4355 [14] contains existing enumservices and there is an entry already for SMS, which can perhaps be utilized, and an excerpt is cited below:

```
5.2.1.  SMS Service Registration with tel: URI
   Enumservice Name: "sms"
   Enumservice Type: "sms"
   Enumservice Subtypes: "tel"
   URI Scheme: 'tel:'
```

```
5.2.2.  SMS Service Registration with mailto: URI
   Enumservice Name: "sms"
   Enumservice Type: "sms"
   Enumservice Subtypes: "mailto"
```

8.6.3.3 MNP Solution Message Flow Diagram


MNO 1
Hub 1
ENUM DNS
Hub2
GRX DNS
MNO 2
Incoming Message:
SMPP deliver_sm
Source_addr = MSISDN sender
Destination_addr = MSISDN recipient
MNP Number Addressing:
DNS NAPTR RR
<Reversed recipient MSISDN>.e164enum.net
Destination_addr = MSISDN recipient
MNP Number Addressing:
DNS NAPTR RR Response:
“sms+e2u” “!^.*$!SMS:e164@sms.mnc<MNO2 MNC>.mcc<MNO2 MCC>.3gppnetwork.org!”
Message relay:
SMPP deliver_sm
Source_addr = MSISDN sender
Source_subaddr = MNO1 MNC MCC
Destination_addr = MSISDN recipient
Dest_subaddr = MNO2 MNC MCC
IP Addressing:
DNS A RR
sms.mnc<MNO2 MNC>.mcc<MNO2 MCC>.3gppnetwork.org
IP Addressing:
DNS A RR response
<IP address of MNO2 smsc>
Message relay:
SMPP deliver_sm
Source_addr = MSISDN sender
Source_subaddr = MNO1 MNC MCC
Destination_addr = MSISDN recipient
Dest_subaddr = MNO2 MNC MCC

Optionally, Submit_SM may be used.

In the event that the destination is not ported, then hubs can relay forward the fact that it has done a dip and the result, by relaying the optional parameter `dest_subaddress` = blank/null.

8.6.3.4 MNP scenario b2 on SS7

It is definitely also possible to use scenario b2 on SS7. The MNP resolution is handled via ENUM, and the message forwarding to HUB3 from HUB1 is using SS7.

8.6.4 MNP scenario c1 on SS7 (method c, hub interface 1 – scenario c1: HUB2 delivers using SS7 based MNP)

For the detailed description of this MNP scenario, please refer to the Annexes section 10.1.1

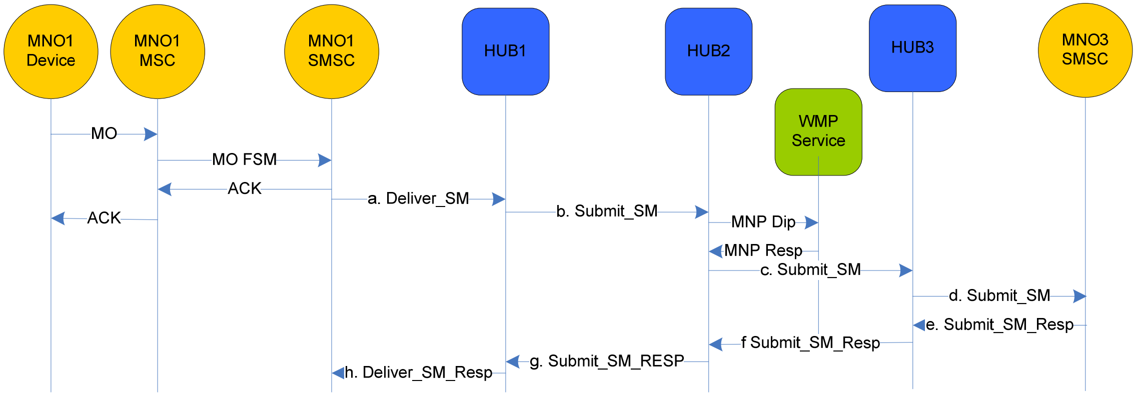
8.6.5 MNP scenario c2 using ENUM (method c, hub interface 2 – scenario c2: HUB2 delivers using ENUM based MNP)

This is a simple extension of the handling detailed in section 8.6.3. The only difference is that instead of HUB1 handling the MNP resolution, it is HUB2 performing this role. ENUM is thereby used as in-MNP domain resolution mechanism. If the message is carried by HUB1 using SS7, this solution has the disadvantage in that it hides the number portability information from HUB1. If HUB1 is using SMPP, there is the possibility to pass back the number portability information in the Submit_SM_Resp as described in section 8.6.2 using the Dest_subaddress optional parameters.

In the event that the destination is not ported, then hubs can relay backwards the fact that it has done a dip and the result, by relaying the optional parameter dest_subaddress = blank/null.

8.6.6 MNP scenario c3 using SMPP 5.0 (method c, hub interface 3 – scenario c3: HUB2 delivers using SMPP based MNP)

This is an extension of the handling detailed in section 8.6.2. The only difference is that instead of HUB1 handling the MNP resolution, it is HUB2 performing this role. SMPP or some other alternate in-MNP domain resolution mechanism could be utilized. SMPP 5.0 extensions provide the possibility to pass back number portability information from HUB2 to HUB1 in the Submit_SM_Resp. SMPP 5.0 extensions also provide number portability information results moving forward from HUB2 to HUB3.



a. MNO1 sends a Submit_SM to HUB1 with no porting information supplied.

b. HUB1 performs an internal lookup to determine if the destination MSISDN is associated with a customer of HUB1. When the lookup is performed it is determined that destination MSISDN is associated with MNO2 connected to HUB2. A Submit_SM is constructed and MNO1 is identified in the `source_subaddress` optional parameter. `dest_subaddress` is not populated. When `dest_subaddress` is not present, it means MNP resolution has not been performed. HUB1 sends the Submit_SM to HUB2.

c. HUB2 receives the message, and recognizes the destination as belonging to its client operator. Since HUB2 belongs to an MNP domain, an MNP lookup must be performed, and HUB2 sees that `dest_subaddress` and `dest_addr_np_resolution` are absent and realizes that the HUB1 did not perform an MNP lookup. HUB2 performs an MNP dip to determine if the destination number has been ported. The response from the dip indicates that the number has been ported. HUB2 elects to handle message forwarding. So, HUB2 sends a Submit_SM to HUB3 with `source_subadress` = MNO1 MCC+MNC, dest_subaddress = MNO3 MCC+MNC and optionally provides also dest_addr_np_resolution = 2, dest_addr_np_information and dest_addr_np_country.

d. HUB3 receives the message, and with dest_subaddress present realizes that the HUB2 is cascading MNP dip results. HUB3 recognizes the destination as belonging to its client operator, based on dest_subaddress. HUB3 at its discretion may perform a second MNP dip to be certain that the MNP information has not changed. HUB3, either relying on the original MNP information or finding the MNP information has not changed, relays the Submit_SM to MNO3 with source_subadress = MNO1 MCC+MNC.

e. MNO3 responds with Submit_SM_Resp to HUB3

f. HUB3 responds with Submit_SM_Resp to HUB2

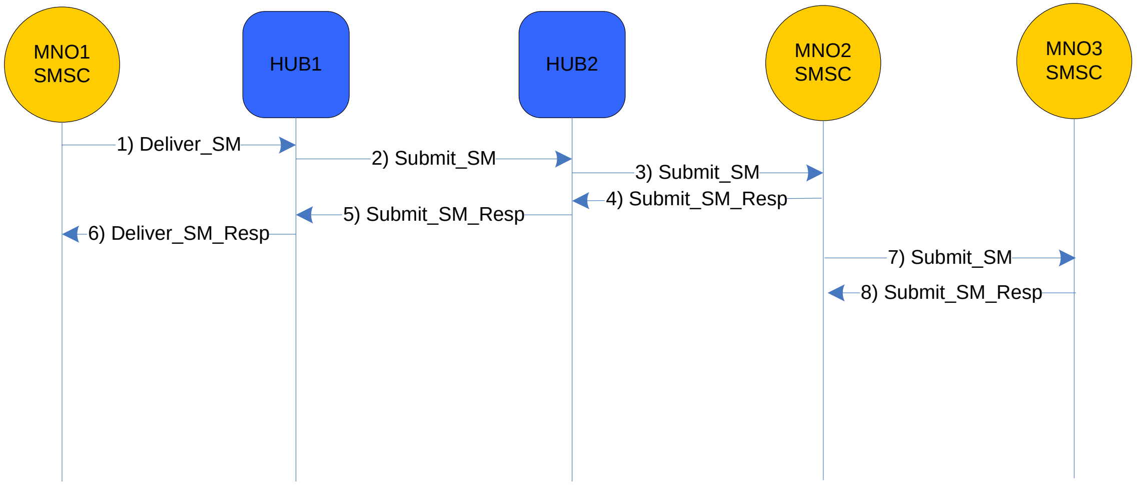
g. HUB2 responds with Submit_SM_Resp to HUB1 with dest_subaddress = MNO3 MCC+MNC.

h. HUB1 responds with Deliver_SM_Resp to MNO1 with dest_subaddress = MNO3 MCC+MNC

In the event that the destination is not ported, then hubs can relay forward the fact that it has done a dip and the fact that the destination is not ported, by relaying the optional parameter dest_subaddress = blank/null.

8.6.7 MNP scenario d3 using SMPP 5.0 passback (method d, hub interface 3 – scenario d3: MNO2 delivers the message by onward-forwarding)

In the specific case that MNO2 is capable of onward forwarding a message and also has the capability to pass-back information on the true message destination, and opts to do so, then HUB2 may terminate the SMS to MNO2 and let MNO2 handle the termination.



1) MNO1 sends Deliver_SM to HUB1
2) HUB1 sends Submit_SM to HUB2
3) HUB2 sends Submit_SM to MNO2
4) MNO2 performs an MNP dip to determine if the destination number has been ported. The response from the dip indicates that the number has been ported.

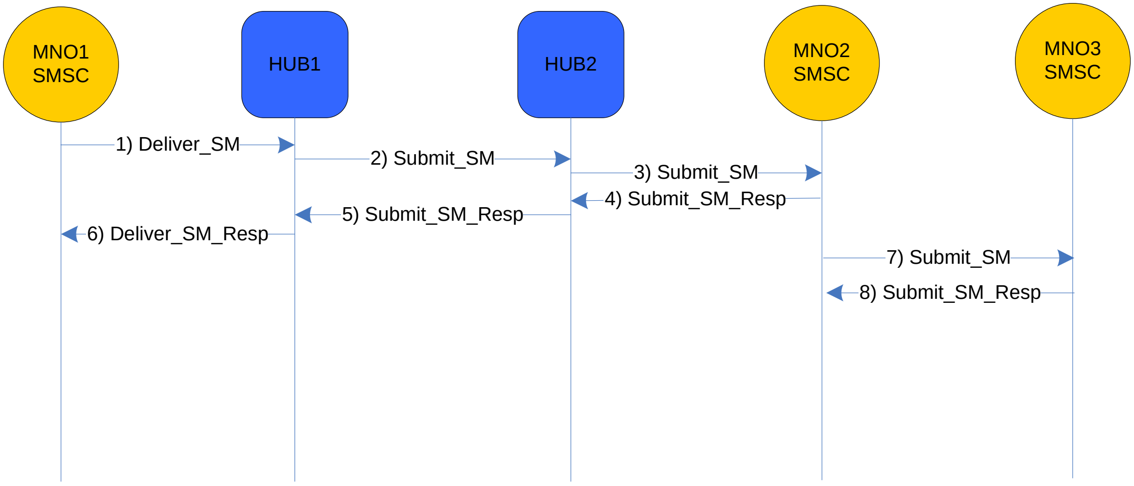
MNO2 responds with Submit_SM_Resp to HUB2 with `dest_subaddress` = MNO3 MCC+MNC. In the event that MNO2 has some other mechanism to relay destination operator information, that maybe utilized as well as long as HUB2 has agreed to use it, which then becomes a private interface between MNO2 and HUB2.

5) HUB2 responds with Submit_SM_Resp to HUB1 with `dest_subaddress =` MNO3 MCC+MNC.
6) HUB1 responds with Deliver_SM_Resp to MNO1 with `dest_subaddress =` MNO3 MCC+MNC
7) MNO2 relays the SMS via Submit_SM towards MNO3
8) MNO3 sends Submit_SM_Resp to MNO3

The last 2 steps could be achieved via SS7 as well.

8.6.8 MNP scenario d0 no passback and MNO2 forwards (method d and no hub interface – scenario d0: simple MNO2 MNP forwarding case)

In the specific case that MNO2 is capable of onward forwarding a message in MNP case, then HUB2 may terminate the SMS to MNO2 and let MNO2 handle the termination.



1) MNO1 sends Deliver_SM to HUB1
2) HUB1 sends Submit_SM to HUB2
3) HUB2 sends Submit_SM to MNO2
4) MNO2 performs an MNP dip to determine if the destination number has been ported. The response from the dip indicates that the number has been ported. MNO2 responds with Submit_SM_Resp to HUB2.
5) HUB2 responds with Submit_SM_Resp to HUB1
6) HUB1 responds with Deliver_SM_Resp to MNO1
7) MNO2 relays the SMS via Submit_SM towards MNO3
8) MNO3 sends Submit_SM_Resp to MNO3

Since the pass-back of MNP results is not considered, it is equally possible to use SS7 inter-working in steps 1 to 6. HUB2 may however have to ignore the VLR address in the SRI response from MNO2.

The last 2 steps could be achieved via SS7 as well.

8.6.9 MNP Scenarios – mixed IP and SS7 on MNP method a or b cases (HUB1 delivers)

In the SS7 to SMPP case, the method a or b MNP handling presents a challenge in the sense that the HUB2 has to return an IMSI and MSC/VLR GT pair if it is to inform HUB1 of the MNP disposition of the destination subscriber. Because of this usually, the originating hub may have to use ENUM or SMPP to resolve MNP. It is recommended that the message delivery be converted into SMPP by the HUB1 (note that this is a specific exemption from the criteria defined in section 6.1 regarding the preservation of the original message inter-working protocol between the destination and originating hub), because it may not be technically feasible. Unless, of course HUB2 has the ability to return an IMSI and MSC/VLR GT pair.

In the SMPP to SS7 case, it is less problematic. The message delivery to the HUB2 can be retained in SMPP

8.6.10 MNP Scenarios – mixed IP and SS7 on MNP method c cases (HUB2 delivers)

There should be no issue here in terms of inter-standard inter-working. It will be possible to carry the message to HUB2, in the original inter-working protocol, and perform conversion only at the last leg of inter-working to the destination operator, and this is the recommended approach.

In the SS7 to SMPP case though, HUB2 may find it necessary to convert the message to SMPP given that onward routing of the MT_FSM in SS7 requires an IMSI+MSC/VLR pair which HUB2 may not have from the MNP information that it has. The guideline to follow is that Hubs must carry the message in the original protocol as far as possible, and convert only when it is necessary.

8.6.11 Destination operator has multiple hubs

In cases where a destination operator has multiple hubs, it is important that they nominate a primary hub which is to handle the role of HUB2 (number range holder hub).

HUB2 has the responsibility of handling the necessary MNP functionality for SMS inter-working, and may have to expose hub-to-hub MNP interface(s).

8.7 Roaming Solution Architecture

There are three solution approaches discussed which should adequately cover all cases of roaming SMS MT application. The roaming solution is thus a superset of several methods, and the potential solution approach will vary depending on the exact scenario. Each solution approach has its key advantages. The three solutions do not conflict with each other and should be able to inter-operate successfully.

Since there are several Roaming SMS termination solution approaches, hubs will have to maintain a list of destinations and their chosen solution approach. The choices are:

1) Solution approach 1 – using HUB2/MNO2' SCCP link and described in section 8.7.2
2) Solution approach 2 – using HUB1 to HUB3 case as described in section 8.7.3.1
3) Solution approach 2 – using HUB2 to HUB3 case as described in section 8.7.3.2

4) Solution approach 3 – MNO2 terminates via onward forwarding

IREG recommends solution approach 2 as the preferred solution approach for roaming SMS MT.

If there should be any conflict or doubt about the correct approach, it shall be the destination operator MNO2's chosen preference that should prevail. In the absence of information on how to route a message, it should be safe to route the message to HUB2 which is the hub of the destination operator, and the HUB2 should be capable of handling the message termination in behalf of its operator via an appropriate roaming SMS termination solution strategy (which can be any of the approaches discussed).

8.7.1 Basic Principles

1) The issue to be resolved is only that for termination of roaming SMS only, and only in the SS7 case. It is also assumed that HUB1 is not able to reach both MNO2 and MNO3 directly otherwise this is a simple roaming case for HUB1 to handle, and should be straightforward to inter-work properly.
2) The issue being addressed is only for the terminating side. The originating side roaming case is presumed to be straightforward.
3) For this discussion, we use the following definitions:
   HUB1 – refers to the originating hub
   HUB2 – refers to the hub of the home network of the destination number
   HUB3 – refers to the hub of the visited network

   Similarly,
   MNO1 – refers to the originating operator
   MNO2 – refers to the home network of the destination number (or HPLMN)
   MNO3 – refers to the visited network or VPLMN
4) Roaming relationship is already pre-existing between the MNO2 and MNO3. Why? It's because, the subscriber needs to have attached to a network already before any teleservice is possible.
5) There is presumed to be no issue with termination of roaming SMS for SMPP for CDMA operators. Only SS7/GSM roaming is being resolved as this is really where the current difficulties and problem of roaming SMS MT for SMS Hubbing really lies.

8.7.2 Roaming Solution approach 1 - Roaming SMS MT solution via HUB2/MNO2:

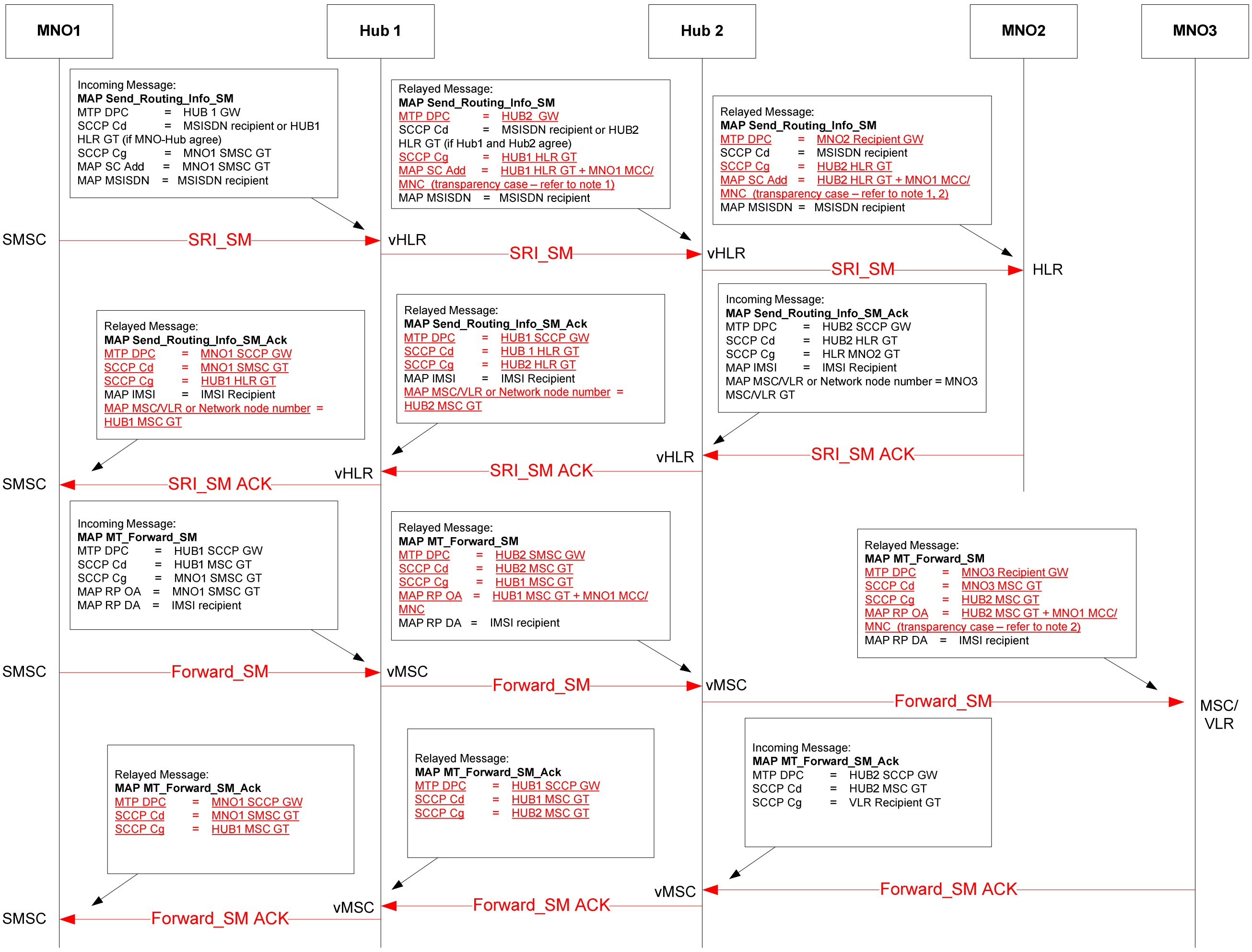
Since the roaming relationship with MNO3 is pre-existing, MNO2 and MNO3 will already have an SCCP link and it is possible to exploit this. The issue of roaming not pre-existing is deliberately avoided here. See item 4 above. Open Connectivity Roaming Project shall be working on the issue of pre-existing roaming, and is not going to be dealt with in the SMS Hubbing Architecture.

8.7.2.1 How HUB2 is able to reach MNO3

1) In the case where there is a route between HUB2 and MNO3 (for example where there is an agreement between HUB2 and MNO3), the message can be directly delivered.
2) In the case where there is no direct route, the message could be sent to MNO3 via MNO2. Because of the pre-existing roaming agreement between MNO2 and

MNO3, there exists a path to reach MNO3 via MNO2. In this case the HUB2 GT can be added in the IR21 of the MNO2 so that MNO3 will not reject the SMS.

8.7.2.2 Diagram



Incoming Message:
MAP Send_Routing_Info_SM
MTP DPC = HUB 1 GW
SCCP Cd = MSISDN recipient or HUB1 HLR GT (if MNO-Hub agree)
SCCP Cg = MNO1 SMSC GT
MAP SC Add = MNO1 SMSC GT
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = HUB2 GW
SCCP Cd = MSISDN recipient or HUB2 HLR GT (if Hub1 and Hub2 agree)
SCCP Cg = HUB1 HLR GT
MAP SC Add = HUB1 HLR GT + MNO1 MCC/ MNC (transparency case – refer to note 1)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = MNO2 Recipient GW
SCCP Cd = MSISDN recipient
SCCP Cg = HUB2 HLR GT
MAP SC Add = HUB2 HLR GT + MNO1 MCC/ MNC (transparency case – refer to note 1, 2)
MAP MSISDN = MSISDN recipient

Incoming Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 HLR GT
SCCP Cg = HLR MNO2 GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = MNO3 MSC/VLR GT

Relayed Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB 1 HLR GT
SCCP Cg = HUB2 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = HUB2 MSC GT

Relayed Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = HUB1 MSC GT

Incoming Message:
MAP MT_Forward_SM
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = MNO1 SMSC GT
MAP RP OA = MNO1 SMSC GT
MAP RP DA = IMSI recipient

Relayed Message:
MAP MT_Forward_SM
MTP DPC = HUB2 SMSC GW
SCCP Cd = HUB2 MSC GT
SCCP Cg = HUB1 MSC GT
MAP RP OA = HUB1 MSC GT + MNO1 MCC/ MNC
MAP RP DA = IMSI recipient

Relayed Message:
MAP MT_Forward_SM
MTP DPC = MNO3 Recipient GW
SCCP Cd = MNO3 MSC GT
SCCP Cg = HUB2 MSC GT
MAP RP OA = HUB2 MSC GT + MNO1 MCC/ MNC (transparency case – refer to note 2)
MAP RP DA = IMSI recipient

Incoming Message:
MAP MT_Forward_SM_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 MSC GT
SCCP Cg = VLR Recipient GT

Relayed Message:
MAP MT_Forward_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = HUB2 MSC GT

Relayed Message:
MAP MT_Forward_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 MSC GT

Notes:
For diagram notes, please refer to the same notes as those for the detailed diagram in section 8.2.3.3.

8.7.2.3 Key advantages

1) The case where MNO3 only has bilateral links is workable
2) Simple and efficient use of signalling.
3) If MNO1 and MNO2 have inter-working present and roaming+inter-working exists between MNO3 and MNO2, and there is no inter-working between MNO1 and MNO3, it is still possible to complete the termination of SMS to the MNO2 subscriber in the roaming case.
4) The solution is very similar to the SMS Router function described in 3GPP TR 23.840 v1.0.0 [12]. Perhaps the correlation ID described in the TR is not necessary as the hubs should be able to perform fraud policing and blocking of

unwanted network nodes. SMS hubs also provide control over the return of the network node number (MNO3 VLR/MSC address).

5) This solution will work even if MNO3 is using SMPP to connect to its Hub as long as MNO3 is a GSM operator.

8.7.2.4 Disadvantages

1) Not a pure SMS HUB solution, as an SCCP provider will likely have to be involved.
2) Some SCCP planning activity has to be done.
3) There may be circumstances where MNO2 and MNO3 have no time to really work on discussions of SCCP connectivity and only simply wish to work with their immediate hubs. This is where the value of the alternative solution 2 applies.
4) The return path from MNO3 to HUB2 is not clear when there are many MNO2 involved.

8.7.2.5 HUB2 may use MNO2 GT

In the case where the MNO3 is not reachable directly by HUB2, it may be possible to reach the MNO3 via the MNO2 using an MNO2 GT for the Cg address of the MT_FW_SMS. Careful planning and discussion will have to be done between MNO2, HUB2 and MNO3 and the SCCP provider involved to come to the best solution approach. If HUB2 has to use the MNO2 GT, it does become more complicated but this is also considered a feasible option to take.

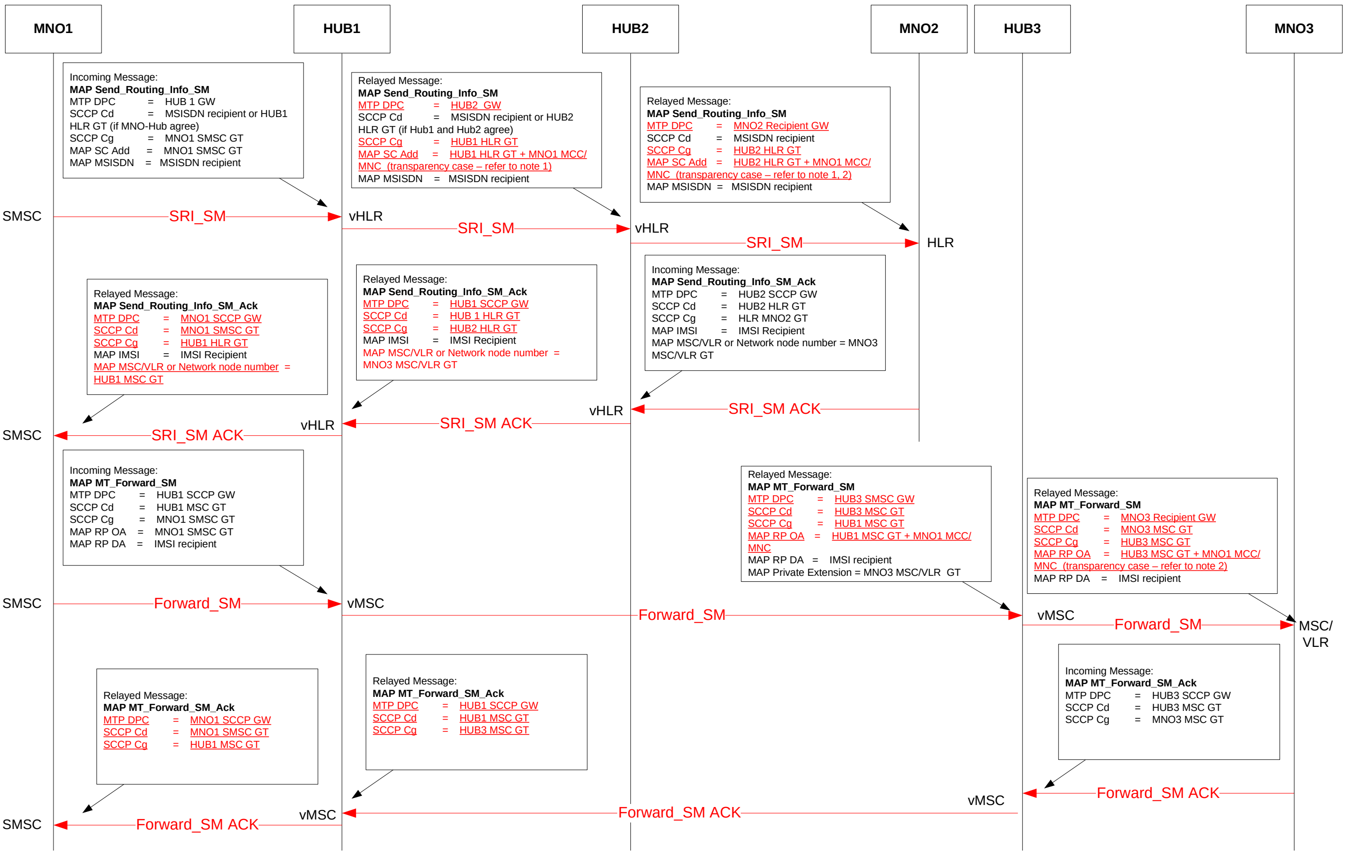
In view of HUB2 may be providing the service described as SMS Router function in 3GPP TR 23.840 [12], the approach described therein becomes virtually similar or compatible to this solution approach described here.

8.7.3 Roaming Solution approach 2 - Roaming SMS MT via HUB3 using private extension to convey the MNO3 VMSC GT address

This is an alternative approach to SMS Roaming MT which relies on HUB3 to handle the inter-working for its client MNO3, and using a private MAP extension field to convey the MNO3 MSC/VLR GT address. IREG recommends solution approach 2 as the preferred solution approach for roaming SMS MT.

8.7.3.1 HUB1 to HUB3 case

HUB2 upon realizing that the destination is roaming decides to let HUB1 handle the message forwarding.



Incoming Message:
MAP Send_Routing_Info_SM
MTP DPC = HUB 1 GW
SCCP Cd = MSISDN recipient or HUB1 HLR GT (if MNO-Hub agree)
SCCP Cg = MNO1 SMSC GT
MAP SC Add = MNO1 SMSC GT
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = HUB2 GW
SCCP Cd = MSISDN recipient or HUB2 HLR GT (if Hub1 and Hub2 agree)
SCCP Cg = HUB1 HLR GT
MAP SC Add = HUB1 HLR GT + MNO1 MCC/MNC (transparency case – refer to note 1)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = MNO2 Recipient GW
SCCP Cd = MSISDN recipient
SCCP Cg = HUB2 HLR GT
MAP SC Add = HUB2 HLR GT + MNO1 MCC/MNC (transparency case – refer to note 1, 2)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = HUB1 MSC GT

Relayed Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB 1 HLR GT
SCCP Cg = HUB2 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = MNO3 MSC/VLR GT

Incoming Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 HLR GT
SCCP Cg = HLR MNO2 GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = MNO3 MSC/VLR GT

Incoming Message:
MAP MT_Forward_SM
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = MNO1 SMSC GT
MAP RP OA = MNO1 SMSC GT
MAP RP DA = IMSI recipient

Relayed Message:
MAP MT_Forward_SM
MTP DPC = HUB3 SMSC GW
SCCP Cd = HUB3 MSC GT
SCCP Cg = HUB1 MSC GT
MAP RP OA = HUB1 MSC GT + MNO1 MCC/MNC
MAP RP DA = IMSI recipient
MAP Private Extension = MNO3 MSC/VLR GT

Relayed Message:
MAP MT_Forward_SM
MTP DPC = MNO3 Recipient GW
SCCP Cd = MNO3 MSC GT
SCCP Cg = HUB3 MSC GT
MAP RP OA = HUB3 MSC GT + MNO1 MCC/MNC (transparency case – refer to note 2)
MAP RP DA = IMSI recipient

Incoming Message:
MAP MT_Forward_SM_Ack
MTP DPC = HUB3 SCCP GW
SCCP Cd = HUB3 MSC GT
SCCP Cg = MNO3 MSC GT

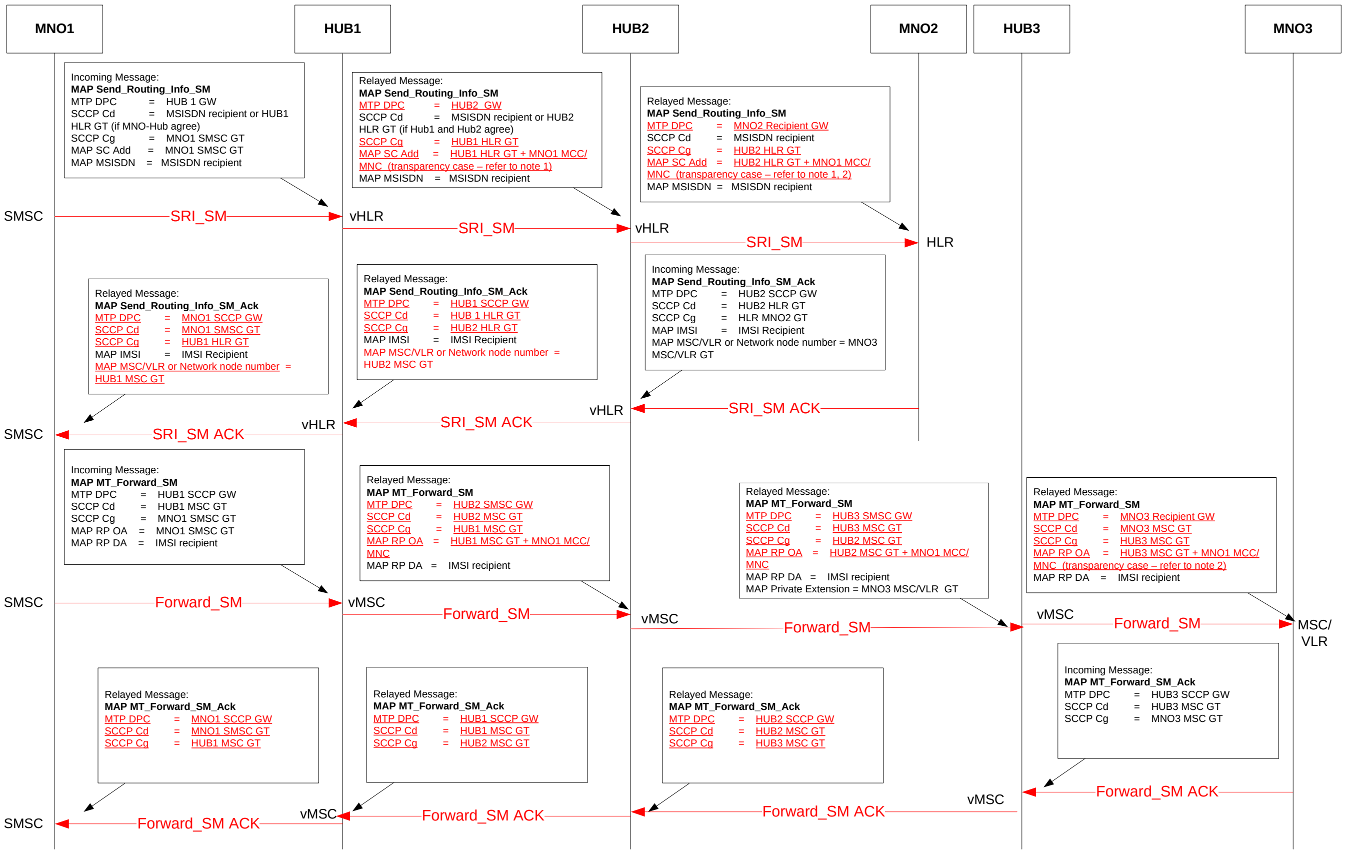
Relayed Message:
MAP MT_Forward_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 MSC GT

Relayed Message:
MAP MT_Forward_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = HUB3 MSC GT

Notes:
For diagram notes, please refer to the same notes as those for the detailed diagram in section 8.2.3.3.

8.7.3.2 HUB2 to HUB3 case

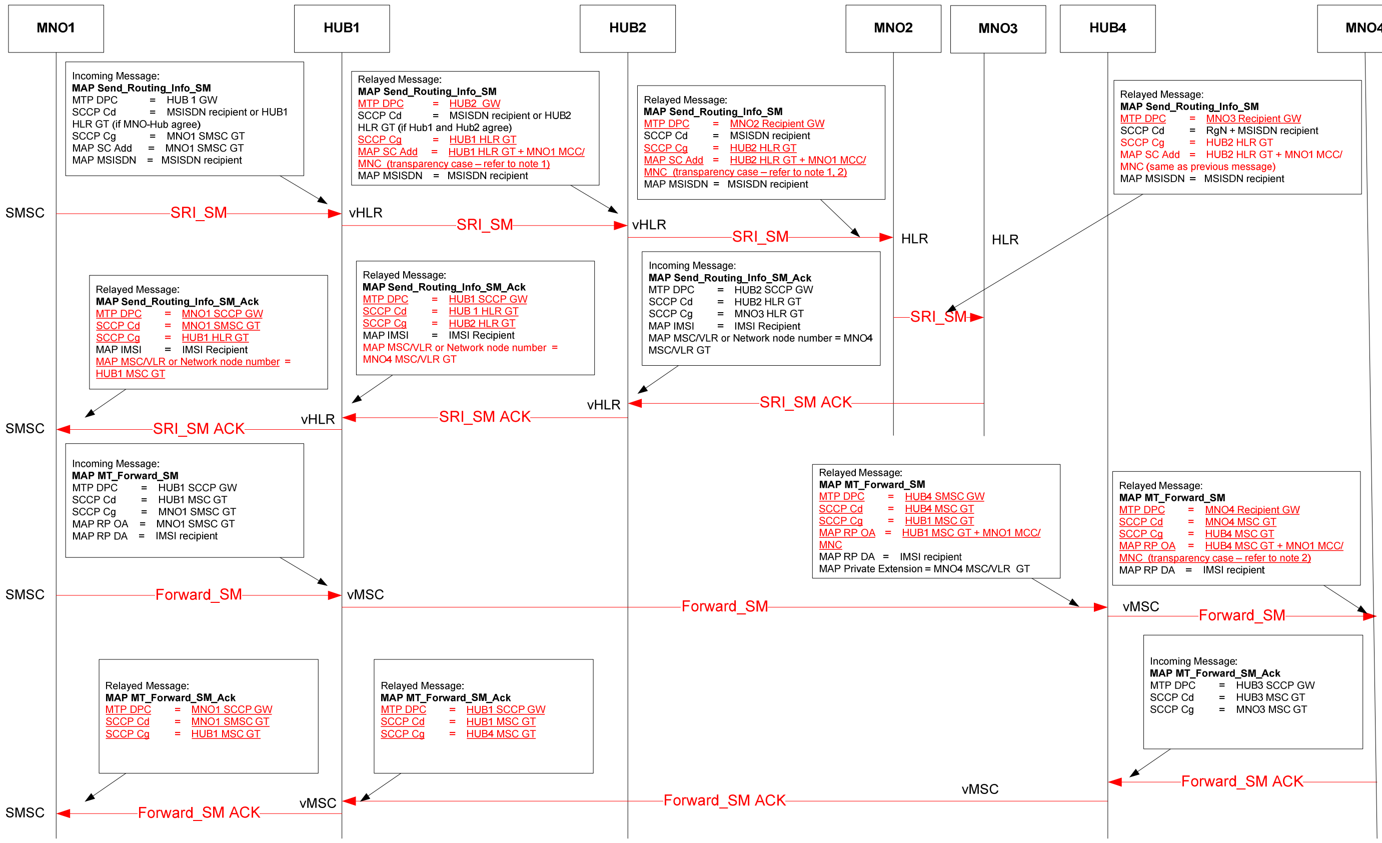
HUB2 upon realizing that the destination is roaming decides to handle the message forwarding.



Notes:
For diagram notes, please refer to the same notes as those for the detailed diagram in section 8.2.3.3.

8.7.3.3 Combined Roaming and MNP case

The destination subscriber is both and ported and roaming and hence there is an MNO3 (ported network) and MNO4 involved (network where the subscriber is roaming). The diagram below shows how the solution works in a combined MNP and Roaming case, and where HUB1 is selected to handle the message forwarding. This of course works equally well with HUB2 handling the message forwarding.



Notes:
For diagram notes, please refer to the same notes as those for the detailed diagram in section 8.2.3.3.

8.7.3.4 Key advantages of this solution approach

1) The case where MNO3 does not wish to do extra GT configuration is addressed. MNO3 is only talking to one HUB, HUB3 who takes care of all inter-working efforts for MNO3.
2) MNP can be handled at the same time.
3) Also simple and provides efficient use of signalling.
4) If it is important to the parties that HUB1 is informed of the actual subscriber location, this solution makes it possible (HUB1 sends to HUB3 solution approach).
5) Will work for Hubs that are not SCCP providers. (Solution 1 should also work equally as well)

8.7.3.5 Disadvantages

1) Can work only when MNO3 has a hub agreement with an SS7 interface
2) This solution approach does require MAP version 2 or higher. Private extension containers are not available at MAP version 1. It is recommended that hubs utilize a per-hop MAP version negotiation approach in order to overcome any issues on MAP version level.

8.7.3.6 MAP Private Extension

For the definition of the MAP private extensions, please refer to section 8.6.1.1.1.

8.7.4 Roaming Solution approach 3 - MNO2 terminates via onward forwarding

In the specific case that MNO2 is capable of onward forwarding a message, and opts to do so, then HUB2 may terminate the SMS to MNO2 and let MNO2 handle the termination.

If the message is SMPP forwarded to MNO2 then the handling is straightforward.
If the message is SS7 forwarded to MNO2, then the HUB2 may have to ignore the SRI location response, or MNO2 returns its address in the MAP MSC-VLR address.

8.7.4.1 Key advantages of this solution approach

1) MNP can be handled at the same time.
2) It's a simple and efficient solution
3) Will work for hubs that are not SCCP providers.

8.7.4.2 Disadvantages

1) Deliver reporting may be broken/fake
2) MNO1/HUB1 is unaware of the true destination of the message.
3) MNO3 loses transparency on MNO1

8.7.5 MNO1 is able to directly reach MNO3

In the specific case that MNO1 has a direct bilateral link to MNO3, then hubs shall allow the option to return the MNO3 VMSC address in the SRI response at the behest of MNO1.

8.7.6 HUB1 is able to directly reach MNO3

In the specific case that HUB1 has a direct bilateral link to MNO3, then hubs can also agree for HUB2 to return the MNO3 VMSC address in the SRI towards HUB1, so that HUB1 may handle the forwarding of the message via MT_FSM (such as the case depicted in section 8.7.3.1).

In the scenario that HUB2 finds that it is unable to reach the MNO3, then it can also simply choose to revert the VLR/MSC GT address to HUB1 to provide an opportunity for the SMS to be terminated by HUB1.

8.7.7 Exclusions for interworking towards MNO3

Before HUB2 terminates a message to MNO3 (or takes the next step to convey the SMS), it must verify that MNO3 has not raised any explicit exclusion of networks it does not want to receive SMS from. This is an opt-out process. In the process of HUB2 and MNO2 agreeing on setting up roaming termination, MNO3 may be requested to add/open the HUB2 GT address (as in solution 1). If MNO3 (or the VPMN) should explicitly specify it does not want

SMS from a certain MNO1, it can do so by request and the hub shall comply. This requirement equally applies in case HUB2 has direct link to MNO3.

Typically, MNO3 is expected not to have such exclusions, since the SMS is terminated to subscribers that are not their own but actually subscribers of MNO2.

8.7.8 SMPP to SS7 case

If MNO1 is using SMPP and MNO2 is using SS7, it is a simple extrapolation to the described solution to inter-work successfully a roaming SMS MT in this case. The message shall be carried in SMPP until HUB2 and HUB2 converts to SS7 towards MNO2. In doing so, HUB2 can employ either solution 1 or solution 2 approach (HUB2 to HUB3 case) to terminate the message.

The opposite case SS7 to SMPP shall not be described as the solution approach for SMS MT roaming towards SMPP is not defined as yet in this architecture document.

8.7.9 Charging for Roaming SMS MT

It is recommended that for the billing and charging aspect, the commercial disposition is guided by the following:

1) There is a standing position in the current market that roaming SMS MT is not charged. If MNO3 should decide to apply a fee, he can do so via TAP charge on the SMS MT.
2) The simplest approach is to apply MNO2 termination fee for SMS MT even if the MNO2 subscriber is roaming and MNO2 is paid the same fee.
3) If a different termination fee from MNO2’s termination fee (or a case of no fee) is to be applied in the roaming case, then HUB1 needs to be informed of the location of the subscriber. This is catered for by the solution approach 2, HUB1 to HUB3 case.
4) Note also that solution approach 1 caters for the specific case where If MNO1 and MNO2 have inter-working present and roaming+inter-working exists between MNO3 and MNO2, and there is no inter-working between MNO1 and MNO3, it is still possible to complete the termination of SMS to the MNO2 subscriber in the roaming case.
5) If MNO3 prefers to apply a fee, this should be applied via SMS MT charge and handled via TAP charge process.

8.8 Error Mapping

This section provides the recommended mapping of SS7 and SMPP errors.

8.8.1 SS7 to SMPP

This provides the mapping of SS7 errors to SMPP errors. A list of SS7 local error values is also provided for reference in section 8.8.3. Whilst there is a mapping provided for temporary SS7 errors, it is expected that this should not typically be used.

SMPP 3.4 Error	Command status	Description	SS7 local error value

ESME_RSYSERR	0x00000008	System Error	11, 12, 15, 34
ESME_RINVDSTADR	0x0000000B	Invalid Dest Addr	1, 9, 5
ESME_RMSGQFUL	0x00000014	Message Queue Full	33
ESME_RX_T_APPN	0x00000064	ESME Receiver Temporary App Error Code	22,29, 31, 21,13,27,32
ESME_RMISSINGOPTPARAM	0x000000C3	Expected Optional Parameter missing	35
ESME_RINVOPTPARAMVAL	0x000000C4	Invalid Optional Parameter Value	36

It may also be possible to carry more information on the SS7 error by using SMPP optional TLV's or SS7 private extensions.

Only the SMPP error ESME_RX_T_APPN is considered to have temporary error treatment among all of the SMPP errors. If it is encountered, then it can be expected that the node receiving the error shall retry at later point in time.

8.8.2 SMPP to SS7

This provides the mapping of SMPP errors to SS7 Errors. This list is based on the SMPP 5.0 error list. Since the SMPP 3.4 errors are a subset of SMPP 5.0, it is straightforward to use this same list for SMPP 3.4. In particular, the command status values which are from 100 hex to 4FF hex are SMPP 5.0 specific, whereas in SMPP 3.4 this range is marked reserved.

In this mapping, the use of temporary SS7 errors has been avoided, since there should be typically no temporary error in SMPP.

SMPP 5	Command Status	Description	SS7 Local Error Code
ESME_ROK	0x00000000	No Error	
ESME_RINVMSGLEN	0x00000001	Message Length is invalid	36
ESME_RINVCMDLEN	0x00000002	Command Length is invalid	36
ESME_RINVCMDID	0x00000003	Invalid Command ID	36
ESME_RINVBNDSTS	0x00000004	Incorrect BIND Status for given c	34
ESME_RALYBND	0x00000005	ESME Already in Bound State	36
ESME_RINVPRTFLG	0x00000006	Invalid Priority Flag	36
ESME_RINVREGDLVFLG	0x00000007	Invalid Registered Delivery Flag	36
ESME_RSYSERR	0x00000008	System Error	34
Reserved	0x00000009	Reserved	
ESME_RINVSRCADR	0x0000000A	Invalid Source Address	9
ESME_RINVDSTADR	0x0000000B	Invalid Dest Addr	5
ESME_RINVMSGID	0x0000000C	Message ID is invalid	36
ESME_RBINDFAIL	0x0000000D	Bind Failed	36
ESME_RINVPASWD	0x0000000E	Invalid Password	38
ESME_RINVSYSID	0x0000000F	Invalid System ID	38
Reserved	0x00000010	Reserved	
ESME_RCANCELFAIL	0x00000011	Cancel SM Failed	34

Reserved	0x00000012	Reserved	
ESME_RREPLACEFAIL	0x00000013	Replace SM Failed	34
ESME_RMSGQFUL	0x00000014	Message Queue Full	33
ESME_RINVSERTYP	0x00000015	Invalid Service Type	36
Reserved	0x00000016	Reserved	
ESME_RINVNUMDESTS	0x00000033	Invalid number of destinations	36
ESME_RINVDLNAME	0x00000034	Invalid Distribution List name	36
Reserved	0x00000035-0x0000003F	Reserved	
ESME_RINVDESTFLAG	0x00000040	Destination flag is invalid (submit_multi)	36
Reserved	0x00000041	Reserved	
ESME_RINVSUBREP	0x00000042	Invalid ‘submit with replace’ request (i.e. Submit_SM with replace_if_present_flag set)	36
ESME_RINVESMCLASS	0x00000043	Invalid esm_class field data	36
ESME_RCNTSUBDL	0x00000044	Cannot Submit to Distribution List	36
ESME_RSUBMITFAIL	0x00000045	Submit_SM or submit_multi failed	32
ESME_RINVSRCTON	0x00000048	Invalid Source address TON	36
ESME_RINVSRCNPI	0x00000049	Invalid Source address NPI	36
ESME_RINVDSTTON	0x00000050	Invalid Destination address TON	9
ESME_RINVDSTNPI	0x00000051	Invalid Destination address NPI	9
Reserved	0x00000052	Reserved	
ESME_RINVSYSTYP	0x00000053	Invalid system_type field	36
ESME_RINVREPFLAG	0x00000054	Invalid replace_if_present flag	36
ESME_RINVNUMMSGS	0x00000055	Invalid number of messages	36
Reserved	0x00000056-0x00000057	Reserved	
ESME_RTHROTTLED	0x00000058	Throttling error	33
Reserved	0x00000059	Reserved	
ESME_RINVSCHED	0x00000061	Invalid Scheduled Delivery Time	36
ESME_RINVEXPIRY	0x00000062	Invalid message validity period (Expiry time)	36
ESME_RINVDFTMSGID	0x00000063	Predefined Message Invalid or Not Found	36
ESME_RX_T_APPN	0x00000064	ESME Receiver Temporary App Error Code	31
ESME_RX_P_APPN	0x00000065	ESME Receiver Permanent App Error Code	12
ESME_RX_R_APPN	0x00000066	ESME Receiver Reject Message Error Code	36
ESME_RQUERYFAIL	0x00000067	query_sm request failed	34
Reserved	0x00000068-0x000000BF	Reserved	
ESME_RINVOPTPARSTREAM	0x000000C0	Error in the optional part of the PDU Body	36
ESME_ROPTPARNOTALLWD	0x000000C1	Optional Parameter not allowed	36
ESME_RINVPARLEN	0x000000C2	Invalid Parameter Length.	36

ESME_RMISSINGOPTPARAM	0x000000C3	Expected Optional Parameter missing	35
ESME_RINVOPTPARAMVAL	0x000000C4	Invalid Optional Parameter Value	36
Reserved	0x000000C5-0x000000FD	Reserved	
ESME_RDELIVERYFAILURE	0x000000FE	Delivery Failure (used for data_sm_resp)	32
ESME_RUNKNOWNERR	0x000000FF	Unknown Error	34
ESME_RSERTYPUNAUTH	0x00000100	ESME Not authorised to use specified service type	36
ESME_RPROHIBITED	0x00000101	ESME Prohibited from using specified	36
ESME_RSERTYPUNAVAIL	0x00000102	Specified service_type is unavailable	12
ESME_RSERTYPDENIED	0x00000103	Specified service_type is denied	12
ESME_RINVDCS	0x00000104	Invalid Data Coding Scheme.	36
ESME_RINVSRCADDRSUBUNIT	0x00000105	Source Address Sub unit is Invalid.	36
ESME_RINVDSTADDRSUBUNIT	0x00000106	Destination Address Sub unit is Invalid.	9
ESME_RINVBCASTFREQINT	0x00000107	Broadcast Frequency Interval is invalid.	36
ESME_RINVBCASTALIAS_NAME	0x00000108	Broadcast Alias Name is invalid.	36
ESME_RINVBCASTAREAFMT	0x00000109	Broadcast Area Format is invalid.	36
ESME_RINVNUMBCAST_AREAS	0x0000010A	Number of Broadcast Areas is invalid.	36
ESME_RINVBCASTCNTTYPE	0x0000010B	Broadcast Content Type is invalid.	36
ESME_RINVBCASTMSGCLASS	0x0000010C	Broadcast Message Class is invalid.	36
ESME_RBCASTFAIL	0x0000010D	broadcast_sm operation failed.	36
ESME_RBCASTQUERYFAIL	0x0000010E	query_broadcast_sm operation failed.	36
ESME_RBCASTCANCELFAIL	0x0000010F	cancel_broadcast_sm operation failed.	36
ESME_RINVBCAST_REP	0x00000111	Broadcast Service Group is invalid.	36
ESME_RINVBCASTSRVGRP	0x00000110	Number of Repeated Broadcasts is	36
ESME_RINVBCASTCHANIND 0x00000112 Broadcast Channel Indicator is invalid.	0x00000112	Broadcast Channel Indicator is invalid.	
Reserved for MC vendor	0x00000400-0x000004FF	Reserved	

8.8.3 SS7 Local Code error values

This is a listing of SS7 errors taken from 3GPP TS 29.002 [2], section 17.6.6. The temporary or permanent disposition is taken from the table in section 8.1.2.

Error	LocalCode	ErrorType	Must not be used	T or P

			in version <3 Tag	
unknownSubscriber	1	IdentificationAndNumberingErrors	Not used	P
unknownMSC	3	IdentificationAndNumberingErrors		P
unidentifiedSubscriber	5	IdentificationAndNumberingErrors	Not used	
absentSubscriberSM	6	ShortMessageServiceErrors		
unknownEquipment	7	IdentificationAndNumberingErrors		
roamingNotAllowed	8	SubscriptionErrors		
illegalSubscriber	9	SubscriptionErrors	Not used	T
bearerServiceNotProvisioned	10	SubscriptionErrors	Not used	T
teleserviceNotProvisioned	11	SubscriptionErrors	Not used	P
illegalEquipment	12	SubscriptionErrors	Not used	P
callBarred	13	CallHandlingErrors		T
forwardingViolation	14	CallHandlingErrors		T
cug-Reject	15	CallHandlingErrors		
illegalSS-Operation	16	SSErrors	Not used	
ss-ErrorStatus	17	SSErrors		
ss-NotAvailable	18	SSErrors	Not used	
ss-SubscriptionViolation	19	SSErrors	Not used	
ss-Incompatibility	20	SSErrors		
facilityNotSupported	21		Not used	T
noHandoverNumberAvailable	25	HandoverErrors		T
subsequentHandoverFailure	26	HandoverErrors		T
absentSubscriber	27	CallHandlingErrors	Not used	T
incompatibleTerminal	28			T
shortTermDenial	29	SSErrors		
longTermDenial	30	SSErrors		
subscriberBusyForMT-SMS	31	ShortMessageServiceErrors		
sm-DeliveryFailure	32	ShortMessageServiceErrors		
messageWaitingListFull	33	ShortMessageServiceErrors		
systemFailure	34			
dataMissing	35		Not used	
unexpectedDataValue	36		Not used	
pw-RegistrationFailure	37	SSErrors		
negativePW-Check	38	SSErrors		
noRoamingNumberAvailable	39	CallHandlingErrors		
tracingBufferFull	40	OperationAndMaintenanceErrors		
targetCellOutsideGroupCallArea	42	HandoverErrors		
numberOfPW-AttemptsViolation	43	SSErrors		
numberChanged	44	IdentificationAndNumberingErrors		
busySubscriber	45	CallHandlingErrors		
noSubscriberReply	46	CallHandlingErrors		
forwardingFailed	47	CallHandlingErrors		
or-NotAllowed	48	CallHandlingErrors		
ati-NotAllowed	49	AnyTimeInterrogationErrors		
noGroupCallNumberAvailable	50	GroupCallErrors		
resourceLimitation	51			
unauthorizedRequestingNetwork	52	LocationServiceErrors		
unauthorizedLCSClient	53	LocationServiceErrors		

positionMethodFailure	54	LocationServiceErrors		
unknownOrUnreachableLCSClient	58	LocationServiceErrors		
mm-EventNotSupported	59	LocationServiceErrors		
atsi-NotAllowed	60	AnyTimeInformationHandlingErrors		
atm-NotAllowed	61	AnyTimeInformationHandlingErrors		
informationNotAvailable	62	AnyTimeInformationHandlingErrors		
unknownAlphabet	71	SSErrors		
ussd-Busy	72	SSErrors		

8.9 OID Allocation Tracking

The following OID is now allocated to the GSM Association, and was primarily requested for the purpose of addressing the current use of MAP private extensions as discussed in this document.

itu-t(0) identified-organization(4) etsi(0) reserved(127) etsi-identified-organization(0) gsm-association(9)
Or 0 4 0 127 0 9

It appears at the ETSI website at http://portal.etsi.org/ptcc/oidlist.asp

There is also a useful browser of the top-level OID allocations at ETSI at:
http://webapp.etsi.org/ASN1ObjectTree/ASN1.asp

This OID allocation shall be tracked with a separate IREG PRD later on. For the meantime, the IREG group has recommended in a meeting dated 6-7th of December 2006 of IREG-adhoc, that this is tracked within this document.

9 OPEN ISSUES

9.1 SCCP Routing Issues

There is a recognized issue that the current SCCP providers of operators will usually carry both their roaming and SMS traffic. Separation of the two may not be straightforward or may entail cost to be levied by the SCCP provider to the operator. At the very least the SCCP provider must be able to perform the separation at the request of the operator.

The MNO1 SMSC must have the intelligence to attempt to deliver the SMS via bi-laterals first and then if there are no appropriate routes send all remaining traffic to HUB1 for onward delivery. Do operators have this capability? Or SMSC's must be able to be configured depending on the destination number up to CC+NDC level to select a link (or SCCP destination)—i.e. up to operator level and not just country level—on which to send messages.

A potential solution is to use SMPP/IP on outgoing SMS inter-working traffic and retain SS7 on incoming SMS. Using SMPP in this manner could allow operators to use the SMSC capability to route their SMS inter-working traffic, and thus overcome the issue.

Another potential solution is to ask SMSC vendors to try and address this issue.
The issue shall be raised by IREG to C7PM as well which is a forum attended by SCCP providers. This is to see if SCCP providers may be able to handle the requirement at their level. The latest response from C7PM as of January 2007 indicates that there is interest, and there is a desire for further discussion and elaboration to take place.

9.2 Hub-to-Hub Backward Compatibility

There may be circumstances where it is necessary for hubs to inter-work with another SMS Hub provider that is not fully compliant to the SMS Hubbing Architecture defined in this document. These are just some crucial points to consider for post-Trial implementation:

Transparency as defined in this architecture document is considered crucial in the long term implementation of SMS Hubbing service. Therefore, provisions must be made by the compliant hub to ensure that this is preserved as much as possible. Some scenarios are discussed below.

In the scenarios below, MNO1 is with HUB1 and MNO2 is with HUB2.

Scenario a. HUB1 does not provide transparency, and HUB2 is providing transparency, and SMS is sent from MNO1 to MNO2, then HUB2 is constrained to perform lookup of the transparency information in behalf of HUB1, and attach it.

Scenario b. HUB1 does provide transparency (either SS7 or SMPP), and HUB2 is providing transparency but only has SS7 hub-to-hub connectivity, and SMS originated using SMPP is sent from MNO1 to MNO2. Then HUB1 is constrained to perform conversion of SMS from SMPP to SS7 in behalf of HUB2, and must also preserve transparency.

Scenario c. HUB1 does provide transparency (either SS7 or SMPP), and HUB2 is providing transparency but only has SMPP hub-to-hub connectivity, and SMS originated using SS7 is sent from MNO1 to MNO2. Then HUB1 is constrained to perform conversion of SMS from SMPP to SS7 in behalf of HUB2, and must also preserve transparency.

9.3 Retry Mechanism for Concatenated Messages

Consider a concatenated SMS composed of 4 messages, and the 4 messages are transferred using the More Message to Send mechanism. And that the first 2 messages are successfully sent to the recipient, and the FSM response for the 3rd message is an error. Then what is the behavior of the originating SMSC? Will the SMSC resend the 4 messages when it retries, or just resend the remaining 2 messages?

It seems that there are some SMSC’s that will resend the 4 messages again when it retries.

Concatenated SMS message segments are in essence independent SMS messages in so far as fixed (MAP) and radio networks are concerned. The only entities that know about the fact that SMS messages are concatenated are the SC and the MS.

In the event of a transmission error occurring in the middle of a concatenated message string sent from an SC, the mobile will know that not all segments have been received and the SC will know that not all segments have been sent. There are of course peripheral error conditions where that will not be true.

What an SC does to re deliver the concatenated message is very much an implementation matter and it could be argued that smart SC’s will try to deliver only the missing segments. However the success of that depends upon what the MS has done with the aborted concatenated message session. If it has discarded the segments it has received then clearly an SC sending only the undelivered segments will be of little use and so it may not be wise for an SC to implement such a strategy as there is no knowledge of what the receiving mobile will do.

In bad radio conditions, segments can get stuck in SC’s and may even be deleted by the SC. How long does a mobile wait for all segments to arrive? How long does a mobile have to store the segments of an incomplete concatenated SM? These are complex issues but are implementation matters which means that such design considerations cannot be relied on by the SC.

Ultimately, concatenated messages is not a concern for the hub, unless there is special consideration between the operator and hub on a private individual basis for this purpose. There shouldn’t be normally though.

9.4 SMPP Response Timer

It seems there is no SMPP response timer defined as such within the SMPP Specifications [10]. Typically 30 seconds could be used. 20 seconds or less would be more applicable when routing hybrid case of SS7 MT-FSM to SMPP; otherwise, there is a risk of timeout on SS7.

10 ANNEXES - INFORMATIONAL

10.1 SS7 MNP

10.1.1 MNP Scenario a1

Currently, if using SS7-MAP for resolving MNP for MT-SMS, Operators in an MNP domain will be required to open their HLR to every Requesting entity which has at least one client MNO in the MNP domain. In terms of the actual routing, it is actually MNO2 that is relaying the SRI to MNO3, and MNO3 is responding to Requesting entity. It is this last leg which is the reason for the requirement.

If an operator does not wish to facilitate the last leg, then SMS delivery to ported MSISDNs will be impacted.

It should be noted that this issue is technically identical and common to the impact of MNP-HLR connectivity on hubbing as well bilateral SMS and MMS services. i.e. the issue applies equally if the requesting entity is an originating operator (MNO1), a “n-1” carrier , a hub or an “in-country-proxy”

10.1.1.1 MNP – IMSI Life Cycle

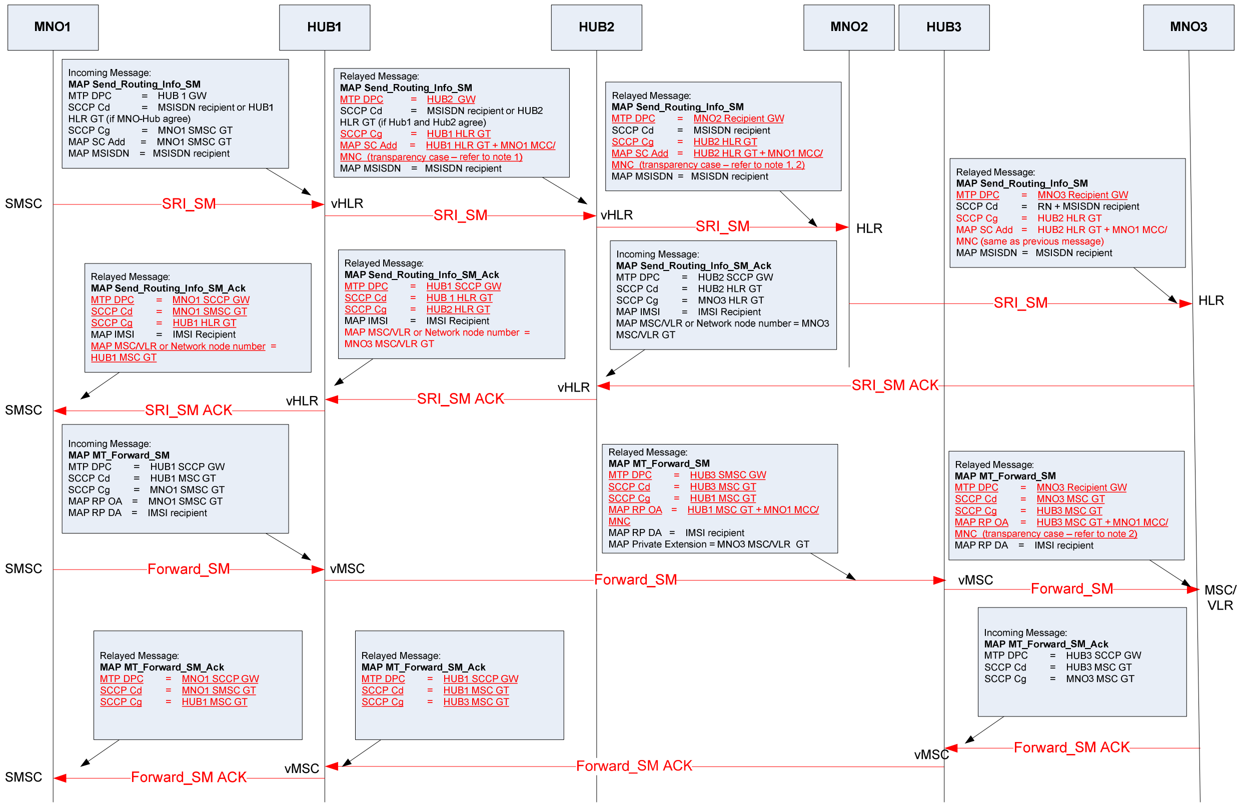
IMSI life cycle is relevant for Hubs that wish to implement an IMSI caching mechanism (i.e. that consider a validity period for the IMSI they receive the response for). This cache refers to the MSISDN to IMSI translation.

10.1.1.2 Identification of MNP RN (Routing Number)

As described in 3GPP TS 123.066 [3] Annex B, in SS7 MNP, an RN (routing number) is utilized to route the SRI from MNO2 to MNO3.

10.1.1.3 MNP Solution Detail Diagram

This section gives a diagram of the technical solution based on the most general case of MNP where there are 3 Hubs and 3 MNOs:



Incoming Message:
MAP Send_Routing_Info_SM
MTP DPC = HUB 1 GW
SCCP Cd = MSISDN recipient or HUB1 HLR GT (if MNO-Hub agree)
SCCP Cg = MNO1 SMSC GT
MAP SC Add = MNO1 SMSC GT
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = HUB2 GW
SCCP Cd = MSISDN recipient or HUB2 HLR GT (if Hub1 and Hub2 agree)
SCCP Cg = HUB1 HLR GT
MAP SC Add = HUB1 HLR GT + MNO1 MCC/ MNC (transparency case – refer to note 1)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = MNO2 Recipient GW
SCCP Cd = MSISDN recipient
SCCP Cg = HUB2 HLR GT
MAP SC Add = HUB2 HLR GT + MNO1 MCC/ MNC (transparency case – refer to note 1, 2)
MAP MSISDN = MSISDN recipient

Relayed Message:
MAP Send_Routing_Info_SM
MTP DPC = MNO3 Recipient GW
SCCP Cd = RN + MSISDN recipient
SCCP Cg = HUB2 HLR GT
MAP SC Add = HUB2 HLR GT + MNO1 MCC/ MNC (same as previous message)
MAP MSISDN = MSISDN recipient

Incoming Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = HUB2 SCCP GW
SCCP Cd = HUB2 HLR GT
SCCP Cg = MNO3 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = MNO3 MSC/VLR GT

Relayed Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB 1 HLR GT
SCCP Cg = HUB2 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = MNO3 MSC/VLR GT

Relayed Message:
MAP Send_Routing_Info_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 HLR GT
MAP IMSI = IMSI Recipient
MAP MSC/VLR or Network node number = HUB1 MSC GT

Incoming Message:
MAP MT_Forward_SM
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = MNO1 SMSC GT
MAP RP OA = MNO1 SMSC GT
MAP RP DA = IMSI recipient

Relayed Message:
MAP MT_Forward_SM
MTP DPC = HUB3 SMSC GW
SCCP Cd = HUB3 MSC GT
SCCP Cg = HUB1 MSC GT
MAP RP OA = HUB1 MSC GT + MNO1 MCC/ MNC
MAP RP DA = IMSI recipient
MAP Private Extension = MNO3 MSC/VLR GT

Relayed Message:
MAP MT_Forward_SM
MTP DPC = MNO3 Recipient GW
SCCP Cd = MNO3 MSC GT
SCCP Cg = HUB3 MSC GT
MAP RP OA = HUB3 MSC GT + MNO1 MCC/ MNC (transparency case – refer to note 2)
MAP RP DA = IMSI recipient

Incoming Message:
MAP MT_Forward_SM_Ack
MTP DPC = HUB3 SCCP GW
SCCP Cd = HUB3 MSC GT
SCCP Cg = MNO3 MSC GT

Relayed Message:
MAP MT_Forward_SM_Ack
MTP DPC = HUB1 SCCP GW
SCCP Cd = HUB1 MSC GT
SCCP Cg = HUB3 MSC GT

Relayed Message:
MAP MT_Forward_SM_Ack
MTP DPC = MNO1 SCCP GW
SCCP Cd = MNO1 SMSC GT
SCCP Cg = HUB1 MSC GT

Notes:
For diagram notes, please refer to the same notes as those for the detailed diagram in section 8.2.3.3.

10.1.1.4 MNP Solution Detail Notes

1) For HUB2, MAP SRI_SM_Ack messages for subscribers that actually belong to a Client Operator not served by the Hub (i.e. recipient Hub is different from HHUB2) are relayed to the Originating Hub (HUB1), and no IMSI/VMSC pair is stored (as no MAP MT Forward SM is expected)
2) MNP scenario a1 has the advantage of keeping HUB1 informed of the actual destination network of the message. This is in contrast to scenario MNP scenario c1 described in section 8.6.4.

10.1.1.5 HLR Access Security Concern

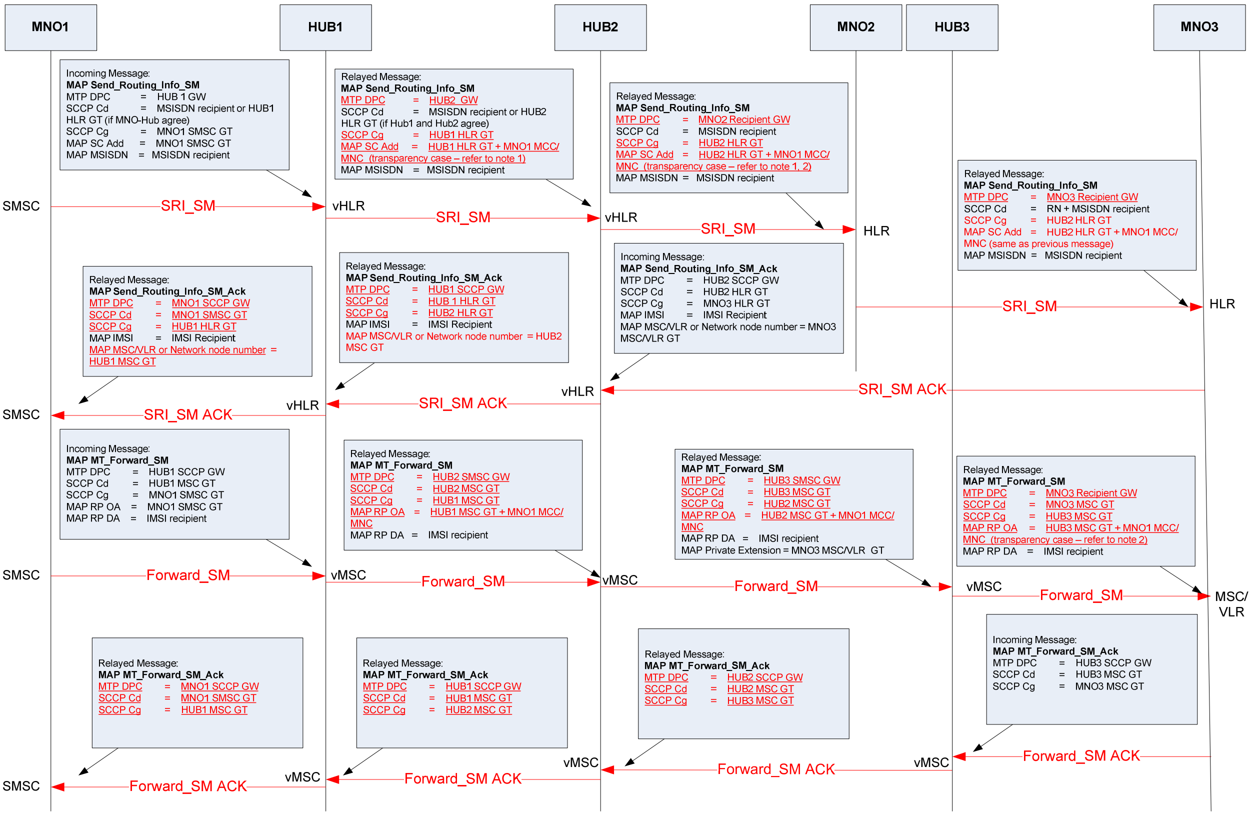
Operators have a concern with the HLR access requirement which is attached to MNP scenario a1 and c1, and this is the reason why the solution description is defined in this informational annex. To alleviate this concern a number of possible measures could be taken:

1) A binding contract is necessary on any third party hub requiring HLR access. Among other things, this contract should ensure that the information collected by the third party is never stored or used for any purpose other than for MNP resolution.

2) Third party hubs could offer to provide CDR or logs of all MAP procedure interfaces to the operator, or perhaps an online monitoring facility for this purpose.

10.1.2 MNP Scenario c1

This is quite similar to scenario a1, however, in this case it is HUB2 that is handling the MNP resolution and message forwarding. This solution has the disadvantage that it hides the number portability information from HUB1. It will be noted also that the cascaded signal flow for SS7 is maintained. The message flow for this scenario is illustrated below.



Notes:

For diagram notes, please refer to the same notes as those for the detailed diagram in section 8.2.3.3.

This solution approach does require MAP version 2 or higher. Private extension containers are not available at MAP version 1. It is recommended that hubs utilize a per-hop MAP version negotiation in order to overcome any issues on MAP version level.