3GPP TR 23.840 V7.1.0 (2007-03)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Study into routeing of MT-SMs via the HPLMN (Release 7)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords
UMTS, GSM, SMS

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2007, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).
All rights reserved.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document provides a study into the current core network architecture for inter-PLMN short message delivery and provides a study into how such an architecture can be improved for the modern day. Wherever possible, backwards compatibility is maintained and impacts are only upon the home network of the destined subscriber.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.066: "Support of Mobile Number Portability (MNP); Stage 1".

[3] 3GPP TS 23.066: "Support of GSM Mobile Number Portability (MNP); Stage 2".

[4] 3GPP TS 23.040: "Technical Realization of the Short Message Service (SMS)".

[5] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[6] 3GPP TS 48.008: "Mobile Switching Centre - Base Station system (MSC-BSS) interface; Layer 3 specification".

[7] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[8] 3GPP TS 23.003: "Numbering, addressing and identification".

[9] 3GPP TS 23.204: "Support of Short Message Service (SMS) over generic 3GPP (Internet Protocol) IP access; Stage 2".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 21.905 [1] and the following apply.

receiving MS: The MS who is the recipient of a Short Message.

originating MS: The MS who is the originator of a Short Message.

Subscribed Network: The network to which the MS currently belongs. This may or may not be the Number Range Owning Network.

3.2 Abbreviations

For the purposes of the present document, the abbreviations defined in 3GPP TS 21.905 [1] apply, as well as those defined below:

SM	Short Message
SMS-IWMSC	Short Message Service – Interworking MSC
SMS-SC	Short Message Service Centre
SRI	Send Routeing Information
NRON	Number Range Owner Network

4 Analysis of current architecture

4.1 Introduction

This clause provides a study into the current core network architecture for inter-PLMN short message delivery as defined in the 3GPP specification set (mainly 3GPP TS 23.040 [4] and 3GPP TS 29.002 [5]). It discusses the draw backs, short falls and current known exploitations that make use of this particular architecture.

4.2 Current architecture

The following signalling flow diagram shows the MT SM transfer procedure in the successful case.

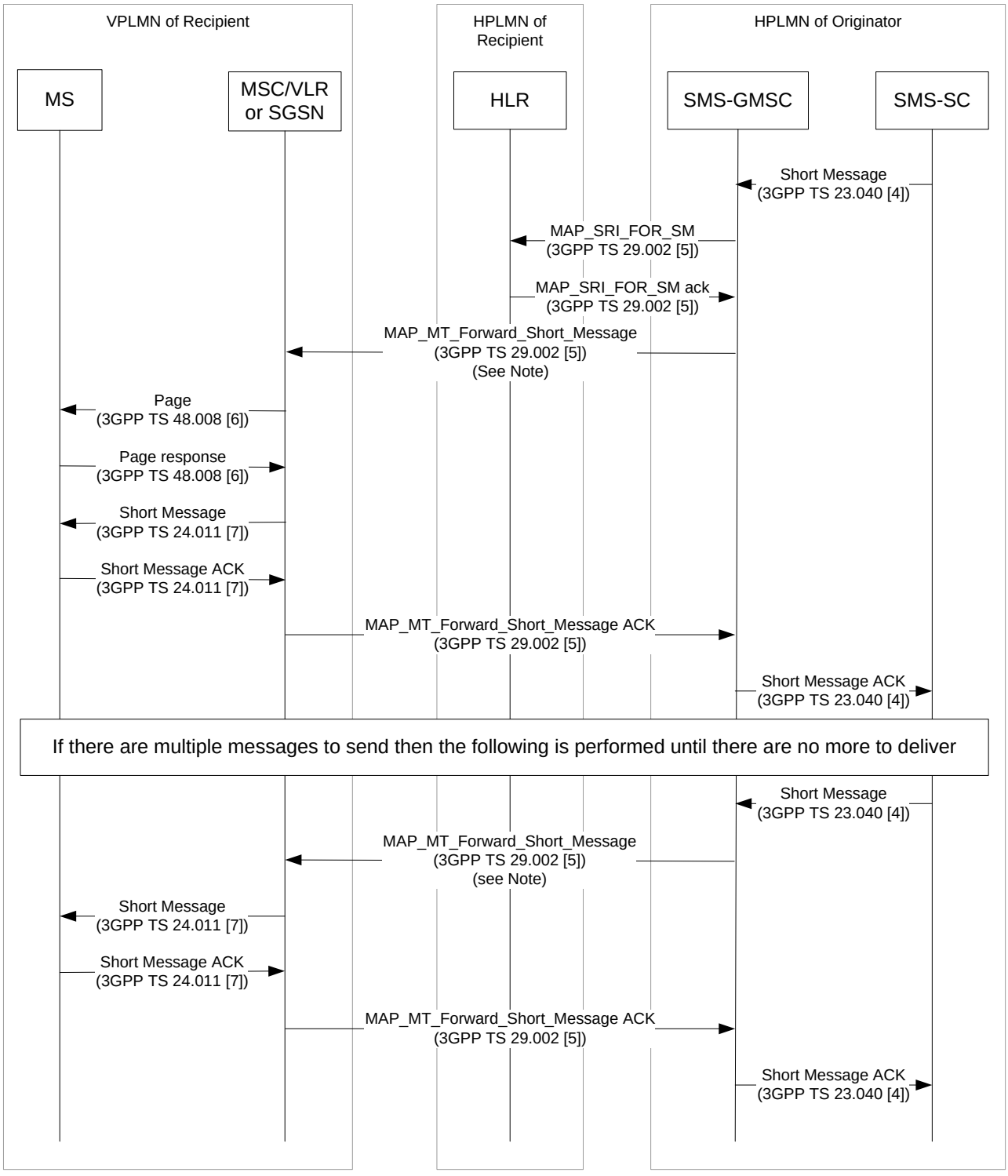

Figure 4.2.1: MT SM Delivery Message Flow

NOTE: The MAP_MT_Forward_Short_Message MAP operation may be preceded by both the sending of an empty TC BEGIN message and the successful receiving of a TC CONTINUE.

As can be seen in Figure 4.2.1, the originating MS's HPLMN delivers the Short Message **directly** to the receiving MS's VPLMN after querying the HLR for the current location of the receiving MS. This means that, unlike CS calls and some PS sessions (i.e. those PS sessions that use a GGSN in the HPLMN), the HPLMN is not present in the MT routeing of the actual data i.e. the SM. The limitations and drawbacks of this architecture are described in the following section.

4.3 Limitations and drawbacks of the current architecture

The following sub-sections describe limitations of the current architecture, some of which have existed since the beginning of GSM but have only come to be a problem now due to the global success of GSM/UMTS (i.e. more operators and in more countries). When SMS was first defined, it was thought that all GSM networks would have roaming agreements with all others, so such problems were deemed to not be an issue in the long term.

Other limitations and drawbacks have come about due to the definition of new features/services e.g. MNP, or due to recent privacy concerns and newly discovered fraud scenarios.

It should be noted that SMS interworking agreements commonly go hand in hand with roaming agreements (except for countries that do not have national roaming and therefore only have SMS interworking agreements). Such agreements exist only between the HPLMNs of MSs.

4.3.1 Receiving MS roaming in PLMN inaccessible to Originating MS's HPLMN

When the receiving MS is roaming (and hence, outside of its HPLMN), if there is no SMS interworking agreement between this PLMN (i.e. the receiving MS's VPLMN) and the originating MS's HPLMN, the delivery of the SM will fail, even though there may be an SMS interworking agreement between the originating MS's HPLMN and the receiving MS's HPLMN.

4.3.2 Effects of Mobile Number Portability

Mobile Number Portability is specified in 3GPP TS 22.066 [2] and 3GPP TS 23.066 [3]. However, real world implementations do sometimes differ quite considerably from these specifications. This section explains only the MNP issues for MT SMS. There are commonly two main architectures for implementations of Number Portability: those that use a central MNP database (either centrally located, or a copy held by each operator in the MNP domain) and those that do not. There are also different architectures for CS calls (MAP_SRI operation) compared to MT SMS (MAP_SRI_For_SM).

For MNP domains where the HLR services the MAP_SRI_For_SM MAP operation (including but not necessarily limited to, those without a central MNP database implementation), the following message flow depicted in Figure 4.3.2.1 occurs. The numbered circles are used to reference each message in the text that follows.

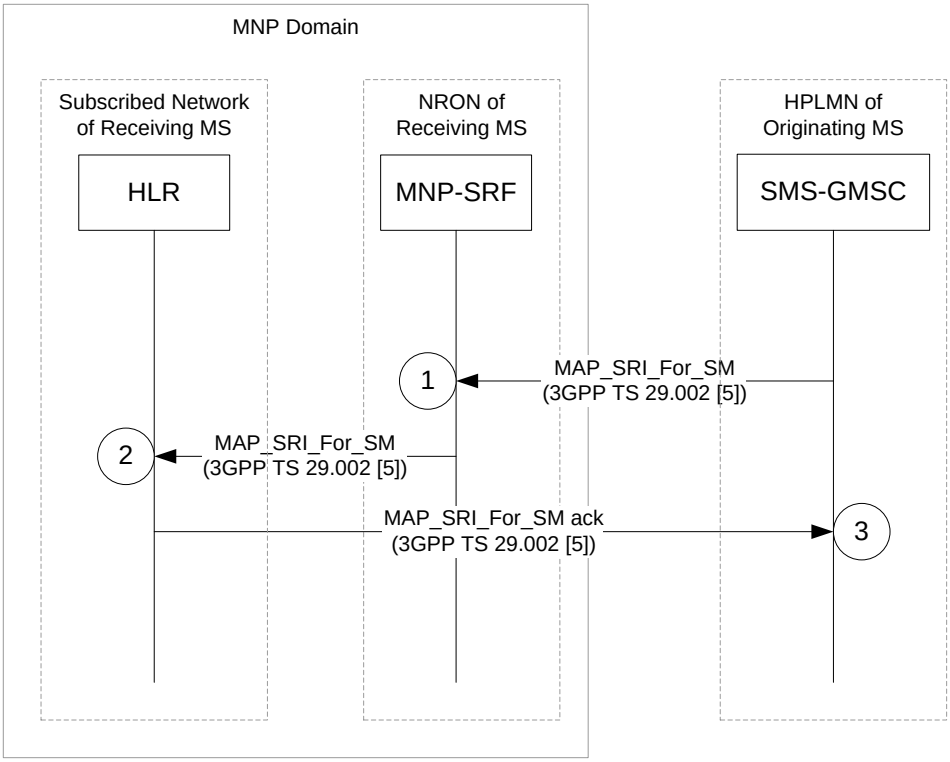

Figure 4.3.2.1: MNP Issues

The delivery of message number 1 will fail if any of the following is true:

- The NRON restricts access to only those networks with which it has an SMS inter-working agreement and there is no agreement in place with the HPLMN of the originating MS.
- The MAP AC version negotiation (of the AC shortMsgGatewayContext) occurs between the NRON and the HPLMN of the Originating MS and the MAP AC negotiated is higher than the MAP AC version that the Subscribed Network of the receiving MS supports.
- The NRON does not recognise MAP e.g. fixed line operator

The delivery of message number 2 is not affected by MNP because in order for MNP to be able to function, routeing between each and every HLR in an MNP domain needs to exist. Such interconnection agreements are set-up before an MNP domain can go live.

The delivery of message number 3 will fail if there is no SMS inter-working agreement between the HPLMN of the originating MS and the Subscribed Network of the receiving MS. However, such a failure is *expected*, because the HPLMN of the originating MS cannot deliver an SM to a network with whom there does not exist an SMS interworking agreement.

Therefore, the effect of MNP on the MAP_SRI_For_SM MAP operation is the routeing of message 1 only. However, the issues highlighted can really only be fixed by careful configuration of operators in the MNP domain; routeing SMs via the receiving subscriber's HPLMN would not have any effects.

The effect of MNP on the MAP_Forward_Short_Message MAP operation is synonymous with the issue discussed in section 4.3.1 i.e. MNP may be an alternative cause, as opposed to the MS just roaming, for why the receiving MS's VPLMN has no inter-working agreement with the originating MS's HPLMN.

4.3.3 Misuse of SM delivery mechanism

There is currently no specific correlation between the MAP_SRI_For_SM MAP operation and the subsequent MAP_MT_Forward_Short_Message MAP operation(s). This has the advantage in that multiple SMs can be delivered to the receiving MS's VPLMN without further involvement from the HLR of the receiving MS, thus keeping load on the HLR, and thereby load on the HPLMN overall, to a minimum.

However, this does have the disadvantage in that the data from the result of the MAP_SRI_For_SM response (e.g. IMSI, MSC/VLR GT, SGSN GT) received by the originating MS's HPLMN, can be shared with other parties to also deliver SMs.

This practice of using previously harvested MAP_SRI_For_SM results has been used by certain parties in order to provide a different (or "faked") originating MS and therefore different sending PLMN. This results in that certain party delivering its SMs (commonly with unsolicited content) for free, because the wrong PLMN is billed. The use of both the sending of an empty TC BEGIN message and the successful receiving of a TC CONTINUE preceding the MAP_MT_Forward_Short_Message being sent, can curb this fraud scenario. However, for the receiving MS's HPLMN, there is reliance upon the originating MS's HPLMN and all SMS inter-working partner's PLMNs to support this feature; the roll out of which is not controlled by the receiving MS's HPLMN (which is the victim in this scenario).

4.3.4 Spam

In recent times, Mobile Subscribers have experienced a rise in receiving unsolicited short messages (commonly called "Spam"). Such SMs range from advertising products/services, to more unscrupulous practices such as duping subscribers into dialling a premium rate number (e.g. on the pretence that they have won a competition).

User Equipment typically does not have the capability for sophisticated Spam identification and processing. In order to provide for this across the whole of a subscriber base (regardless of UE capability), such functionality is typically provided for by the HPLMN (usually on either an opt-in or opt-out basis, depending on local regulations). However, as discussed in section 4.3.2, if the receiving MS is roaming outside of the HPLMN, then the HPLMN is not in the path of the delivery of SMs and therefore cannot intercept such SMs, resulting in the receiving MS receiving such "Spam" SMs while roaming and occasionally, depending on the VPLMN, incurring a roaming charge for receiving it.

Therefore, in the current world, the general trust of the identity of the sending MS and its HPLMN, has diminished and so wherever possible, some kind of authentication should take place before accepting to deliver an SM.

4.3.5 Lawful Interception

There exist regulations in certain countries that a PLMN must be able to intercept all types of traffic, including SMs, to/from their subscribers. Providing for this when the MS is roaming outside of the HPLMN is not possible in the current 3GPP defined SMS architecture. Interception when roaming requires a non-standardised solution, which may not inter-work properly or have unexpected behaviour for the originating MS's HPLMN (from a technical and/or commercial perspective).

4.3.6 Inability to offer certain value added services

Similar to the issue in 4.3.4, simple value added services such as SMS Forwarding cannot be provided by a PLMN for their subscribers, as it would fail indefinitely when the subscriber is roaming outside of their HPLMN. This is also true for offering alternative delivery mechanisms to the MS e.g. delivering SMs over an IP connection (see 3GPP TS 23.204 [9]).

4.4 Conclusion

It has been identified that the current architecture of the MT SM transfer procedure, although more than fit for purpose at the time of its conception, has a number of limitations and drawbacks in the current day. These include issues that were known but thought to not be of any significance (such as the receiving MS roaming in a PLMN inaccessible to the originating MS's HPLMN), issues that have only become apparent recently (such as the fraud issues of SMS faking and the distribution of "Spam") and also new regulatory requirements that PLMNs are compelled to meet such as (Mobile) Number Portability and new laws regarding Lawful Interception.

Finally, due to the current architecture it is currently not possible offer value added services to SMS that subscribers expect due to such services already being available for CS calls. The offering of such services would allow PLMNs to serve their customers better as well as realise new revenue opportunities.

Therefore, any modifications to the current architecture of the MT SM transfer procedure should take the above into account. Any solution shall also be limited to the HPLMN of the receiving MS, thus avoiding the reliance upon SMS inter-working partner PLMNs and roaming partner PLMNs to perform any upgrades before any benefits can be realised. As always, backwards compatibility (inter-working with PLMNs using the current architecture) shall be maintained.

5 Proposed solution

5.1 Introduction

This clause discusses a new core network architecture for inter-PLMN short message delivery that addresses most, if not all, of the drawbacks and short falls of the current architecture documented in clause 4.

5.2 Architecture and procedures

5.2.1 Discussion

In order to meet all of the requirements in sub-clause 4.4 of the present document, it is proposed that all MT SMs shall have the capability to be routed via an SMS-SC-like logical entity located in the HPLMN of the receiving MS.

NOTE: Throughout the rest of the present document, the "SMS-SC-like" logical entity is referred to as an "SMS Router". In reality, such a node would not necessarily need all the functionality of a traditional SMS-SC and in some cases, it may need different/extra functionality e.g. support of different MAP ACs, different storage requirements.

In countries that implement MNP, the HPLMN of the receiving MS shall be assumed to be the Subscribed Network, unless explicitly stated otherwise.

The routeing retrieval for SMS is realised by the MAP_SRI_For_SM operation. The messaging involved with this operation already involves the HPLMN of the receiving MS. This means that this messaging can be used to force the subsequent delivery of the SM (which uses the MAP_Forward_Short_Message operation) to a different node other than the serving MSC/VLR or SGSN; specifically, a node located in the subscribed network of the receiving MS.

Once the subscribed network of the receiving MS receives the subsequent MAP_Forward_Short_Message, the HPLMN of the receiving MS can then take care of the actual delivery. However, due to the absence of the MSISDN of the destination MS in subsequent MAP_Forward_Short_Message messages, some kind of correlation is required with the original MAP_SRI_For_SM.

NOTE: There is not the option to insert the MSISDN of the destination MS in the MAP_Forward_Short_Message as this would impact the SMS inter-working PLMNs and roaming partner PLMNs, which is a requirement of clause 4.

5.2.2 Transparent Mode

The following signalling flow diagram shows the new MT SM transfer procedure in Transparent Mode for the successful case. The numbered circles are used to reference each step in the text that follows.

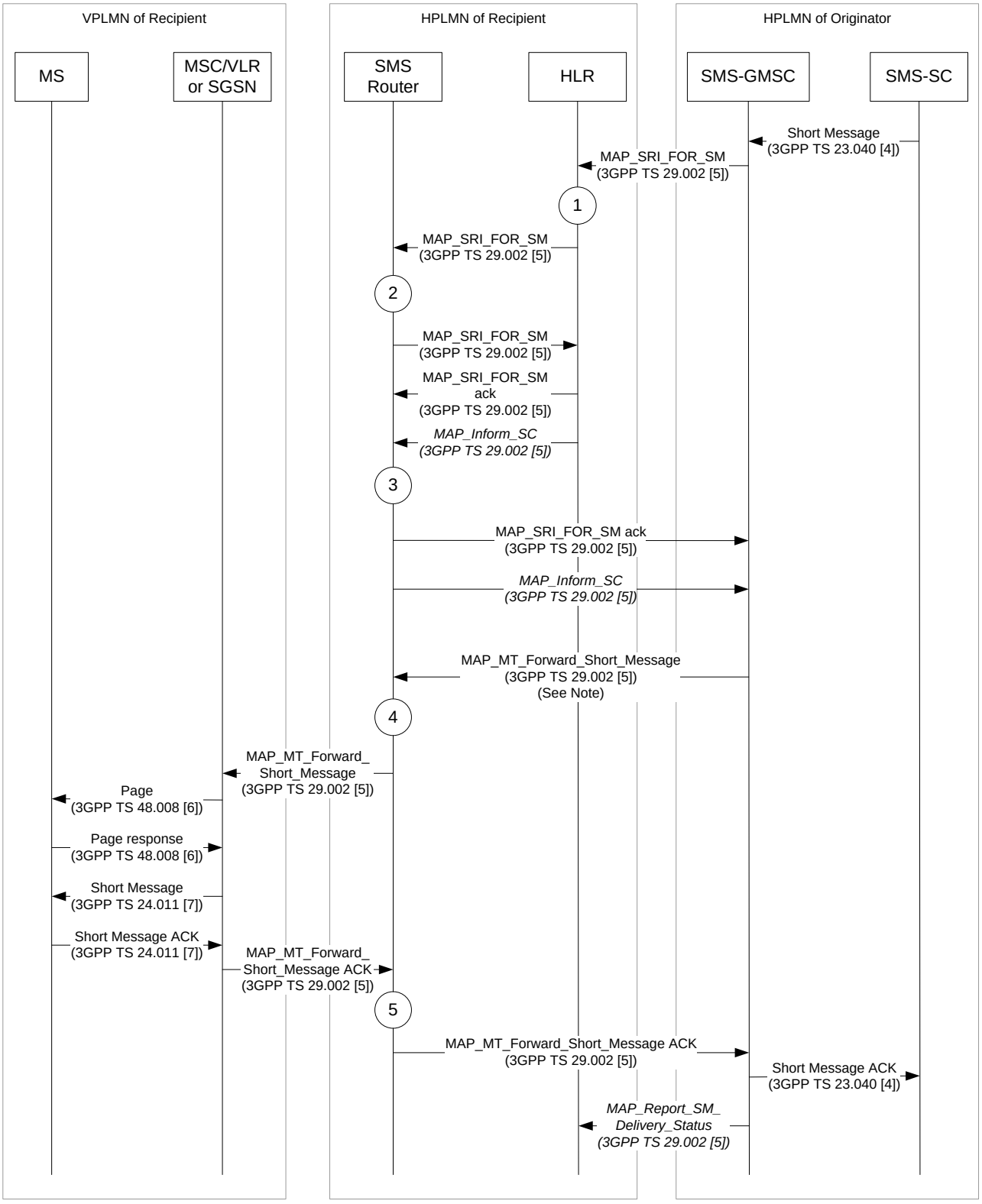

Figure 5.2.2.1: New MT SM Delivery Message Flow in Transparent Mode

NOTE 1: The MAP_MT_Forward_Short_Message MAP operation may be preceded by both the sending of an empty TC BEGIN message and the successful receiving of a TC CONTINUE.

NOTE 2: Messages shown in italic are conditional.

1) In order to correlate subsequent MAP_Forward_Short_Message messages with the previous MAP_SRI_For_SM (which, as mentioned previously, is needed due to the absence of the MSISDN of the destination MS in the MAP_Forward_Short_Message message) the SMS Router needs to service the MAP_SRI_For_SM.

NOTE: If the HLR itself replies to the MAP_SRI_For_SM then it would need to somehow inform the SMS Router of the correlation ID. This would require completely new messaging between the HLR and the SMS Router and therefore is much larger impacting on the MAP protocol.

Upon receiving the MAP_SRI_For_SM ind, the HLR shall determine whether or not to answer the request itself or relay (at the SCCP level) on to the SMS Router. The exact method by which it does this is operator specific, but can be done by SCCP GT analysis e.g. forward all MAP_SRI_For_SM messages on to the SMS Router that have not come from the SMS Router, or even on a per subscriber basis by usage of a flag in the subscriber's profile.

NOTE: As an alternative/temporary solution to the above, an incoming MAP_SRI_For_SM message could be intercepted by an intermediary node (e.g. using MAP AC filters) and redirected to the SMS Router in all cases. This would have the added benefit of reducing signalling load on the HLR, but may require a non-3GPP logical element. Also, it would prohibit operators to enable/disable the use of SMS Router on a per subscriber basis.

2) Upon receiving the MAP_SRI_For_SM ind from the HLR, the SMS Router shall then immediately create its own MAP_SRI_For_SM req message, using the information from the received MAP_SRI_For_SM ind message (including the received Service Centre Address) and send this to the HLR, which in turn responds with a MAP_SRI_For_SM conf and possibly a MAP_Inform_SC in the normal way.

3) Upon receiving the MAP_SRI_For_SM conf from the HLR, the SMS Router shall check the result. If it is a negative response (e.g. unknown subscriber) this information is sent back to the SMS-GMSC in a MAP_SRI_For_SM res (a response to the MAP_SRI_For_SM originally received from the SMS-GMSC).

In the successful case, the SMS Router shall create a Correlation ID and store this along with the IMSI, Network Node Number, Additional Number (obtained from the MAP_SRI_For_SM conf from the HLR), as well as the MSISDN (obtained from the MAP_SRI_For_SM ind originally from the SMS-GMSC) of the receiving subscriber in a local cache for a certain amount of time. For security purposes, the GT of the SMS-GMSC may also be stored. The SMS Router shall then send a MAP_SRI_For_SM res, using the data received from the MAP_SRI_For_SM conf from the HLR, but with the following modifications:

- The Network Node Number and/or the Additional Number are replaced by the GT of the SMS Router, however the SSN of each original GT is retained.

- The IMSI IE is populated with a Correlation ID (see section 5.3.1 for more information).

In any case, if the message MAP_SRI_For_SM conf received from the HLR was accompanied by a MAP_Inform_SC message, the SMS Router shall also forward this MAP_Inform_SC message to the SMS-GMSC.

4) Upon receiving a MAP_MT_Forward_Short_Message ind from the SMS-GMSC, the SMS Router shall take the Correlation ID received in the IMSI IE and use this as a key to look-up the real IMSI, Network Node Number, Additional Number and MSISDN of the originating MS stored in step 3.

If no match is found, a MAP_MT_Forward_Short_Message res is sent back immediately to the SMS-GMSC with an error of "System Failure". The SMS-GMSC may then perform another MAP_SRI_For_SM operation, as per normal procedures for the SMS-GMSC.

If a match is found, then the SMS Router may optionally check the GT of the SMS-GMSC that the MAP_MT_Forward_Short_Message originated from against the stored GT of the SMS-GMSC (i.e. the GT of the SMS-GMSC that issued the MAP_SRI_For_SM). If the CC and NDC of the GT do not match, the SMS Router shall send a MAP_MT_Forward_Short_Message res back immediately to the SMS-GMSC with an error of "System Failure". Otherwise the SMS Router shall then keep the TCAP dialogue with the SMS-GMSC open and shall then create and send a MAP_MT_Forward_Short_Message req containing the received SM to the MSC/VLR or SGSN where the subscriber is currently residing (as identified in the Network Node Number and/or Additional Number retrieved from the local cache). The SMS Router shall analyse the SSN in the GT of the received MAP_MT_Forward_Short_Message ind to determine whether to use the GT from the Network Node Number or the Additional Number.

5) Upon receiving the MAP_MT_Forward_Short_Message conf message(s) from the MSC/VLR or SGSN, the SMS Router shall copy the relevant data (e.g. SM-RP-UI, User error) received in this/these message(s) to populate and send the MAP_MT_Forward_Short_Message res message(s) to the SMS-GMSC. The SMS-GMSC shall then perform normal handling e.g. when a negative response is received, retry delivery via the alternative domain and after that send a MAP_Report_SM_Delivery_Status message to the HLR if required.

5.2.3 Non-Transparent Mode

The following signalling flow diagram shows the new MT SM transfer procedure in Non-Transparent Mode for the successful case. The numbered circles are used to reference each step in the text that follows.

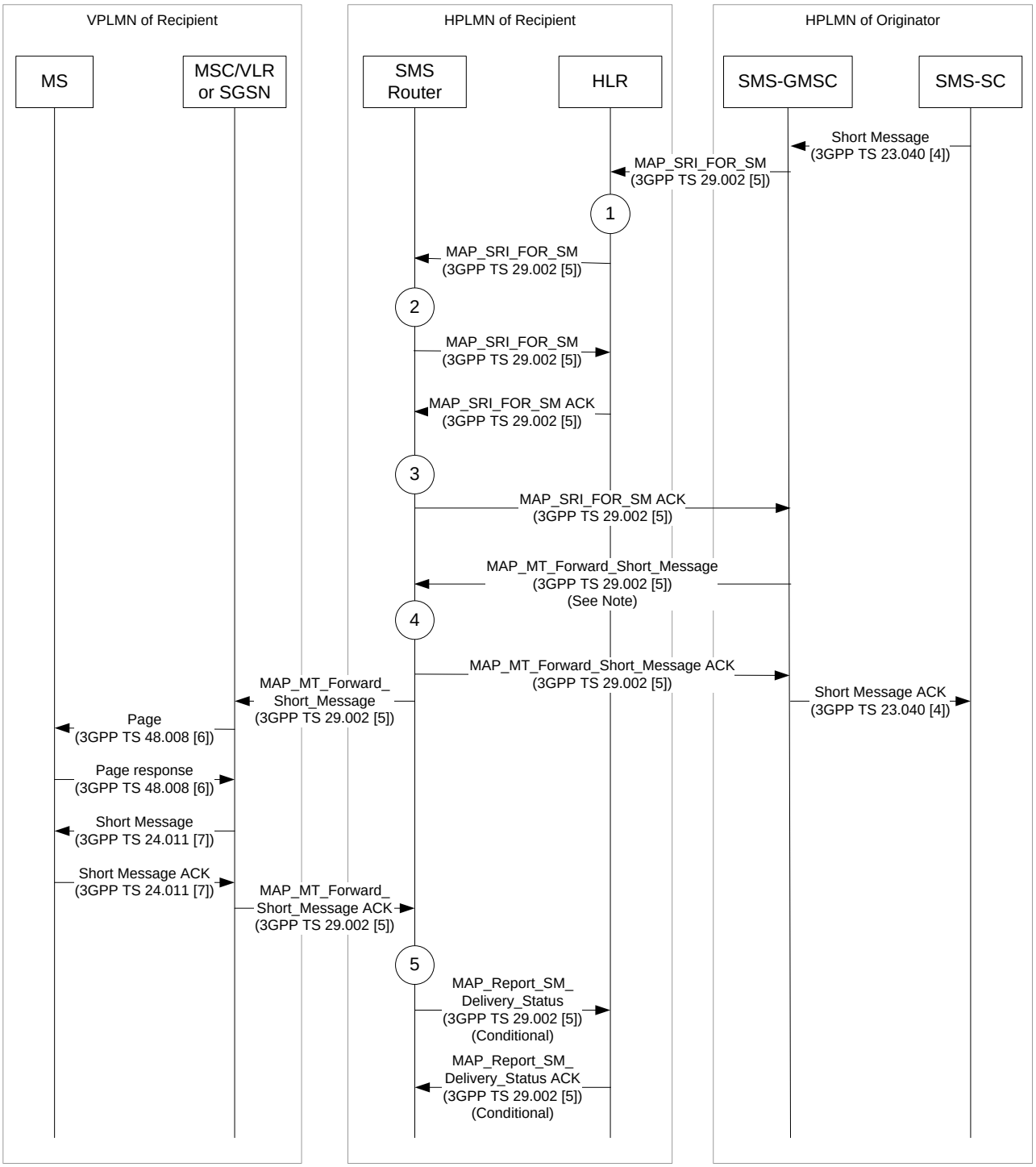

Figure 5.2.3.1: New MT SM Delivery Message Flow in Non-Transparent Mode

NOTE: The MAP_MT_Forward_Short_Message MAP operation may be preceded by both the sending of an empty TC BEGIN message and the successful receiving of a TC CONTINUE.

1) In order to correlate subsequent MAP_Forward_Short_Message messages with the previous MAP_SRI_For_SM (which, as mentioned previously, is needed due to the absence of the MSISDN of the destination MS in the MAP_Forward_Short_Message message) the SMS Router needs to service the MAP_SRI_For_SM.

NOTE: If the HLR itself replies to the MAP_SRI_For_SM then it would need to somehow inform the SMS Router of the correlation ID. This would require completely new messaging between the HLR and the SMS Router and therefore is much larger impacting on the MAP protocol.

Upon receiving the MAP_SRI_For_SM ind, the HLR shall determine whether or not to answer the request itself or relay (at the SCCP level) on to the SMS Router. The exact method by which it does this is operator specific, but can be done by SCCP GT analysis e.g. forward all MAP_SRI_For_SM messages on to the SMS Router that have not come from the SMS Router, or even on a per subscriber basis by usage of a flag in the subscriber's profile.

NOTE: As an alternative/temporary solution to the above, an incoming MAP_SRI_For_SM message could be intercepted by an intermediary node (e.g. using MAP AC filters) and redirected to the SMS Router in all cases. This would have the added benefit of reducing signalling load on the HLR, but may require a non-3GPP logical element. Also, it would prohibit operators to enable/disable the use of SMS Router on a per subscriber basis.

2) Upon receiving the MAP_SRI_For_SM ind from the HLR, the SMS Router may then immediately create its own MAP_SRI_For_SM req message, using the information from the received MAP_SRI_For_SM ind message (including the received Service Centre Address) and send this to the HLR, which in turn responds with a MAP_SRI_For_SM conf in the normal way.

3) Upon receiving the MAP_SRI_For_SM conf from the HLR, the SMS Router shall check the result. If it is a negative response (e.g. unknown subscriber) this information is sent back to the SMS-GMSC in a MAP_SRI_For_SM res (a response to the MAP_SRI_For_SM ind originally received from the SMS-GMSC).

In the successful case, the SMS Router shall create a Correlation ID and store this along with the IMSI, Network Node Number, Additional Network Node Number (obtained from the MAP_SRI_For_SM conf from the HLR), as well as the MSISDN and the Priority bit field (obtained from the MAP_SRI_For_SM ind originally from the SMS-GMSC) of the receiving subscriber in a local cache for a certain amount of time. For security purposes, the GT of the SMS-GMSC may also be stored. The SMS Router shall then send a MAP_SRI_For_SM res, using the data received from the MAP_SRI_For_SM conf from the HLR, but with the following modifications:

- The Network Node Number and/or the Additional Number are replaced by the GT of the SMS Router, however the SSN of each original GT is retained.

- The IMSI IE is populated with a Correlation ID (see section 5.3.1 for more information).

4) Upon receiving a MAP_MT_Forward_Short_Message ind from the SMS-GMSC, the SMS Router shall take the Correlation ID received in the IMSI IE and use this as a key to look-up the real IMSI, Network Node Number, Additional Network Node Number, MSISDN and the Priority bit field of the originating MS stored in step 3.

If no match is found, a MAP_MT_Forward_Short_Message res is sent back immediately to the SMS-GMSC with an error of "System Failure". The SMS-GMSC may then perform another MAP_SRI_For_SM operation, as per normal procedures for the SMS-GMSC.

If a match is found and the Priority bit is set, processing shall continue from paragraph 3 of step 4 in the Transparent Mode. If a match is found and the Priority bit is not set, then the SMS Router may optionally check the GT of the SMS-GMSC that the MAP_MT_Forward_Short_Message originated against the stored GT of the SMS-GMSC (i.e. the GT of the SMS-GMSC that issued the MAP_SRI_For_SM). If the CC and NDC of the GT do not match, then the SMS Router shall send a MAP_MT_Forward_Short_Message res back immediately to the SMS-GMSC with an error of "System Failure". Otherwise the SMS Router shall then create and send a MAP_MT_Forward_Short_Message res to the SMS-GMSC, closing the TCAP dialogue with the SMS-GMSC after receiving any further MAP_MT_Forward_Short_Message ind messages due to the "More Messages To Send" flag being set. The SMS Router shall then send the SM(s) in new MAP_MT_Forward_Short_Message message(s) to the MSC/VLR or SGSN where the subscriber is currently residing (as identified in the Network Node Number retrieved from the local cache. The SMS Router shall analyse the SSN in the GT of the received

MAP_MT_Forward_Short_Message ind to determine whether to use the GT from the Network Node Number or the Additional Number.

5) Upon receiving the MAP_MT_Forward_Short_Message conf message(s) from the MSC/VLR or SGSN, the SMS Router shall check the result. If it is a negative response (e.g. Absent Subscriber for SM), then the SMS Router shall forward the SM on to an SMS-SC (not specified in the diagram above but could be achieved e.g. using MAP or SMPP) for later delivery (as per normal "store and forward" procedures in SMS). In addition to this, the SMS Router shall send a MAP_Report_SM_Delivery_Status req message to the HLR, of which shall contain the appropriate reason for delivery failure (as received from the MSC or SGSN where the receiving MS is currently residing) and shall have the Service Centre Address parameter set to the address of the SMS-SC that the SM has been forwarded to for later delivery.

5.2.4 Analysis

In Transparent Mode, a timeout could occur in the SMS-GMSC while waiting for a response to the MAP_MT_Forward_Short_Message, as unbeknown to the SMS-GMSC, it the SM is having to be forwarded on further. The chance of this happening increases the further away (geographically) from the HPLMN the receiving MS is roaming.

In Non-Transparent Mode, delivery reports may no longer correctly reflect actual delivery to the MS; they only reflect delivery to the HPLMN of the destination MS. Although, if waiting for a response from the HLR, it will still reflect this in most part.

Also, the "Reply Path" back to the foreign SMS-SC will not be possible i.e. the option of the destination MS to use the SMS-SC of the originating MS in any replies he or she later may send.

Support of Transparent Mode by an SMS Router is mandatory, however, support of Non Transparent Mode is optional.

5.3 New fields

5.3.1 MT-SMS Correlation ID

5.3.1.1 Discussion

The need for correlation of MAP_SRI_For_SM and MAP_MT_Forward_Short_Message is explained in sub-clause 5.2. In order to negate any impacts on the HPLMN of the originating MS, a common field between the MAP_SRI_For_SM and the MAP_Forward_Short_Message needs to be identified in order to transparently (to the HPLMN of the originating MS) convey an MT-SMS Correlation ID in the MAP_SRI_For_SM res/conf that will appear in subsequent MAP_MT_Forward_Short_Message req/ind message(s).

Since the IMSI IE appears in both MAP_SRI_For_SM and MAP_MT_Forward_Short_Message (its value being copied from the former to the latter) it is proposed to use this IE as the carrier of the MT-SMS Correlation ID. However, due to the MCC and MNC part being used for such services as MMS, the MT-SMS Correlation ID shall need to begin with the MCC and MNC of the subscriber.

Since some countries use 3 digit MNCs and other countries use only 2 digit MNCs (and countries are susceptible to change this), it shall be assumed that the Sender ID is always 9 digits. Therefore, the first 6 digits from the left of the IMSI shall be used as the first 6 digits from the left for the MT-SMS Correlation ID. This keeps operator equipment immune to changes in MNC length by the local numbering authority.

5.3.1.2 Definition

Therefore, the MT-SMS Correlation ID shall be composed as shown in figure 5.3.1.2.1.

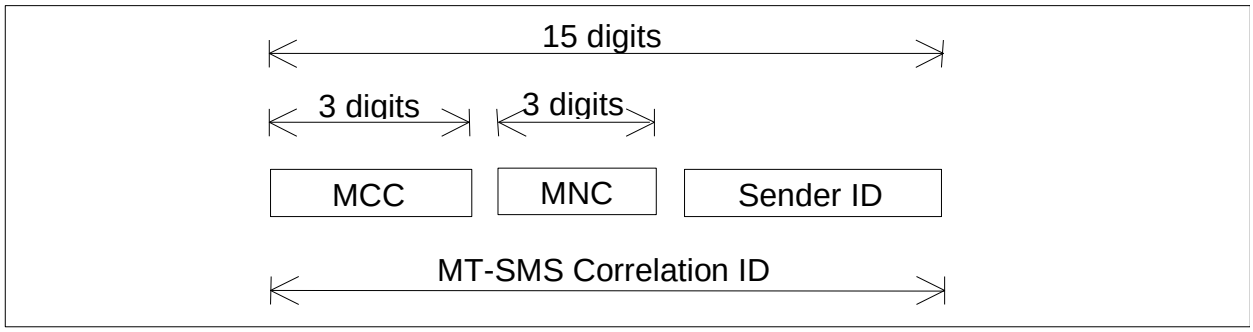

Figure 5.3.1.2.1: Structure of MT-SMS Correlation ID

The MT-SMS Correlation ID is composed of three parts:

1) Mobile Country Code (MCC) of the HPLMN of the receiving MS. It consists of three decimal digits.

2) Mobile Network Code (MNC) of the HPLMN of the receiving MS. It consists of three decimal digits. If the MNC of the HPLMN of the receiving MS is 2 digits only in length, the first digit of the MSIN shall be appended to the right-hand side.

3) Sender ID. This is used to map inbound MAP_MT_Forward_Short_Message messages to a previous MAP_SRI_For_SM operation. It consists of nine decimal digits and shall be unique for its lifetime. For security purposes, its value shall be a number allocated at random, rather than sequentially.

An example of the MT-SMS Correlation ID is:

Sender ID: 569123006

IMSI in use: 234151234567890

Where:

MCC = 234;

MNC = 15;

MSIN = 1234567890,

Which gives the MT-SMS Correlation ID: 234151569123006

5.4 Security enhancements

By using a Correlation ID, this adds to subscriber privacy in that the full IMSI is no longer shared with the HPLMN of the originating MS (for cases when the LMSI is not available). Also, by checking the Correlation ID received in MAP_MT_Forward_Short_Message messages, it can be easily checked from where the associated MAP_SRI_For_SM originated, thus resulting in detection of "fake" and "spoofed" SMs.

5.5 Charging enhancements

By having all SMs go through the HPLMN of the receiving MS, this allows for pre-pay subscribers to receive SMs while roaming outside of the HPLMN without necessarily having to rely on the VPLMN to support CAMEL Phase 4 (which is the only 3GPP solution for pre-pay MT SMS at time of writing). This also means that in VPLMNs that have no CAMEL support at all, a pre-pay subscriber could be allowed to roam in that network and simply be allowed to use SMS only i.e. no CS calls and no GPRS (although, GPRS could also be allowed if using a GGSN in the HPLMN of course).

5.6 Supplementary Services enhancements

With the introduction of the SMS Router there is the possibility to provide Value Added Services e.g. SMS Forwarding. This is FFS.

5.7 Other enhancements

In order to provide the greatest flexibility to their subscribers, operators may benefit from having the option to be able to enable and disable routeing of MT SMs via the HPLMN on a per subscriber basis. Not only would this allow for the option of value added services, it would enable trouble shooting on an individual subscriber basis. This could be realised by extending the subscriber profile in the HLR to include a flag field.

6 Impacts on existing features and functionality

6.1 Introduction

This clause discusses impacts on *existing* network features/services that would arise from the proposed core network enhancements as defined in clause 5.

6.2 MMS

By keeping the MCC and MNC of the IMSI intact in the MAP_SRI_For_SM message returned by the SMS Router to the SMS-GMSC, the MMSC in the HPLMN of the originating MS can still derive a correct FQDN of an MMSC to which to deliver the MM.

Therefore, there are no impacts on MMS.

6.3 SMS delivery reports

SMS delivery reports are affected only in Non-Transparent Mode delivery. The difference is that the originating MS will receive a delivery report when the SM has been delivered to the HPLMN of the receiving MS, instead of when it is actually delivered. This already happens today when interworking SMS with CDMA2000 networks. For privacy reasons, this behaviour may be considered an enhancement as it means that the originating MS can no longer determine whether or not the receiving MS is switched on and/or in coverage. However, it could also change the way an operator is allowed to charge for delivery reports.

6.4 Supplementary Services

There are no impacts on Supplementary Services. The new mechanism is advantageous in that new value added services can be offered.

6.5 Charging

There are no impacts on charging. The new mechanism is advantageous in that operators now have the flexibility to charge on MT SMs destined for pre-pay subscribers who might be roaming in a VPLMN that does not support CAMEL Phase 4 (CAMEL Phase 4 is the only 3GPP defined mechanism for pre-pay MT SMS).

6.6 Concatenated SMs and SMs with UDH

In Transparent Mode, Concatenated SMs are not impacted. However, pre-delivery analysis (e.g. for SPAM protection) in the HPLMN of the receiving MS can only be performed on each SM individually.

In Non-Transparent mode, concatenated SMs are also not impacted. Pre-delivery analysis in the HPLMN of the receiving MS is possible on an oversized SM using this mode.

6.7 Mobile Number Portability

There are no impacts on MNP. The new mechanism is advantageous in that the roaming and/or SMS inter-working partners of the HPLMN of the receiving MS no longer have to have roaming and/or SMS inter-working agreements with all operators of the MNP domain to which the HPLMN of the receiving MS is a member of.

6.8 Lawful Interception

There are no impacts on LI. The new mechanism is advantageous in that the HPLMN of the receiving MS can now more easily provide details to requesting LI authorities of MT SMs.

6.9 MAP

There are no impacts on MAP. The new mechanism allows for the MAP protocol to be used with no changes. However, the SMS Router needs to support the same AC versions for "shortMsgGatewayContext" as the HLR.

Optionally (therefore not a mandatory requirement for the new architectures to be realised), a flag can be added to the MAP_SRI_For_SM ack to denote when the IMSI field contains the MT-SMS Correlation ID and a flag can optionally be added to the MAP_MT_Forward_SM ack when used in the Non-Transparent Mode to denote when the SM has been delivered to the SMS Router (and not necessarily the receiving MS).

6.10 Sub-System Numbers

Existing SSNs can be used by the SMS Router, as opposed to the SMS Router being allocated an SSN of its own. When the SMS Router sources a MAP_SRI_For_SM and a MAP_MT_Forward_SM it shall use an SMS-GMSC SSN. When the SMS Router sources a MAP_SRI_For_SM ack, it shall use an HLR SSN. When the SMS Router sources a MAP_MT_Forward_Short_Message it shall use an MSC SSN or an SGSN SSN.

The practice of re-using SSNs is nothing new and has already been used in CAMEL and also the Presence service, amongst others.

6.11 Setting of MWI in the HLR

The MWI (Messages-Waiting-Indication) information in the HLR of the receiving MS consists of the following fields:

- MWD (Messages-Waiting-Data)
- MNRF (Mobile-station-Not-Reachable-Flag)
- MNRG (Mobile-station-Not-Reachable-for-GPRS)
- MNRR (Mobile-station-Not-Reachable-Reason)
- MCEF (mobile-station-Memory-Capacity-Exceeded-Flag)

All of the above are defined in 3GPP TS 23.040 [4].

The MWD is set using the GT contained in the Service Centre Address parameter of the MAP_Report_SM_Delivery_Status message or the MAP_SRI_For_SM message (if the MS is known in the HLR to be detached – see 3GPP TS 29.002, sub-clause 23.3, process MT_SM_HLR). Where the SMS Router sends such messages to the HLR, it populates the Service Centre Address parameter with the GT of the SMS-SC that is to deliver the message, rather than itself. Therefore, impacts on the setting of this flag are avoided.

The MNRF, MNRG MNRR and MCEF are flags that are set in the HLR when a new address is added to the address list contained in the MWD field. They are populated using the Absent Subscriber Diagnostic SM parameter, and/or the Additional Absent Subscriber Diagnostic SM parameter, from a received MAP_Report_SM_Delivery_Status message or by using information already available in the HLR e.g. when the HLR has previously been informed that the receiving MS is detached. Therefore, the only possible impact on these fields could be from the MAP_Report_SM_Delivery_Status message, but since the SMS Router sends this message only in the Non-Transparent Mode after a delivery attempt failure, it has the same information from the MSC or SGSN where the receiving MS is

currently residing compared to the normal MT SMS procedure. Therefore, there are no impacts on the setting of these flags in the HLR.

7 Conclusion and recommendations

7.1 Summary

There are advantages and disadvantages with both Transparent Mode and Non-Transparent Mode. The following table summarises these (more specific detail can be found in clause 6):

Table 7.1.1: Disadvantages with both Transparent Mode and Non-Transparent Mode

Capability	Existing MT SMS mechanism	Transparent Mode	Non-Transparent Mode
Ability to hide the actual location of the receiving MS (enhanced user privacy)	No	Yes	Yes
Ability to hide the IMSI from the originating PLMN of the SM	No	Yes	Yes
Ability to correlate MAP_SRI_For_SM with subsequent MAP_MT_Forward_SM messages	No	Yes	Yes
Ability to collocate MMSC and SMS-SC/SMS Router on same platform	No	Yes	Yes
Ability to determine when an MT SM has been delivered to the receiving MS	Yes (but possibly "No" when delivering to a non-GSM subscriber)	Yes (but possibly "No" when delivering to a non-GSM subscriber)	No (but able to determine when SM is delivered to HPLMN of the receiving MS, which commonly will also mean delivery to the receiving MS. If the SM was not delivered then the HPLMN is in charge of delivering the SM later on. This implies an impact to the HPLMN SMS-SC)
Ability to hide when an MT SM is delivered to the receiving MS	No	No	Yes
Ability to charge pre-pay subscribers for received MT SMs when roaming outside of the HPLMN, without relying on support of CAMEL Phase 4 in the VPLMN	No	Yes	Yes
Support for local regulatory LI requirements for all MT SMs, including those received by an MS when it is roaming	No (visibility of querying network only i.e. no visibility of the actual message)	Yes	Yes
Pre-delivery analysis (e.g. for SPAM protection) in the HPLMN of the receiving MS for a concatenated SM when roaming outside the HPLMN.	No	Yes (but for concatenated SMs and SMs with UDH, analysis can only be peformed on each SM individually)	Yes
Support of Priority SMs	Yes	Yes	No

7.2 Recommendation

Due to the advantages and disadvantages of each architecture described above, it is recommended to define the Transparent Mode architecture in 3GPP Technical Specifications.

Due to the drawbacks of no support for true delivery reports and no support for handling of SMs with the Priority bit field set, the Non-Transparent Mode as defined in the present document is not recommended.

7.3 Way Forward

It is recommended to 3GPP that the enhancements to the MT SMS functionality are specified in existing specifications, as opposed to creating a new TS. Creating a new TS specifically for the enhanced MT SMS functionality runs the risk of harming inter-working with the existing SMS functionality, of which shall be avoided (according to the Scope of the present document).

The following table lists the existing 3GPP Technical Specifications that will be impacted by the solutions documented in clause 5:

Table 7.3.1: 3GPP TSs impacted by the solutions in clause 5 of the present document

3GPP TS	Responsible WG	Brief summary of impacts
3GPP TS 23.040 [4]	CT1	Architecture and procedural descriptions from clause 5.
3GPP TS 29.002 [5]	CT4	Optional insertion of flags. Signal flow diagrams (not the SDLs) in clause 23 may need to be updated.
3GPP TS 23.003 [8]	CT4	Addition of MT-SMS Correlation ID.

Annex A:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
12-2006	CT#34	CP-060578			V7.0.0 approved in CT#34	2.0.0	7.0.0
01-2007					The associated diagram files added in zip-file.	7.0.0	7.0.1
03-2007	CT#35	CP-070018	0001	1	Adding InformServiceCentre and ReportSM-DeliveryStatus to the transparent mode	7.0.1	7.1.0