SMS SS7 Fraud
3.1
16 February 2005

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

Security Classification Category (see next page)
This is an UNRESTRICTED official document

Security Classification (Unrestricted)

Copyright Information

GSM Association References

- IR.71 SMS SS7 Fraud Prevention
- BA.43 SMS Handbook
- AA.50 SMS Fraud Criteria

Document History

Version	Date	Brief Description
1.0.0	December 15th, 2003	Produced by Matthieu FOUQUET Bouygues Telecom (France) and T-Mobile Group
1.1.0	Mach 29th, 2004	First remarks added.
2.0.0	July, 19th 2004	Rename as IR.71 document
2.1.0	July, 20th 2004	Title modification
2.2.0	July, 20th 2004	Final version for approval
3.0.0	August, 4th 2004	Version approved
3.1	February, 16th 2005	GT Scanning case added
NOTE	11 July 2005	This document has been declassified from RESTRICTED to UNRESTRICTED. This was approved by GSMA/CTO.

Other Information

Item	Description
Document Owner	IREG
Editor / Company	Matthieu Fouquet / Bouygues Telecom
Revision Schedule	Semi-annual
Key words	Fraud

Feedback

This document is designed to help GSMA members in their work. If you find any errors in this document, or wish to suggest changes to this document, please contact (mailto:prd@gsm.org) with your comments.

Executive Summary

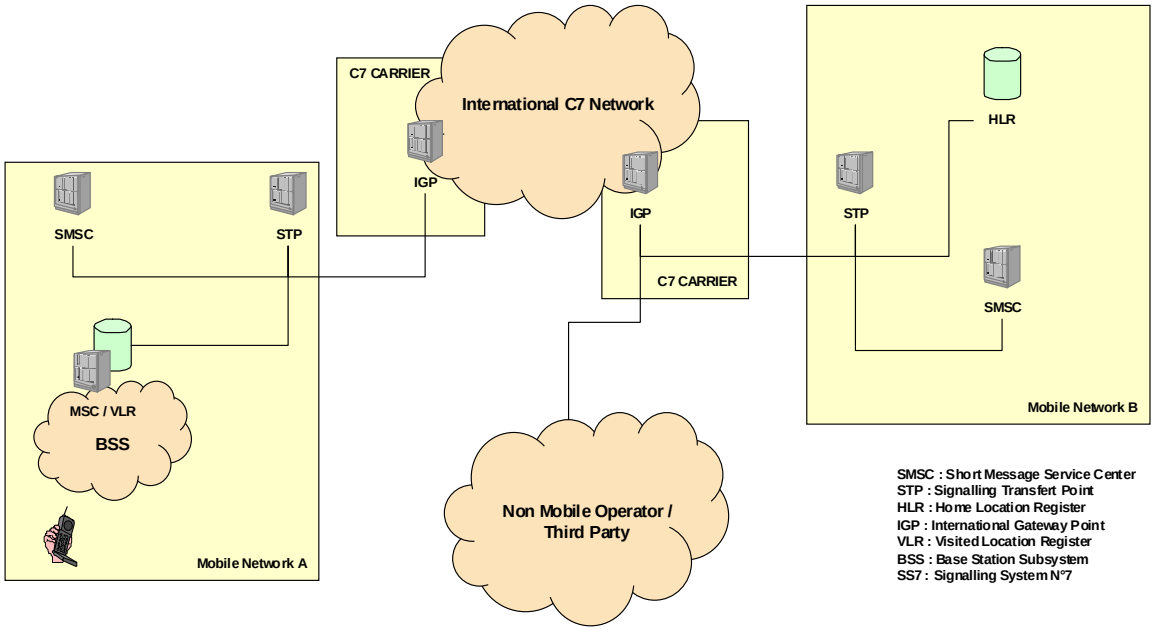
Many Mobile operators are facing with SMS problems (Spamming, Fraud or illegal use of their SMS-C addresses).

The document:

- Defines each SMS Fraud case
- Describes technical aspects for each case

Table of Contents

1 Introduction

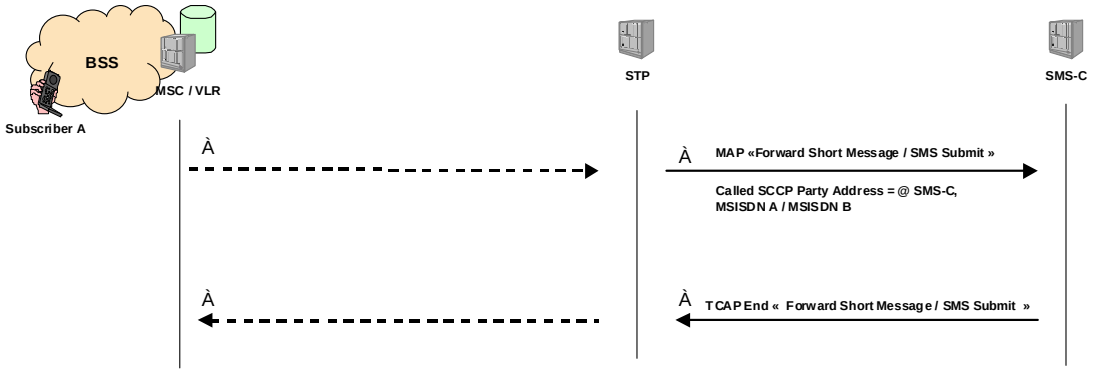


First, you will find in this figure the C7 architecture with all the necessary nodes.

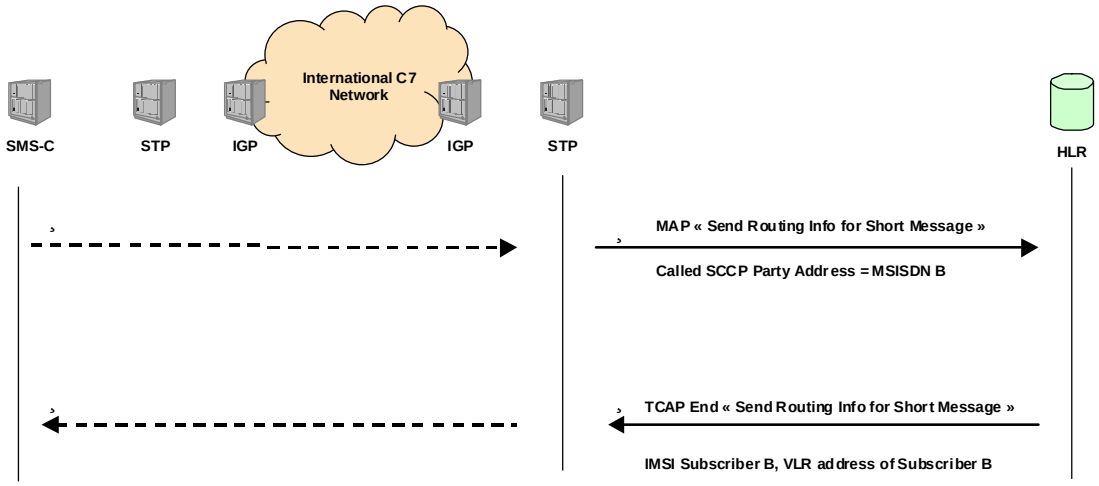
The International Gateway Point (IGP) is the gate to the C7 Network for roaming or SMS interworking services.

Below, the message flow related to the normal SMS sending:

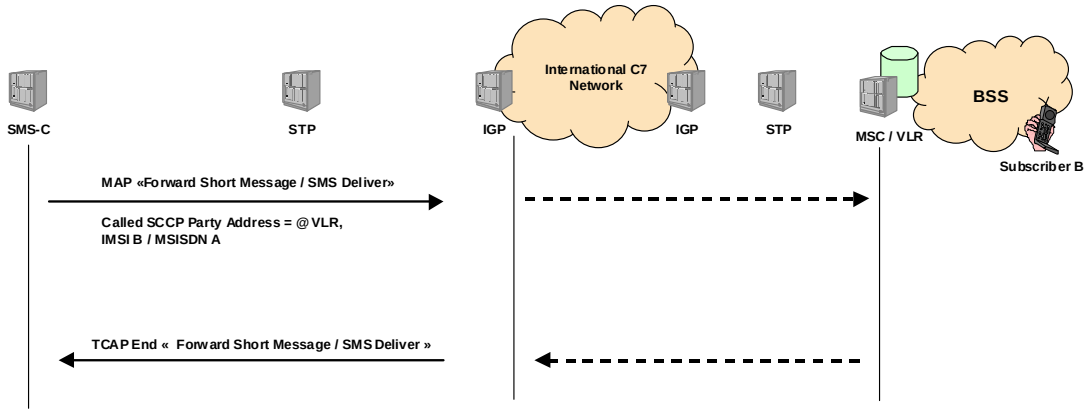
Step one: the mobile sends the SMS to the SMS-C:



Step two: the SMS-C recovers the VLR address and the IMSI of the recipient subscriber:



Step three: the SMS-C sends the SMS to the subscriber B:



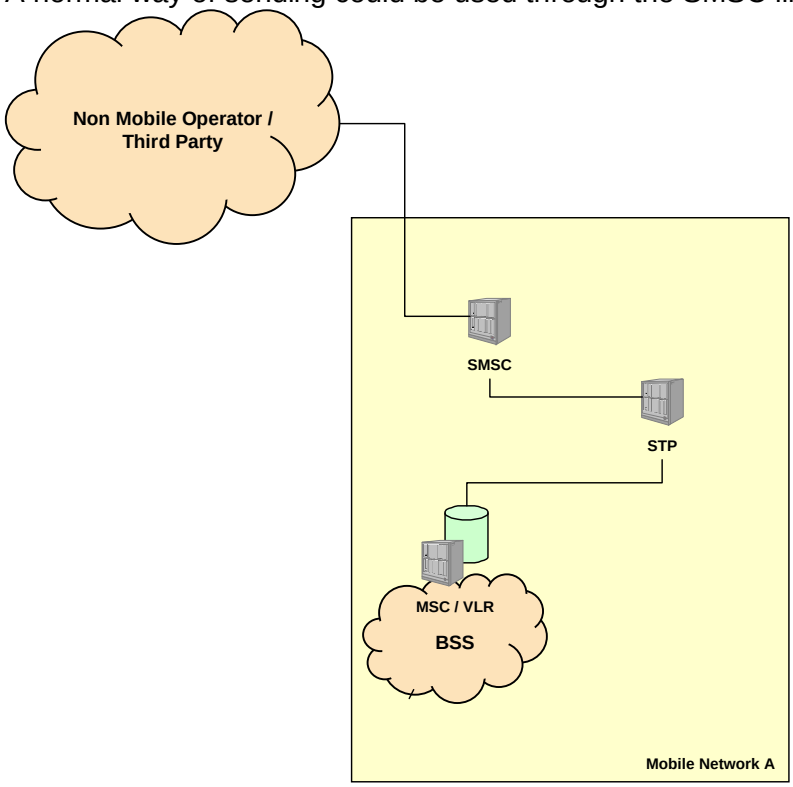
2 Spamming Case

2.1 Definition

Spamming is an action where the subscriber receives an unsolicited SMS. As an unsolicited SMS, the subscriber did not request to receive this message.
The act of spamming does not define the content but only the fact that the SMS was received without solicitation. The content of the spam SMS is incidental to the act. The spam SMS may take on various forms of content to include: commercial information, bogus contest and other message generally intended to invite a response from the receiver.

It is important to note that the SMS could be sent from a valid originator and may be correctly billed to the sender.
Technical Aspect
In the Spamming case, there are no specific technical aspects. The spamming Originator could be a single person, a commercial company or a mobile operator.

A normal way of sending could be used through the SMSC like described below:



The SMS is submitted by a mobile phone or by a third party connected to the SMS-C (Content provider for example).

3 Flooding case

3.1 Definition

The act of flooding is when a large number of messages are sent to one or more destinations. These messages may be either valid or invalid. The value or parameter used to define flooding is the extraordinary number of messages sent.

The flooding parameter is compared to the average or normally expected load, and the expected peak value of a selected message flow. When the parameter is unusually high, without other explanation, then this is considered 'flooding'.

3.2 Technical Aspect

The sending of the messages in a case of 'flooding' is within the normal methods of sending messages. Consequently, there is no specific technical aspect for this case.

4 Faking Case

4.1 Definition

A fake SMS is originated from the international C7 Network and is terminated to a mobile network. This is a specific case when SCCP or MAP addresses are manipulated. The SCCP or MAP originator (for example: SMSC Global Title, or A_MSISDN) is wrong or is taken from a valid originator.

4.2 Technical Aspect

In general, a SM-SC is used to send mobile terminated SMs to a PLMN user but in a manner that hides the true identity of the source SM-SC. Typically, this is done by substituting a valid address with another PLMN address. When the faking case technique is used in conjunction with spam content, the complaints are then sent to the incorrect, that is, the innocent PLMN. Furthermore, any protective escalation actions by the receiving PLMN, such as suspension of MT-SMS service from the apparent-source PLMN are both ineffective and damaging to proper users of SMS between the two PLMNs.

An example of commercial model for Spammers using the “Faking Case” for PRS (Premium rate service) fraud is described below:

The spammer leases Premium rate lines ’0906‘from a fixed-line carrier in the country of PLMN ‘A’. The spammer arranges for an overseas SM-SC to send messages to customers of PLMN ‘A’ that read like: “*This is the 2nd attempt to contact U. You have won this week’s top prize of either 1000 cash or a holiday in Bahamas. Just call 0906xxxxx TcsBox6017 1.50ppm*”.

PLMN “A” customers call the number but discover after some expensive minutes that there is no prize. The spammer collects the premium rate revenue from PLMN “A”, pays off the access charges to the fixed line carrier and disappears with the profit.

Subsequently the mobile customers complain to their network operator or mobile service provider, in this case PLMN “A”. PLMN “A” raises the issue with the Regulatory Authority, but the fraudster has disappeared. PLMN “A” contacts the source of the SMs (owner of the SM-SC), who denies any knowledge of the SMS-Spam messages.

The delivery of a Mobile Terminated SM is in two parts:

1. The SM-SC uses the destination MSISDN to address a MAP message <Send Routing Information for Short Message>, to the Home Location Register (HLR) for that customer to find out whether the MSISDN is valid, can receive SMs, and if so, to determine the current switch (MSC) that the destination user is registered on. The HLR responds to the SM-SC with the information.

2. The SMSC sends the actual text of the SM to the currently registered MSC and a MAP message <Forward Short Message>. The MSC responds to confirm the message was delivered, and generates a CDR containing all relevant information including the SM-SC address.

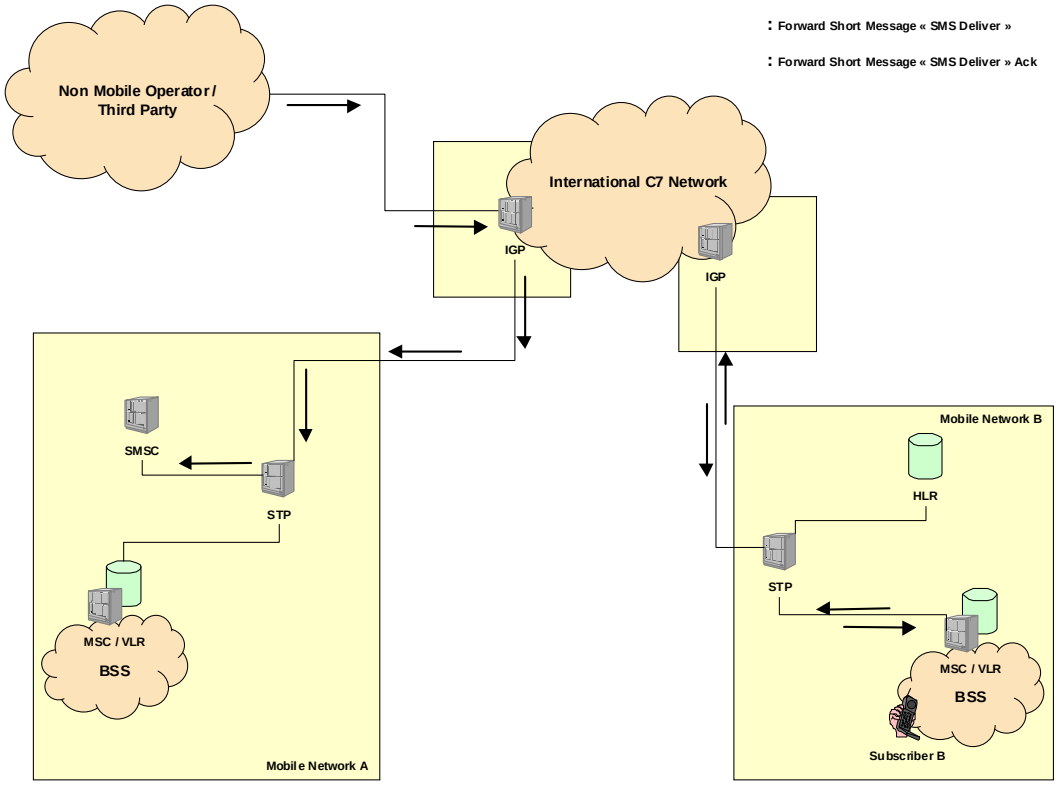
In the faking case, the first part is done exactly as described above. However, the second part is changed so that the source address in the MAP message <Forward Short Message> is changed, often to someone else’s SM-SC address. The manipulation of the SM-SC address causes any inter-PLMN SM accounting to be in error, and means that any policing against the apparent Spam generator harms innocent parties and is ineffective against the real Spam generator.

The faking of the source address in the SCCP called party Global Title and the Service Centre Address in the MAP message <Forward Short Message> whilst having the correct equivalent address in the MAP message <Send Routing Information for Short Message> is impossible without considerable efforts by the technical staff running the SM-SC. In other words, it does not happen either by accident, faulty configuration data or as the result of raw text messages received from the Internet. It happens because in most cases it requires a software patch on the SM-SC. Therefore; any instances of this happening are as the result of direct action by SM-SC staff, and probably in conjunction with assistance from the staff of the Associated PLMN.

Consequently, it is fair to state that the “Faking Case” can only be caused by deliberate activities by a Spam-generating PLMN, a Spam-sponsoring PLMN, or a Spam-generating SM-SC operator acting in conspiracy with a PLMN.

The figure below describes the example of a third party using the real SMSC address from another mobile network. The SMS is sent to a real subscriber of mobile network B (The originator must have the correct IMSI) or could be sent to a wrong IMSI (Just to generate C7 Overload).

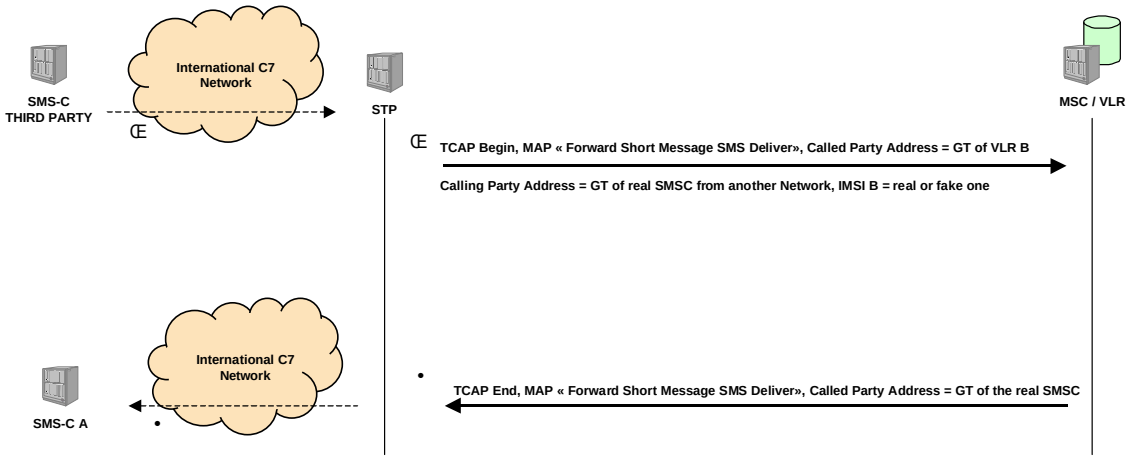
The IMSI can be recovered by detecting the “Send Routing Information for Short Message". In this case, the third party must use their own real SCCP / MAP SMSC address.



The third party could send the SMS to all VLRs of mobile network B if he cannot recover the location of the subscriber (SRI for SM blocked by Mobile Network B).

The A_MSISDN could be wrong or manipulated.

Below displays the transaction flow, for the SMS delivery:



The acknowledgement is sent to the real SMSC.
Billing Impact associated with Faking
If MSISDN B is roaming, when the message is delivered, and if, the visited network has a charging agreement in place with MSISDN B's HPLMN. In this scenario, faking would impact inter-operator accounting (or would at least give rise to discrepancies in the number of messages the HPLMN and VPLMN believe were sent from one to another).

If MSISDN B is on its own, HPLMN when it receives the message, if this HPLMN has an SMS inter-working agreement with the network whose SMSC is faked then once again there could be inter-operator accounting issues.

5 Spoofing Case

5.1 Definition

The spoofing case is related to an illegal use of the HPLMN SMS-C by a third party.

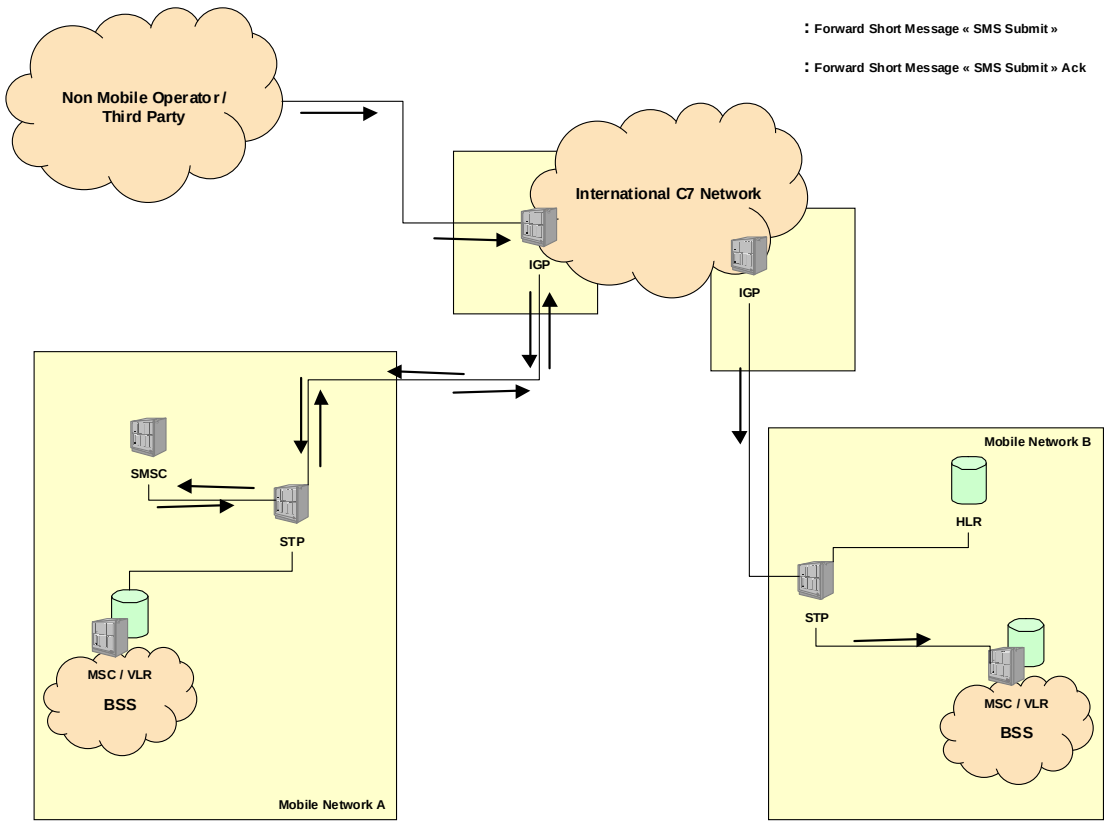
In this case, a SMS MO with a manipulated A-MSISDN (real or wrong) is coming into the HPLMN network from a foreign VLR (real or wrong SCCP Address).

5.2 Technical Aspect

To a HPLMN point of view, one subscriber is roaming and sending a SMS. In fact, this is not a real subscriber; the message is not sent by a real mobile but is generated from a specific system with a C7 application.

The A-MSISDN being used may in fact be real or not depending on the screening in place in the HPLMN SMS-C (Screening on CC+NDC or No A-MSISDN screening in place).

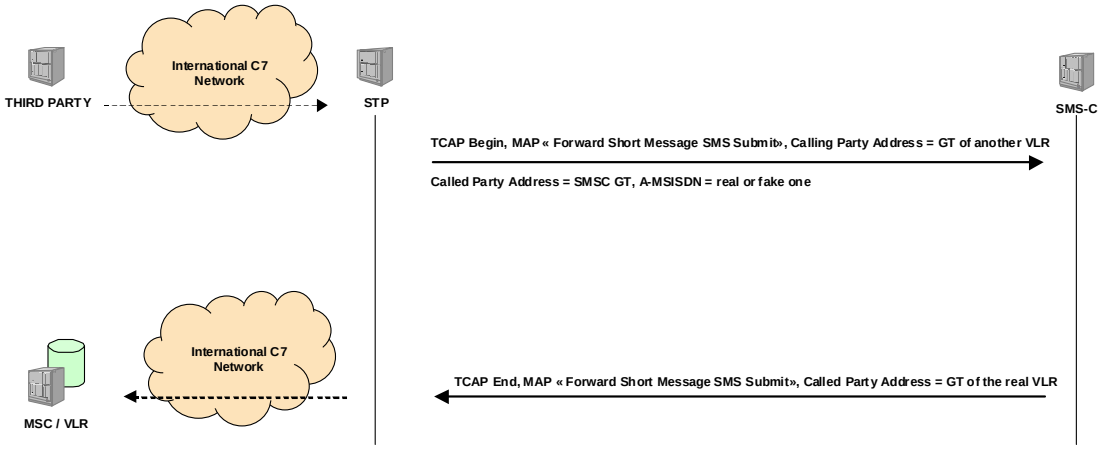
The figure below describes the case with a real A-MSISDN and real VLR SCCP address from another Mobile Network.



The Map message "Forward Short Message / SMS Submit acknowledge" is sent to the real VLR.

If the billing is made from the SMS-C data, the real subscriber will be invoiced. If the Billing is made from the TAP file, no one will be invoiced.

Below the message flow for the SMS Delivery:


THIRD PARTY
International C7 Network
STP
SMS-C
TCAP Begin, MAP « Forward Short Message SMS Submit», Calling Party Address = GT of another VLR
Called Party Address = SMSC GT, A-MSISDN = real or fake one
MSC / VLR
International C7 Network
TCAP End, MAP « Forward Short Message SMS Submit», Called Party Address = GT of the real VLR

6 GT Scanning

6.1 Definition

The GT scanning is the fact to send SMS MO to all Global Title address from one mobile operator in order to find unsecured SMS-C (SMS-C that are not controlling the A number).

6.2 Technical aspect

Multiple SMS Forward SM Submits are received, generally, from the same mobile MSISDN with the Called SCCP Address and Service Centre Address incremented on each attempt.

It would appear that individuals using a mobile with a computer connection are instigating these scans.

The easiest of these scans to spot are sequential in nature scanning 10,000 GT at a time. It has also been seen randomised scans, though on sorting the data it is clear that blocks are being scanned.

This type of messaging is picked up in normal statistics in monitoring expected and unexpected combinations of direction, GT and message type.

There can be no valid reason for such scanning of networks other than locating unsecured SMSC. With simpler computer integration with mobiles and SMS emulation software readily available this type of activity is likely only to increase. It would be desirable for such activities to be reported to the Home PLMN of the originating MSISDN in order to have service removed.

Appendix A: Abbreviations

Term	Definition
MAP	Mobile Application Part
SMS	Short Message Service
SMS-C	SMS Centre
VPLMN	Visited PLMN
C7	SS7
SS7	Signalling System N° 7
STP	Signalling Transfer Point
HLR	Home Location Register
IGP	International Gateway Point
VLR	Visitor Location Register
BSS	Base Station Subsystem
SCCP	Signalling Connection Control Part
GT	Global Title
MSU	Message Signalling Unit
IMSI	International Mobile Subscriber Identity
TCAP	Transaction Capabilities Application Part
MSISDN	Mobile Subscriber ISDN