SMS SS7 Fraud Prevention
Version 6.1
May 2024

Security Classification: Confidential - Full, Rapporteur, Associate and Affiliate Members

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

.

Table of Contents

1 Introduction

1.1 Executive Summary

This document defines methods for operators to identify SMS (Short Message Service) SS7 (Signalling System N° 7) attacks on their networks and to make recommendations for both individual operators and the GSM Industry who may require to contain these issues short term.

- Section 2 will define the rules in order to identify SMS attacks based on traffic monitoring
- Section 3 will define solutions in order to prevent SMS attacks

Implementation within a three-month-time period is considered as Short Term Containment.

NOTE: GSMA PRD IR.70 SMS SS7 Fraud must be read before this document. GSMA PRD IR.70 SMS SS7 Fraud contains all SMS Fraud scenarios and technical definitions. Fraud and Security procedures could be found in BA.20 [2].

1.2 Technical Explanation

Technical descriptions and definitions could be found in the GSMA PRD IR.70 SMS SS7 Fraud White Paper.

1.3 Definition of Terms

Term	Description
BSS	Base Station Subsystem
C7	SS7
DOS	Denial of Service
ENUM	E.164 NUmber Mapping (or tElephone NUmber Mapping)
GT	Global Title
HLR	Home Location Register
IGP	International Gateway Point
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
MMS	Multimedia Messaging Service
MSC	Mobil Switching Centre
MSISDN	Mobile Subscriber ISDN
MSU	Message Signalling Unit
MWI	Message Waiting Indicator
PRD	Permanent Reference Document
PRS	Premium Rate Services

SCCP	Signalling Connection Control Part
SMS	Short Message Service
SMS-C	Short Message Service Centre
SSN	Sub System Numbers
SS7	Signalling System N° 7
STP	Signalling Transfer Point
TCAP	Transaction Capabilities Application Part
UDT	Unit Data message
UDTS	Unit Data Service
VLR	Visitor Location Register
VPMN	Visited PMN

1.4 Document Cross-References

Ref	Document Number	Title
1	IR.70	SMS SS7 Fraud
2	BA.20	Fraud & Security Procedures
Void		
4	3GPP TS 23.040	Technical realization of the Short Message Service (SMS)
5	AA.19	Addendum to the International Roaming Agreement SMS Interworking Agreement v15.1
6	IR.82	SS7 Security Network Implementation Guidelines

2 Identifying SMS attack

2.1 Faking Case

2.1.1 SCCP Own Address / MAP Own Address Measuring [1.1.1 Own Address Criteria]

Operators should measure, the number of SMSs received with a SCCP Calling party address or SC OA Address (incoming international Signalling System SS7 traffic, also known as N° 7 Traffic), which are the Operator's own source address. These types of messages only occur in a Mobile number portability scenario. Just one received message with its own address can indicate fraud (SMS fake).

This measurement could be made using:

- A counter and statistic tables in the Mobile Switching Centre/Visitor Location Register (MSC/VLR) or in a Signalling Transfer Point or STPs (On interconnection links)
- The toll ticketing system
- A specific SS7 supervision based on C7 (SS7) probes

All these solutions are already available for the majority of manufacturers.

2.1.2 Incorrect Operator Link Set Detection [1.1.2 Incorrect Operator Link Criteria]

This case is only relevant with multiple international connections between different SS7 Carriers.

Operators should check the incoming SS7 messages from all partners on the interconnection links. If a message is received on an unexpected interconnection from a particular partner there is a possibility of fraud (Except for rerouting due to outage or a specific event).

This measurement could be made using:

- A counter and statistic tables in STPs (On interconnection links)
- A specific SS7 supervision based on C7 probes

All these solutions are already available for the majority of manufacturers.

2.1.3 Measuring the number of Unexpected 'End' Messages [1.1.3 Unexpected 'End Message Criteria]

Operators should measure the number of TCAP End messages (Transaction Capabilities Application Part End messages) received for transactions not being originated by the Operator. The number of unexpected 'End' messages should be analysed for a specific period and per Roaming or SMS Interworking partners.

This measurement could be made using:

- A counter and statistic tables in SMSCs
- A specific SS7 supervision based on C7 probes (on STPs or SMSCs links)

All these solutions are already available for the majority of manufacturers.

2.1.4 Measuring the Load Traffic for a Specific Period [1.1.4 Abnormal Load Criteria]

Operators should measure the number of SMSs received from each SMS-C or SMS Centre, for a specific period of time. If the number of SMS received from a specific SMS-C is abnormal for that period, there may be a problem. The problem could be related to a special event (New Year’s Eve, for example) or be due to a faking case. A third party could have used this SMS-C address.

This measurement could be made using:

- A counter and statistic tables in MSC/VLRs
- A specific SS7 supervision based on C7 probes (on MSC/VLRs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.1.5 UDTS message Measurement [1.1.5 No Address Found Criteria]

a) UDTS "No Translation for this specific address" Measurement:
Operators should measure the number of UDTS generated with the cause value "No translation for this specific address" for each SMS-C addresses that sends a Forward Short Message.
An abnormal level of these UDTS could indicate that a SMS-C is sending a number of SMSs randomly for a range of MSC/VLR Global Titles (Because the third party doesn't really know the real addresses).

b) UDTS "Unequipped User"
Operators should measure the number of UDTS generated with the cause value "Unequipped User" for each SMSC-C addresses that generates a Forward Short Message.
An abnormal level these UDTS could indicate that the SMS-C is sending a number of SMSs with incorrect SSNs (Sub System Numbers).
This measurement could be made using:

- A counter and statistic tables in MSC/VLRs or STPs
- A specific SS7 supervision based on C7 probes (on MSC/VLRs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.1.6 Compare MAP and SCCP addresses [1.1.6 MAP Only Fake Criteria]

The MAP SMSC address should be compared to the SCCP address. There should be no difference (Global Title, GT range of sending network). This comparison can only be made manually at this time.

Another method is to analyse for each SCCP and MAP addresses the number of Forward Short Messages received. If there are discrepancies between SCCP and the MAP SMS-C addresses, there could be a faking problem.

This measurement could be made using:

- A counter and statistic tables in MSC/VLRs or STPs
- A specific SS7 supervision based on C7 probes (on MSC/VLRs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.1.7 Measuring the format of originating address of MAP [1.1.6c MAP Only Fake Criteria]

The MAP originating address should be checked to see whether it is in short code format (premium short code).

Operators should check to see if they receive SPAM traffic with premium short codes in their MAP originating address from abroad. They could check the most used short codes format or the complete range of premium short codes available in their network.

Companies with premium services, could terminate SPAM via foreign SMSC’s to their own mobile customers. Moreover the fraud case can be mixed with SMS Fake.

Measurement could be conducted by using the following:

- A log file or specific traces in MSC/VLRs or STPs
- A specific SS7 supervision based on C7 probes (on MSC/VLRs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.1.8 Measuring the number of illegal message content [1.1.7 Illegal Message Contents Criteria]

Operators should also measure the number of messages containing illegal or illogical addresses or parameters (For example, Service Centre Address equals to 111111)

This measurement could be made using:

- A log file or specific traces in MSC/VLRs or STPs
- A specific SS7 supervision based on C7 probes (on MSC/VLRs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.1.9 Measuring the number of "unidentified Subscriber" and “unknown Subscriber” Cause Value messages [1.1.8 MAP error 'unidentified subscriber' Criteria]

When an SMS is sent to the MSC/VLR and if the subscriber is not located in this area, the MSC/VLR will answer with an "Unidentified Subscriber" message. An abnormal level of "Unidentified subscriber" could indicate that the SMS-C forwards the SMS without the subscriber’s location.

When a “SPAM attack” is done to a range of Mobile Subscriber ISDNS or MSISDN, and whether the MSISDNs are valid or not is irrelevant, the Home Location Register, HLR, will answer by an “Unknown Subscriber” message. An abnormal level of “Unknown Subscriber” messages, could indicate a SPAM attack (or faked SPAM).

This measurement could be made using:

- A counter and statistic tables in MSC/VLRs
- A specific SS7 supervision based on C7 probes (on MSC/VLRs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.1.10 Measuring per Agreement [1.2.1 Invoice Validation Criteria]

Operators should compare between the total number of outgoing international SMSs and the incoming total number of International SMSs from each PLMN with a Roaming agreement. The difference is usually close in quantity unless one PLMN is generating Bulk SMS traffic. If this number is widely unbalanced, the suspect source should be notified and asked to resolve it.

This measurement could be made using:

- Counter and statistic tables in MSC/VLRs
- A specific SS7 supervision based on C7 probes (on MSC/VLRs or STPs links)
- Billing system information

All these solutions are already available for the majority of manufacturers.

2.1.11 Identification of the SMS Faking Perpetrator

The perpetrator (source) of SMS faking can be identified for all faking scenarios using the “SCCP calling address” of the SRI_for_SM (BEG) message.

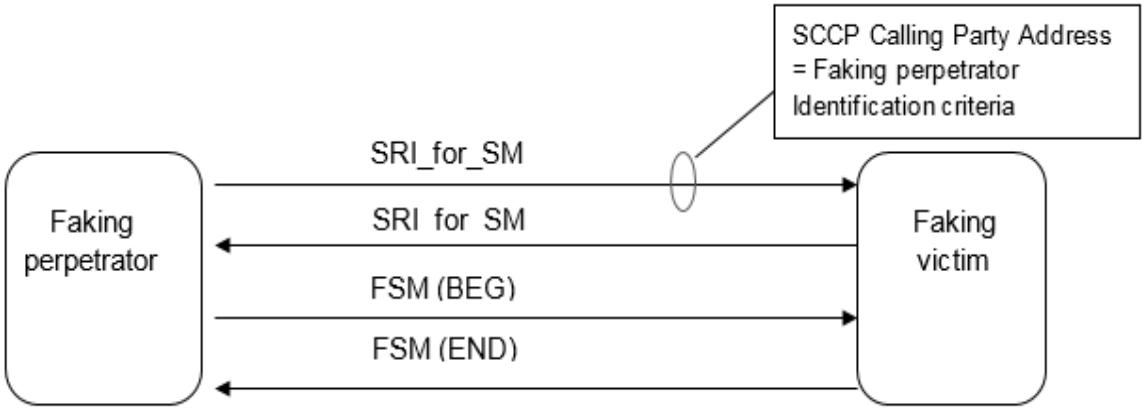

Figure 1: Identification of the SMS Faking Perpetrator

2.1.12 Measuring the number of "SRI_For SM" Messages

Operators should measure the number of SRI_For_SM messages received from each SMS-C address (or from each network based on CC + NDC GT address).

Abnormal quantities could indicate that a Spam attack is happening. Furthermore an abnormal number of MAP <Send Routing Information for Short Message> without the matching number of SMs detected (see section 3.2.2) indicates a “Faking Case”.

This measurement could be made using:

- A counter and statistic tables in MSC/VLRs or STPs
- A specific SS7 supervision based on C7 probes (on MSC/VLRs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.1.13 Compare SRI_For_SM and Forward Short Message Procedures

The MAP message SRI_For_SM should not be used without the associated MAP "Forward Short Message".

Operators should compare the number of SRI_For_SM received with the number of Forward Short Message received from each SMS-C address (or network). The Ratio should not exceed of 2.5 (2.5 more SRI_For_SM than FSM Deliver messages per SMS-C).

If the difference between Forward Short Message and SRI_For_SM shows an abnormal low level of Forward Short Message, this could indicates a “faking network”.

If the difference between Forward Short Message and SRI_For_SM shows an abnormal low level of SRI_For_SM, this could indicate a “faked network (pretended network)”.

Please note that SRI_For_SM message could also be used for other routing purposes not related to SMS (MMS, ENUM proxy for IMS interconnection) and in this case the ratio will be affected. Such a mechanism should not be activated without the HPLMN agreement.

This measurement could be made using:

- Counters and statistic tables in MSC/VLR/HLRs or STPs
- A specific SS7 supervision based on C7 probes (on MSC/VLR/HLRs or STPs links)

2.2 Spoofing Case

2.2.1 Invalid MSISDN Calling Number [2.1.1 MSISDN Criteria]

Operators should measure the number of invalid MSISDNs that submit a SMS to the SMS-C for a specific period of time. If a screening is in the SMS-C, the reject causes (For example "System Failure") should be measured. If there is no screening, the number of request with an invalid calling MSISDN must be measured.

An abnormal number of requests or reject causes indicates that there is a spoofing attack.

This measurement could be made using:

- A counter and statistic tables in SMS'C or STPs
- A specific SS7 supervision based on C7 probes (on SMSCs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.2.2 SMS MO traffic Measurement

Operators should measure the number of SMS submitted from their subscribers abroad as per their Roaming partners. An abnormal load of traffic could indicate a spoofing problem as long as this is not related to a special event (for example New Year’s Eve).

This measurement could be made using:

- A counter and statistic tables in SMS'C or STPs
- A specific SS7 supervision based on C7 probes (on SMSCs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.2.3 Compare Location updating messages with the number of SMS Submitted [2.1.3 Unusual Traffic Pattern Criteria]

Operators should compare the Number of Location Updating messages received with the number of SMS Submitted from their subscribers abroad as well as from their Roaming partners.

- LocUp (outbound) /SMSMO
- > [0,5] normal
- <= [0,5]

Please note that the [0,5] ratio could be different for each network. Each network should define its ratio.

This measurement could be made using:

- A counter and statistic tables in SMS'C or STPs
- A specific SS7 supervision based on C7 probes (on SMSCs or STPs links)

All these solutions are already available for the majority of manufacturers.

2.3 Denial of service attack

2.3.1 Malicious use of the MAP-REPORT-SM-DELIVERY-STATUS Message

This section describes how the abnormal use of the MAP-REPORT-SM-DELIVERY-STATUS Message can be used to achieve a MT-SMS Denial of Service (DOS) attack on a specific customer.

3GPP TS 23.040 “Technical realization of the Short Message Service (SMS)” specifies a Message Waiting function that provides HLR, VLR and SGSN with information that an SM should be delivering to a specific subscriber.

The purpose of this function is to enable quick delivery of a SMS to a MS when becomes available for the delivery of MT-SM. This function is used once the prior delivery has failed due to temporary absence.

The Message Waiting Indication (MWI) is updated differently in both the HLR and VLR.

In the VLR, the MWI is updated when SMS delivery fails via local MSC (SET MNRF (MS-Not-Reachable-Flag)) and the MNRF flag is cleared once it is detected that the particular MS is reachable again (for example, responds to page or MS indicates that memory has been restored).

Once the MNRF is cleared in the VLR, the VLR will inform the HLR about it sending a MAP-READY-FOR-SM message. This enables SMS delivery to be resumed quickly after absence.

In the HLR, the MWI is set only by information from the SMSC using the MAP-REPORT-SM-DELIVERY-STATUS message.

The MWI (MNRF flag) can be cleared either by the SMSC message informing that the SMS delivery was successful (MAP-REPORT-SM-DELIVERY-STATUS message) or the HLR can interpret other messages as an indication that the subscriber became available again, for example, clearing the MNRF flag if the HLR receives MAP-UPDATE-LOCATION.

While MWI is set in the HLR, the HLR will respond to any non-priority MAP-SEND-ROUTING-INFO-FOR-SM messages with MAP-INFORM-SERVICE-CENTRE, informing the requesting SMSC that the MS for that particular MSISDN stored in the Message Waiting Data file of the HLR is not yet available for MT-SMS.

Consequently if a MAP-REPORT-SM-DELIVERY-STATUS message is received while unsolicited and sent without any prior failed SMS delivery attempt, is not in accordance with

SMS protocols. The impact will be that the targeted customer is set in an abnormal MW state which makes it unable to receive normal SMs. As can be derived from the above description, the MWI flags in the MSC (SGSN) and HLR are out-of-synchronisation

The flag de-synchronisation state is not automatically recoverable. There are no simple actions that a customer can take to restore the service. While the subscribers do not change MSC/VLR or receive any priority SMS (where the sending SMSC clears the MWI-MNRF via MAP-REPORT-SM-DELIVERY-STATUS messages), they are not able to receive any non-priority SMs. (In some circumstances a customer can attempt to manually select a competitor network, and this will result in the flags clearing, even if the manual registration attempt fails.)

In normal network operation, and unless specific SS7-MAP-Operational-Measurement “traps” have been set, the abnormal use of the MAP-REPORT-SM-DELIVERY-STATUS message would only be noted if end user complaints.

2.4 Open SMS-C case

2.4.1 Monitoring the MAP MT-Forward-SM on the international SS7 connection

Operators usually monitor the SS7 messages received on the international SS7 connections with their carriers. They can further analyse the MAP MT-Forward-SM messages received on the interface of the external SS7 networks. The monitoring system can analyse the following parameter of the MAP MT-Forward-SM messages (Deliver-SM):

- TP-Originating-Address: Address of the originating Short Message Entity i.e. the number of the subscriber who sent the SMS to the open SMS-C.

If the address number range belongs to the HPMN then this indicates the use of an Open SMS-C.

2.4.2 Monitoring the TAP-IN SMS records

Operators can also control the content of the TAP-IN records. They can look at the following parameter:

- Called Number: In the case of SMS MO usage, the called number item contains the SMSC address.

If the Called Number is different than the HPMN SMS-C address then it indicates the use of an Open SMS-C.

2.4.3 Monitoring Near Real Time Roaming Data Exchange records

Operators can control the content of the NRTRDE records. They can look at the following parameter:

- Connected Number: In the case of SMS MO usage, the connected number item contains the SMSC address.

If the Connected Number is different than the HPMN SMS-C address then it indicates the use of an Open SMS-C.

3 Solution for the prevention

3.1 Control of C7 Network Access

The GSMA requests to apply C7 carrier polices for all SCCP addresses used for every C7 direct link within their normal service package.

On every C7 direct access links, a screening could block all Message Signalling Units, MSUs with a SCCP Calling address different than the operator's SCCP addresses.

The C7 Carrier should not forward any message sent with the wrong SCCP calling address. The C7 Carrier may take other actions if necessary.

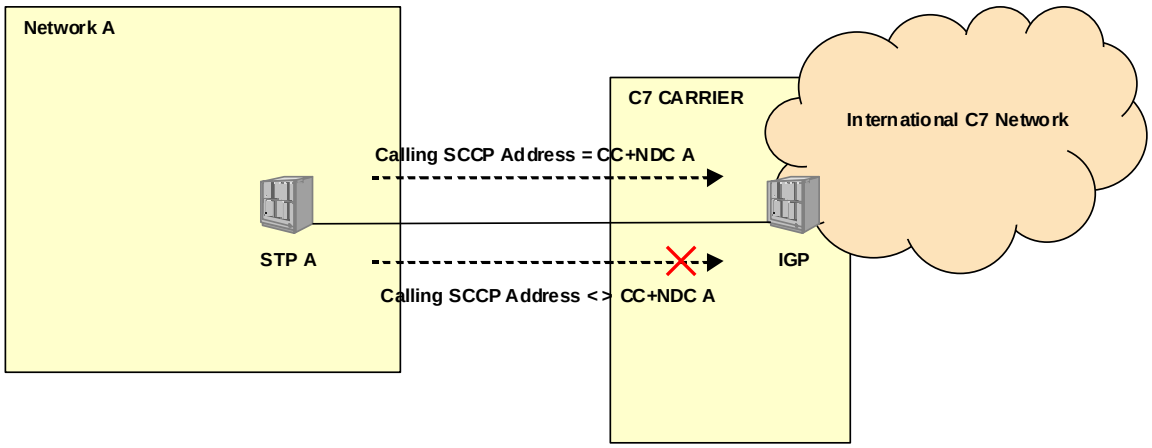

Figure 2: C7 Carrier Actions (allow and block)

3.2 SCCP / MAP Policing on GSM Network

Every GSM operators must implement SCCP and MAP screening tools in their own network nodes (MSC/VLRs, STPs and HLRs)

3.2.1 SRI For SM

On HLRs, a screening based on Calling SCCP Global Title for the MAP Message SRI For SM should be activated. The HLRs will reject the entire SRI For SM request, in case it is not sent from an implemented SMS-C Global Title.

The allowed SMS-C Global Title is implemented every time a GSMA AA.19 agreement is signed.

This type of screening is already available for most manufacturers.

3.2.2 Forward Short Message

On every MSC/VLR, a screening based on Calling SCCP Global Title for the MAP Forward Short Message should be activated. The MSC/VLRs will reject the entire MAP Forward Short Message request in case it is not sent from a defined SMS-C Global Title.

The Allowed SMS-C Global Title is defined every time an GSMA AA.19 Agreement is signed.

This type of screening is available for most manufacturers.

3.3 SMS Home Routing

In order to prevent the SMS faking case, “SMS Home Routing” feature will force the SMS to be routed back to the Home Network. This mechanism will guarantee the calling SCCP address in the ForwardSM message by correlating with the calling SCCP address received in the SendRoutingInfoforSM.

SendRoutingInfoforSM (SRI_SM) response will be secured by

- Anonymising the IMSI (still using the correct MCC/MNC for MNP issue)
- Providing Home as the VLR location in order to protect customer location
- Hiding the HLR GT by using the SMS Home Routing/Firewall GT in the SRI-SM_Response calling SCCP address.

3.4 Check SMS MO to prevent spoofing

3.4.1 Check the Calling MSISDN for SMS MO

In order to avoid the spoofing case, a control access based on the MSISDN must should be activated on the SMS-C. All SMS MO with a MSISDN different than the operator own MSISDN range should be rejected.

This type of screening is available for most manufacturers.

The International Mobile Subscriber Identity, IMSI of the subscriber must also be checked through the use of MAP version 3 or by sending a SRI For SM to the HLR in order to recover the IMSI.

This type of mechanism is already available for some manufacturers.

3.4.2 Comparison between VLR location and stored MSC address

In addition of the IMSI check for the SMS MO request, a comparison between the VLR location and the calling SCCP address (MSC/VLR where the subscriber should be located) is also done.

If the Location stored in the HLR is different than the SCCP calling address from which the SM MO is coming, the SM MO will be rejected.

Please note that some networks could have different SCCP Addresses for the VLR and the MSC (the majority of operators, have the same SCCP address for both the MSC and the VLR). If the SCCP addresses (VLR and MSC) are different, a check is possible with a GT proxy filter function.

This mechanism could use the SRI For SM to recover the VLR address stored in the HLR. In this case, the C7 signalling load will increase.

3.5 Control of Denial of Service Attacks

Control of Denial of Service (DoS) attacks used by SS7 is generally only possible by blocking the SCCP Global Title of the Originator. However in the absence of TCAPsec, many SS7 DoS attacks do not need the originating address to be genuine because no response is needed. Hence it may be necessary to work with the international carriers to trace back the routing of the incoming SS7 message to establish the real source country/network.

3.6 Blocking for open-SMSC

3.6.1 Implementing SMS Barring of Outgoing International Calls except those directed to the Home Country (BOICexHC)

Operators are recommended to provision the BOICexHC supplementary service to their subscribers for the SM Service.

Operators are also recommended to support the BOICexHC supplementary service in the MSC and in the SGSN in case SMS over GPRS is supported.

BOICexHC supplementary service ensures that any subscriber roaming into a visited country can only send SMS Mobile Originating to a SMS-C in its home country or to a SMS-C in the visited country.

With the BOICexHC supplementary service, operators protect themselves against the risk of fraud due to Open SMS-Cs but for scenario 1 only, in which the SMS-C is located outside the visited country.

BOICexHC supplementary service does not protect against the Open SMS-C scenario 2 in which the SMS-C is located in the visited country. For that scenario, other protection measures need to be implemented.

3.6.2 Implementing filtering of SS7 messages

If an operator acknowledges any Open SMS-Cs located in its own country it is recommended to implement a filter of all SS7 messages sent to the Called Party Addresses of the Open SMS-Cs.

The filter can be implemented directly at the MSC or at the SGSN if SMS over GPRS is supported. Alternatively, it can be implemented at the Signalling Transfer Point or at the SCCP Gateways.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0.0	June 2004	Produced by Matthieu FOUQUET Bouygues Telecom (France)		Matthieu FOUQUET, Bouygues Telecom
1.1.0	July, 15th 2004	First update, Measurement based on AA.50 Fraud Criteria		Matthieu FOUQUET, Bouygues Telecom
2.0.0	July, 20th 2004	IR.70 SMS Fraud Reference Change		Matthieu FOUQUET, Bouygues Telecom
2.0.1	July, 20th 2004	Final Draft after SMS Fraud Call conference		Matthieu FOUQUET, Bouygues Telecom
3.0.0	5 August 2004	Version for approval after T-Mobile Comments		Matthieu FOUQUET, Bouygues Telecom
3.1	30th March 2005	3.1.7 where a new case is added, following cases re-numbered		Matthieu FOUQUET, Bouygues Telecom
4.0	28th Dec 2011	MCR002: Documenting the mechanism of the DoS attack enables other operators to be made aware of both the symptoms of the attack and the potential countermeasures.	IREG#61 DAG#88 EMC#99	Matthieu FOUQUET, Bouygues Telecom
5.0	April 2013	CR1001 A new fraud threat has been identified that is referred to as the open SMS-C case. Operators must protect themselves from the fraud risk and the proposed CR describes appropriate means to identify and prevent the case	DAG#105,. PSMC115	Laurent Dequidt, Bouygues Telecom
5.0	August 2016	Maintenance of document.	NG leadership	Javier Sendin (GSMA)
6.0	September 2016	CR1002 Add guidance on how to identify an SMS faking perpetrator CR1003 intends to : - add the Home Routing SMS as a major solution in order to prevent Fraud - reorganise, clarify section content where section 2 is for monitoring and section 3 for active solution (open SMSC)	SIGNAL #87 SIGNAL #89	Antoine Janiaud Bouygues Telecom
6.1	May 2024	Include CR1004: Remove old BA references	NG/NRG	Marc Balon Orange

Other Information

Type	Description
Document Owner	IREG
Editor / Company	Laurent Dequidt, Bouygues Telecom

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 prd@gsma.com

Your comments or suggestions & questions are always welcome.