SS7 Interconnect Security Monitoring and Firewall Guidelines

Version 4.0

04 May 2018

This is a Non-binding Permanent Reference Document of the GSMA

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

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

This document is designed to outline at a high level how mobile operators can monitor and sample interconnect Signalling System 7 (SS7) traffic to investigate if they have experienced, or are likely to experience, unwanted or malicious SS7 traffic that may affect their network, and to improve the protection of their networks against such traffic. It outlines signs of abnormalities, how operators can handle these abnormalities to protect their networks, and how an operator can report these abnormalities to the GSMA.

This document is not designed to be an exhaustive reference for different SS7 attacks or ways to detect them, or to provide a comprehensive set of SS7 signalling firewall requirements. It merely guides mobile operators, at a high level and in a non-vendor specific way, on how to monitor SS7 traffic and establish associated firewall rules and data sharing capabilities.

The SS7 “messages” that are referred to in this paper are SS7 GSM MAP (Mobile Application Part) operations and CAMEL operations only. MAP is a layer of the SS7 protocol stack that is used to facilitate mobility management, call handling, SMS and other functions in cellular networks. CAMEL is a layer of the SS7 protocol stack used to enable intelligent network functions to the mobile network.

1.2 Scope

This document provides guidelines (in sections 2, 3, 4 and 5 respectively) on how SS7 traffic on the interconnect links can be monitored, what abnormalities to look for, and how to report them.

Annex A contains a risk assessment of all GSM-MAP and CAMEL packet types and serves as an in-depth reference for the rest of the document.

Annex B of this document provides descriptions of recommended SS7 firewall rules for the handling of MAP and CAMEL vulnerabilities, as well as guidelines for the associated SS7 firewall data sharing formats. These rules define a set that an operator could enable to protect its network, and should be considered along with the functional and operational information provided in IR.82 [5].

1.3 Abbreviations

Term	Description
AC	Application Context
CAMEL	Customised Applications for Mobile networks Enhanced Logic
CAP	CAMEL Application Part
CCBS	Call Completion to Busy Subscriber
CdPA	SCCP Called Party Address
CgPA	SCCP Calling Party Address
CUG	Closed User Group

Term	Description
DAUD	Destination State Audit
DAVA	Destination Available
DDOS	Distributed Denial-Of-Service
DoS	Denial of Service
DTID	Destination Transaction ID
DUNA	Destination Unavailable
E.164	ITU Recommendation: List of Assigned Country Codes
E.214	ITU Recommendation: Mobile Network Codes for the International Identification Plan for Public Networks and subscriptions
FSM	ForwardShortMessage
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
gsmSCF	GSM Service Control Function
GT	Global Title
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
IDP	Initial Detection Point
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IPFIX	IP Flow Information Export
IPSM GW	Internet Protocol Short Message Gateway
KPI	Key Performance Indicator
LBS	Location Based Services
LCS	Location Services
LS	Link Set
M3UA	MTP Level 3 User Adaptation
MAP	Mobile Application Part
MGT	Mobile Global Title
MGW	Media Gateway
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber
MY	Mobile Terminated
MTP	Message Transfer Part
MVNO	Mobile Virtual Network Operator
NAI	Nature of Address Identifier
NPI	Numbering Plan Indicator
O&M	Operations and Maintenance
OA-	Originating Address MSISDN

Term	Description
MSISDN	
OpCode	Operation Code
OTID	Originating Transaction ID
PDU	Protocol Data Units
PLMN	Public Land Mobile Network
PRD	Permanent Reference Document
SCCP	Signalling Connection Control Part
SCF	Service Control Function
SCMG	SCCP Management
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
SGSN	Serving GPRS Support Node
SM-RP-OA	Short Message Originator Address
SMS	Short Message Service
SMSC	Short Message Service Centre
SMS-FW	SMS Firewall
SPAN	Services and Protocols for Advanced Networks
SRI-SM	SendRoutingInformation – Short Message
SS7	Signalling System 7
SSN	SubSystem Number
STP	Signal Transfer Point
TC	Transaction Capabilities
TCAP	Transaction Capabilities Application Part
UDTS	UNITDATA Service
VAS	Value-Added Services
VLR	Visited Location Register
VPLMN	Visiting Public Land Mobile Network

1.4 References

Ref	Doc Number	Title
[1]	GSMA PRD FS.07	SS7 and SIGTRAN Network Security Issues
[2]	GSMA PRD IR.70	SMS SS7 Fraud
[3]	GSMA PRD IR.71	SMS SS7 Fraud Prevention
[4]	3GPP TS 29.002	TS 29.002 Mobile Application Part (MAP) specification. V11.5.0 (2012-12)
[5]	GSMA PRD IR.82	SS7 Security Network Implementation Guidelines
[6]	GSMA PRD IR.88	LTE and EPC Roaming Guidelines
[7]	GSMA PRD IR.21	GSM Association Roaming Database, Structure and Updating Procedures

Ref	Doc Number	Title
[8]	IETF RFC 7011	Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information (2013)
[9]	IETF RFC 4666	SS7 Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA)

2 Monitoring SS7 Interconnect Traffic

2.1 Where to Monitor

The focus of the reported SS7 attack techniques are GSM MAP packets being sent to and from mobile operators, so it is recommended that monitoring be done at nodes that receive interconnect traffic. This could be achieved by:

- An SS7 firewall function[1]
- Gateway STPs (Signal Transfer Points)
- Nodes which send/receive interconnect traffic (MSC Mobile Switching Centre, SGSN Serving GPRS Support Node, HLR Home Location Register, VLR Visited Location Register etc.)
- SMS firewall/home routing nodes
- Network probes/monitoring systems
- Or any other network element, passive or active which encounters interconnect SS7 traffic

Monitoring by nodes such as HLRs or MSCs is limited to only the specific traffic types they receive in everyday operation. Monitoring by nodes such as STPs, SS7 firewalls and network probes, deployed at appropriate locations, gives a wider viewpoint of all the SS7 activity that an operator may be experiencing.

When monitoring, operators should ensure that the interconnect points represent all of the possible ingress and egress points for the network. Operators should be careful that no other interconnect points exist that they are not aware of. Some examples which may be overlooked are peering points with other national operators on which international interconnect traffic could be received or mobile virtual network operator (MVNO) interconnects.

It is generally assumed that peering SS7 traffic with other home operators in each country is a lower risk and may not necessarily need to be monitored. However, there is no guarantee that those networks are not being exploited if some part of the international traffic is re-routed or received over these national interconnects because of number portability. Traffic being submitted through those networks should, if possible, receive the same scrutiny. This becomes especially important if additional security has been put in place on the international but not national interconnects, making the national interconnects a more attractive route for attackers.

[1] An SS7 firewall is considered to be any node capable of executing SS7 firewalling functionality

2.2 How to Monitor

The goal of monitoring is to gauge whether suspicious/malicious SS7 activity is occurring. How this is achieved will vary between operators and the capabilities of each operator, as well as their objectives. The monitoring effort can vary from:

- Sampling a part of the interconnect traffic for a limited time period, looking for known problems, to determine if the problem is occurring, or
- Monitoring all of the interconnect traffic continuously, both inbound and outbound, to determine the maximum extent of the problem, and looking for any potential new attacks.

2.2.1 Time Period

Operators should be aware that SS7 network attacks are likely to be low-volume and periodic events, and simply executing a limited monitoring period (e.g. 5 minutes during the night) is not likely to be of value and is likely to give a false impression of the true level of any malicious SS7 activity that the operator is experiencing.

For the most accurate representation of SS7 interconnect traffic it is recommended that at least 30 days of traffic be collected, if possible. Many operators already collect this much SS7 traffic for the purposes of interconnect billing/billing verification, so the collection and analysis of 30 days of data provides value to other business functions. This length of time may not be possible for all operators but, as a general rule, the longer the monitoring period the better, and multi-day analysis should be aimed for.

The frequency of monitoring is a matter and decision for each operator and the three main options possible are as follows:

- Continuous monitoring
- Periodic monitoring
- Ad-hoc (once off)

In many cases it is expected the frequency will be dependent on the tools and the setup in place at each operator to enable the monitoring and to analyse the results. However, operators must be aware that SS7 network attacks are likely to be low volume events so simply taking a limited time dump - even over one or two days – is unlikely to be enough to give a true idea of whether or not there is suspicious activity happening. Special patterns will appear for day/night time, work days/weekends, public holidays, etc. The absence of a detected problem does not mean the absence of a problem so operators are encouraged not to undertake a single analysis over a small time period and base all assumptions on that experience.

2.2.2 Direction

While it is assumed that the vast majority of SS7 abnormalities may be received from external sources, and so inbound traffic needs to be monitored, it will also be necessary to profile outbound traffic. This is needed to correlate requests and responses, and also to detect the possibility of the home network instigating abnormal or suspicious activity. This also helps to discover potentially compromised internal nodes quickly and to avoid potential accidental blacklisting with interconnect partners. Therefore, monitoring should be bi-directional.

2.2.3 What to Monitor with

The overall objective is to apply the necessary analysis, over representative SS7 interconnect traffic, for a long enough time period. How that is done depends on the capability of individual operators and some example methods could include the following:

- Monitoring and analysing all traffic received at interconnect based STPs, firewalls or network probes already in place that can detect abnormalities
- Getting a copy of signalling traffic (e.g. with a Services and Protocols for Advanced Networks (SPAN) port) from STP nodes or other network elements (MSC, SMSC, HLR, VLR etc.) and forwarding to existing network probes or SS7 firewalls that look for abnormalities
- Obtaining statistics/reports from SMS firewalls, home routing nodes and/or other network elements, that can help determine whether there are abnormalities impacting these nodes
- Taking records from billing systems that can be used alone or correlated with other network traffic data to detect or confirm anomalies

These are just some examples and there are many individual or combined steps that can be taken to undertake traffic monitoring with a view to identifying anomalies.

The ideal monitoring method is by a system or systems that can process and analyse all interconnect traffic, both inbound and outbound, to detect if any known and potentially new SS7 attacks are being experienced. However, it is understood that not many, if any, operators will have this ability initially. Therefore, operators should start with the capabilities they have and proceed from that point, adding monitoring points and data as they become available.

2.2.4 Reducing Data

In many cases, the volume of data to be analysed may be very large. If this happens there can be some ways to reduce the total data volume as follows:

- If an operator has several interconnect points, it may not be easily possible to sample traffic at all points. In that case many operators have pairs of points (i.e. where all traffic for a particular dialog always travels in/out via a pair of points) so they could only monitor those pairs, assuming they are representative of the overall network.
- Sampling or monitoring frequencies can be higher on less trustworthy interconnection points or particular Global Title (GT) ranges.
- For analysis of SS7 traffic, operators may decide that only some SS7 packet protocols are of interest, and not others, e.g. GSM-MAP and Customised Applications for Mobile networks Enhanced Logic (CAMEL) are of interest, but ISUP is not.

2.2.5 Dealing with Traffic Trying to Bypass Monitoring

It should be noted that abnormal or suspicious traffic may also attempt to avoid detection, especially after an operator receiving such traffic has started to put defences in place. Therefore, operators should take into consideration how traffic is captured and monitored in case it leads to traffic being unexamined. Some examples are:

- Routing of traffic to a monitoring node by GT routing, which may route exactly by taking into account the GT plus parameters such as SCCP Nature of Address

Indicator (NAI) or Numbering Plan Indicator (NPI). These rules could be avoided if an attacker changes the NAI to a different value.

- The inclusion of a non-standard packet extension, or the corruption of SS7 packets, in order to avoid triggering rules for monitoring.
- The use of non-standard addresses, such as addressing a HLR directly by its Global Title, rather than a MSISDN, or by using a MGT type address or by indicating different routing at the SCCP level. Again, these non-standard addresses may be selected to avoid detection.
- The use of unexpected combinations of Application Context and OpCode, in order to avoid triggering rules for monitoring based on expected combinations.
- Assembling the messages into multiple PDUs, where reassembling is required and other anomalies. An example of this is breaking a message into different parts, such as a placing the MAP packet into a TC-Continue where it would normally be sent in a TC-Begin.

The use of bypass behaviour is more likely to be common in operators that have begun to secure or are actively monitoring their SS7 networks. However, all operators should review how they capture traffic to ensure they are not missing any potential anomalous activity. This can be detected through the creation of key performance indicators (KPIs) designed to identify messages that carry abnormal parameters. For example, a KPI that looks for MAP messages, with a Signalling Connection Control Part Numbering Plan Indicator (SCCP NPI) of E.212 should raise an alarm as this value should be E.164. Likewise, there are other indicators that can be defined in KPIs for easy detection when they are encountered.

3 Abnormal Traffic to Monitor For

3.1 Unusual Lower Level SS7 Activity

There are a number of indicators of suspicious/abnormal traffic on lower levels and the following list contains examples which, if encountered, should be investigated:

- MAP messages, where the SCCP Calling Party Address (CgPA) and SCCP Called Party Address (CdPA) GTs are in the same destination HPLMN range. This could indicate the spoofing of an operator's GTs.
- TCAP Continue, TCAP Abort or TCAP End transactions which can't be correlated to any TCAP Begin transaction. For example, TCAP end messages of MT-FSM transactions that don't have a corresponding TCAP Begin could indicate SMSC spoofing.
- SCCP Management (SCMG) messages coming from outside the home operator network. This may indicate a Denial of Service or TCAP scanning attack to a particular user or to a set of users. As these packets cannot normally be routed by GT then they are highly unlikely to reach or be correctly interpreted by a receiving node from a remote source, and therefore the risk comes primarily from adjacent nodes.
- Large amounts of TCAP Begin messages without a TCAP End. This has been used by hackers to profile network nodes within an operator (GT scanning) without their knowledge. In particular, if the receiving GT is increased/decreased in regular steps.

- Large amounts of SCTP INIT chunks followed by ABORT chunk or large amounts of incomplete SCTP associations or large amounts of SCTP Cookie Echo chunks. This could indicate SCTP scanning.
- Large numbers of M3UA DAUD/DUNA/DAVA packets. This could indicate M3UA scanning from an adjacent compromised node (and so may not come over the interconnect).
- Large numbers of packets being generated (e.g. TCAP Aborts) which don't have an operation code, and so cannot be categorised according to the scheme below.
- Unusual or unexpected SCCP packets being received. An example is connection-oriented SCCP packets (e.g. Class 2 & 3), that an operator would not normally expect to receive from outside the home operator network. Another example would be unusual XUDT, LUDT, XUDTS, LUDTS etc. messages – i.e. an operator may not expect, or be capable of handling XUDT messages at all, and so if these are received then these may be an indication of unusual activity.
- Receiving non-valid M3UA Message Classes /Types. It would not be expected to receive reserved (see [9]) Messages Class values, or reserved Message Type values within valid Message Classes, from outside the home operator network and doing so may indicate unusual activity such as Denial of Service.
- Unusual or unexpected MTP3 packets being received. An example would be MTP3 packets whose Service Indicator code is for a reserved or home operator unused value. Again, this could be an indication of Denial of Service.

3.2 Category 1

The following are a **sample** of packets which are widely regarded as unauthorised at interconnect level, and should not be sent between operators unless there is an explicit bilateral agreement between the operators to do so:

- SendRoutingInfo
- SendRoutingInfo for GPRS
- SendRoutingInfo for LCS
- SendIMSI
- AnyTimeInterrogation
- AnyTimeSubscriberInterrogation
- AnyTimeModification
- SendIdentification
- ResumeCallHandling
- FailureReport
- CheckIMEI
- NoteSubscriberDataModified
- Unknown PDU: Any GSM-MAP packet with an Unallocated/Unknown Operation Code

Note: The list above is a sample of Category 1 packets and is **not** the full list. The full list and the basis of categorisation can be found in Annex A.

To emphasise, it should be remembered that in some cases specific packet types may be authorised to be sent between operators - if there is an agreement in place or due to their configuration. For example, AnyTimeInterrogation packets could be allowed over

interconnect links if the CgPA belongs to an authorised third party LBS partner who has an agreement in place with the receiving operator. Similarly SendRoutingInfo can be allowed if an operator has Optimal Routing in place. Both these packets would then be subject to Category 2 packet filtering type checks. Operators should confirm for themselves if they have any agreements in place that specifically allow these packets to be sent or received over interconnect links.

Operators should also keep in mind that, if exceptions exist, attackers may attempt to spoof these 'authorised' addresses and so the type of packet and impact it could have (whether it attempts to retrieve information or is a simple 'fire-and-forget' packet) would impact the monitoring of these.

Operators may have a long-term aim to reduce the 'attack surface' by reclassifying packets normally treated as Category 2 or Category 3 to Category 1 where these messages are not expected over the interconnect for their network. For example: SS or USSD messages which would normally be treated as Category 3 or PSL messages which would normally be treated as Category 2 could have Category 1 packet-type checks applied on them by an operator, and so be filtered and potentially blocked on the interconnect. This should be done on a case by case basis only by each operator and after research on whether such filtering is suitable for the operator in question.

3.3 Category 2

Certain GSM-MAP packets are authorised to be received on interconnects between mobile operators and these include SS7 packets that should normally only be received from an inbound roamer's home network. These require intra-packet logic to be applied to detect anomalies on packets either inbound or outbound. The following packets are a **sample** of those worthy of monitoring and analysis on this basis:

- InsertSubscriberData[2]
- DeleteSubscriberData
- Reset
- ForwardCheckSSIndication[2]
- ProvideSubscriberInfo
- ActivateTraceMode
- DeactivateTraceMode
- ProvideRoamingNumber[2]
- SetReportingState
- RemoteUserFree
- AlertServiceCentre
- CancelLocation
- ProvideSubscriberLocation
- BeginSubscriberActivity
- ISTCommand

[2] Not all usage of this packet would fall under Category 2, some would fall under Category 1. See Annex A for the complete classification and treatment of each packet.

- UnstructuredSSNotify[2]

Note: The list above is a sample of Category 2 packets and is **not** the full list. The full list and the basis of categorisation can be found in Annex A.

Operators should remember that they are free to choose how to classify packets and what checks to apply. For example, if their network infrastructure does not support certain packet types then they could be blocked (i.e. reclassify as Category 1 packets).

3.3.1 Addressing Mismatches for Home Subscribers and Inbound Roamers

For these suspicious packets, abnormality is indicated by intra-packet checks such as:

- For incoming MAP packet requests: Comparing CgPA and the IMSI or MSISDN within the MAP layer. If they do not belong to the same operator (i.e. there is a mismatch in terms of Country Code and Operator Code – if known), this indicates a potential anomaly. Note that the impact of any number portability implementation has to be considered
- For outgoing MAP packet requests: Comparing CgPA and the IMSI or MSISDN within the MAP layer. If they do not belong to the same operator (i.e. there is a mismatch in terms of Country Code and Operator Code – if known), this indicates an anomaly.

There are some notes that operators should consider in performing these checks:

Note 1: Most, but not all, Category 2 packets contain an IMSI that can be compared against the relevant SCCP address.

Note 2: Comparing Operator Codes in MSISDNs with the relevant SCCP addresses should be done with care due to the effects of mobile number portability, as mismatches can easily occur.

Note 3: For all SS7 address correlation, care should be taken in the presence of intermediate elements such as SMS or roaming hubs, or number portability, which (depending on type and configuration) can change network and/or subscriber addresses as part of normal operations (such as adding prefixes). In these cases, analysis will be more complex and dependent on knowledge of how the authorised addressing is being modified.

Note 4: The above incoming/outgoing MAP packet request checks are examples. Other specific intra-packet correlations may also be possible to determine anomalies, e.g. for Reset the correlation of CgPA and SendingNodeNumber address. See section 3.4.2 for more details.

Monitoring for these mismatches can detect attempts to send packets that query the network about home subscribers, which is something that should not occur without prior explicit agreement. It is also possible for operators to apply the same logic to inbound roamers i.e. to examine all packets that are addressed to inbound roamer IMSI/MSISDNs, and compare against the CgPA address in those packets received. However, this makes comparisons significantly more complex and so is likely to be of secondary value for mobile operators. See section 3.3.1.1 for more discussion on this.

3.3.1.1 Potential Methods to Improve Inbound Roamer Addressing Mismatches

The standard Category 2 packet filtering checks for inbound roamers are likely to raise false positives because of the inconsistencies in numbering plans with shared infrastructure and roaming hubs. In such situations, cross checking the source of the message with the user identity inside the message could fail. This could be caused for example by a shared HLR/HSS across multiple countries or sharing the same MCC/MNC across countries.

By monitoring the HLR addresses used by outbound Update Location messages for inbound roamers, such discrepancies in the numbering plans (as typically registered in GSMA PRD IR.21) can be detected and used either to update the numbering plan for the Category 2 filtering of inbound roamers manually (after confirmation of any numbering plan discrepancies) or automatically.

This HLR tracking procedure would consist of the following high-level method:

1. Trace the Update Location message of the inbound roamer to retrieve the IMSI
2. Trace the corresponding response messages (ISD. etc.) to get the HLR address as well as to collect the MSISDN
3. Use the IMSI (MCC, MNC), HLR Address and MSISDN (CC) to detect numbering plan discrepancies.

This approach is suitable for both SS7 and Diameter including situations with user profiles in a combined HLR/HSS. However, it needs careful consideration because this would require sufficient performance for message correlation and Location Update request/answer tracking for all inbound roamers. It also would not cover cases where network infrastructure may be distributed across multiple countries

3.3.2 Traffic not from Roaming Partners

An additional monitoring method is to compare the CgPA in all packets against known and allowed roaming partners. Packet activity that originates from a country/operator that is not currently a roaming partner should be considered abnormal in this case. This is also true if the traffic received does not match the actual service roaming contract with that partner. It should be noted that anomalies may arise as new roaming partnerships are established and, in some cases, agreements may not be entirely finalised before traffic is generated.

3.3.3 Sub-Classification of Category 2 Messages

Category 2 messages can be further broken down into 2 categories. These are:

- Category 2.1: MAP messages requiring an answer (example: PSI, PRN, PSL)
- Category 2.2: MAP messages not requiring an answer (example: ISD, DSD)

It can be seen that messages in category 2.1 are easy to monitor by association of SCCP and MAP addresses as outlined in section 3.3.1, as the answer must go back to the indicated address. Unauthorised messages in category 2.2 are harder to detect, as the origination address could be faked. This is only likely to affect inbound roamers, as opposed to home network subscribers.

3.3.4 Spoofed Traffic to Inbound Roamers

If an operator decides to apply Category 2 packet checking logic to inbound roamers, then it should be aware of the possibility that the source GT may be spoofed. In this case an

inbound roamer in the VPLMN could be targeted by a Category 2.2 message with a spoofed GT, which would appear to come from the right source i.e. from the same country or network as the inbound roamer subscriber. Ways to identify and deal with spoofed traffic are discussed in section 4.

3.4 Category 3

Category 3 packets are GSM-MAP packets that are authorised to be sent on interconnects between mobile operators. These require additional, advanced inter-packet logic to be applied to detect anomalies. The following packets are a **sample** of those worthy of monitoring and analysis on this basis:

- UpdateLocation
- UpdateGPRSLocation
- PurgeMS
- RegisterSS[3]
- EraseSS
- ActivateSS
- DeactivateSS
- InterrogateSS
- ProcessUnstructuredSSRequest
- SendAuthenticationInfo
- RestoreData
- NoteMMEvent
- SendParameters

Note: The list above is a sample of Category 3 packets and is **not** the full list. The full list and the basis of categorisation can be found in Annex A.

Operators should remember that they are free to choose how to classify packets and what checks to apply. For example, if their network infrastructure does not support certain packet types, then they could be blocked (i.e. reclassify as Category 1 packets)

3.4.1 Location Correlation

For these packets, the CgPA for the IMSI or MSISDN identified in the message should be compared against the last known location of the subscriber, specifically to see whether it matches the network where the subscriber is currently located.

Note 1: It can be difficult to confirm these correlations, as location update means that a subscriber is moving. Therefore, it may not be possible to compare and correlate the exact location. In addition, some of these attacks may involve one-way type logic, such as a DoS involving a PurgeMS packet using a spoofed CgPA address. In this case the spoofed address could be the correct address. Therefore, more complex analytic logic will be required

[3] Not all purposes of this packet would fall under Category 3, some would fall under Category 1. See Annex A for the complete classification and treatment of each packet.

to fully validate these packets. However, location correlation does allow some suspicious abnormalities to be detected.

Note 2: The presence of roaming hubs or other specific network elements that alter SCCP addresses can also significantly impact the logic required to determine the last previous location of a subscriber, and affect whether a new indicated location is accurate. Operators should be aware of any roaming hubs which may be active and influencing their subscribers in order to validate the 'true' location of subscribers.

This correlation against the last known location of the subscriber can be done via different methods:

- One method would be to 'remember' old locations of a subscriber and then making a logical deduction whether the new location in the received packet is plausible or not. This may require the processing of mobility management events (like MAP Update Location packets) on the interconnect interface only, or on both the interconnect and internal interfaces. From a practical perspective processing all interconnect events has less processing impact, but means knowledge of when a subscriber returns to the home network may be missed. Processing all mobility management packets gives a more complete picture of the subscriber's location but leads to a greater processing load and possibly a more invasive integration.
- Another method would be to query network elements like the HLR with a HLR lookup for the subscriber, and then correlating the new location in the received packet against the location the HLR returns. This HLR lookup can additionally be done in such a way as to cause the network to actively 'page' the subscriber, so the location returned by the HLR could be a location where the subscriber is still presently reachable, thus helping determine if the new location received is plausible or not.

3.4.2 Additional Addressing Correlation

Certain packets have several address fields, where inconsistencies in country or operator data could indicate abnormality. For example, UpdateLocation and PurgeMS have several addressing fields, so the MSC address, VLR number and CgPA could be checked to validate that they belong to the same operator. This logic, similar to category 2 packet-type like correlation (intra-packet) can be used to detect obvious abnormalities in this type of traffic, and therefore enable extra checks for packets classified as category 3.

3.4.3 Traffic not from Roaming Partners

As with category 2 packet type, the CgPA of all packets should be monitored to ensure they relate to allowed roaming parties. Packet activity that originates from a country/operator that is not currently a roaming partner should be considered abnormal and suspicious. It should be noted that anomalies such as these may arise as new roaming partners come on board over time and, in some cases, agreements may not be entirely finalised before traffic is generated.

3.4.4 CAMEL Packets

In performing SS7 monitoring, analysis should also be performed on CAMEL activity, as these packet types can also be used to execute attacks. In particular, InitialDP (IDP) packets

can be used to execute voice call interception, while IDP-SMS & IDP-GPRS can be used to execute SMS or GPRS control. All inbound and outbound CAMEL packet activity should be examined for anomalies and other suspicious activity. The following packets are especially worthy of monitoring and analysis:

- IDP
- IDP-SMS
- IDP-GPRS

Inbound CAMEL packets from this list should be examined for category 3.1 packet type location correlation, i.e. they should come from that subscriber's current visited network. Outbound packets can have logic similar to category 2.1 packet type like addressing correlation applied on them, that is they should only be sent to the home network of the subscriber involved.

3.4.5 Sub-Classification of Category 3 Messages

Category 3 messages can be further broken down into several categories. These are:

- Category 3.1: SGSN/VLR check – Messages where the location can be validated by past/current VLR information (example: MO-FSM, USSD, RegisterSS, IDP)
- Category 3.2: Time/location check - Messages where the location cannot be validated by past/current VLR information (example: UL, SAI)
- Category 3.3: IPSM GW – SMS messages where SMS security specific checks need to be applied

Messages in category 3.1 can be monitored by validating the past/current known VLR address against the packet than has been received, as outlined in section 3.4.1. Unauthorised messages in category 3.2 are harder to detect, as the known VLR information cannot normally be directly compared against the packet information, as these messages are expected to come from new VLR/SGSN addresses. One exception to this is if a HLR lookup is done and the known VLR information is confirmed as being current, as also outlined in section 3.4.1. Unauthorised messages in category 3.3 are MT-FSM and SRI-SM that fail specific SMS spoofing or faking checks. Home routing may also be used to detect and prevent anomalies. Further details on SMS logic to apply is described in section 3.7.

3.4.6 Dealing with Traffic trying to bypass Category 3 protection

Operators should be careful of traffic which may attempt to avoid or defeat specific Category 3 type checks. One example is that for outbound roamers in a VPLMN, Category 3 protection could be bypassed if it is based on a too simple 'plausible movement' check (see section 3.4.1). This can be performed by first sending hostile Location Updates from non-suspicious locations which might bypass the protection (e.g. a bordering country) and then proceed with latter Category 3 messages. Additionally, if the initial Location Update is not successful the attacker could start an advanced version of the attack by spoofing a Cancel Location first to the subscriber's current VPLMN.

- Some potential ways to deal with this are to HLR query and actively 'page' the subscriber in its old location, as part of the process of validating a received hostile Location Update. This will determine that the subscriber may still be in its old location in the VPLMN, and so the new location is not plausible.

- In the case of the attacker executing a more advanced attack by first spoofing a Cancel Location to the VPLMN, this would make paging at the old location fail, however it relies on the attacker knowing or determining the IMSI and exact VLR/SGSN address of the subscriber in advance, which makes the attack more difficult. Some potential ways to deal with this is the operator should ensure that this information is not obtainable from its network. GT spoofing protection in the VPLMN (see section 4.2) would also defeat this attack but this relies on the VPLMN in question having adopted these checks, and is outside the home operator's control.

3.5 Inconsistent Message Format

Attack messages may contain inconsistencies to hide or spoof a sender or the aim of the packet. One way to discover a potential attack is to perform consistency checks between the layers or in the messages themselves.

As described in section 3.4.2, one possible efficient check is to perform cross-layer checking on addressing information, for example, to validate if the CgPA in the SCCP layer and the information available, e.g.GT(s), in the MAP layer belong to the same operator.

Other inconsistencies may exist in how the messages themselves are comprised. The 3GPP specifications outline a semantic for messages, so syntax checking may reveal malicious insertion of unauthorized commands and fields. This kind of syntax checking also allows misconfigurations in an operator's own nodes or their partner nodes to be discovered.

Other inconsistences may involve comparison of expected parameters based on usage. For example, comparison of the TCAP Application Context used per packet type/operation code, i.e. the use of a MAP InsertSubscriberData packet with a vcsgLocationUpdate application context which could be classed as abnormal. In this case, the check is to ensure that the context needs to be consistent with the usage.

3.6 Other Anomalous Behaviour

While this document describes some known SS7 attacks it is important to note that not all attacks over SS7 are known at this time, and many attacks are difficult to detect. This is particularly important for category 3 type scenarios, or any packet type that could evade the checks above.

Therefore, operators should also consider monitoring for other behaviour. This is a complex area that requires more sophisticated analysis (such as state-full/history based analysis). As a result, exact monitoring requirements cannot be specified. However, some practical examples of additional monitoring include:

- If operators detect suspicious/abnormal traffic from a particular GT, they could also investigate what other types of packets these nodes have generated to see whether any other, previously unknown, attacks are ongoing. This could be used to build a 'profile' of potential malicious nodes.
- For monitoring traffic from GTs, operators should be aware that even if they whitelist GT ranges, misbehaving individual GTs may occur in a range of well-behaving GTs. Therefore, monitoring should take into account potentially known individual misbehaving GT addresses within the range of those controlled by partners. This monitoring approach allows operators to identify potentially compromised nodes from

partners and to differentiate the traffic from the compromised 'black' nodes within the remaining range of 'white' nodes.

- If an operator detects that an internal or external global title is now acting strangely or inconsistently when compared to its past behaviour, this could be an indication that the node associated with the GT has been compromised.
- If an operator detects that a new global title is generating traffic within its network and is routing this traffic to a network that it has not encountered before.
- If an operator detects an unusual sequence of aborts being generated or errors being sent to a particular global title different to what would normally be expected.
- If an operator detects a series of packets being sent to iterative or related Global Titles, this could be indicative of GT scanning.
- If an operator detects a non-standard sequence/order of packets in a certain time period from a specific node. i.e. a ReportSMDeliverStatus from a specific SMSC and related to a specific IMSI may be legitimate only if a previous SRI-SM from the same SMSC related to the same IMSI has been received within a short time.

These monitoring techniques are an area of continuing research and are likely to be increasingly needed over time as attacks evolve to evade SS7 defences that have been deployed.

3.7 Abnormal SMS Activity

In performing SS7 monitoring, it is also worth performing analysis on SMS related packets because some SMS packet types, such as SRI-SM, have been used to harvest information that can be used in SS7 attacks. Various types of attack have been described in great detail in PRD IR.70 [2] and so will not be covered here, but some things to monitor for include the following:

- If an SMS firewall solution has been deployed, check that:
    - The SMS-FW implements rules defined in the IR.71 guidelines [3].
    - There are SMS FW statistics/reports being generated to identify and report anomalous behaviours
    - Home routing isn't bypassed (e.g. MT-FSM SMS with a SCCP called party address different from the home routing GT, or the HLR being addressed other than via MSISDN routing, i.e. via MGT (E.214 addressing) or by the HLR's GT directly)
- If a SMS firewall is not deployed, but home routing is implemented, the following checks can be implemented:
    - All incoming MT-FSM SMS with originating MSISDN (TP OA) belonging to destination HPLMN numbering plan. See rules in IR.71 [3].
    - All incoming MT-FSM SMS to identity OA-MSISDN (originating address MSISDN) spoofing. See rules in IR.71 [3].
    - All incoming MT-FSM SMS to identity fake SMSC (SM-RP-OA). See rules in IR.71 [3].

- If no SMS firewall or home routing is in place, implement rules from IR.71 [3] to identify abuses (e.g. on STP, MSC). Otherwise, implement rules to post-process mirrored signalling traffic.

3.7.1 External SRI-SM Activity

A particular area to investigate is the number of SRI-SM messages that are received from external sources compared to the number of subsequent MT-FSMs. If certain operators are generating large volumes of SRI-SMs, with very little subsequent SMS activity, then this is an indication that these operators might be engaged in simply scanning other operator HLRs or engaged in some other anomalous behaviour. On the other hand, operators should be aware that SRI-SMs may be used by other services or applications that are legitimate. In each case, operators should investigate further to determine what is suitable for, and authorised on, their networks.

4 SCCP Calling Party Address (CgPA) Spoofing

In the case where the SS7 attackers may not care about the response to a sent SCCP message (even if the response contains data), they may use a spoofed CgPA in their SS7 attacks. This approach could apply to attacks like subscriber or network node denial-of-service (DoS), SS7 overload, and illegitimate charge attacks.

Regardless of the category to which the message belongs, the following list includes the SS7 messages which can be abused with a spoofed CgPA:

- AnyTimeModification
- NoteSubscriberDataModified
- CancelLocation
- InsertSubscriberData
- DeleteSubscriberData
- Reset
- RegisterSS
- ActivateSS
- DeactivateSS
- RegisterPassword
- ProcessUnstructuredSS
- BeginSubscriberActivity (for USSDv1)
- PurgeMS
- ReportSMDeliveryStatus
- ForwardSM (MO)
- ISTCommand
- AlertServiceCentre
- ForwardCheckSSIndication
- ActivateTraceMode
- ProvideRoamingNumber

In general, a targeted network element is vulnerable to SCCP spoofing if it executes logic directly after receiving a spoofed TCAP Begin that contains the SS7 message. For example, network elements may initiate logic before they have received all parts of a transaction, i.e. if

a network element is expecting to receiving multiple ISDs (first in a TCAP Begin and then subsequent multiple TCAP Continues), then it may make logic changes before the final TCAP Continue has been received.

Detecting SCCP Global Title (GT) spoofing can be quite complex. However, the sections below provide recommendations that the MNO (i.e. the home operator) can use to try and detect it in the following cases:

- If the MNO's GTs are being spoofed in the CgPA field of messages sent by an attacker to another mobile network operator; or
- If the CgPA of incoming SS7 messages to the MNO network from other networks are being spoofed.

4.1 Detecting Spoofing of an MNOs Own Global Titles

One major risk is that an attacker may misuse the SCCP GT of a roaming or interconnect partner of the attacked operator. Monitoring for this scenario can be performed by the MNO whose GT has been misused (referred to as the spoofed MNO). This spoofed MNO should have an interest in detecting the misuse of its GT due to potential disputes e.g. associated fraud, industry reputation damage, or to avoid having its GTs added to some operator blacklists.

Spoofing of a MNO's own GTs can be suspected if the spoofed MNO observes the following messages or behaviour:

- Many messages containing unknown SSNs are received without corresponding send messages (indicates a possible scan of the attacked operator's network)
- If SCCP User Adaptation (SUA) is used, messages containing Destination unavailable (DUNA) or Destination User Part Unavailable (DUPU) are received without corresponding send messages.
- TCAP Continue, TCAP Abort or TCAP End transactions are received that can't be correlated to any TCAP Begin transaction.

An attack against another mobile network can be suspected if the error messages received by the spoofed MNO cannot be paired with previous outgoing messages. But even without that pairing, if there are many messages of that type, then this may indicate a brute force attack and a vulnerability screening of a roaming or interconnect partner network.

In general, a spoofed MNO can detect GT spoofing when answer messages are received and they cannot be correlated to an outgoing request.

A spoofed MNO can also check for MAP messages that are received with CgPA and CdPA GTs within the range of the same network. If the GTs are within its own range, this indicates spoofing of the operator's own GTs.

If the spoofed MNO suspects that its GTs are being misused, then it should inform the source of the error messages as fast as possible to stop the attack and to avoid being held accountable for it. This can occur via:

- Direct approach via contacts in GSMA PRD IR.21.

- Modification and return of the received message to the sending operator to indicate the GT misuse. The modification can be a commonly agreed way to indicate GT misuse e.g. replacing the sending identity in the upper protocol layers with the one of the operator that is under attack. The lower layer SCCP would still indicate which network has really sent the message and whose GT has been misused. If the attacked operator is also deploying monitoring software it can catch this “mismatch” and evaluate the related message and identity the potential attack (see next section).

Note: Care should be taken if modifying and returning messages, to avoid amplifying an existing DoS attack to another operator that may be on-going from spoofed GTs. In this case simply sending back another copy of the message to the attacked network will have the side-effect of making any DoS attack worse

4.2 Detecting CgPA Spoofing in incoming SS7 messages

In order to detect CgPA spoofing in incoming SS7 messages, a MNO can monitor:

- MAP messages with an unexpected point code, and MAP messages with a point code expected for the invoked MAP procedure but unexpected for the used CgPA. One example of this would be MAP messages with internal CgPA GTs entering the HPLMN from an external interconnect link.
- Inconsistent message format (see section 3.5 for more details).
- Other anomalous behaviour (see section 3.6 for more details)

Beyond monitoring, a MNO with a suitable SS7 firewall capability can actively insert a message dialogue to validate the CgPA. For example (after validating the CgPA is a valid roaming partner and a valid entity for the message), the address can be checked for spoofing by adding a TCAP continue message which would normally result in an error from the CgPA if the address has been spoofed. GSMA IR.82 [5] has more details on methods to achieve this.

5 Reporting Suspicious/Abnormal Activity

5.1 What to Report

As it is beneficial to the whole operator community to know the scale and extent of malicious SS7 activity, it would be very useful for reports of abnormal behaviour detected during monitoring to be made available, anonymously or otherwise, to GSMA members and the wider industry. Things to report could include the following:

5.1.1 Types of Suspicious/Anomalous Activity

Some examples of these include:

- Unusual lower level SS7 activity
- Prohibited interconnect packets

5.1.2 Volumes of Suspicious/Anomalous Activity

Some potential examples of these reports are:

- 20,000 unauthorised PSI packets in 24 hours
- Several dozen unauthorised ISDs over 1 week

5.1.3 Origin Point/Analysis Results

Some examples of this include:

- Suspicious UpdateLocation packets received from region/country/operator. (This could also indicate a misconfigured node in another network).
- Unauthorised ISDs from GT X caused CAMEL (gsmSCF) node to be changed. Believe subsequent fraud executed for subscriber.

5.2 Who to Report to

GSMA members are encouraged to report details of anomalous and suspicious behaviours to GSMA and details of findings can be sent to fasg@gsma.com. Use of the following reporting form is recommended, although reports in other formats are welcome.


Incident Report

5.3 Anonymity

Prior to sending a report to GSMA, members should consider the level of anonymity they want to preserve. Of particular importance is whether they want to include the reporting operator's name/country/region, whether to indicate exact volumes, and whether to share the detailed results of their investigation, such as attack origin. If the reporting member wishes to anonymise any report, it can do so by either sending a redacted/anonymised report to the GSMA, or, if they wish to discuss it, they could send an original version to the GSMA, and then discuss what is suitable to be shared more widely.

5.4 Distribution of Reports

Once the report has been submitted to GSMA it will be distributed to the relevant mailing lists and published on the Infocentre.

Annex A SS7 Packet Risk Classification

The embedded spreadsheet below provides a risk assessment of all GSM-MAP & CAMEL packet types. It also indicates the attack category/ies and object manipulation(s) relevant to each packet type, and provides a template for logging an operator's mitigation strategy and tracking progress.

Packet Classification_v1_7.x

A.1 Explanation of Format of SS7 Packet Risk Classification

The packet risk classification is a spreadsheet that contains a number of sheets.

The sheet termed MAP INT0 is a classification of each MAP opcode under the headings of:

- Application Context;
- Expected Subsystem Usage;
- Risk Assessment;
- Attack Categories;
- Object Manipulation;
- Filter Classification; and
- Other historic information

Generally, the filter classification is the most important piece of information, and describes the recommended, and highest, filter classification of each opcode over international interconnect links.

Note 1: Discussion of the potential use of the MAP packet risk classification for national links is provided in section A.3.2.

A.2 Basis of Categorization

Categorisation of the different MAP packets is based on the on the function and source of the Application layer message ~~logic that is to be applied per packet to determine whether it is suspicious or not~~. The SS7 packet risk classification spreadsheet embedded above contains the complete classification[4]. These fall into 3 main types of increasing complexity:

- Category 1: Interface-Unauthorised Packet. This refers to checks for a type of Application Packet which should not be sent over this particular interface. Category 1 filtering especially refers to messages that should normally only be received from within the same network, and not on the Point-of-Interconnects (POI) with other networks, unless there is an explicit bilateral agreement between the operators to exchange them.

[4] The packet classification in the text in this document normally shows the highest classification that can apply to a packet type.

- Category 2: Home-Network Packet. This refers to checks for a type of Application Packet which is sent from the 'Home' or allocated network (e.g. in the case of shared infrastructure) of a Subscriber. Typically this is done by screening to see if there are no inconsistencies between the information in lower layers and in the application layer. Category 2 filtering especially refers to messages that should normally be about subscribers and related to their home networks.
- Category 3: Plausible-Network Packet. This refers to checks for a type of Application Packet which is sent from the current or purported network a Subscriber is present at. It also covers a subset of SMS-related Application Packets which can be sent from a SMS node in any network. Typically checks on these packets are based on inter-message correlation, and may involve plausibility of messages in terms of location, velocity and time, as well as specific messaging related checks. Category 3 filtering typically refers to packets that should normally only be sent about a visiting subscriber from that subscriber's current visited network, or SMS-related packets which can be sent from any network

This classification system leads to a few outcomes:

Packets can have multiple categories, based on the packet and the type of message flow.

For example, the SendParameters packet can in general[5] be classified as either a category 1 (if going from VLR to VLR) message flow, or a category 3 (if going from VLR to HLR) message flow

A.3 Use of the SS7 Packet Risk Classification 'Grid'

Operators are free to use the SS7 packet risk classification based on their signalling security objectives, risk profiles, network capabilities, roaming and inter-operator agreements and their own investigations of traffic in their network. The spreadsheet does not have to be strictly applied if it is not feasible or desirable to do so.

A.3.1 Using Partial Information from the Packet Risk Classification

Assume that an operator was not able to monitor/block by detailed analysis of a packet, but was only able to monitor/block by Application Context alone. In this case - based on the information in the SS7 packet risk classification - there would be a certain number of routing contexts that could be blocked on the interconnect links (such as locInfoRetrieval or callControlTransfer), as packets that use these would map to Category 1. This would provide a measure of security to a mobile operator.

However, operators should be wary of this giving a false sense of security, as using partial information and methods inevitably will give partial security at best. In this case due to the impreciseness of using Application Contexts only, there would be a number of other Application Contexts that would not map 'cleanly' to Category 1 (such as networkFunctionalSs, having MAP packets with different opcodes that would be filtered using Category 1 or Category 3). In addition, the 'allowed' Application Contexts would

[5] See Section B.3.1.4.3 for the full treatment of SendParameters

include packets that would still need to be filtered at a deeper Category 2 and Category 3 level.

A.3.2 Using the Packet Risk Classification for National Traffic

As well as using the packet risk classification for international traffic, operators could potentially use the spreadsheet as a resource to help them start to monitor signalling activity on their national links. However, it is critical for mobile operators to remember that the main sheet – MAP INT0 is **not designed for use for national traffic**, and there is not a specific sheet supplied for national traffic.

The reason for this this is that every mobile operator has typically developed its own specific use cases and agreements with the other national operators in each country or region, and to make a specific set of recommendation would not be possible. In general the nature of MAP packets sent over the national interconnect links could vary widely, from almost the full set of MAP packets being permitted (and therefore much more than would be allowed over international links), to a much smaller sub-set (again, much smaller than would be expected over international links), or any amount in between - depending on the age of the networks and links, what agreements have been put in place, network technologies in the country or region, whether national roaming is in use and so on. This is different from international interconnect, which generally - but not always - follow the same accepted set of agreements and procedures (although individual exceptions can exist).

In this case, if mobile operators wish to implement monitoring - and potentially filtering - of their national interconnect links, that they do so after first-hand examination of the national traffic, and make their own decisions based on that.

Annex B SS7 Firewall Recommendations

B.1 Introduction

This section provides guidelines aimed at mobile operators implementing and/or maintaining SS7 signalling firewall solutions and seeking to achieve an adequate protection of their network and the mutual protection between networks against signalling vulnerabilities in SS7. Solutions may vary and be implemented differently to, or go beyond these rules. These rules are however intended to provide a description of an adequate, broadly implementation agnostic version of the required rules to protect against the potential threats currently understood and documented in Annex A. This annex does not attempt to address the specific issues encountered in “real world” signalling such as roaming hubs, operator group services and value-added service (VAS) implementations. This section does not address Diameter or other signalling protocols.

The requirements in this section focus on two aspects to be supported by an SS7 signalling firewall solution:

1. The rules specification in a vendor-agnostic and human readable ‘pseudo-code’ with the purpose to provide operators the same type of protection for vulnerabilities irrespective of the vendor of the SS7 signalling firewall solution.
2. The logging generation in a vendor-agnostic manner to define standard contents and formats of logging data to enable:

    - The minimal set of information outputted by the SS7 signalling firewall in order to exchange information about SS7 vulnerabilities between networks
    - The exchange of information between operators about threats and new vulnerabilities.

The implementation of specific rules needs to take into account roaming hubs, technology gateways, network changes and centralised services in an operator group. These are not considered in this document.

An overview of the signalling vulnerabilities, prevention and recommended counter measures is to be found in other GSMA documents like the SS7 classification of GSM-MAP packets in FS.07 [1] and IR.82 [5], the prevention against SMS Fraud situation in IR.70 [2] and IR.71 [3], LTE and EPC Roaming Guidelines in IR.88 [6], and further GSMA fraud and security related documents and guidelines.

B.2 Definitions

The rules described later in this section require a number of concepts to be defined. The list of definitions in the following table avoids repeated use of references within the SS7 firewall rules specification later in this section.

Ref	Title	Description
inbound		Message received from the insecure side of the firewall (i.e. international SCCP transit provider, or direct from a roaming partner)
ownNetworkGTlist		The set of global titles and/or ranges of global titles allocated

Ref	Title	Description
		to the protected network's own elements.
roamingPartnerGTlist	All roaming partners	The union of all GTs of roaming partners identified by GT, GTList
gt		Individual GTs
gtRange		A set of GTs defined by prefix
gtSet		A set of GTs defined as a list of gt, gtRange and/or gtSet
blackListGT		A list of GTs that require specific handling as described in section
whiteListGT		A list of GTs that require specific handling as described in section
intraPlmn (Category 1 features)		MAP OpCode = 4 (provideRoamingNumber) *see Note 1 5 (noteSubscriberDataModified) 6 (resumeCallHandling) 7 (insertSubscriberData) *see Note 1 9 (sendParameters) *see Note 1 10 (registerSS) *see Note 1 11 (eraseSS) *see Note 1 12 (activateSS) *see Note 1 13 (desactivateSS) *see Note 1 14 (interrogateSS) *see Note 1 17 (registerPassword) *see Note 1 18 (getPassword) *see Note 1 19 (processUnstructuredSsData) *see Note 1 20 (releaseResources) 21 (forwardSm-Vgcs) *see Note 2 22 (sendRoutingInfo) 24 (sendRoutingInfoForGprs) 25 (failureReport) 26 (noteMsPresentForGprs) 28 (performHandover) *see Note 3 29 (sendEndSignal) *see Note 3 30 (performSubsequentHandover) *see Note 3 31 (provideSiwfsNumber) 32 (siwfs-SignallingModify) 33 (processAccessSignalling) *see Note 3 34 (forwardAccessSignalling) *see Note 3 35 (noteInternalHandover) 36 (cancelVgcsLocation) *see Note 2 38 (forwardCheckSsIndication) *see Note 1 39 (prepareGroupCall) *see Note 2 40 (sendGroupCallEndSignal) *see Note 2

Ref	Title	Description
		41 (processGroupCallSignalling) *see Note 2 42 (forwardGroupCallSignalling) *see Note 2 43 (checkIMEI) 52 (trace SubscriberActivity) 53 (updateVgcsLocation) *see Note 2 55 (sendIdentification) 58 (sendIMSI) 59 (processUnstructuredSS-Request) *see Note 1 60 (sendUnstructuredSS-Request) *see Note 1 61 (sendUnstructuredSS-Notify) *see Note 1 62 (anyTimeSubscriptionInterrogation) 65 (anytimeModification) 66 (readyForSM) *see Note 1 68 (prepareHandover) *see Note 3 69 (prepareSubsequentHandover) *see Note 3 71 (anyTimeInterrogation) 72 (ss-Invocation-Notification) *see Note 1 76 (registerCcEntry) *see Note 4 77 (eraseCcEntry) *see Note 4 84 (sendGroupCallInfo) *see Note 2 85 (sendRoutingInfoForLCS) 86 (subscriberLocationReport) Note 1: Handling of this OpCode as Intra-PLMN (Category 1) or other depends on the context as described in section B.3.1.4 Note 2: The definition for ‘Category 1’ OpCodes 21, 36, 39, 40, 41, 42, 53 and 84 are covered in this Table under CugOpCodes Note 3: The definition for ‘Category 1’ OpCodes 28, 29, 30, 33, 34, 68 and 69 are covered in this Table under HandoverOpCodes Note 4: The definition for ‘Category 1’ OpCodes 76 and 77 are covered in this table under CcbsOpCodes
hPlmnOriginating (Category 2 features)		MAP OpCode = 3 (cancelLocation) 4 (provideRoamingNumber) *see Note 1 7 (insertSubscriberData) *see Note 1 8 (deleteSubscriberData) 18 (getPassword) *see Note 1 37 (reset) 38 (forwardCheckSsIndication) *see Note 1 44 (mt-forwardSM) *see Note 1 49 (alertServiceCentreWithoutResult) 50 (activateTraceMode)

Ref	Title	Description
		51 (deactivateTraceMode) 60 (sendUnstructuredSS-Request) *see Note 1 61 (sendUnstructuredSS-Notify) *see Note 1 63 (informServiceCentre) 64 (alertServiceCentre) 70 (provideSubscriberInfo) 73 (setReportingState) *see Note 2 75 (remoteUserFree) *see Note 2 83 (provideSubscriberLocation) 88 (istCommand) Note 1: Handling of this OpCode as hPlmnOriginating (Category 2) or other depends on the context as described in section B.3.1.4 Note 2: The handling as 'Category 2' for OpCodes 73 and 75 applies where CCBS is supported between networks and not screened anymore by the Rule "CCBS" as in section B.3.1.6 and associated definition in this table under CcbsOpCodes
vPlmnOriginating (Category 3 features)		MAP OpCode = 2 (updateLocation) *see Note 2 9 (sendParameters) *see Note 1 10 (registerSS) *see Note 1 11 (eraseSS) *see Note 1 12 (activateSS) *see Note 1 13 (desactivateSS) *see Note 1 14 (interrogateSS) *see Note 1 15 (authenticationFailureReport) 17 (registerPassword) *see Note 1 19 (processUnstructuredSsData) *see Note 1 23 (updateGprsLocation) *see Note 2 44 (mt-forwardSM) *see Note 1 45 (sendRoutingInfoForSM) 46 (mo-forwardSM) 47 (reportSMDeliveryStatus) 48 (noteSubscriberPresent) 54 (beginSubscriberActivityUSSDv1) 56 (sendAuthenticationInfo) 57 (restoreData) 59 (processUnstructuredSS-Request) *see Note 1 66 (readyForSM) *see Note 1 67 (purgeMS) 72 (ss-Invocation-Notification) *see Note 1 74 (statusReport) *see Note 4 87 (istAlert)

Ref	Title	Description
		89 (noteMmEvent) Note 1: Handling of this OpCode as vPlmnOriginating (Category 3) or other depends on the context as described in section B.3.1.4 Note 2: The special handling of 'Category 3' message UpdateLocation and UpdateGPRSLocation are described in section B.3.1.9 and not covered by this definition Note 4: The handling as 'Category 3' for OpCode 74 applies where CCBS is supported between networks and not screened anymore by the Rule "CCBS" as in section B.3.1.6 and the associated definition in this table under CcbsOpCodes
unusedOpCode		MAP OpCode = 0,1,16,27,78-82, 90-255
capIdp		CAMEL Application Part (CAP) messages IDP, IDP-SMS and IDP-GPRS
capImsi		IMSI within the CAMEL layer of the message
mapImsi		IMSI within the MAP layer of the message
ownMccMnc		List of IMSI prefixes (MCC+MNC) allocated to the protected network
MapOpCode		Each MAP Operation Code is contextualised within an application context typically. Note: See section B.3.1.10 for the handling of related abnormalities.
operatorByMap		OperatorID (e.g. TADIG code) referenced by all parameters in the MAP layer of the message comprising: IMSI HLR ID VLR ID gsmSCF address Note: An explicit identification of the OperatorID by MSISDN can't be achieved due to the effect of number portability. The MSISDN is only suited to retrieve the country code, see definition.
operatorByImsi		OperatorID (e.g. TADIG code) referenced by IMSI value
operatorByHlr		OperatorID (e.g. TADIG code) referenced by the MAP HLR-Number or SCCP CallingGT (CC+NDC) to the HLR instance of that operator in IR.21 [7]
operatorByVlr		OperatorID (e.g. TADIG code) referenced by the MAP VLR-Number or SCCP CallingGT (CC+NDC) to the VLR instance of that operator in IR.21 [7]
operatorByGsmScf		OperatorID (e.g. TADIG code) referenced by the MAP

Ref	Title	Description
		gsmSCF-Number or SCCP CallingGT (CC+NDC) to the gsmSCF instance of that operator in IR.21 [7]
countryByMsisdn		Country referenced by the country digits of the included MSISDN
operatorByGt		OperatorId (e.g. TADIG code) referenced by CallingGT (CC+NDC)
operatorByCgPA		OperatorId (e.g. TADIG code) determined by matching IR.21 [7] nodal GT ranges
operatorByMsc		OperatorId (e.g. TADIG code) referenced by the MAP MSC-Number or SCCP CallingGT (CC+NDC) to the MSC instance of that operator in IR.21 [7]
CugOpCodes		MAP OpCode = 21 (mt-ForwardSM-VGCS) 36 (cancelVcsgLocation) 39 (prepareGroupCall) 40 (sendGroupCallEndSignal) 41 (processgroupCallSignalling) 42 (forwardGroupcallSignalling) 53 (updateVcsgLocation) 84 (sendGroupCallInfo)
CcbsOpCodes		MAP OpCode = 73 (setReportingState) *see Note 74 (statusReport) *see Note 75 (remoteUserFree) *see Note 76 (registerCC-Entry) 77 (eraseCC-Entry) Note: The handling as ‘Category 2’ for OpCodes 73 and 75 and ‘Category 3’ for OpCode 74 applies where CCBS is supported between networks and not screened anymore by the Rule “CCBS” as in section B.3.1.6 and associated definition CcbsOpCodes
HandoverOpCodes		MAP OpCode = 28 (performHandover) 29 (sendEndSignal) 30 (performSubsequentHandover) 33 (ProcessAccessSignalling) 34 (forwardAccessSignalling) 68 (prepareHandover) 69 (prepareSubsequentHandover)
mixedSSmessage Cat1andCat2		MAP OpCode = 18 (getPassword) 38 (forwardCheckSsIndication)

Ref	Title	Description
		60 (unstructuredSS-Request) 61 (unstructuredSS-Notify)
mixedSSmessage Cat1andCat3		MAP OpCode = 10 (registerSS) 11 (eraseSS) 12 (activateSS) 13 (deactivateSS) 14 (interrogateSS) 17 (registerPassword) 19 (processUnstructuredSS-Data) 59 (processUnstructuredSS-Request) 72 (ss-Invocation-Notification)
Spoofing		Spoofing is an attack aiming to falsify an identity (spoof) forging messages which use it. The effect is that the attacker impersonate illegitimately the owner of the identity. In a SIGTRAN/SS7 network, a spoofing attack can occur at different protocol stack layers, for example at IP layer (if SIGTRAN is used), at SCCP layer or MAP layer for SS7 e.g. using global titles of an unconscious MNO. IP Spoofing is out of scope in this document. Note: Please also refer to IR.70 [2] and IR.71 [3] for the definitions of spoofing and faking in the context of SS7 signaling traffic.

Table 1 – SS7 definitions for firewall rules

B.3 SS7 Firewall Rules

The SS7 firewall rules in sections B.3.1.1 through B.3.1.10 cover the filtering of the MAP based category 1, category 2 and category 3 packet type vulnerabilities as described in both FS.07 [1] and IR.82 [5]. In addition, sections B.3.2.1 and **Error! Reference source not found.** provide the SS7 firewall rules to filter CAMEL-based category 2 and 3 vulnerabilities as described in IR.82 [5]. Lastly, sections B.3.3 through B.3.3.7 describe the rules and associated considerations that are general to both MAP and CAP messages.

The MAP related SS7 firewall rules reference the MAP packet risk classification table in Annex A for the categorisation of vulnerabilities. This table also outlines what MAP packets may be used for the different type of attacks (tracking, intercept, DoS, fraud and spam).

Please note that the descriptions in the GSMA documents above especially refer to the security issues with MAP v2 and MAP v3. Less priority is given to address the vulnerabilities that may be involved with MAP v1. This especially applies to the security risks with the MAP v1 related IMSI Attach procedure and the MAP Open service. It is observed that these older versions are more error prone and more sensitive to security risks so MAP v1 implementations may require specific attention. Handling of the MAP v1 specific

vulnerabilities by a SS7 firewall requires further study and is not covered in this version of the document.

The implementation of the SS7 firewall needs flexibility to add additional codes based on learning and/or updates suggested in future versions of PRD FS.07 [1] and IR.82 [5].

B.3.1 SS7 Firewall Rules for MAP

B.3.1.1 MAP Category 1

This rule covers the case:

- Blocking of MAP messages that are for intra-PLMN use only (GSMA PRD IR.82 [5])

In these cases, the MAP messages should be blocked on incoming routes.

Title	Rule	Rationale
MAP Cat 1	for each inbound message If MAP OpCode = intraPlmn and the CgPA is not on the GT whitelist then BLOCK	Block all received messages with MAP OpCode values in support of intra-network operations within the GT whitelist all addresses of intra-network MAP nodes

Table 2 – MAP Category 1 rule

B.3.1.2 MAP Category 2

This rule covers two cases:

- A category 2 MAP message (as per GSMA PRD IR.82 [5]) where the IMSI at MAP layer relates to one of the protected network's own customers
- A category 2 MAP message where the IMSI relates to an inbound roamer, but the operator id determined from the IMSI (i.e. MCC + MNC) at MAP layer is not consistent with that derived from the Calling GT at SCCP layer

Title	Rule	Rationale
MAP Cat 2a	for each inbound message, if MAP OpCode = hPlmnOriginating and mapImsi = ownMccMnc THEN BLOCK	Block all messages from home-PLMN messages where target IMSI is using the network's own MCC+MNC
MAP Cat 2b	for each inbound message, if MAP OpCode = hPlmnOriginating and operatorByMap != operatorByCgPA THEN BLOCK	Block all messages from home-PLMN for inbound roamers where OperatorID referenced by all parameters in MAP and OperatorID in CgPA do not match

Table 3 – MAP Category 2 rule

With an alternative solution for rule Cat 2b also cases of voice intercept and SMS intercept can be detected and stopped. This would require that the SS7 firewall maintains status of all inbound roamers and screen all inbound requests to known roamers when received from the

appropriate HLR address to detect (as a visitor network) via a consistency check between layers that a spoofed CgPA is used with a legitimate IMSI.

Though the MAP risk classification in Annex A and IR.82 [5] identify MAP Reset as a Category 2 message, the format of the MAP Reset message requires special handling. In case of a MAP Reset the HLRid (indicated by operatorByMap) may be repeated multiple times.

Title	Rule	Rationale

MAP Reset	for each inbound message
	if MAP OpCode = reset then
	if OperatorByHlrId != OperatorByCgPA then
	BLOCK
		If ANY HLRid is not consistent with the CgPA then the message should be blocked

Table 4 – MAP Reset rule

B.3.1.3 MAP Category 3

According to GSMA PRD IR.82 [5], the SS7 firewall needs to check MAP messages that normally only be received in relation to an outbound roaming subscriber from the visited network that the subscriber is currently roaming in.

Title	Rule	Rationale
MAP Cat 3a	for each inbound message, if MAP OpCode = vPlmnOriginating and operatorByMap != operatorByCdPA THEN BLOCK Else if MAP OpCode = vPlmnOriginating and operatorByMap != OperatorByHLR THEN BLOCK	Block messages in relation to outbound roaming subscribers where MCC+MNC of IMSI and CdPA or prefix ID of the HLR do not match
MAP Cat 3b	if MAP OpCode = vPlmnOriginating and operatorByVlr != operatorByCgPA THEN BLOCK	Block messages in relation to outbound roaming subscribers where VLR Id and CgPA do not match

Table 5 – MAP Category 3 rule

With an alternative solution for rule Cat 3b, certain attacks on the HLR using an invalid VLR id can be detected and stopped. This would require that the SS7 firewall stores the VLR id of all outbound roamers during updateLocation dialogs and screen requests with certain OpCodes originating from the VPLMN if the currently valid VLR id is used.

See section B.3.1.9 for further details of the specific rule that applies to the handling of the ‘Category 3’ MAP messages UpdateLocation and UpdateGPRSLocation which requires specific treatment.

B.3.1.4 Specific Handling of Mixed Category MAP Messages

Depending on the circumstances, a MAP message may only be allowed intra-network or may be permitted inter-network and require more checks for consistency or location. The detailed MAP packet risk classification table in Annex A indicates under what circumstances extra checks are needed and therefore specifies the category based on the MAP message AND full context (i.e. OpCode, version, sending and receiving subsystem, and application context).

In general, the higher category (i.e. more checks) should be referred to if in any context a MAP message is of that category.

Some MAP messages may require a specific handling by the SS7 firewall rules depending on the context in which these are transferred. This applies to the Note 1 messages in the list of definitions in section B.2 for “intraPlmn”, “hPlmnOriginating” and “vPlmnOriginating”.

Please note that this section may not be exhaustive in listing all mixed-category operations.

B.3.1.4.1 MAP OpCode 4 - ProvideRoamingNumber

This message should be classified in the general case as category 2 (although if sent from VLR to VLR this should be considered category 1), as follows:

- Category 1 - when received from a VLR, the MAP packet can be used to pass information associated with the handover of active calls. Where a network does not support handover across network boundaries, these messages should be blocked
- Category 2 - when received from an HLR, the MAP message needs to be screened for abuse of Category 2 vulnerabilities

Title	Rule	Rationale

MAP provideRoaming Number Cat 1	`for each inbound message,`
	`  if MAP OpCode = 4 (provideRoamingNumber) and`
	`  the CgPA is not on the GT whitelist and`
	`  ssn in CgPA = vlr THEN`
	`  BLOCK`
		Block received VLR-to-VLR provideRoamingNumber packets within the GT whitelist all addresses of intra-network MAP nodes

MAP provideRoaming Number Cat 2a	`for each inbound message,`
	`  if MAP OpCode = 4 (provideRoamingNumber) and`
	`  ssn in CgPA = hlr and`
	`  mapImsi = ownMccMnc THEN`
	`  BLOCK`
		Block received HLR-to-VLR provideRoamingNumber packets according the Cat 2a Rule

MAP provideRoaming Number Cat 2b	`for each inbound message,`
	`  if MAP OpCode = 4 (provideRoamingNumber) and`
	`  ssn in CgPA = hlr and`
	`  operatorByMap != operatorByCgPA THEN`
	`  BLOCK`
		Block received HLR-to-VLR provideRoamingNumber packets according the Cat 2b Rule

Table 6 – MAP ProvideRoamingNumber rules

B.3.1.4.2 MAP OpCode 7 - InsertSubscriberData

This message should be classified in the general case as category 2 (although in some contexts as defined in Annex A this should be considered as category 1), as follows:

- Category 1 - when addressed to a VLR, the MAP packet can be used as part of the CUG and GroupCall services. Where CUG and GroupCall services are not supported across network boundaries, these MAP messages should be blocked
- Category 2 – in other cases the MAP message can be used to push subscriber data for a roaming subscriber and needs to be screened for abuse of category 2 vulnerabilities

Title	Rule	Rationale
MAP insertSubscriberData Cat 1	for each inbound message, if MAP OpCode = 7 (insertSubscriberData) and the CgPA is not on the GT whitelist and AC = 46 (vgcsLocationUpdate) THEN BLOCK	Block insertSubscriberData packets with application context vcsgLocationUpdate within the GT whitelist all addresses of intra-network MAP nodes
MAP insertSubscriberData Cat 2a	for each inbound message, if MAP OpCode = 7 (insertSubscriberData) and AC = 16 (subscriberDataMngt) or AC = 1 (networkLocUp) or AC = 32 (gprsLocationUpdate) and mapImsi = ownMccMnc THEN BLOCK	Block insertSubscriberData packets with application context values 16, 1 or 32 according the Cat 2a rule
MAP insertSubscriberData Cat 2b	for each inbound message, if MAP OpCode = 7 (insertSubscriberData) and AC = 16 (subscriberDataMngt) or AC = 1 (networkLocUp) or AC = 32 (gprsLocationUpdate) and operatorByMap != operatorByCgPA THEN BLOCK	Block insertSubscriberData packets with application context values 16, 1 or 32 according the Cat 2b rule

Table 7 – MAP InsertSubscriberData rules

B.3.1.4.3 MAP OpCode 9 - SendParameters

This message should be classified in the general case as category 3 as it is typically addressed to the HLR (although if sent between VLRs this should not leave the network and would be considered category 1);

- Category 1 - when addressed to a VLR, the MAP packet can be used to pass information associated with the handover of active calls. Where a network does not

support handover across network boundaries, these MAP messages should be blocked

- Category 3 - when addressed to an HLR, the MAP message can be used to request authentication vectors and subscriber data. Blocking of these MAP messages would have an adverse impact on roaming with networks that use this old format

Title	Rule	Rationale
MAP sendParameters	for each inbound message, if MAP OpCode = 9 (sendParmeters) and the CgPA is not on the GT whitelist then if ssn = vlr of the CdPA then BLOCK Else if ssn = hlr of the CdPA AND RequestParameter = 0 OR RequestParameter > 2 THEN BLOCK	Block sendParameters packets based on Cat.1 handling if the packet is addressed to a VLR Block SendParameters packets based on Cat.1 handling if the packet is addressed to a HLR and if requestIMSI (“0”, similar to sendIMSI) or all values > 2 including requestKi (“4”). For other RequestParameter values (if SendParameters addressed to a HLR) base on Cat.3 handling.

Table 8 – MAP SendParameters rules

NOTE Please note that the RequestParameter field is an enumerated list and can contain 1 or 2 values at the same time. Therefore, these checks should be applied to both values if they are included.

B.3.1.4.4 MAP OpCode 44 – MT-ForwardSM

Messages with MAP OpCode 44 are classified as both category 2 and category 3 packets. This implies that these messages require SS7 firewall rules handling as defined in either B.3.1.2 or B.3.1.3, respectively, depending on the type of message flow.

B.3.1.4.5 MAP OpCode for mixed SS messages Cat.1 and Cat.2

These messages should be classified as category 2 if sent by a HLR. In other cases, this message type is used for internal network purposes i.e. sent by VLR or gsmSCF, and to be considered as category 1.

Title	Rule	Rationale

MAP ss-Cat1andCat2	for each inbound message,
	if MAP OpCode = mixedSSmessageCat1andCat2 and
	if ssn = hlr of the CgPA then
	if mapImsi = ownMccMnc THEN
	BLOCK
	If operatorByMap != operatorByCgPA THEN
	BLOCK
	Else if the CgPA is not on the
	GT whitelist THEN
		Block SS-related MAP packets needing Cat.2 handling when received from a HLR
		
		Block on Cat.1 handling in other cases

Title	Rule	Rationale
	BLOCK	

Table 9 – MAP SS-Cat1 and Cat2 rules

B.3.1.4.6 MAP OpCode for mixed SS messages Cat.1 and Cat.3

These messages should be classified as category 3 if sent by a VLR. In other cases, this message type is used for internal network purposes i.e. sent by MSC or HLR, and to be considered as category 1.

Title	Rule	Rationale

MAP ss-Cat1andCat3	for each inbound message,
	if MAP OpCode = mixedSSmessageCat1andCat3 and
	if ssn = vlr of the CgPA then
	if operatorByMap != operatorByCdPA THEN
	BLOCK
	If operatorByMap != OperatorByHLR THEN
	BLOCK
	If operatorByVlr != operatorByCgPA THEN
	BLOCK
	Else if the CgPA is not on the
	GT whitelist THEN
	BLOCK
		Block SS-related MAP packets needing Cat.3 handling when received from a VLR
		
		Block on Cat.1 handling in other cases

Table 10 – MAP SS-Cat1 and Cat3 rules

B.3.1.4.7 MAP OpCode 66 - ReadyForSM

These messages should be classified as category 3 if sent to a HLR. In other cases, this message type is used for internal network purposes i.e. sent by MSC, and to be considered as category 1.

Title	Rule	Rationale

MAP readyForSM	for each inbound message,
	if MAP OpCode = 66 (readyForSM) and
	if ssn = hlr of the CdPA then
	if operatorByMap != operatorByCdPA THEN
	BLOCK
	If operatorByMap != OperatorByHLR THEN
	BLOCK
	If operatorByVlr != operatorByCgPA THEN
	BLOCK
	Else if the CgPA is not on the
	GT whitelist THEN
	BLOCK
		Block MAP readyForSM packets needing Cat.3 handling when send to a HLR
		
		Block on Cat.1 handling in other cases

Table 11 – MAP ReadyForSM rules

B.3.1.5 MAP GroupCall / CUG

Where GroupCall and CUG functions are not supported across network boundaries, the MAP operations associated with these functions can be blocked. There is no known vulnerability in these MAP messages, but this rule is based on the 'least privilege' approach.

Title	Rule	Rationale
MAP GroupCall	for each inbound message, if MAP OpCode = CugOpCodes and the CgPA is not on the GT whitelist then BLOCK	Block all received messages with GroupCall related MAP OpCodes in support of intra-network within the GT whitelist all addresses of intra-network MAP nodes

Table 12 – MAP GroupCall rule

B.3.1.6 MAP CCBS

Where CCBS is not supported across network boundaries, the MAP operations associated with these functions can be blocked. There is no known vulnerability in these MAP messages, but this rule is based on the 'least privilege' approach.

Title	Rule	Rationale
MAP CCBS	for each inbound message, if MAP OpCode = CcbsOpCodes and the CgPA is not on the GT whitelist then BLOCK	Block all received messages with CCBS related MAP OpCodes in support of intra-network within the GT whitelist all addresses of intra-network MAP nodes

Table 13 – MAP CCBS rule

B.3.1.7 MAP gsmSCF

For the support of CAMEL services within an operator group the SS7 firewall is proposed to support the following Rule for the CAMEL related MAP OpCode for SubscriberData.

Title	Rule	Rationale
MAP CamelService	for each inbound message, if MAP OpCode = insertSubscriberData and operatorByImsi != operatorByGsmScf and the CgPA is not on the GT whitelist then BLOCK	Stops 3rd parties place their own CAMEL triggers on a subscriber to intercept mo/mt calls.

Table 14 – MAP gsmSCF rule

B.3.1.8 MAP Handover

Where call handover between networks is not supported, the MAP operations associated with these functions can be blocked.

Title	Rule	Rationale
MAP Handover	for each inbound message,	Block all received messages with

Title	Rule	Rationale
	if MAP OpCode = HandoverOpCodes and the CgPA is not on the GT whitelist then BLOCK	Handover related MAP OpCodes in support of intra-network within the GT whitelist all addresses of intra-network MAP nodes

Table 15 – MAP Handover rule

B.3.1.9 MAP 'Reasonableness' / 'Velocity' Check

This section proposes different handling of the MAP UpdateLocation message as well as the MAP UpdateGPRSLocation message, both of which are defined in GSMA PRD IR.82 [5] as category 3 messages. These MAP operations can be blocked based on the 'reasonableness' of the MAP message considering the last known location.

This 'reasonableness' / 'velocity' check rule applies to comparing the VLR address in the inbound MAP UpdateLocation, MAP UpdateGPRSLocation or MAP SendAuthentication message with the VLR address last known. The last known VLR address can be retrieved either:

- The VLR address stored in the SS7 firewall based on stateful monitoring of the SS7 transactions by the SS7 firewall by monitoring all outbound UpdateLocation MAP operations and updating an internal database based on successful location updates.
- By HLR lookup to retrieve the VLR address stored in the HLR. This scenario may require additional protection of the HLR against mass queries by the SS7 firewall instances in case of DDOS attacks. The use of a HLR lookup to retrieve the VLR address can be further expanded if the HLR is instructed to actively 'page' the subscriber. This can potentially determine if the subscriber is still active at its old stored VLR location.

If distinct, checking the locations of the different VLRs with plausibility data to determine if the velocity between old fix and new fix is within an acceptable range (e.g. shortest great-circle distance between closest possible subscribe locations).

Title	Rule	Rationale
MAP UpdateLocation MAP UpdateGPRSLocation MAP SendAuthentication	for each inbound message, if MAP OpCode = UpdateLocation, UpdateGPRSLocation or SendAuthentication and the CgPA is not on the GT whitelist then if VLR in CgPA or SGSN in CgPA is not reasonable to last known destination then BLOCK	Block inbound UpdateLocation, UpdateGPRSLocation and SendAuthentication packets if the received VLR or SGSN address in the CgPA is not reasonable compared with the last known location

Table 16 – MAP Reasonableness / velocity check rule

B.3.1.10 Application Context and MAP versions

The MAP OpCode which is the key identifier for MAP category 1 or 2 threats. Recommendations and evidence to date tells us that using the MAP OpCode alone is sufficient to apply rules to such MAP messages.

It is however anticipated that the application context which the MAP operation is associated with may provide the environment to carry out different attacks. Therefore, the application context identifier should be taken into account from a rules definition perspective as a possible factor in the rule definition for the MAP operation. Furthermore, anomalies may be distinguishable by the absence of the application context identifier, the OpCode value or even both.

B.3.2 SS7 Firewall Rules for CAMEL

B.3.2.1 CAMEL Category 3

For an inbound roamer, the CAMEL Initial Detection Point (IDP) messages (and subsequent TCAP dialogues) should be sent to the roaming subscriber's home network SCF (unless VAS are provided externally)

Title	Rule	Rationale

CAMEL category 3	for each outbound message,
	if CAP OpCode = capIdp and
	CdPA is not in WhiteListGT then
	if operatorByIMSI != operatorByGsmScf then
	BLOCK
	if countryByMsisdn != countryByGsmSCF then
	BLOCK
		Block all types of IDP unless CdPA is the subscribers home network (unless on whitelist for IDPs)
		
		Block all types of IDP unless the CdPA (MSISDN) matches destination country

Table 17 – CAMEL Category 3 Outbound rule

For outbound roamers CAP IDP messages (and the subsequent dialogues) should only be received in relation to an MNO's own subscribers, and originate from the correct location (VLR).

Title	Rule	Rationale

CAMEL category 3	for each inbound message,
	if CAP OpCode = capIdp and
	if CgPA is not in WhiteListGT then
	if CapImsi != ownMccMnc then
	BLOCK
	If operatorByVlr != operatorByCgPA
	BLOCK
	If operatorByMsc != operatorByCgPA then
	BLOCK
	if VlrId != current VlrId then
	BLOCK
		Check own subscriber
		
		Check VLR address consistency
		
		Check MSC address consistency
		
		Check Cg SCCP VLR address comes from last known location (from HLR query or from tracking location updates)
		
		(velocity check would be performed on update of

Title	Rule	Rationale
		location)

Table 18 – CAMEL Category 3 Inbound rule

B.3.3 SS7 Firewall Rules for MAP and CAMEL

B.3.3.1 GT Screening

Although GT screening is an obvious protection action to be implemented by an operator, this rule covers a cases that is not explicitly stated in IR.82:

The effect of GT spoofing for which the rule is defined is described in section B.3.3.5. The rule is summarised as follows:

- Do not allow messages with a calling GT that is not associated with either:
  - a network element with a GT relationship in the own network (please see the text following Table 19 for a clarification of the service levels involved).
  - a roaming partner
- Do not allow messages with a calling GT that is on the black list of GTs
- Pass on messages with a calling GT that is on the white list of GTs

NOTE Combinations of these rules may apply. For example, the “pass on” action per white list of GTs may take precedence over the other GT screening actions. This refers to situations where messages from a specific GT instance are allowed, even though its GT address is not part of the GT addresses associated with a roaming partner.

Title	Rule	Rationale

Block own network GTs	`for each inbound message,`
	`  if CgPA = ownNetworkGTlist then`
	`  BLOCK`
		Block all received messages with a Calling GT address that have a relationship in the own network (see the exceptions hereafter)

Block non-roaming partner GTs	`for each inbound message,`
	`  if CgPA != roamingPartnerGTlist then`
	`  BLOCK`
		Block all received messages with a Calling GT address without a relationship of roaming partners

Block Black Listed GTs	`for each inbound message,`
	`  if CgPA = blackListGT then`
	`  BLOCK`
		Block all received messages with a Calling GT address that is registered on the black list of GTs

Allow White Listed GTs	`for each inbound message,`
	`  if CgPA = whiteListGT then`
	`  PASS ON`
		Pass on all received messages with a Calling GT address that is registered on the white list of GTs

Table 19 – GT screening rules

Different levels of service are agreed between mobile operators, for example:

- Basic inbound/outbound roaming

- Roaming with CAMEL services
- SMS interworking only

Depending on the service, different nodes will need to communicate between the networks (e.g. for an SMS termination service, a distant SMSC will need to communicate with local HLR and VLR resources). Complying with the security principle of 'least privilege', a signalling firewall may be configured to restrict nodes and message types to those strictly necessary to support the commercially agreed services.

There are a number of scenarios where the GT that originates a message may not directly correlate with the user identities within the message For example:

- Where an operator group chooses to centralise services for their networks on a shared platform;
- Where a network chooses to use the services of an SS7 hub provider; or
- Where a network relies on an 'inter-standard roaming' platform

Rules implemented on a SS7 firewall need to take account of these valid scenarios.

B.3.3.2 No OpCode present and Unused OpCodes

This rule covers a number of cases;

- Blocking messages with no OpCode present in the message,
- Blocking of messages with OpCodes that are not defined in 3GPP TS 29.002 [4].

Title	Rule	Rationale

No OpCode present	`For each inbound message`
	`  If no MAPOpCode is present then`
	`  BLOCK`
		Block all received messages that do not include a MAP OpCode (see also Note 1)

Unused OpCodes	`For each inbound message`
	`  If MAPOpCode = unusedOpCode then`
	`  BLOCK`
		Block all received messages that include an undefined MAP OpCode value (see also Note 2)

Table 20 – OpCode rules

Note 1 For some operations a TC-BEGIN may be sent with no OpCode but included in a TC-CONTINUE message because TC handshake is a valid anti-spoofing function to ensure two-way communication before accepting requests.

For example, the omission of the OpCode in a TC-BEGIN is a valid anti SMS fraud check. It has a SMS application content (shortMsgMT-RelayContext-v2).

Hence the SS7 firewall logic should always check on MAP OpCode in conjunction with the application context.

Note 2 In specific cases non-defined OpCode values are used for specific services within networks or between networks.

B.3.3.3 TC Transactions

The SS7 firewall could be implemented to monitor all open TC dialogues and subsequently block all related messages if TCAP messages are received without context or when other irregularities are detected as part of the dialogue handling for the TC transactions.

- For each TC_BEGIN, a new entry in a list needs to be stored including CgPA, CdPA, OTID and application context
- For each TC-CONTINUE, an existing entry in the list needs to be present conforming the stored TC dialogue parameter values, and to be updated with the DTID.
- For each TC-END or TC-ABORT, an existing entry need to be deleted that conforms the stored TC dialogue parameter values.
- If no entry can be found for a received TC-DIALOGUE, TC-END or TC-ABORT, the inbound message is suspicious and needs to be blocked and logged. Also an alert should be configured because it can be used to detect GT spoofing.

Real-time distribution of stateful information between the SS7 firewall instances present in a network helps to ensure more effective and accurate operation of the total SS7 firewall solution, and avoids false warnings and false positives because SS7 routing is asymmetric and is subject to hysteresis.

In addition, please note that stateful behaviour checks by the SS7 firewall can be envisaged as part of the following 3 protocol layers:

- Stateful information at the SCTP protocol layer
- Stateful information as part of the TCAP protocol layer
- Stateful information as part of the MAP / CAP protocol layer.

B.3.3.4 Consistency SS7 layers

The SS7 firewall could be implemented to check for consistency of the information between the SS7 layers based on session stateful checks between:

- The GT addresses at the SCCP level and the addresses at the MAP level
  The SSN value at the SCCP level and the type of network element (HLR, VLR, …) transaction in the message at the MAP / CAP level

In case of irregularities, the SS7 firewall could terminate the TC transaction and block all related MAP / CAP messages.

B.3.3.5 GT Spoofing

The SS7 firewall should implement anti-spoofing rules able to be able to block MAP / CAP messages with spoofed identities/data (e.g. GT) belonging to external PLMNs and detect the improper use of the identities/data (spoofing) of the internal PLMN.

In particular, to detect the spoofing of the identities/data (spoofing) of the internal PLMN, the SS7 firewall should be able to:

- Check that any received response message is correlated to a sent request.
- Detect and block messages where the CgPA and CdPA GTs are in the same destination HPLMN range.

- Enable this check for each protocol stack layer
- Enable alerting.

To detect spoofing of external PLMN, the SS7 firewall should be able to:

- Detect and block MAP / CAP messages with an unexpected SS7 MTP3 point code
- Detect and block MAP /CAP messages with a SS7 MTP3 point code expected for the invoked MAP / CAP procedure but unexpected for the used CgPA. See also the profiling checks in section B.3.3.6.
- Insert dialogue (e.g. a TCAP continue) to validate CgPA.

B.3.3.6 Profiling Checks based on Correlating Messages

The SS7 firewall detection capabilities could be further refined with equipment profiling by inspecting the MAP / CAP messages exchanged. This profiling can be either based on:

- Static information being provisioned in the SS7 firewall like the GT and SSN as documented in IR.21 [7]
- Automated learning by active monitoring of the MAP / CAP messages exchanged between the equipment.

The SS7 firewall is then in a position to use this profiling information to flag abnormalities if different information is detected than normally would be expected like:

- On the equipment profile the MAP messages received from a specific GT would infer the sending node is a VLR
- Assuming the sending node is profiled as a VLR then it is allowed to send specific MAP OpCodes only.

This assessment of being a VLR is independent of the SSN and other information contained in the message, and thus it is more likely to accurately detect potential abnormalities. With learning, it may offer mobile operators the ability to detect abnormalities without the need to perform up-to-date provisioning of the SS7 firewall because the profiling data is automatically learned, and via the flagged changes the operator can grant updates of the learned profile changes.

B.3.3.7 GT Hierarchy

The definition of GT ranges may be considered with a multi-level hierarchy of the GT list concept in conjunction with the rules sets provisioned in the SS7 firewall.

Figure 1 shows an example GT hierarchy in support of a particular operator situation (not one consistent hierarchy for all operators) consisting of a 5-level hierarchical classification scheme for GTs that may be used as follows:

- The top level is all roaming partners.
- 2nd level is operator groups (e.g. Vodafone/Deutsche Telekom/Telefonica/Orange) OR service groups (e.g. standard roaming, CAMEL roaming, SMS interconnect etc.)
- 3rd level is at the market level (e.g. Vodafone UK, Vodafone Germany, Telefonica Spain)
- 4th level is the set of GTs that are associated with the market

- 5th level is that gtSets are made from individual GTs, contiguous ranges of GTs, or more gtSets

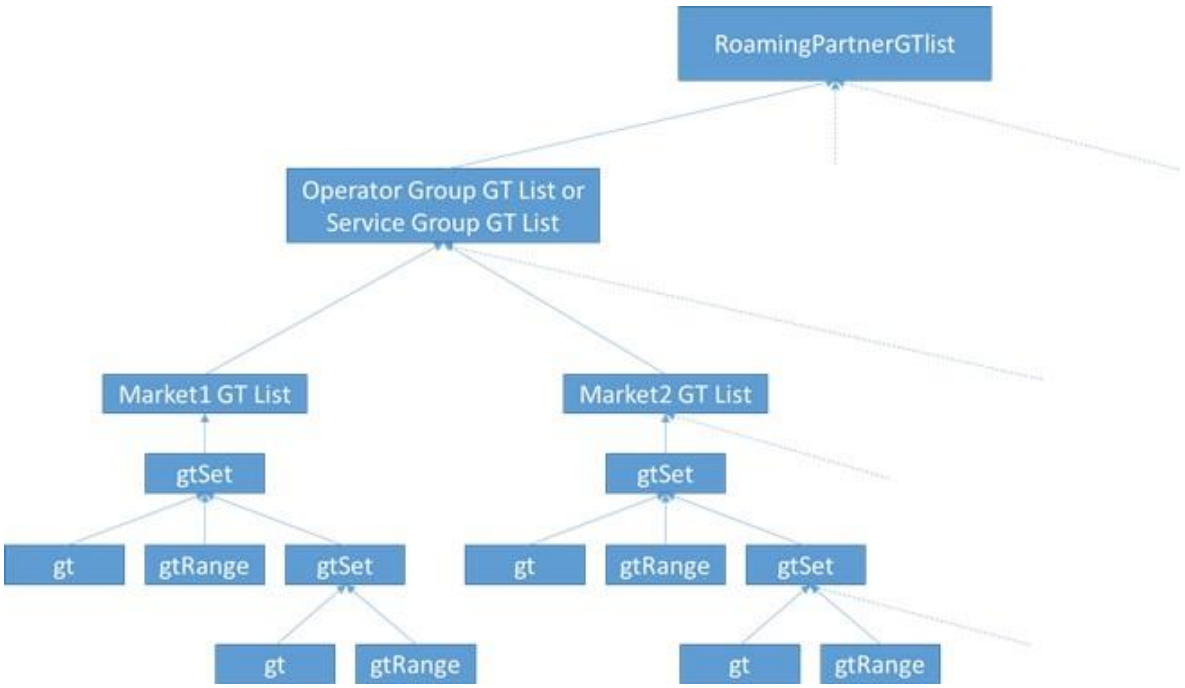

Figure 1 – GT Hierarchy

Having the flexibility to define rules for different parts of the hierarchy tree may ease the operation of the firewall application, as some operators may prefer a split based on operator group, while others may choose to split based on services (e.g. CAMEL roaming networks, CCBS networks etc.).

This proposed hierarchical classification scheme for GT ranges in a GT hierarchy is under consideration between different groups in the GSMA. The aim is that this proposed GT hierarchy becomes adopted for the data being recorded in GSMA IR.21. A future version of this document will reflect the outcome of this study.

B.4 Firewall Data Sharing

B.4.1 General

The aim of this section is to provide advice on standard contents and formats of logging data generated by the SS7 signaling firewall as a result of the firewall rules execution service logic as specified in section B.3. This may ease both the integration of the signaling firewall with other technical elements like third party systems for analytics and reporting, and sharing information between operators to quickly implement protection against vulnerabilities and new threats.

Such data may be generated in real-time for the interfaces with analytics systems in order to facilitate immediate alarming of new vulnerabilities. Solutions like Internet Protocol Flow Information Export (IPFIX) as defined in IETF RFC 7011 [8] may be considered for this purpose. This universal IETF standard will facilitate the formatting and transfer of the data

streams of multiple firewall instances to a central collector for further processing. The data to monitoring systems may be near real-time or offline as this refers to aggregated data.

B.4.2 SS7 Firewall Data Sharing

The specification of the SS7 firewall data sharing in this section refers to the SS7 firewall rules in section B.3 in conjunction with elements of the SS7 signalling messages.

B.4.3 Data Sharing for SS7 Analytics

This refers the data generated by the SS7 firewall where the SS7 firewall rules execution service logic detects violations of which the details need to be reported. The reported data should contain all relevant details associated with the specific SS7 vulnerability occurrence and the handling by the SS7 firewall.

The specification below provides a general format that equally applies to the individual rules in section B.3. The advised format below is based on the SS7 firewall rule in section B.3.1.1 (MAP Category 1) as an example.

Field	Value
SS7 Firewall Rule (name as in Rule table)	MAP Cat 1
• Action (Passed or Blocked)	Blocked
○ Associated return action	With
○ OpCode in return message	###
○ …	…
• Calling GT details:	…
○ GT address	…
○ SSN value	…
○ MTP3 address	…
○ Incoming SS7 LS	…
○ …	…
• Called GT details	…
○ GT address	…
○ SSN value	…
○ MTP3 address	…
○ Incoming SS7 LS	…
○ …	…
• TC details	…
○ Message type	TC-Begin
○ Application Context value	…
○ Component type	Invoke
○ …	…
• MAP details	…
○ Operation	…

Field	Value
○ OpCode value	…
○ …	…

Table 21 – Example data sharing format for SS7 analytics

B.4.4 Data Sharing for SS7 Monitoring

This refers to the data generated by the SS7 firewall for KPI reports, statistics, etc. This should contain aggregated data associated with the execution of the SS7 firewall rules.

The specification below provides a general format that equally applies to the individual rules in section B.3. The advised format below is based on the SS7 firewall rule in section B.3.1.1 (MAP Category 1) as an example.

Field	Value
SS7 Firewall Rule (name as in Rule table)	
• Passed Normal	
○ MAP OpCode a	
▪ CgPA z	
▪ …	
○ MAP OpCode b	
▪ CgPA y	
▪ …	
○ …	
• Passed Monitor	
○ MAP OpCode c	
▪ CgPA x	
▪ …	
○ MAP OpCode d	
▪ CgPA w	
▪ …	
○ …	
• Blocked Silently	
○ MAP OpCode e	
▪ CgPA v	
▪ …	
○ MAP OpCode f	
▪ CgPA u	
▪ …	
○ …	
• Blocked with Error	
○ MAP OpCode g	

Field	Value
▪ CgPA t	
▪ …	
○ MAP OpCode h	
▪ CgPA s	
▪ …	
○ …	

Table 22 – Example data sharing format for SS7 monitoring

Annex C Document Management

C.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	19 Nov 2015	First approved version.	PSMC	Cathal Mc Daid, AdaptiveMobile
2.0	23 Jun 2016	Added Annex on SCCP CallingPartyAddress (CgPA) Spoofing	FASG	Rosalia D'Alessandro, Telecom Italia
3.0	16 Nov 2016	Added SS7 firewall rule and data sharing recommendations. Development and alignment with PRDs FS.07 and IR.82	FASG	Pieter Veenstra, NetNumber Cathal Mc Daid, AdaptiveMobile
3.1	5 May 2017	Added notes on category 2 outbound monitoring and intra-packet correlation	FASG	Cathal Mc Daid, AdaptiveMobile
3.2	20 Sep 2017	Error correction in section 3.3.1. "…*For outgoing MAP packet requests: Comparing **CgPA** and the IMSI or MSISDN within the MAP layer*…"	FASG	Cathal Mc Daid, AdaptiveMobile
4.0	4 May 2018	Expansion of Annex A text, addition of CAMEL Sheet, added category 2 home network + category 3 location correlation notes, & minor corrections in packet classifications.	FASG	Cathal Mc Daid, AdaptiveMobile Martin Kacer, P1 Security

C.2 Other Information

Type	Description
Document Owner	GSMA Fraud and Security Group (FASG)
Editor / Company	Cathal Mc Daid, AdaptiveMobile

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.