sinch

SMS 365 International SMS Product Description

Version 4.6 – January 2021

sinch.com

Table of Contents

1 Introduction **2**
2 Executive Summary **3**
3 Global SMS Network **6**
3.1 Network Operations Centre 6
4 Functional Description **8**
4.1 Block Diagram 8
4.2 GSM MAP Connectivity 9
4.2.1 Relay Mode 9
4.2.2 Transparent Mode 10
4.3 Retry Capability 11
4.4 Anti-Spoofing Functionality 12
4.5 Anti-SPAM Functionality 13
4.5.1 Statistical Based Detection & Blocklisting 13
4.5.2 Manual Block by Customer Request 14
4.5.3 Keyword Based Detection 14
4.5.4 Repeated Content Based Detection 15
4.5.5 Global Threat Database 15
4.5.6 SPAM Detection Procedures 15
4.6 SMS 365 Connectivity Options for Originating Operators 16
4.6.1 Direct HLR Addressing 16
4.6.2 Prefix Addressing 17
4.6.3 Short Messaging Peer-to-Peer (SMPP) 18
4.6.4 SIGTRAN 18
4.7 Mobile Number Portability 20
4.8 Intelligent Hubbing 365 22
4.8.1 Intelligent Hubbing 365 Message Flow 23
4.9 Messaging Proxy 365 24
5 GSMA Open Connectivity **25**
6 Message Detail Records **27**
6.1 MDR Accounting and Procedures 27
6.2 MDR Format 28
6.2.1 Ticket Code 29
6.2.2 Error Code 29
7 Reporting **30**
8 Message Flows **32**
8.1 SS7 End to End Delivery – Mobile Originator to GSM Subscriber in Home PLMN 32
8.2 SS7 End to End Delivery – Mobile Originator to GSM Roaming Subscriber – Scenario 1 33
8.3 SS7 End to End Delivery – Mobile Originator to GSM Roaming Subscriber – Scenario 2 34
8.4 SS7 End to End Delivery – Mobile Originator to GSM Roaming Subscriber – Scenario 3 35
8.5 SS7 to SMPP Delivery – Similar for other IP Based Protocols 36
8.6 SMPP to SS7 Delivery – Similar for other IP Based Protocols 37
8.7 Intelligent Hubbing 365 – If Destination Operator is on Preferred List 38
8.8 Intelligent Hubbing 365 – If Destination Operator is not on Preferred List 39
8.9 Intelligent Hubbing 365 – with Origin MCC/MNC Post-Pended 40

1 Introduction

SMS 365 provides solution sets to meet the needs of virtually any operator around the world and the focused concept provides regional and global markets a tailored solution designed for specific business models and technical requirements.

The solution-based capabilities of Sinch’s inter-carrier SMS interoperability suite provides the best mix of features for any one operator. Capabilities required by one operator in a specific region may not apply to operators in other regions. Additionally, in different parts of the world, business models are different. SMS 365 is an extremely flexible set of features that provide reach and reliability for global inter-carrier SMS interoperability.

SMS 365 hosted in the US provides inter-carrier SMS interoperability for operators in North America, Latin America and South America, along with domestic interoperability and connectivity into North America (USA and Canada).

SMS 365 hosted in Paris, France, provides a very flexible global SMS interoperability solution for operators throughout the world.

2 Executive Summary

SMS 365 provides a reach into more than 1000 operators worldwide. This is accomplished by its global connectivity into wireless networks at major points in France and the US. For wireless operators connecting to SMS 365 for SMS interoperability services, the key benefit is the ability to route messages to virtually any operator in the world and across technologies.

SMS 365‘s global SMS connectivity makes it possible for operators to resolve issues such as routing messages from roaming subscriber to recipient subscribers (either in their Home network or roaming), almost anywhere in the world. In addition, by utilizing multiple connectivity points throughout the world, SMS 365 is able to provide delivery capabilities into significantly more networks than single operators would be able to provide individually.

SMS 365 provides operators – especially those connecting via GSM MAP over SS7 – a number of unique capabilities including:

1. GSM MAP Connectivity (all SMS related MAP commands are supported). Two types of service options are available for GSM MAP Customers:
   a. Relay Mode – with this method, SMS 365’s is acting as a full-fledged SMSC. In the SRI response to the customer, the MSISDN is returned as the IMSI value and SMS 365‘s Global Title is returned as the MSC value. If the SRI or FSM response from the destination operator contains a permanent error, then this error is returned immediately back to the customer. If a temporary error (for example, absent subscriber) is returned, then SMS 365 will store the message and retry it as necessary.
   b. Transparent Mode – customers that sign up for the transparent service are responsible for the store and forward operations. In this model, SMS 365 is acting as a roaming agreement between the source and destination operators.

2. SMPP for both client and server roles.

3. Web based provisioning system and advanced troubleshooting interface used by the provisioning or customer care personnel.

4. A very flexible routing capability:
   a. Routing based on static numbering tables,
   b. Routing based on IMSI,
   c. Re-routing based on the Visited MSC (for roaming subscribers),
   d. Routing based type of traffic – Peer to Peer (P2P) or Application to Peer (A2P).

5. Routing based on Mobile Number Portability (MNP), including integration with Sinch’s comprehensive Number Resolution System (NRS) that is used to manage all country numbering plans including MNP countries.

6. Sophisticated Anti-Spoofing capabilities including support for specific operators as well as a global anti-spoofing capability. Anti-spoofing is also standard on any SMPP over IP links.

7. SPAM protection through:
   a. Allow lists/Blocklists by operator
   b. Management of the resolution process after SPAM detection

8. Comprehensive and Detailed Reporting – SMS 365 has a reporting interface called Report Manager, that provides near-real-time to real-time reporting.

9. Fully compliant with the GSMA Open Connectivity SMS Hubbing – IR.75:
   a. GSMA Self Certified
   b. Single Multilateral Agreement replacing Bilateral Agreement (AA.71)
   c. End-to-End Delivery
   d. Pricing Transparency
   e. Multilateral Settlement
   f. Testing

10. Intelligent Hubbing 365 – the Intelligent Hubbing service enables mobile operators to have the best of both worlds – bilateral connectivity to valued partners and the convenience of a completely outsourced, hub-based SMS interworking solution to complete full coverage across the globe.

    Key Benefits of Intelligent Hubbing 365 includes:

    a. Enabling mobile operators to use their existing SS7 SMS interworking agreements in conjunction with the full global reach of Sinch, thus immediately increasing retail and wholesale revenues,
    b. Addressing bilateral MNP issues, by taking advantage of Sinch’s globally distributed Number Resolution System (NRS) that supports number portability in many key regions around the world,
    c. Improved customer experience (QoS) through more accurate delivery reports as non-bilateral destinations are converted from IP to SS7 signalling
    d. Reducing the complexity and OPEX costs (primarily operational resources) associated with managing and updating number ranges (SMSC Datafill),
    e. Using existing SS7 connectivity, with options to switch to SIGTRAN via IPX 365 for further cost savings,
    f. Gaining immediate benefit from of Sinch’s network additions.

11. Messaging Proxy 365 – enables the splitting and routing of Application to Peer (A2P) and Peer to Peer (P2P) messages to the appropriate platform for more accurate delivery to subscribers and invoicing of messaging traffic.

3 Global SMS Network

Sinch operates a global SMS network that provides both highly reliable IP connectivity and SS7 (C7) connectivity. Primary network backbone connections are redundant along with multiple connections into the global SS7 network.

Sinch's primary SMS interoperability hubs are located in Virginia, USA; Illinois, USA and Paris, France. Each hub is located in a secure data center. The Paris hub is primarily used for SS7 interconnection and the US hubs for IP interconnection, and are themselves, connected.

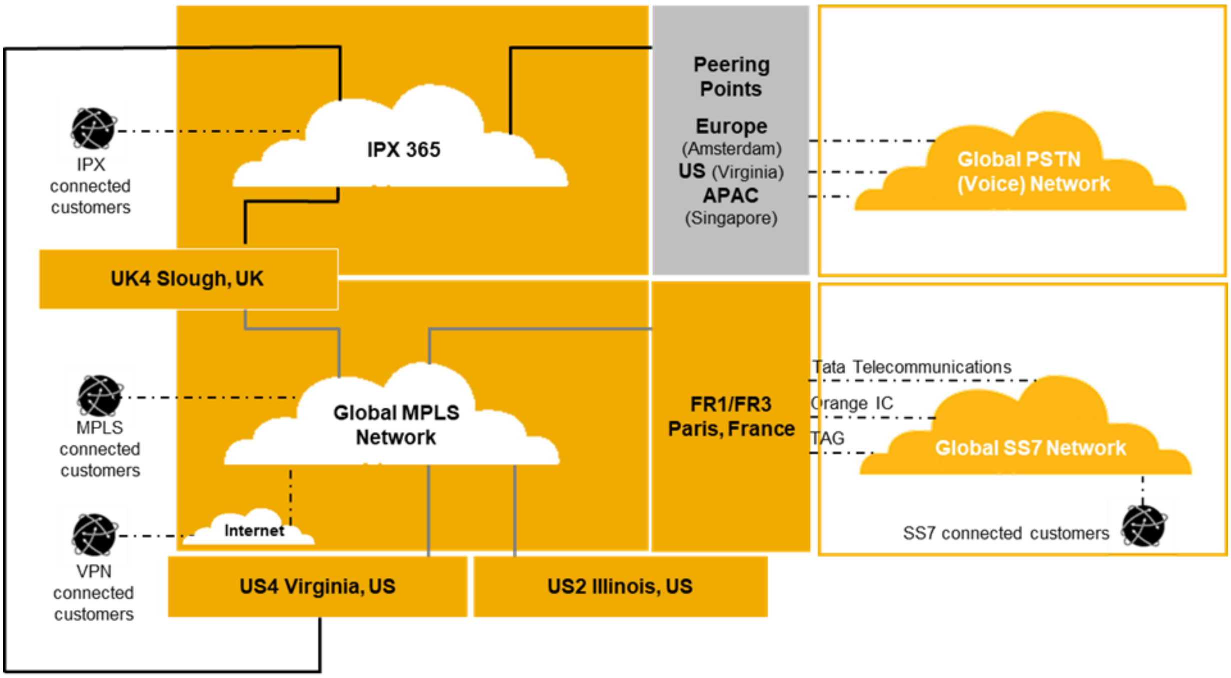


Figure 1: Global SMS Network

3.1 Network Operations Centre

Sinch's Network Operations Centre (NOC) operates 24x7 and is uniquely qualified to provide a number of specialized services to enable first class SMS interoperability including:

- Specialized data capture and analysis, in addition to the extensive reporting capabilities of SMS 365's web-based portal for monitoring traffic, connectivity and reporting.

- Proactive problem identification. Sinch’s Network Operations and Customer Care Centre (NOC) are staffed with highly trained professionals who proactively monitor all the gateways and are trained to identify key trends, identify and resolve potential problems before the customer experiences a problem. In addition, if a problem should materialize, the NOC has state-of-the-art tools that result in quick trouble identification and resolution. In many cases, the NOC is able to identify problems on an operator’s network, before the operator identifies it.
- Single Consumer Support. The NOC provides and uses tools to support the investigation and resolution of routing-related single-user issues (or SUIs).

The Sinch NOC is fully staffed and will provide access to an operations centre on a 24x7 basis for any customer service provider.

4 Functional Description

SMS 365 hosted in Paris, France is a full-featured inter-carrier SMS Interoperability Hubbing environment, providing a wide variety of routing, security, and value-added capabilities on behalf of Sinch's customers.

4.1 Block Diagram

The SMS 365 architecture is shown in the diagram below. Modules are connected using Inter-Process Communications queues. The hardware architecture is based on redundant servers, with external servers for billing and other external activities.

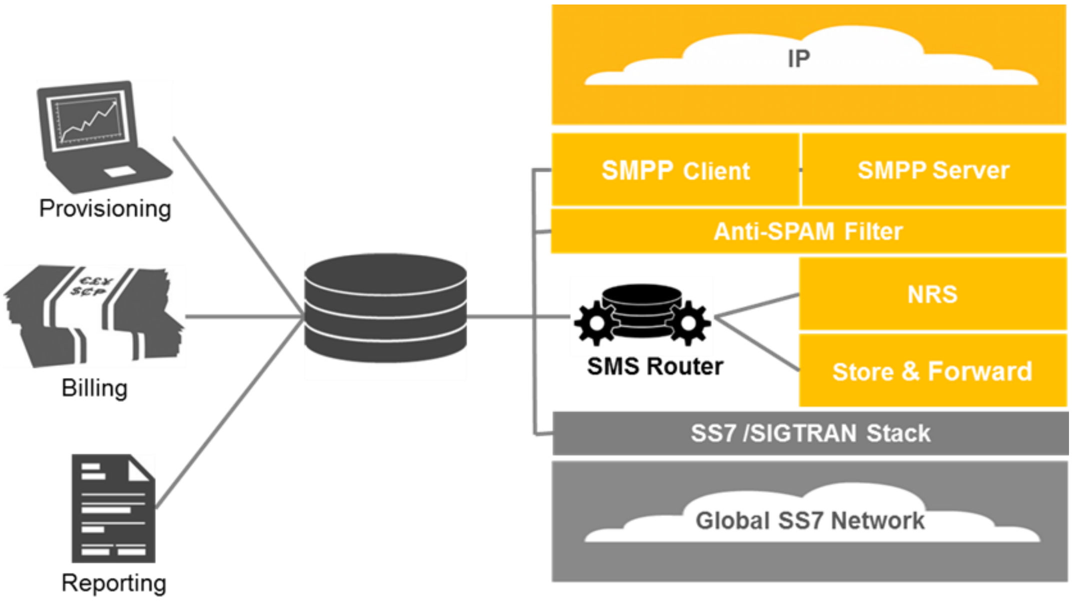


Figure 2: Block Diagram

The Router component is composed of multiple physical servers sharing the same Global Title and different IP addresses, behind a load-balancer. The Reporting databases are synchronized which means that all information inserted in one of them will be stored in the other. The solution includes 3 databases:

1. A configuration database,
2. A MDR database, and
3. A temporary information database on the Routers.

The configuration database contains static configuration and provisioning information that is created and maintained by a Provisioning Tool, available to Sinch Engineers.

The MDR database contains the billing and logs tickets created on each router of the platform. The raw MDR data is transferred to the databases from the routers periodically. Message statistics and reporting utilize information from this database. Additionally, all records eventually end up within a comprehensive Sinch Data Mart for availability to reporting and analytical capabilities.

The temporary information database contains message elements waiting for a response from the network (in the case of MAP-REPORT-SM-DELIVERY-STATUS for example) and also contains the latest raw MDRs. This database is located on each router.

4.2 GSM MAP Connectivity

SMS 365 hosted in Paris; France is fully compliant to GSM MAP. The Router supports two main modes of operation for SS7 origin/destination:

1. Relay Mode: SMS 365 provides store, forward, and retry capabilities on behalf of the originating operator.
2. Transparent Mode: All GSM MAP messages are transparently forwarded from the originating operator to the destination operator.

4.2.1 Relay Mode

SMS 365 customer operators that sign up for the relay service hand off all of the responsibility of delivering messages to SMS 365. In this model, SMS 365 is acting as an SMSC.

In the Map-Send-Routing-For-SM (SRI) response to the customer operator, the MSISDN is returned as the IMSI value and the SMS 365 Global Title (GT) is returned as the MSC value. If the SRI or Forward-Short-Message (FSM) response from the destination operator contains a permanent error (for example, unknown subscriber), then this error is returned immediately to the customer operator. If a temporary error (for example, absent subscriber) is returned, then SMS 365 will store the message and retry it as necessary. This is accomplished by first issuing a ReportSM-DeliveryStatus and then resending the message once the AlertServiceCenter message is received from the destination network.

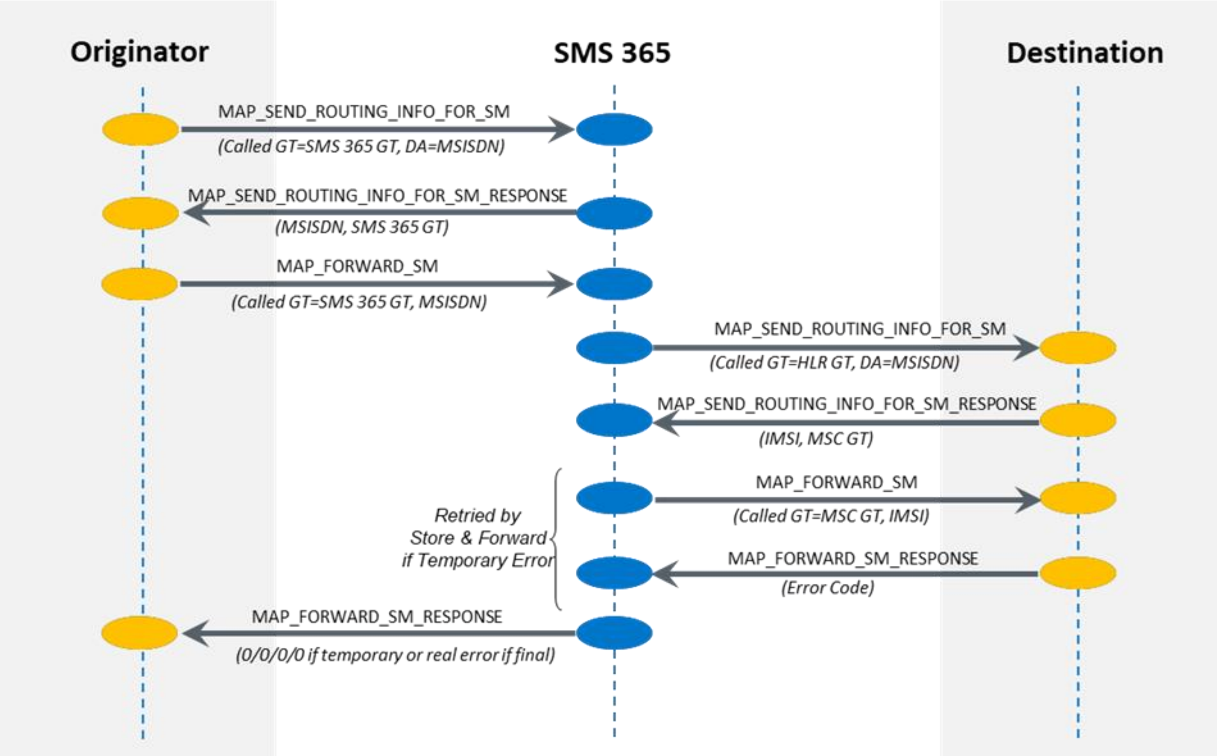

Originator
SMS 365
Destination
MAP_SEND_ROUTING_INFO_FOR_SM
(Called GT=SMS 365 GT, DA=MSISDN)
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(MSISDN, SMS 365 GT)
MAP_FORWARD_SM
(Called GT=SMS 365 GT, MSISDN)
MAP_SEND_ROUTING_INFO_FOR_SM
(Called GT=HLR GT, DA=MSISDN)
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(IMSI, MSC GT)
MAP_FORWARD_SM
(Called GT=MSC GT, IMSI)
Retried by Store & Forward if Temporary Error
MAP_FORWARD_SM_RESPONSE
(Error Code)
MAP_FORWARD_SM_RESPONSE
(0/0/0/0 if temporary or real error if final)

Figure 3: Relay Mode

One of the benefits of Relay Mode for the customer operator is lower MSU costs from a SCCP perspective; however, a key limitation is the lack of end-to-end visibility on the final status of a message.

4.2.2 Transparent Mode

SMS 365 customers that sign up for the transparent service are responsible for the store and forward operations. In this model, the SMS 365 node is acting as a roaming agreement between the source and destination operators.

The SRI response that is sent from SMS 365 to the customer operator contains the actual IMSI and either the real MSC or a fake MSC, depending on the customer's preference. If it is the real MSC then the customer is responsible for modifying the called party on the ensuing FSM to point to the SMS 365 Global Title.

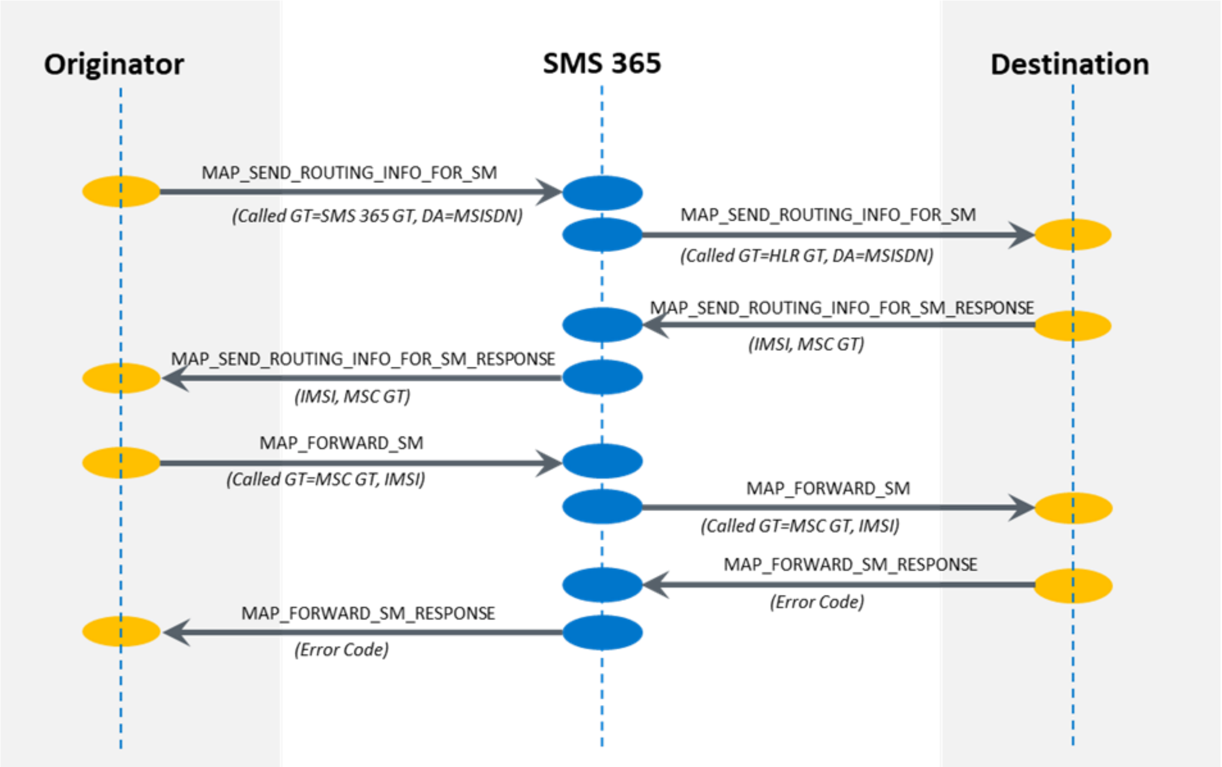


Figure 4: Transparent Mode

If the Fake MSC is used, then the Send_Routing_Info_for_SM_response contains the Global Title of the SMS 365 node. The Forward_SM comes into the SMS 365 network without any modification within the client SMSC.

4.3 Retry Capability

The Router provides functionality of a SMS Centre, compliant with GSM and 3GPP specifications. The following parameters of the retry policy may be configured. The retry algorithm can be different for each of the configured errors:

- Type of error to be retried: absent subscriber, SIM card full,
- Number of retries per minute,

- Number of retries per hour,
- Number of retries per day.

4.4 Anti-Spoofing Functionality

The purpose of the SMS 365 anti-spoofing functionality (especially for SS7 connected routes) is to make sure that the originator operator or some other connected entity is not using another operator's identity to send SMS traffic on its behalf.

The anti-spoofing functionality on the SS7 links are activated or de-activated on a per operator basis. Several levels of matching are provided:

- Calling SCCP Address is authorized to access the platform.
- The Calling SCCP Address and the Service Centre Address are well in the same NDC range.
- The Service Centre Address is one of the declared SMSC of the operator according to its IR.21 (and provisioned in the system).
- The Originating Address belongs to the NDC range corresponding to the SCCP Address and the SC Address.

For IP connected networks, it is difficult to spoof as there are separate physical connections for each connected operator; therefore, ingress/egress into the SMS 365 network is strictly controlled and monitored. The originating network is validated by IP address verification. Moreover, to avoid incorrect usage of the service, the “source_address” (also called Originating Address or sender address) is verified as it should be part of the origin network NDC ranges.

It should be noted that there is built-in protection for customers traffic coming to us from SIGTRAN (SS7 over IP) connections as these are specific, high-QoS, high-security, point-to-point networks.

After the above items are validated and isolated, the SMS gateway applications also checks the originating information against specific blocklists for additional filtering. Any suspected SPAM indications are noted by the NOC and acted upon, if confirmed that the originator was in fact, a spamming originator.

4.5 Anti-SPAM Functionality

SMS 365 has the capability to establish strict anti-SPAM policies as a key component of the inter-carrier SMS services. The anti-SPAM module has been designed with security in mind but also taking into account efficiency and flexibility. All SMS coming through any connections are filtered through multiple anti-spamming modules. These modules are located between the protocol, the routing service layers and after the routing services layer, so any SMS rejected by the modules does not impact overall routing performance and does not reach the out-bound message protocols (either SS7 or IP output).

The key anti-SPAM parameters are as follows:

- Message originator (both operator and originating address):
  - Statistical based detection and blocklisting of originating numbers
  - Manual blocklisting of originating numbers as requested by customer service providers
- Quantity of messages sent (linked with the origin of the message)
- Content analysis:
  - Keyword based detection and automatic blocking
  - Repeated content-based detection and automatic blocking
  - Advanced algorithms
  - Global threats database

4.5.1 Statistical Based Detection & Blocklisting

The primary statistical anti-SPAM methodology determines the number of unique or distinct destinations each originator sends to, over a period of time. Any originating numbers that send to over a specified number of distinct destinations over a period of time are added to a blocklist.

Two threshold levels are defined by time intervals:

- Number of identical SMS sent to the same destination address with a given OA (Originating Address).
- Number of identical SMS sent to different destination addresses with a given OA (Originating Address).

4.5.2 Manual Block by Customer Request

Many operators will escalate numbers or a list of numbers that they have identified as spamming subscribers in their networks. Mobile Operators, Fixed Operators, and OTTs use a variety of methods to detect SPAM. Some use the GSMA SPAM Reporting Service to identify SPAM content and originating operators; others employ different methods.

However, operators may request that traffic be blocked from specific operators. When asked, these numbers are added to the blocklist by the NOC and/or On-Call engineers.

4.5.3 Keyword Based Detection

Message traffic may be subject to Keyword filtering. Keyword is a term that represents URLs, call-to-action phrases, specific words, as well as specific phrases that may appear in an SMS message. Regular expressions are used in some cases to overcome lower/upper case changes that would defeat this filter.

Specific keywords are actively searched for as well as content review. Keywords are added (and occasionally deleted) all the time. Messages containing a positive match to this keyword filter would be automatically blocked.

4.5.4 Repeated Content Based Detection

The repeated content filter looks at content originating from specific operators (same content from same operator). If the message is over a certain length or the volume of SMS with repeated content surpasses pre-set thresholds. Additionally, we have incorporated variables to further identify the SPAM message:

- Leading words can be ignored when identifying SPAM.
- Trailing words can be ignored when identifying SPAM.
- Numeric characters [0-9] can be ignored when identifying SPAM.
- Non-alphanumeric characters can be ignored when identifying SPAM.

4.5.5 Global Threat Database

SMS 365 is connected with an independent global threats database enabling proactive protection based on Global Sender reputation.

4.5.6 SPAM Detection Procedures

When a spamming case is detected, a specific status is sent back to the originator. Depending on its input protocol (SS7 or IP), detected SPAM messages generate MDRs with a specific ticket code. An email alarm alerts the NOC and/or On-Call engineers to take further action on the detected SPAM.

- For a SS7 input, the returned status (“x/y/z/t” parameter) will be:
  - 0/0/0/94 = spoofing from a direct operator
  - 0/0/0/95 = spoofing traffic from a peer
  - 0/0/0/96 = blocked spam (keyword)
  - 0/0/0/97 = blocked spam (repeated content)
  - 0/0/0/98 = blocked spam
- a MDR will be generated with a specific MDR ticket code “901” or “902”.
- For a SMPP input, the command status returned will be “0x00000499” and a MDR will be generated with a specific MDR (ticket code “901” or “902”).

- Messages blocked in IXNG are recorded with the reason code 1120.
- Messages blocked in Routing Service are recorded with the following reason codes:
  - Blocklisted originating addresses are blocked with reason code 1121
  - Blocklisted content is blocked with reason code 1125

4.6 SMS 365 Connectivity Options for Originating Operators

SMS 365 supports two SS7 options for originating operators to connect depending upon operator SMSC capabilities:

- Direct HLR addressing
- Prefix method

These routing options make use of the destination network and do not impact originating operators' subscribers if they are roaming.

4.6.1 Direct HLR Addressing

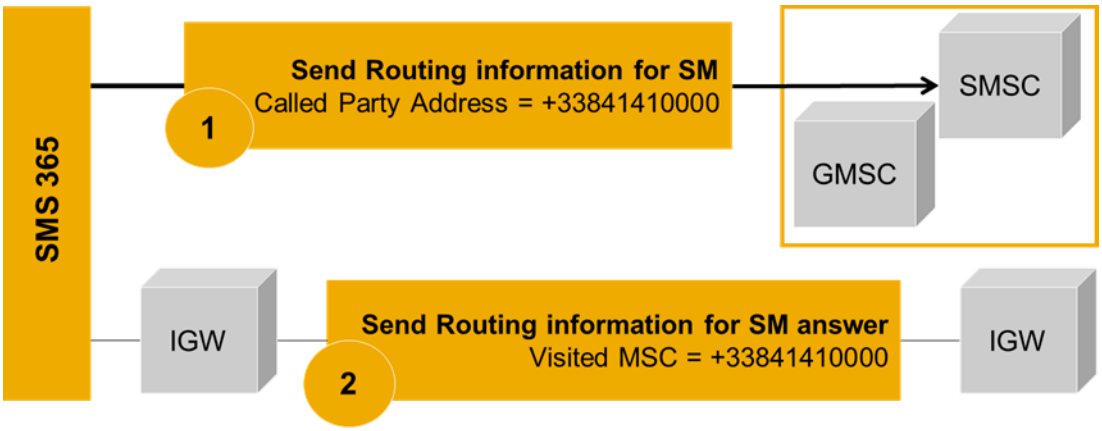

SMS 365
Send Routing information for SM
Called Party Address = +33841410000
1
SMSC
GMSC
IGW
Send Routing information for SM answer
Visited MSC = +33841410000
2
IGW

Figure 5: Direct HLR Addressing

For this option, operators simply specify the SMS 365 HLR address in their SMSC Routing table configurations for the Send Routing Information for SM GSM MAP command (SRI).

For example, the SMS 365 HLR Address is: +338xxxxxxxx . If an operator wished to route all of their France traffic and SingTel traffic to SMS 365 for delivery, their SMSC routing tables would look similar to the following:

+33; +338xxxxxxxx

+6590; +338xxxxxxxx

+6591; +338xxxxxxxx

+6592; +338xxxxxxxx

+6593; +338xxxxxxxx

+6594; +338xxxxxxxx

+6596; +338xxxxxxxx

+6597; +338xxxxxxxx

+6598; +338xxxxxxxx

SMS 365 will respond to the SRI with SMS 365 indicated as the visited MSC.

4.6.2 Prefix Addressing

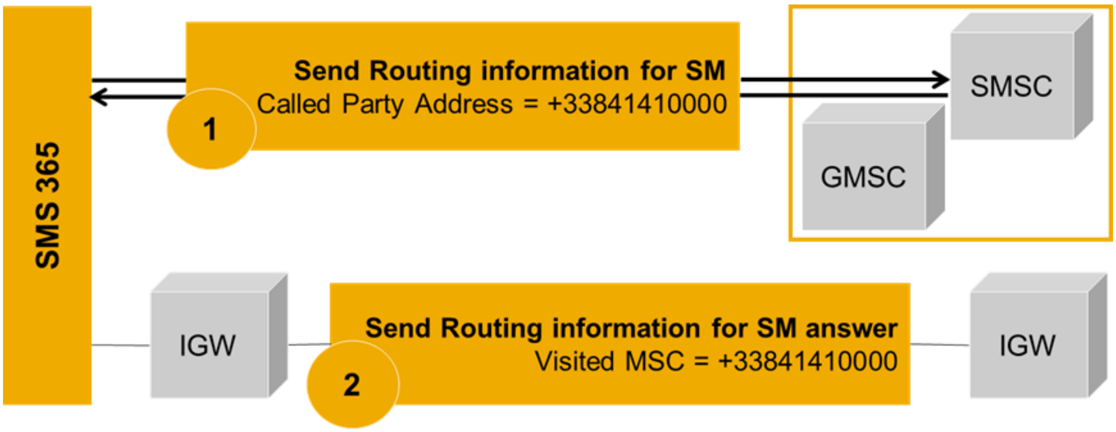

SMS 365
1
Send Routing information for SM
Called Party Address = +33841410000
SMSC
GMSC
IGW
2
Send Routing information for SM answer
Visited MSC = +33841410000
IGW

Figure 6: Prefix Addressing

This option is available to operators for situations where it may not be possible to modify their routing tables. The prefix +338 is pre-pended to the destination MSISDN.

For example, if the destination number is +44771234567, then the operator will send the number to +33844771234567. Most SMSCs have the ability to alter the destination number (for example, to account for different dialling plans), prior to forwarding the message.

The corresponding SRI for SM is routed directly to SMS 365. SMS 365 will respond to the SRI with SMS 365 indicated as the visited MSC.

4.6.3 Short Messaging Peer-to-Peer (SMPP)

SMS 365 supports two-way SMPP connections and the platform can be either the client or server. The preferred connectivity is SMPP v3.4, along with mid-version updates. SMS 365 uses its own proprietary protocol stack for SMPP, so changes can be implemented in a short period of time (days instead of months) without reliance on third parties:

- Multiple SMPP connections over one physical connection
- Multiple SMPP ports over the same physical connection, limited only by the bandwidth provided
- Throttle of each SMPP link separately
- Support of auto-bind and re-bind on all SMPP links
- Support of individual character mapping on each SMPP link

4.6.4 SIGTRAN

SMS 365 supports connectivity to its SMS Messaging environment via SIGTRAN – or SS7 over IP – more precisely GSM MAP over IP. SIGTRAN offers many advantages to customers that wish to retain the benefits of SS7-based SMS hubbing, while eliminating 3rd-party MSU charges that are typically incurred between the mobile operator and the messaging hub. The transport is over IP – either IPSEC VPN or through the SMS IPX; however, leveraging our IPX infrastructure for connectivity is heavily favored.

The SIGRAN Protocol stack consists of three main components:

- The IP Layer

- A Common signalling transport protocol called Stream Control Transmission Protocol (SCTP) that provides a reliable connection-oriented transport of messages between users or adaptation layer protocols. The SCTP layer replaces the normal TCP/UDP layer.
- The Adaptation Layer. The protocols for this layer are M2PA, M2UA, M3UA and SUA. SMS 365 supports M2PA as a preferred Adaptation layer protocol, but can also support M3UA, upon request.

The following diagram outlines both preferred and alternative network architecture for SIGTRAN connectivity to the SMS 365 messaging hub environment.

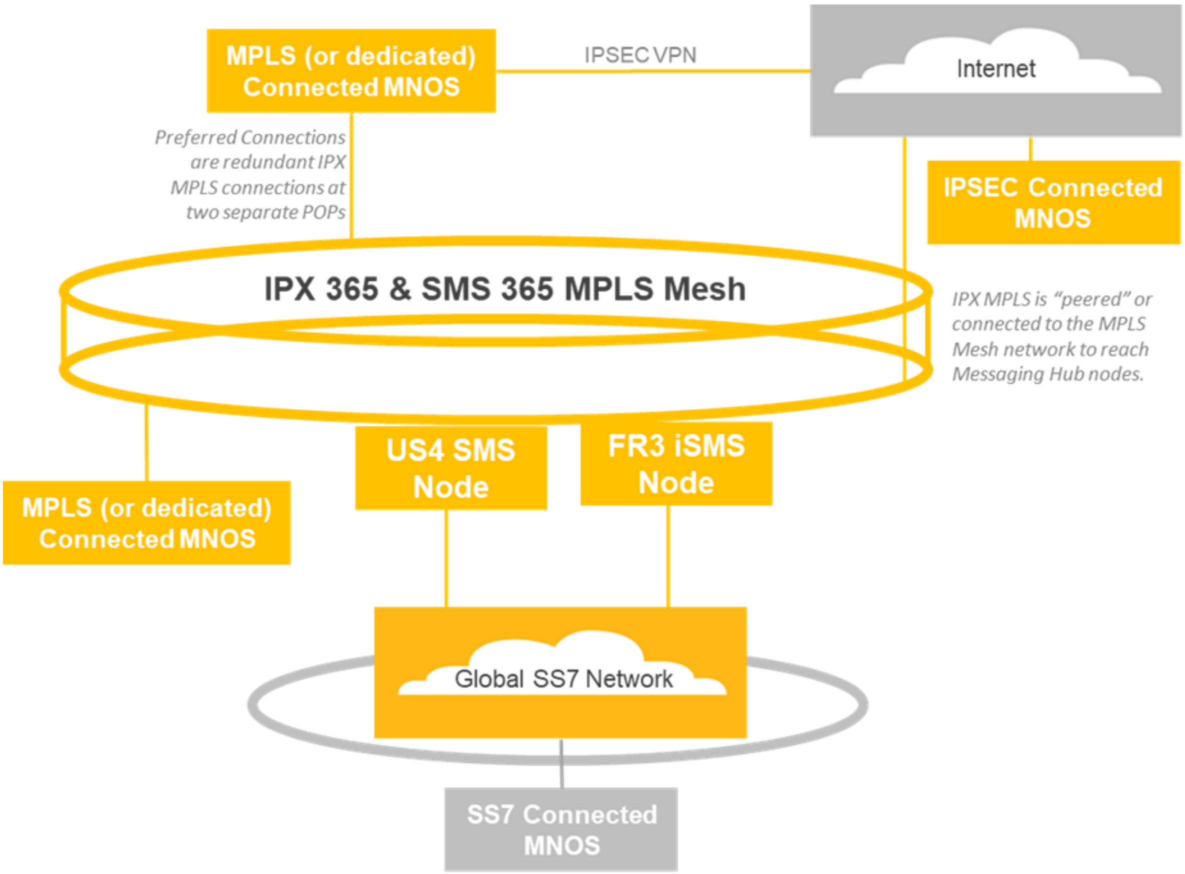

MPLS (or dedicated) Connected MNOS
IPSEC VPN
Internet
Preferred Connections are redundant IPX MPLS connections at two separate POPs
IPSEC Connected MNOS
IPX 365 & SMS 365 MPLS Mesh
IPX MPLS is "peered" or connected to the MPLS Mesh network to reach Messaging Hub nodes.
US4 SMS Node
FR3 iSMS Node
MPLS (or dedicated) Connected MNOS
Global SS7 Network
SS7 Connected MNOS

Figure 7: SIGTRAN Connectivity

The preferred connectivity is using the IPX as the transport for the SIGTRAN traffic to the SMS 365 Messaging environment; however, a VPN over the Internet is also supported, but not recommended. Existing IPX customers may leverage their existing connections, providing enough bandwidth is available by creating a separate VRF for SMS over SIGTRAN. Bandwidth needed for international SMS traffic should be minimal, but this is dependent upon MNO messaging volume.

The selection of Adaptation Protocol (M2PA or M3UA) is typically dependent upon the capabilities of the customer's infrastructure connecting to SMS 365 messaging node. If there is a choice, Sinch recommends using M2PA as it is designed to provide peer-to-peer communications between SS7 endpoints. M2PA essentially maps the SS7 network over the IP network and is completely transparent to the SS7 network. The MTP3 layer which routes on point codes is present, so each IP Signalling Point requires a Point Code.

M3UA can also be supported. M3UA supports the transport of any SS7 MTP3-User signalling (to another IP Signalling Point (IPSP) using the services of SCTP. M3UA is IP aware in that it translates the contents of the incoming SS7 MSU using a Routing Key (for example, a routing table) to map to the relevant IP address. MNOs typically use M3UA to connect to multiple other endpoints (such as SMSCs) when an operator is part of an operator group (for example, one-to-many).

4.7 Mobile Number Portability

SMS 365 makes full use of the Sinch's Number Resolution System (NRS) that is used to manage all country numbering plans including MNP countries. The Sinch NRS supports number ranges of operators around the world as well as number portability in many countries. MNP supported countries are available in Sinch's Global Coverage List.

Sinch's NRS consists of the following major components:

1. A unified interface called the Number Resolution Query Node. The NRS Query Node is one of the key elements that enable Sinch to have a single, complete, global number resolution capability across all hubs and data centres.

2. The MNP Feed Manager (or sometimes called the "Feed Loader."). The Feed Manager is a software application that retrieves periodic numbering plan update data (typically adds, deletes) and updates the Global Numbering Plan Database. The Feed Manager may be configured for a variety of countries and situations

whereby a central authority pushes data via FTP or SFTP or even CFT. The Feed Manager is highly customizable allowing customer operator personnel to integrate a new file-based feed to be supported without software integration. The Feed Manager supports FTP, SOAP/XML and HTTP protocols. Many countries supply a daily file of ported numbers from the previous 24 hours to Sinch in this manner. Some, such as the United States and Canada provide a real-time feed for continuous updating of Sinch's Global Numbering Plan Database.

Many countries require that Aggregators and Hub providers (as well as the operators themselves) perform an active "dip" for numbers, instead of providing a daily feed. Sinch has this capability built into its overall NRS ecosystem to support various types of dipping scenarios, depending upon the MNP requirements of a particular country.

3. Datamining capabilities are supported in Sinch hubs which can be used to automatically update numbers based on SRI_SM Responses and MCC-MNC codes received from the destination networks. The IMSI which is returned as part of a SRI is analysed, checking that the MCC-MNC matches a list of allowed MCC-MNCs in a country. Once validated, the MDN is assigned to an operator and loaded into NRS. These checks are run once a day for select countries. Operator IDs are pulled from the messaging databases for select countries and then mapped to operators in NRS. This data is loaded once a day.

4. The NRS Administrative Tool is a web-based administration tool for management of the NRS system.

   Not all countries in the world have Mobile Number Portability in effect. Sinch still maintains static (or nearly static) ranges for hundreds of operators (in many cases, for operators that provide services in MNP countries as well). This requires some degree of manual coordination and administration. The NRS Administrative Tool allows:

   - A user to either upload a file or manually update number ranges for any country. The change set will be versioned and must be approved before being applied to the NRS system;

- A Number Administrator to approve change sets that have been submitted so that number updates will become effective;
- An administrator to rollback changes that were previously made against the system;
- A user to query results for any number;
- Operations to monitor as well as remotely configure the NRS platform.

4.8 Intelligent Hubbing 365

Intelligent Hubbing 365 enables the SMS 365 customer to have the best of both worlds. To seamlessly combine their existing footprint with Sinch’s Global SMS Reach List of 1000+ destinations to provide the optimum subscriber experience while growing revenues.

The Intelligent Hubbing service leverages advanced origin-based routing features allowing SMS 365 to act as a centralized point of aggregation for SMS connectivity, enabling traffic to be screened and delivered to the correct destination, using either a bilateral or hub-based delivery model. The solution is fully transparent to the SMS 365 customer‘s routing network configuration, removing the need for cumbersome and complex modification of the SMS 365 customer’s routing tables by operational teams already focused on all aspects of international business.

The key benefits of Intelligent Hubbing 365:

- Enables mobile operators to use their existing SS7 SMS interworking agreements in conjunction with the full global reach of Sinch, thus immediately increasing retail and wholesale revenues,
- Addresses bilateral MNP issues, by taking advantage of Sinch’s globally distributed Number Resolution System (NRS) that supports number portability in many key regions around the world,
- Improves customer experience (Quality of Service) through more accurate delivery reports as non-Bilateral destinations are converted from IP to SS7 signalling,

- Reduces the complexity and OPEX costs (primarily operational resources) associated with managing and updating number ranges (SMSC Data fill),
- Uses existing SS7 connectivity, with options to switch to SIGTRAN via Sinch's IPX for further cost savings,
- Gains immediate benefit from Sinch's network additions (~7 new operators per month),
- Fully compliant with the GSMA and ITU standards, such as 3GPP 23.040, IR.75 and 3GPP 09.02

4.8.1 Intelligent Hubbing 365 Message Flow

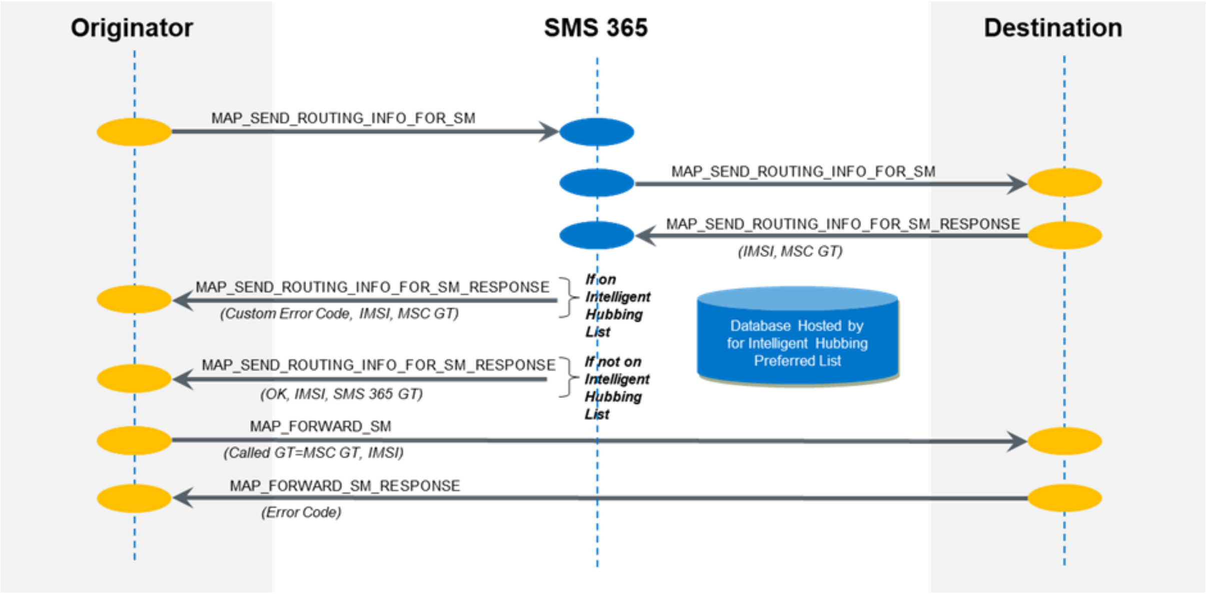

Originator
SMS 365
Destination
MAP_SEND_ROUTING_INFO_FOR_SM
MAP_SEND_ROUTING_INFO_FOR_SM
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(IMSI, MSC GT)
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(Custom Error Code, IMSI, MSC GT)
If on Intelligent Hubbing List
Database Hosted by for Intelligent Hubbing Preferred List
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(OK, IMSI, SMS 365 GT)
If not on Intelligent Hubbing List
MAP_FORWARD_SM
(Called GT=MSC GT, IMSI)
MAP_FORWARD_SM_RESPONSE
(Error Code)

Figure 8: Intelligent Hubbing message flow

The Intelligent Hubbing 365 service enables the SMS 365 customer to specify specific partner operators that should not be delivered to via SMS 365. SMS 365 will then return the traffic back to the SMS 365 customer for partner operators that is on its Intelligent Hubbing preferred list. SMS 365 customer can then deliver these messages, bilaterally. For all other destinations, SMS 365 will deliver traffic to these mobile operators, normally.

4.9 Messaging Proxy 365

Messaging Proxy 365 is a cloud-based service hosted and managed by Sinch. This service enables the splitting and routing of A2P and P2P messages to the appropriate platform for more accurate delivery to subscribers and invoicing of messaging traffic. Operators simply reroute messaging traffic to the cloud service and Sinch does the rest.

By more, accurately classifying and routing an operator’s A2P and P2P messages, Messaging Proxy 365 allows an operator to realize numerous benefits, including:

1. Maximized use of its existing infrastructure and network capacity,
2. Improved revenue by optimizing existing messaging streams and closing revenue leaks,
3. Increased monetization by bringing higher-quality traffic into its network, identifying and unblocking “illegitimate” P2P traffic, and properly routing it so it can capture its rightful revenue,
4. Reducing complexity by connecting messaging streams to Sinch using existing points of contact for automated classification and routing of messages to the right platform for delivery,
5. Faster time to value by leveraging a managed, cloud-based service that avoids additional capital expenditures and the commitment of internal resources to manage an on-premise solution,
6. Increased visibility and control of messaging traffic with online reporting tools,
7. Better long-term investment by adopting a future-proof platform that is supported and maintained by Sinch.

For more detailed information on how Messaging Proxy 365 splits and routes A2P and P2P messages and message flows, please refer to the Messaging Proxy 365 Product Description.

5 GSMA Open Connectivity

SMS hubbing allows operators to significantly expand the reach of their SMS services by simplifying the interworking arrangements between operators. Sinch is GSMA Self Certified and is fully compliant with the GSMA's Open Connectivity SMS Hubbing initiative.

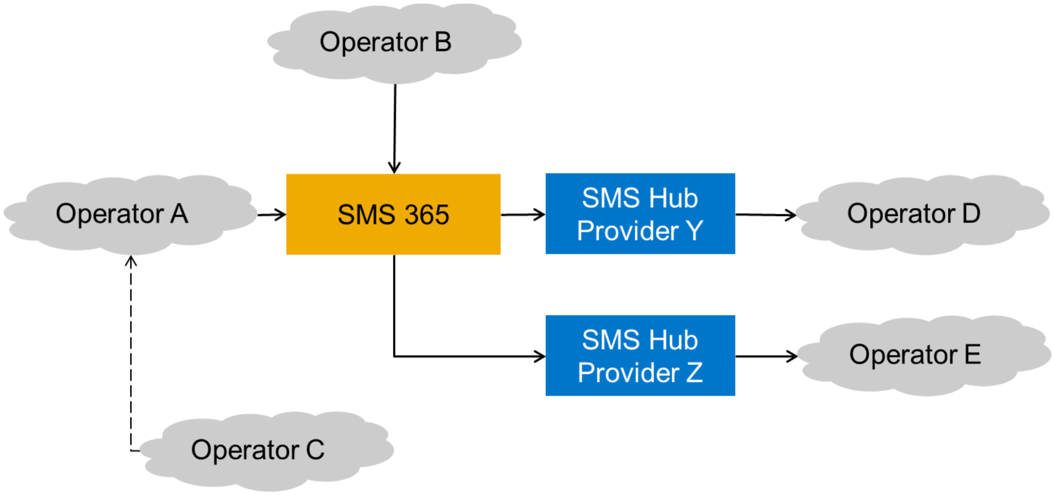


Figure 9: GSMA Open Connectivity

As a hub provider Sinch continues to take a leading role in the Open Connectivity initiative launched by the GSM Association. Sinch recognizes the potential benefits that can be brought to its customers through peering relationships with other hubs. Sinch peers with several other hub providers and has done so, in some cases, for several years but it always forms a judgment on what is in the interests of its customers and the security of their networks before it engages in peering activity. Thus, Sinch follows a path of value-based peering where its customers' interests are paramount.

SMS 365 is fully compliant with GSMA IR.75's Technical and Hubbing Architecture requirements which include:

- Single Multilateral Agreement replacing Bilateral Agreement (IR.71)
- End-to-End Delivery
- Pricing Transparency

- Revenue Management
- End to end SLA
- Prevention of unsolicited messaging
- Security and Anti-SPAM
- Centralized Service Support
- Fraud Management
- Flexibility and Scalability

6 Message Detail Records

SMS 365 generates a MDR for every inbound and outbound message. While these MDRs are not utilized for billing purposes, they validate message traffic and routing issues.

SMS 365 generates a MDR each time it relays a MAP or an SMPP message. If a message fails, either GSM MAP or SMPP, all errors are recoded via the MDRs. Only the successful delivery of a Short Message shall trigger billing. Therefore, only the reception by SMS 365 of a positive acknowledgement to a MAP_Forward_SM, SMPP_Deliver_SM, or SMPP_Submit_SM will trigger billing.

MDRs have specific “ticket codes” to distinguish:

- The input traffic: to be billed to the SMS purchaser
- The output traffic: to be billed to the SMS seller

Input traffic, output traffic and internal traffic are distinguished by using specific “ticket codes” within the generated MDR.

Each Router generates one record for:

1. Each entry,
2. Each internal transaction, and
3. Each exit (when the final status of the message is ascertained. After several retries when the message sending is OK or if it abandoned – in store and forward cases).

In input, the length may be several SMSs (length > 140 octets).

6.1 MDR Accounting and Procedures

MDRs are generated and stored locally on each router. Raw MDRs are generated as flat files on each of the routers. Flat files are separated by the “|” character. MDRs range in length from 200 to 400 bytes. To help minimize data loss in case of software failure, all MDRs are persisted in local message queues prior to being written to local flat files.

The accumulated MDRs are sent to the database storage platform for database insertion. If the MDRs cannot be forwarded to the database, alarms are generated.

SMS 365’s monitoring system checks the generation of MDRs and the transfer to the back-office platform. The following information is continually verified in real-time on each of the routers:

- Generation of MDRs: If no MDR generation is detected, the monitoring verifies the status of the “MDR logger” module and restarts it. If no MDR is generated, then an alert is raised.
- Transfer Module: this module raises the alert if there are no MDRs to transfer or if cannot connect to the database storage arrays.

Additionally, the Database Storage servers validate specific “check-tags” that are inserted into the MDRs for syntax verification. Periodically, the monitoring system creates statistics on the transferred MDRs and can detect certain abnormal conditions such as a jump in traffic or lack of traffic from a specific router.

6.2 MDR Format

SMS 365’s current MDR has the following fields (delimited by “|”):

For SMS-MO:
<Ticket code>|*<Error code>*|*<Destination network>*|*<Origination network>*|*<Destination number>*|*<Origination number>*|*<YYYYmmDD>*|*<HHMMSS>*|*<Type of delivery>*

For SMS-MT:
<Ticket code>|*<Error code>*|*<Destination network>*|*<Origination network>*|*<Visited network>*|*<Destination number>*|*<Origination number>*|*<YYYYmmDD>*|*<HHMMSS>*|
<Type of delivery>

6.2.1 Ticket Code

This is single digit code. Acceptable values are:

Ticket Code	Description
1	Entry from customer (IP and SS7)
3	Exit ticket code (IP and SS7)
0	Internal Entry. This message is sent to another SMS 365 SS7 router as this router cannot reach the destination operator.
2	Internal Exit. This message comes from another SMS 365 SS7 router as this router cannot reach the destination operator
4	Internal Entry for Re-Roaming. The actual SMS 365 SS7 router could reach the HLR but due to the end-user roaming situation, the MSC of the visited network could not be reached. This message is then sent to another SMS 365 SS7 router which has the visited network agreement for message delivery.
6	Internal Exit for Re-Roaming. The previous SMS 365 SS7 router could reach the HLR but due the end-user roaming situation, the MSC of the visited network could not be reached. The SMS 365 SS7 router which has the visited network agreement for message delivery received the request to terminate the message.
10x (x = 0 to 6 from above)	Status Delivery Report MDRs
90x (x = 0 to 6 from above)	SPAM SMS Blocked. The associated X/Y/Z/T value is then 0/0/0/96 – 97 – 98.

6.2.2 Error Code

The field is composed of 4 fields: X/Y/Z/T:

Error Code	Description
X	MAP User Error
Y	Provider Error
Z	Delivery Failure Cause
T	Network Result

The MAP User Error is as per GSM 09.02. X/Y/Z/T is a proprietary syntax. For more information on the different Error Codes and what they represent, please refer to the SMS 365 SS7 Error Code User Guide.

7 Reporting

The Report Manager feature of SMS 365 is a web-based reporting portal that gives users the ability to view SMS traffic statistics, research messages, and analyse traffic/financial trends. The reports and graphs are displayed based on user specified entries for time period, destination operator and country to provide insights into traffic statistics.

The Report Manager is easy to use and provides the ability to:

- Manage user accounts, roles and access for your organization.
- Troubleshoot delivery issues by number lookup and search messages function.
- Generate detailed traffic reports to understand traffic volume patterns, trends and errors.
- Display financial information and view traffic reports with pricing.
- Analyse Intelligent Hubbing 365 and Messaging Proxy 365 traffic data.
- Download CDR data and export all reports to .xlsx, .csv, .pdf format.
- Access using portable devices (smartphone, tablet) which will automatically re-size for the screen.

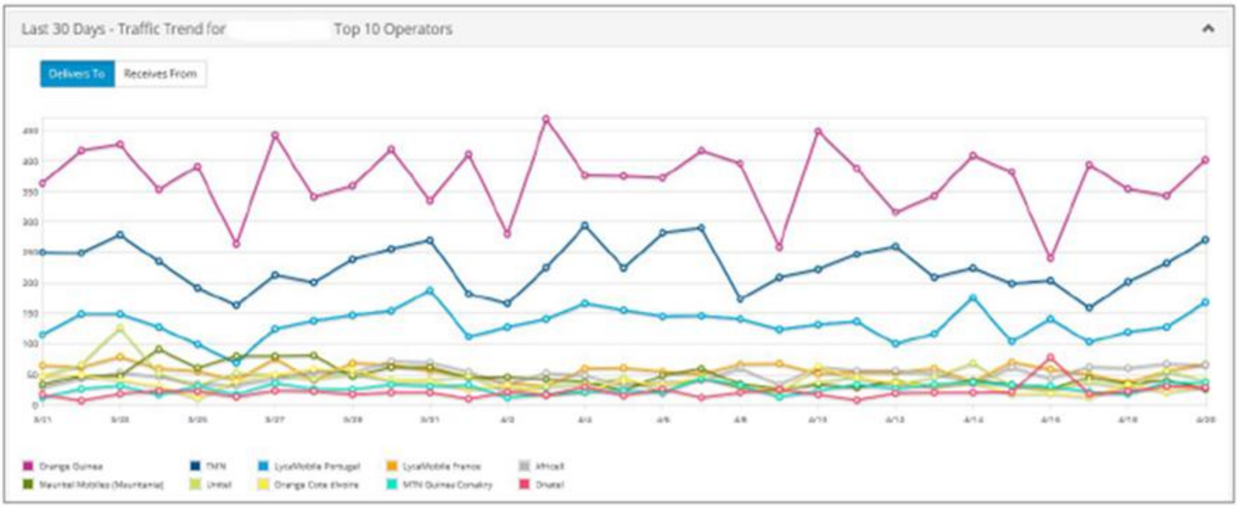
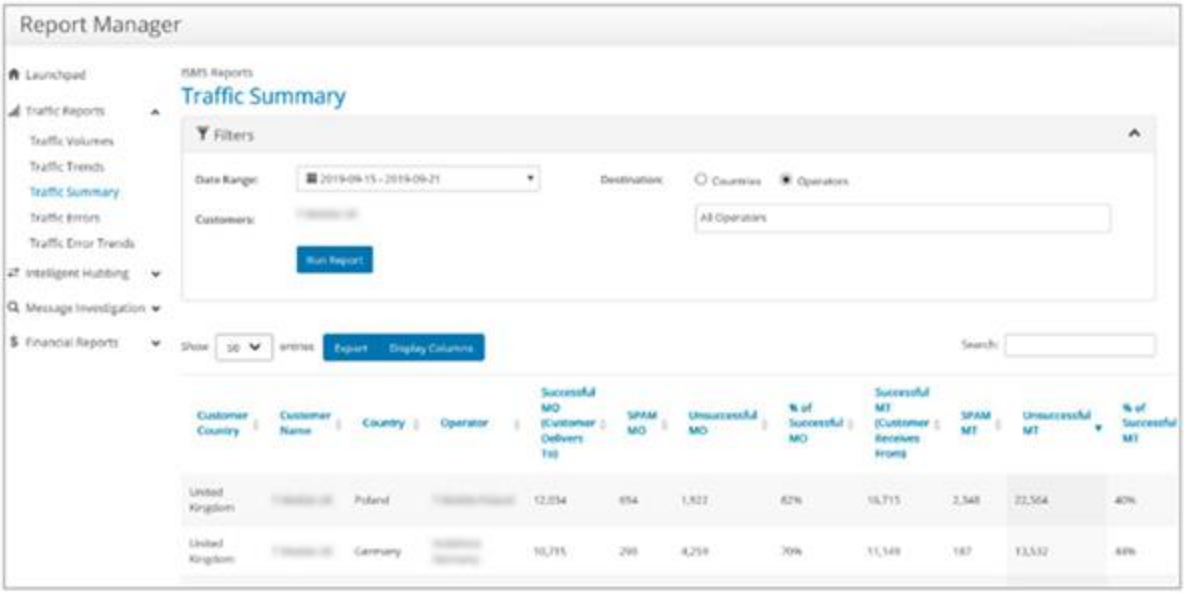


Figure 10: Traffic Trend



Report Manager

ISMS Reports

Traffic Summary

Filters

Date Range: 2019-09-15 - 2019-09-21

Destination: ○ Countries ● Operators

Customers: [redacted]

All Operators

Customer Country	Customer Name	Country	Operator	Successful MO (Customer Delivers To)	SPAM MO	Unsuccessful MO	% of Successful MO	Successful MT (Customer Receives From)	SPAM MT	Unsuccessful MT	% of Successful MT
United Kingdom	[redacted]	Poland	[redacted]	12,034	654	1,922	82%	16,715	2,348	22,564	40%
United Kingdom	[redacted]	Germany	[redacted]	10,795	298	4,259	70%	11,149	187	13,532	44%

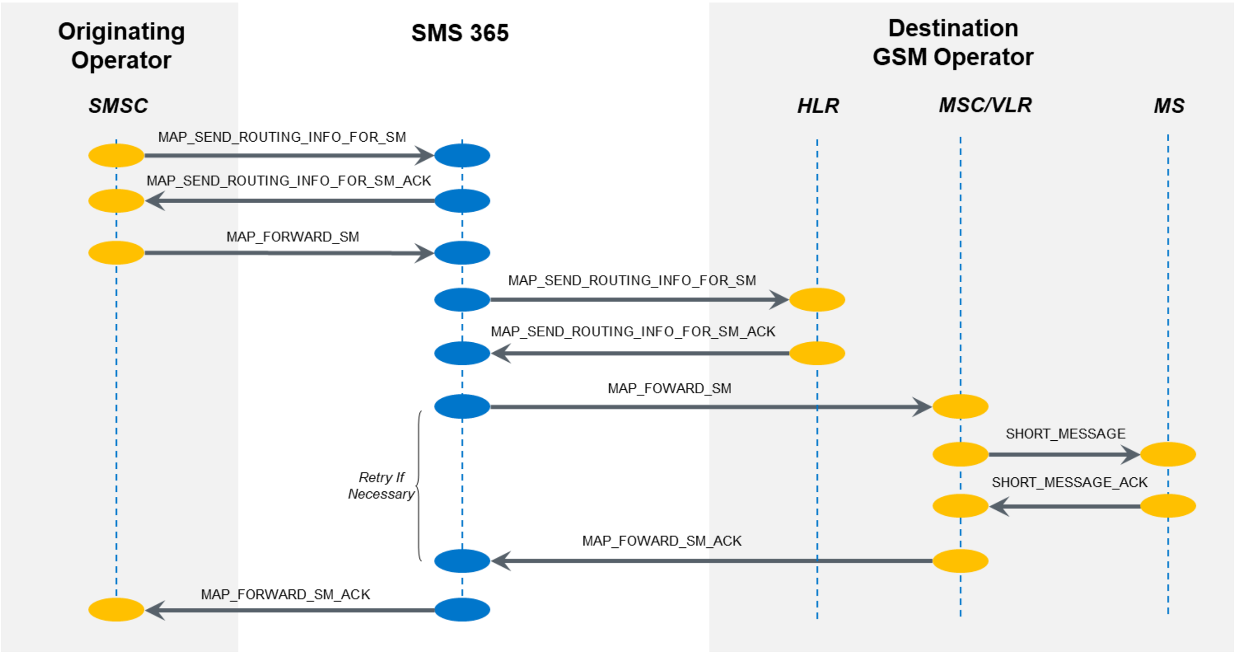
Figure 11: Traffic Summary

For more information on Report Manager, please refer to the Report Manager User Guide

8 Message Flows

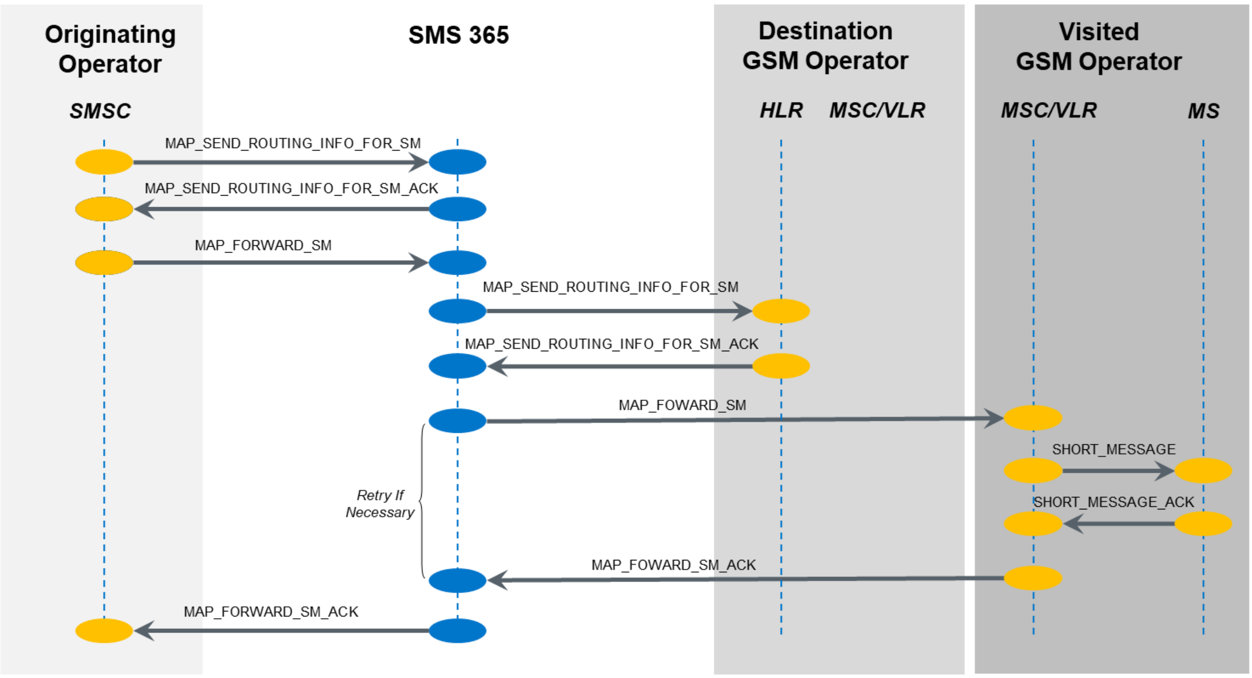
8.1 SS7 End to End Delivery – Mobile Originator to GSM Subscriber in Home PLMN

This message flow scenario illustrates delivery by Relay Mode, where the subscriber is in the Home PLMN. Both the originating and destination operators are connected via SS7 to SMS 365.



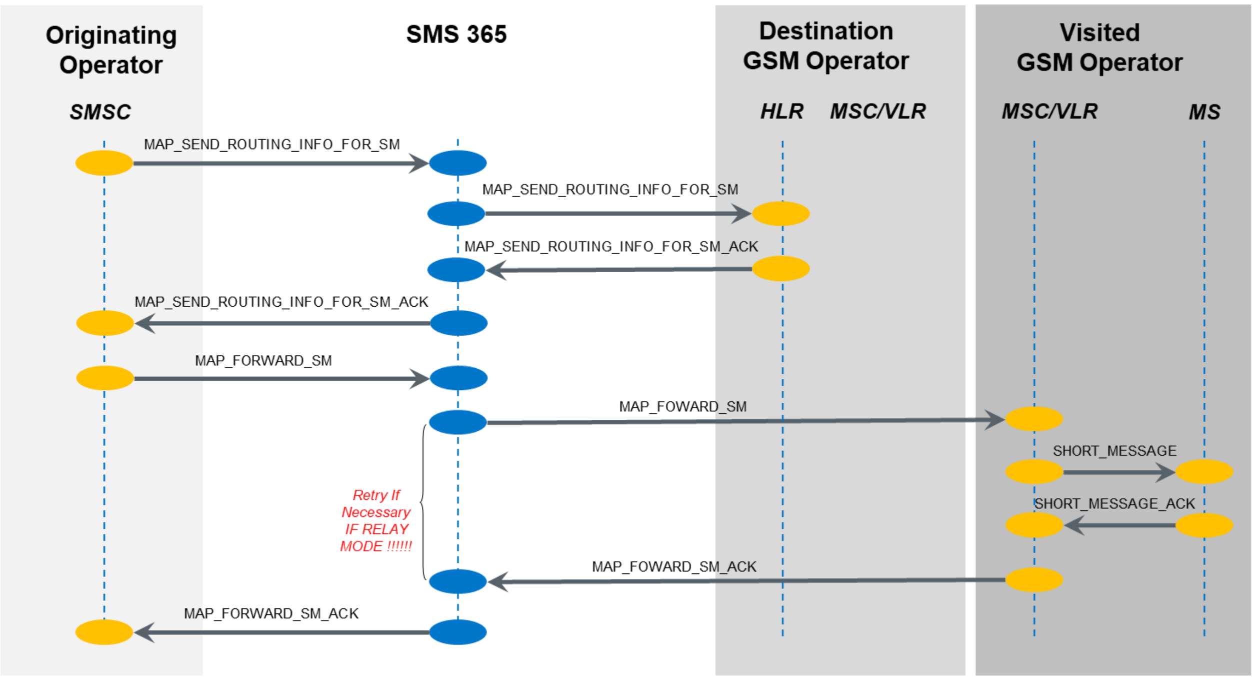
8.2 SS7 End to End Delivery – Mobile Originator to GSM Roaming Subscriber – Scenario 1

In this message flow scenario, the originating operator is a SMS 365 customer in Relay Mode, sending a message to a GSM roaming subscriber in a Visited PLMN.



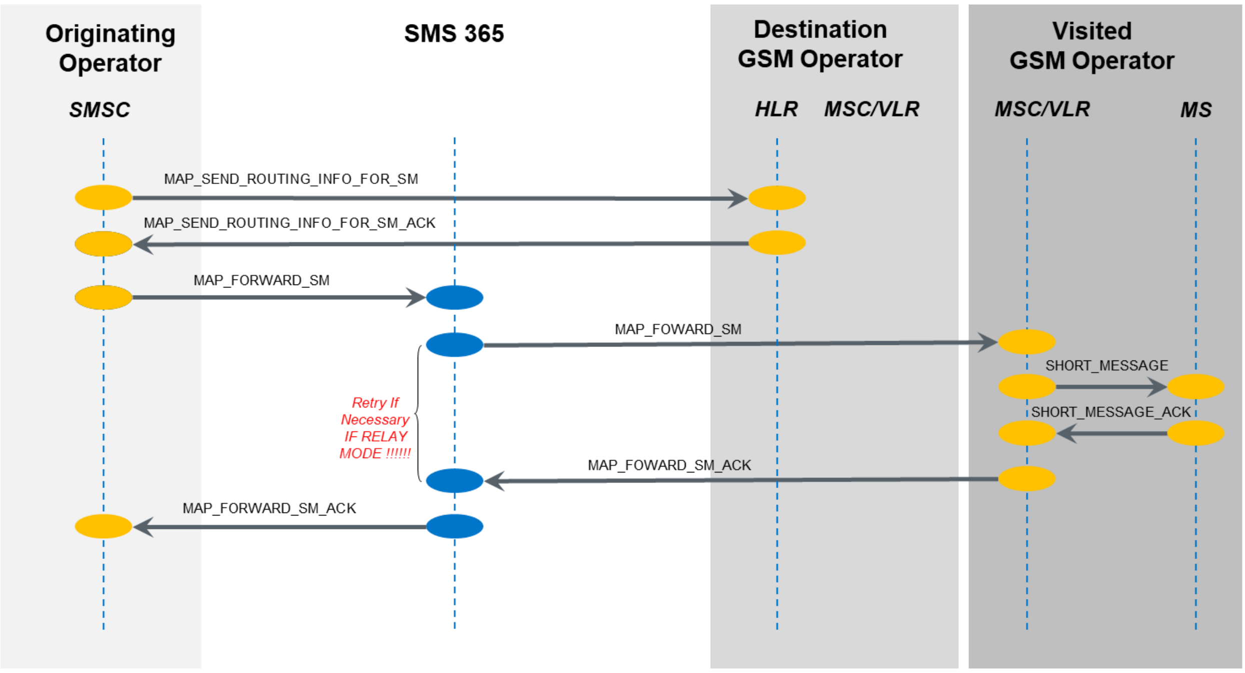
8.3 SS7 End to End Delivery – Mobile Originator to GSM Roaming Subscriber – Scenario 2

In this message flow scenario, the Originating Operator is in Transparent Mode and has no direct relationship with the Destination HPLMN, therefore, the SRI for SM and FSM MT are both managed by SMS 365.



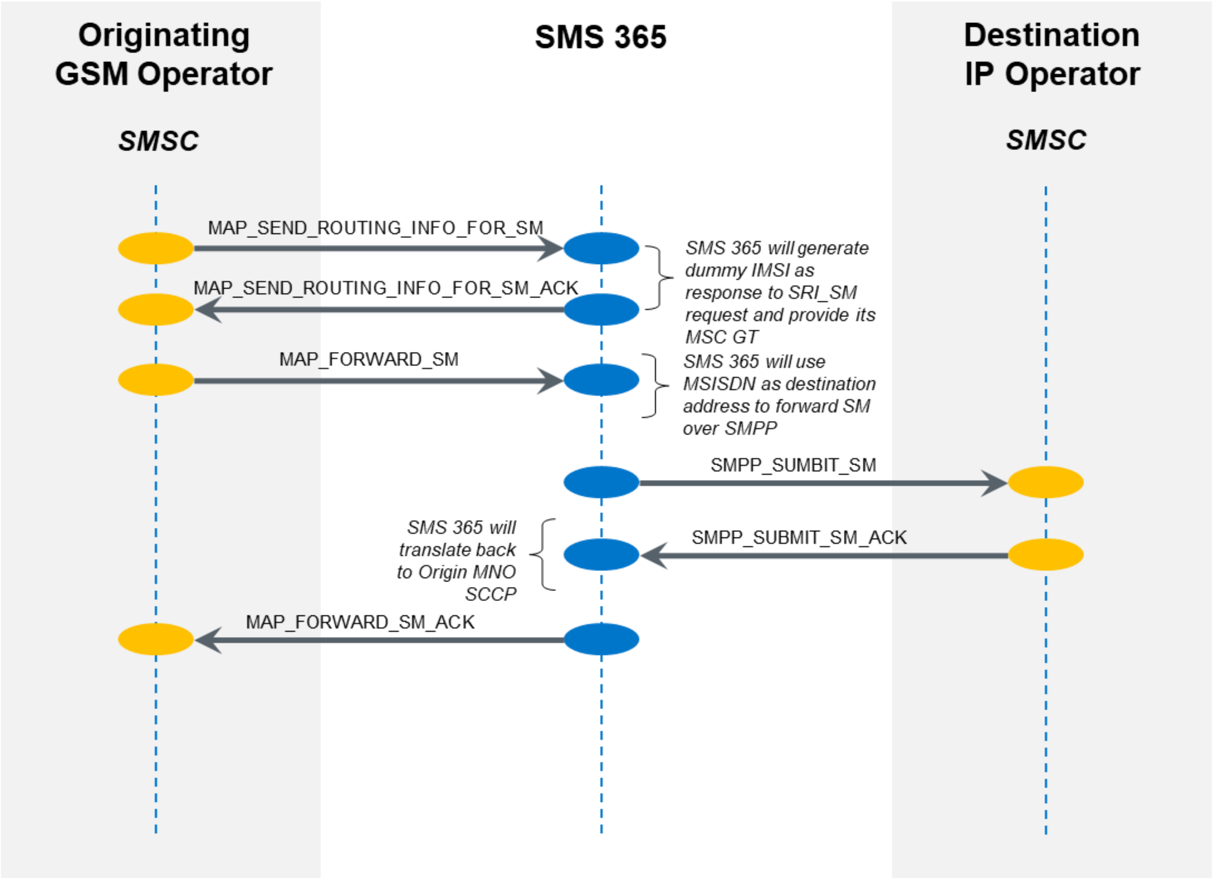
8.4 SS7 End to End Delivery – Mobile Originator to GSM Roaming Subscriber – Scenario 3

In this message flow scenario, the Originating Operator is in Relay Mode and has a direct relationship with the Destination HPLMN; therefore, the SRI for SM is sent directly from Originating Operator to the HLR of the Destination HPLMN. The subscriber is roaming on a VPLMN that the Originating Operator can only reach via SMS 365. SMS 365 will only receive the FSM MT.



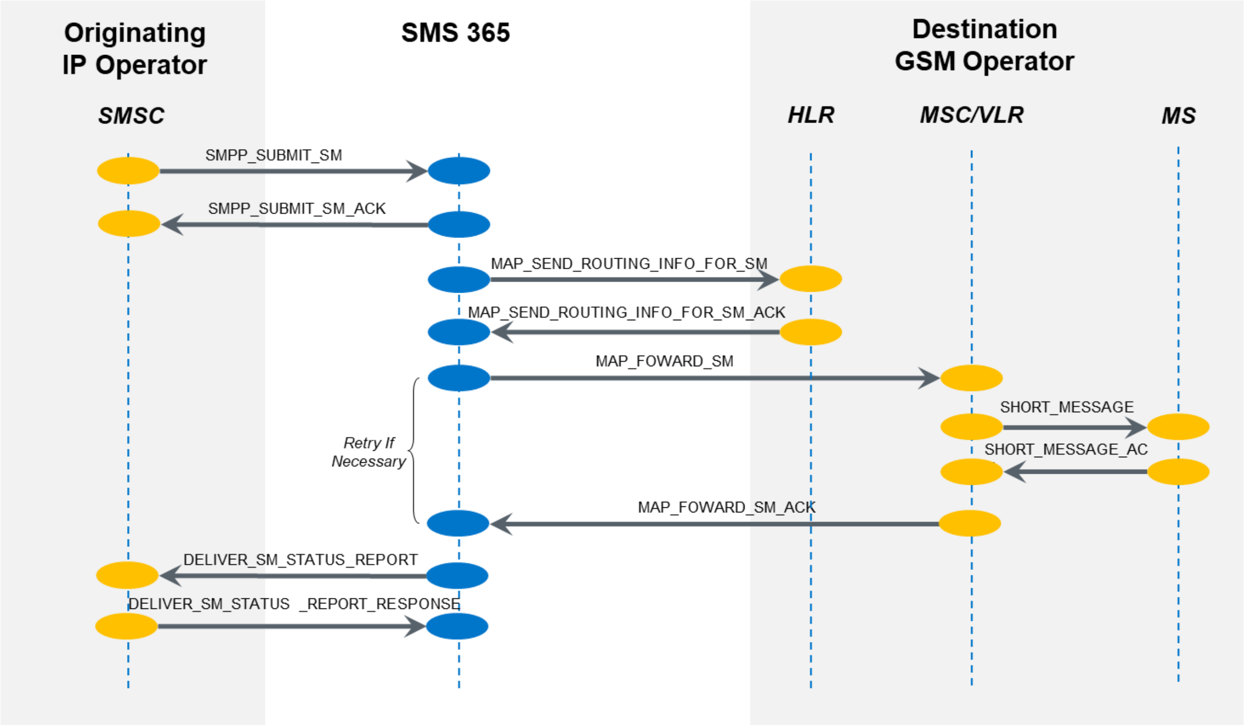
8.5 SS7 to SMPP Delivery – Similar for other IP Based Protocols

In this message flow scenario, the originating operator is a SMS 365 SS7 connected customer, sending a message to a SMS 365 IP connected operator.


Originating GSM Operator
SMSC
SMS 365
Destination IP Operator
SMSC
MAP_SEND_ROUTING_INFO_FOR_SM
MAP_SEND_ROUTING_INFO_FOR_SM_ACK
SMS 365 will generate dummy IMSI as response to SRI_SM request and provide its MSC GT
MAP_FORWARD_SM
SMS 365 will use MSISDN as destination address to forward SM over SMPP
SMPP_SUMBIT_SM
SMS 365 will translate back to Origin MNO SCCP
SMPP_SUBMIT_SM_ACK
MAP_FORWARD_SM_ACK

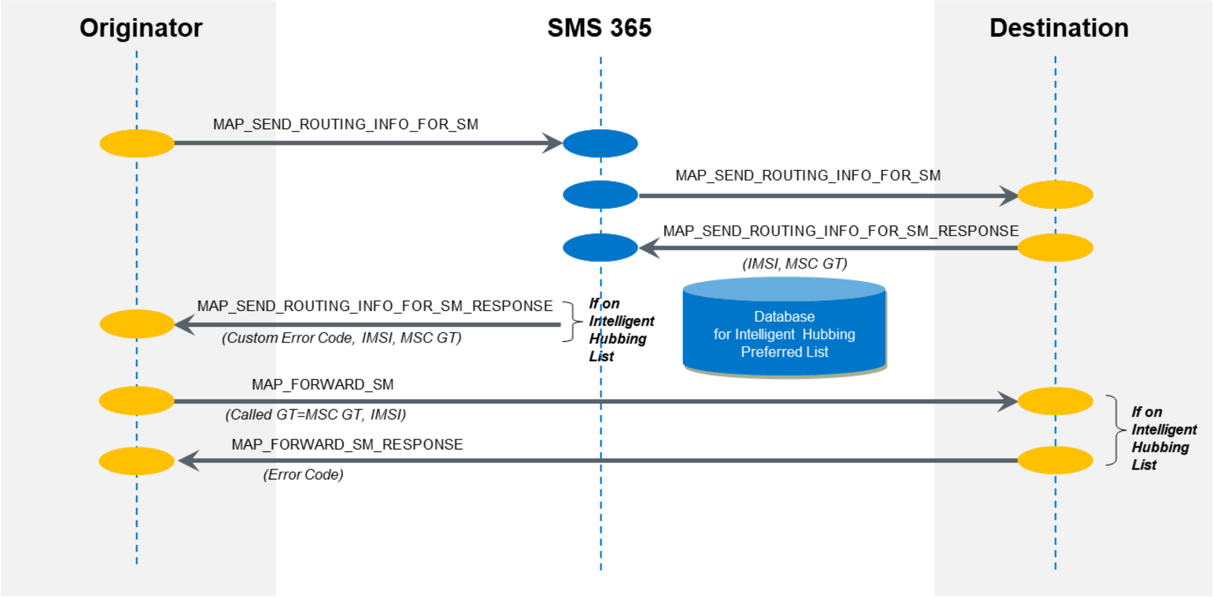
8.6 SMPP to SS7 Delivery – Similar for other IP Based Protocols

In this message flow scenario, the originating operator is a SMS 365 IP connected customer, sending a message to a SMS 365 SS7 connected operator.



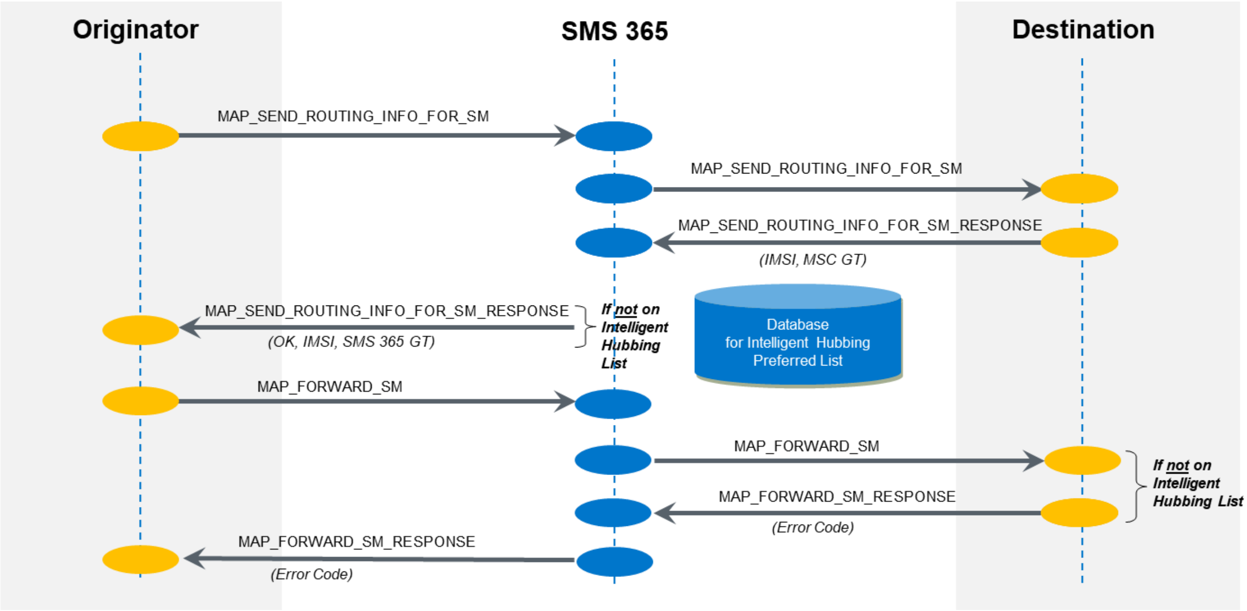
8.7 Intelligent Hubbing 365 – If Destination Operator is on Preferred List

In this Intelligent Hubbing 365 message flow scenario, the destination operator is on the Intelligent Hubbing preferred list.


Originator
SMS 365
Destination
MAP_SEND_ROUTING_INFO_FOR_SM
MAP_SEND_ROUTING_INFO_FOR_SM
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(IMSI, MSC GT)
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(Custom Error Code, IMSI, MSC GT)
If on Intelligent Hubbing List
Database for Intelligent Hubbing Preferred List
MAP_FORWARD_SM
(Called GT=MSC GT, IMSI)
MAP_FORWARD_SM_RESPONSE
(Error Code)
If on Intelligent Hubbing List

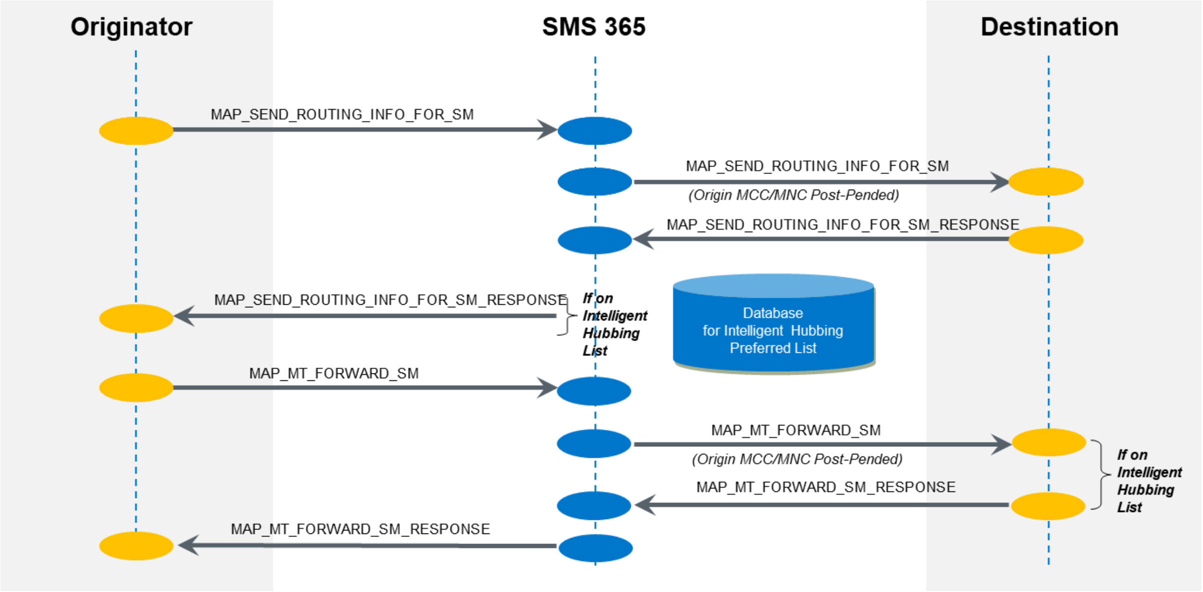
8.8 Intelligent Hubbing 365 – If Destination Operator is not on Preferred List

In this Intelligent Hubbing 365 message flow scenario, the destination operator is not on the Intelligent Hubbing preferred list.


Originator
SMS 365
Destination
MAP_SEND_ROUTING_INFO_FOR_SM
MAP_SEND_ROUTING_INFO_FOR_SM
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(IMSI, MSC GT)
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
(OK, IMSI, SMS 365 GT)
If not on Intelligent Hubbing List
Database for Intelligent Hubbing Preferred List
MAP_FORWARD_SM
MAP_FORWARD_SM
If not on Intelligent Hubbing List
MAP_FORWARD_SM_RESPONSE
(Error Code)
MAP_FORWARD_SM_RESPONSE
(Error Code)

8.9 Intelligent Hubbing 365 – with Origin MCC/MNC Post-Pended

In this Intelligent Hubbing 365 message flow scenario, the Origin MCC/MNC is post-pended at the MAP Level SC Address.


Originator
SMS 365
Destination
MAP_SEND_ROUTING_INFO_FOR_SM
MAP_SEND_ROUTING_INFO_FOR_SM
(Origin MCC/MNC Post-Pended)
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
MAP_SEND_ROUTING_INFO_FOR_SM_RESPONSE
If on Intelligent Hubbing List
Database for Intelligent Hubbing Preferred List
MAP_MT_FORWARD_SM
MAP_MT_FORWARD_SM
(Origin MCC/MNC Post-Pended)
MAP_MT_FORWARD_SM_RESPONSE
If on Intelligent Hubbing List
MAP_MT_FORWARD_SM_RESPONSE