



Telstra Mobile SMS ACCESS MANAGER Technical Guide.

Table of Contents

1.	Introduction	4
2.	Selection of Access Method	4
3.	Access Method Requirements	5
4.	Access Method Details	6
4.1	Dial-Up Access	6
4.2	SMPP Access	6
4.2.1	Connection via Internet VPN	6
4.2.2	Connection via SMS Private Network	7
4.2.3	Connection via Frame Relay	8
4.2.4	Firewall Configuration	9
4.3	Bandwidth Requirements	9
4.3.1	Quick Reference Table	10
5.	SMS Protocols	10
5.1	SMPP	10
5.1.1	Feature Set	11
5.1.2	SMPP Toolkit	16
5.1.3	Other SMPP Toolkits	16
5.2.	Consultancy Services	16
	Glossary	17

1. Introduction

This technical guide should be read in conjunction with the Telstra MobileNet® SMS Access Manager Product Guide. It provides a technical overview of the service, describes how to connect to it and the associated interfaces that you must have prior to connecting.

2. Selection of Access Method

There are three methods of accessing the SMS Access Manager service and these are described in Section 5 and Section 7 of the SMS Access Manager Product Guide.

Consider the following summary:

Wireless Access

This method provides on-the-road access to Telstra's SMS network anywhere in Australia. This is achieved via a mobile handset (or GSM modem) and a computer. The handset needs to be interfaced with a computer equipped with handset compatible software. This solution is suited to minimal throughput requirements eg: < 5000 messages per month.

Dial-Up Access

This method provides access via a computer equipped with a modem. With this solution you can choose between two levels of access: single message dial up and multi-message dial up. Both levels of access are designed to allow connection of your own message sending software based on the TAP protocol. This solution is suited to small throughput requirements eg: < 10,000 messages per month.

SMPP Access

This method provides access via TCP/IP. It utilises an open protocol called the Short Message Peer to Peer protocol ("SMPP") to allow sending and receiving of messages with advanced delivery options. This solution is suited to medium to high throughput requirements eg: > 10,000 messages per month.

Consider the following TCP/IP connection methods:

Internet VPN Connection

This connection method lets you use your existing Internet connection (dial up modem, ISDN, Cable, ADSL and Frame Relay) in conjunction with the provided VPN configuration to securely connect into the SMS network.

SMS Private Network Connection

This connection method lets you dial directly into a private IP network using a dial up modem or ISDN service and is provisioned with a dedicated access number.

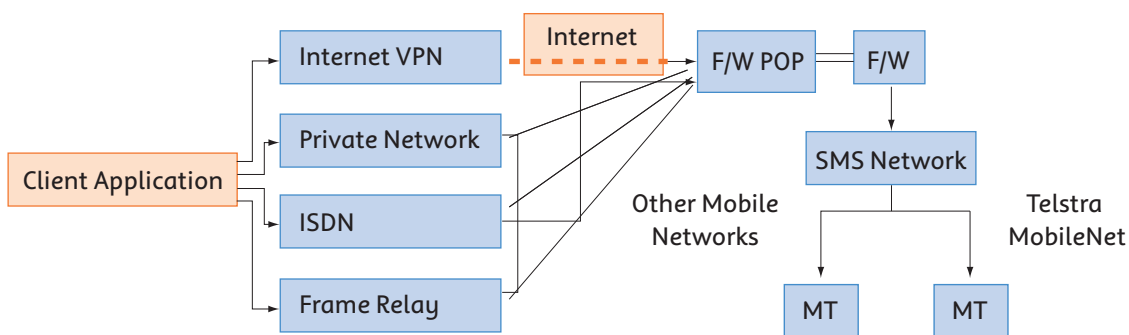
Frame Relay Connection

This connection method provides you with constant bandwidth and direct physical connectivity.

3. Access Method Requirements

Depending on the chosen method of access, you will require some of the following.

(Items marked with an * can be provided by Telstra):



Wireless Access

- Telstra SIM Card*
- Mobile Connection Kit suitable for use with your brand and model of mobile phone* OR a GSM modem OR other SMS generation device*.

Dial-Up Access

- PC/Server running client software supporting the Telocator Alphanumeric Protocol (TAP).
- PC modem.
- PSTN line service* (eg Telstra HomeLine).

SMPP Access

Connection via Internet VPN

- PC/Server running client software supporting the SMPP Protocol.
- IPSEC capable router (Cisco VPN concentrator 3000 compatible) Cisco VPN client* which supports IPSEC.
- Internet service* (eg. Telstra Big Pond).

Connection via SMS Private Network

- PC/Server running client software supporting the SMPP Protocol.
- PC modem or ISDN modem*.
- PSTN line service* (eg Telstra HomeLine) or ISDN line service* (eg Telstra OnRamp).

Connection via Frame Relay

- PC/Server running client software supporting the SMPP Protocol.
- Cisco router.
- Frame relay service* (eg Telstra Frame Relay).

4. Access Method Details

4.1. Dial-Up Access

The single message dial-up option provides for one message per phone call and a maximum connection time of one minute. This option is charged to your originating line as a timed mobile call.

The multi message dial-up option provides up to 99 messages per phone call and a maximum connection time of three minutes. You will be provided with a username and password as part of service provisioning. This service is charged to your SMS Access Manager service with applicable tariffs.

This access method should be used for existing TAP equipment and cannot be used to receive SMS messages.

4.2. SMPP Access

4.2.1. Connection via Internet VPN

Two types of Internet VPN are available:

Access VPN	Allows a single machine to remotely access this service (Client to LAN VPN) over shared infrastructure (the Internet)
ExtraNet VPN	Allows a corporate Intranet to access this service over (LAN to LAN VPN) shared infrastructure (the Internet)

For a description of what a Virtual Private Network (VPN) is, terminology and typical deployment options please refer to:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/vpn.htm

4.2.1.1. Certificate Details

Telstra uses the following protocols for VPN encryption and authentication:

Authentication	ESP/MD5/HMAC-128
Encryption	3DES-168
IKE Proposal	IKE-3DES-MD5

All certificate keys are 168bits.

4.2.1.2. Access VPN

Consider the following steps and system requirements:

- ensure that you have the appropriate ports open to the Internet;
- ensure that you have an Internet routable IP address for each machine wishing to access the SMS Network;
- ensure that you have altered your firewall (if any) to allow access to all the ports used by the VPN tunnel;
- ensure that you are not using Network Address Translation (NAT);
- a pre-configured VPN Client suitable for use with Windows 95/98/NT/2000 will be provided – for other systems you will need to obtain your own VPN client or IPSEC router and configure it using the provided details.

4.2.1.3. ExtraNet VPN

Consider the following steps and system requirements. You will need to ensure that:

- your intranet has a connection to the Internet;
- you have a static, Internet routable IP address for each machine within the LAN wishing to access the SMS Network;
- you have altered your firewall (if any) to allow access to all the ports used by the VPN tunnel;
- you have an IPSEC capable router (Cisco VPN Concentrator 3000 compatible) and it is configured accordingly;
- you have not installed any application-level proxy servers between your LAN and the Internet. Ensure that you record the following:
 - the static, Internet routable IP address for each machine within the LAN which will be accessing the Internet VPN;
 - the IPSEC router's static, Internet routable IP address;
 - the LAN's static Netmask.

Please note, for the relevant port numbers refer to Section 6: Firewall Configuration.

4.2.2. Connection via SMS Private Network

A private IP network facilitates connection via the SMS Private Network. For a description of private IP networks, and typical deployment options please refer to:

<http://www.telstra.com.au/dialip/>

While a private IP network connection can be provided via a range of methods, SMS Access Manager currently supports the following connection methods:

- Dial Up Modem
- ISDN Modem

4.2.2.1. Dial up modem

Consider the following steps and system requirements:

- for this option, you will require a modem and PPP software on your Client PC configured as if you are connecting to a standard ISP;
- by connecting using the provided dial up number and authenticating using the provided username and password a connection to the SMS Private network is established – an Internet registered IP address is automatically assigned.

4.2.2.2. ISDN modem

Consider the following steps and system requirements:

- apply for a Telstra ISDN connection or related product using <http://www.telstra.com.au/onramp/>
- ensure that you have an ISDN modem or Terminal Adaptor – the ISDN modem configuration parameters are located at: <http://www.telstra.com.au/dialip/configuration.htm>
- configure your Client PC to connect to the SMS Private Network using the provided ISDN FNN and username/password.

Calls to the ISDN FNN from Telstra fixed line services are charged at the local rate applicable to the access service. A single access number applies across Australia.

Multilink ISDN 128Kbps connections can be supported using MP+ or BACP protocols.

Multilink ISDN connections greater than 128K are not supported.

4.2.3. Connection via Frame Relay

For a description of a Frame Relay connection, and typical deployment options please refer to:

http://www.telstra.com.au/products/product.cfm?prod_id=3132. There are two possible

implementations of a Frame Relay connection:

- installing a new Frame Relay connection;
- leveraging off an existing Frame Relay connection and installing additional PVC's with appropriate CIR's.

4.2.3.1. New Frame Relay Connection

Consider the following steps and system requirements:

- provision one Primary PVC and one Secondary PVC configured in failover fashion between your site and the SMS network – where a physical redundant link to the Frame Relay network is required, two independent lines should be installed with each containing one PVC;
- ensure that the following is recorded;
- your Primary FNN;
- your Primary DLCI;
- SMS network Primary DLCI;
- your Secondary FNN;
- your Secondary DLCI;
- SMS network Secondary DLCI;
- CIR for the PVCs;
- your site contact details;
- an IP address will be assigned to the Frame Relay facing side of your router and to the Frame Relay facing side of the SMS network router – these are static Internet Registered IP addresses located in a private segmented network protected by router access classes;
- you will need to assign an Internet Registered IP Address to your Client PC and supply this, along with the LAN net mask;
- you will need to configure a route in your LAN network from your Client PC to your router and out on the Frame Relay link.

The SMS network has points of presence for Frame Relay connections in Brisbane and Sydney. The relevant details will be made available during the provisioning process. Also note, Telstra will automatically allocate DLCI's during the provisioning process from the next available DLCI for that network.

4.2.3.2. Existing Frame Relay Connection

Consider the following steps and system requirements:

- apply for a modification of a Telstra Frame Relay service or related product;
- provision two additional PVC's as described above.

4.2.4. Firewall Configuration

4.2.4.1. Connection via Internet VPN

If you are using an Internet VPN connection you will need to ensure that the following bi-directional connections are allowed in your firewall to allow the IPSEC tunnel to pass through it:

Machine	VPN Server
Internet Address	<i>Provided upon Provisioning</i>
Port Address	UDP 500 UDP 10000
Protocols	50 & 51

4.2.4.2. Connection via Frame Relay

If you are using a Frame Relay connection you will need to ensure that the following bi-directional connections are allowed in your firewall to allow the SMPP packets to pass through it:

Machine	SMS Network
Internet Address	<i>Provided upon Provisioning</i>
Port Address	TCP 8490
Protocols	SMPP

4.3. Bandwidth Requirements

This table provides guidelines as to what bandwidth you need to provision between your site and the Telstra SMS network to cope with a given message transmission rate. This message rate is not the end-to-end message rate, only the message rate between your site and the SMS Network. Actual end-to-end message rate will be affected by traffic congestion, quality of service parameters and other issues.

4.3.1. Quick Reference Table

Access Method	Bandwidth	Approx. Messages per second
Wireless Access	Na	1 per 7 seconds
Dial-Up Access	Na	Varies according to product feature selection.
Dial-up modem	28.8Kbit/s	5
ISDN (1 B Channel)	64Kbit/s	15
ISDN (2 B Channels)	128Kbit/s	30
Frame Relay	64Kbit/s	15
Frame Relay	128Kbit/s	30
Internet VPN	Select any access method listed above and take into account reduction factor	Varies according to Internet Access method.

5. SMS Protocols

5.1. SMPP

The SMPP protocol is an open standard protocol designed to provide a flexible data-communications interface for the transfer of short messages. It has been specifically designed to enable applications and value-added products to communicate with an access gateway. For a more comprehensive discussion of the SMPP protocol please refer to the specification at : <http://www.smpp.org>

Document	SMPP (Short Message Peer To Peer) Protocol Specification v3.4
Document Version	12-October-1999 Issue 1.2

5.1.1. Feature Set

The following table details the SMPP operations supported by SMS Access Manager. Please note there may be instances where the usage of unsupported features will be permitted. Please consult your Telstra Mobile representative for further information. Features not listed here are not supported.

Item	Functional Unit/Description	SMPP REF.	Support	
			YES	NO
PDU-OUTBIND	Is the outbind PDU supported?	4.1.7		•
PDU-BIND-TRANSMITTER	Is the bind transmitter PDU supported?	4.1.1 4.1.2	•	
PDU-BIND-RECEIVER	Is the bind receiver PDU supported?	4.1.3 4.1.4	•	
PDU-BIND-TRANSCIEVER	Is the bind transceiver PDU supported?	4.1.5 4.1.6		•
PDU-UNBIND	Is the unbind PDU supported?	4.2.1 4.2.2	•	
PDU-ESME-GENERIC-NACK	Is the generic_nack PDU initiated by the EMSE supported?	4.3.1	•	
PDU-SMSC-GENERIC-NACK	Is the generic_nack PDU initiated by the SMSC supported?	4.3.1	•	
PDU-SUBMIT-SM [Refer to 5.1.1.1]	Is the submit_sm PDU supported?	4.4.1 4.4.2	•	
PDU-SUBMIT-MULTI	Is the submit_multi PDU supported?	4.5.1 4.5.2		•
PDU-DELIVER-SM [Refer to 5.1.1.2]	Is the deliver_sm PDU supported?	4.6.1 4.6.2	•	
PDU-ESME-DATA	Is the data_sm PDU initiated by the EMSE supported?	4.7.1		•
PDU-SMSC-DATA	Is the data_sm PDU initiated by the SMSC supported?	4.7.1		•
PDU-QUERY*	Is the query_sm PDU supported?	4.8.1 4.8.2		•
PDU-CANCEL*	Is the cancel_sm PDU supported?	4.9.1 4.9.2		•
PDU-REPLACE*	Is the replace_sm PDU supported?	4.10.1 4.10.2		•
PDU-ESME-ENQUIRE-LINK	Is the enquire_link PDU initiated by the EMSE supported?	4.11.1 4.11.2	•	
PDU-SMSC-ENQUIRE-LINK	Is the enquire_link PDU initiated by the SMSC supported?	4.11.1 4.11.2	•	
PDU-ALERT	Is the alert_notification PDU supported?	4.12.1		•

5.1.1.1. PDU-Submit

5.1.1.2. PDU-Deliver

Item	Functional Unit/Description	SMPP REF.	Support	
			YES	NO
SUBMIT-1	Is the use of different values in the <i>service_type</i> field allowed?	5.2.11		•
SUBMIT-2	Is the use of default values in the <i>source_addr</i> fields supported?	5.2.8	•	
SUBMIT-3	Is <i>scheduled_delivery</i> supported?	5.2.15		•
SUBMIT-4	Is the <i>replace_if_present</i> functionality supported?	5.2.18	•	
SUBMIT-5	Are pre-defined short messages supported?	5.2.23		•
SUBMIT-6	Is the use of the <i>validity_period</i> field supported?	5.2.16	•	
SUMBIT-26	What is the maximum length of <i>message_payload</i> data supported?	5.3.2.32	140 Binary Octets or 160 ANSI Characters	

Consider the following specific questions

relevant to PDU-Submit:

SMPP field	Issue and question	SMPP REF.	Answer
Submit-Field1	What, if any restrictions are imposed upon the value used in the <i>service_type</i> field?	5.2.11	Must be MHS or as assigned by Telstra. This value is overwritten in the incoming SMPP packet to enforce this.
Submit-Field2	What values in the <i>esme_class</i> field are supported, and in what circumstances?	5.2.12	<ul style="list-style-type: none"> • SMSC Delivery Receipt • UDHI Indication • Reply Path Indication
Submit-Field3	What values in the <i>protocol_id</i> field are supported, and in what circumstances?	5.2.13	Described in Engineering Document SMI091.
Submit-Field4	What values in the <i>priority</i> field are supported, and in what circumstances?	5.2.14	Must be Level 1 Priority. This value is overwritten in the incoming SMPP packet to enforce this.
Submit-Field5	What, if any restrictions are imposed upon the value used in the <i>schedule_delivery_time</i> field?	5.2.15	Must be NULL This value is overwritten in the incoming SMPP packet to enforce this.
Submit-Field6	What, if any restrictions are imposed upon the value used in the <i>validity_period</i> field?	5.2.16	Maximum of 7 days . The message is 'Expired' after this time.
Submit-Field7	Which values in the <i>registered_delivery</i> field are supported?	5.2.17	<ul style="list-style-type: none"> • No SMSC Delivery Receipt requested • SMSC Delivery Receipt on success and failure
Submit-Field8	Are there any restrictions set upon the values specified in the <i>data_coding</i> field?	5.2.19	No.
Submit-Field9	How many canned messages are supported via the <i>sm_default_allowed</i> field?	5.2.20	Function not supported.

5.1.1.2. PDU-Deliver

Item	Functional Unit/Description	SMPP REF.	Support	
			YES	NO
DELIVER-1*	Is the use of different values in the <i>service_type</i> field allowed?	5.2.11		•
DELIVER-16	What is the maximum length of <i>message_payload</i> data supported?	5.3.2.32	140 Binary Octets or 160 ANSI Characters	

Consider the following specific questions relevant to PDU-Deliver:

SMPP field	Issue and question	SMPP REF.	Answer
Deliver-Field1	What, if any restrictions are imposed upon the value used in the <i>service_type</i> field.	5.2.11	Must be MHS or as assigned by Telstra. This value is overwritten in the outgoing SMPP packet to enforce this.
Deliver-Field2	What values in the <i>esme_class</i> field are supported, and in what circumstances?	5.2.12	<ul style="list-style-type: none"> • SMSC Delivery Receipt • UDHI Indication • Reply Path Indication
Deliver-Field3	What values in the <i>protocol_id</i> field are supported, and in what circumstances?	5.2.13	Described in Engineering Document SMI091.
Deliver-Field4	What values in the <i>priority</i> field are supported, and in what circumstances?	5.2.14	Must be Level 1 Priority. This value is overwritten in the outgoing SMPP packet to enforce this.
Deliver-Field5	Which values in the <i>registered_delivery</i> field are supported?	5.2.17	<ul style="list-style-type: none"> • No SMSC Registered Message requested • SMSC Registered Message on success and failure
Deliver-Field6	Are there any restrictions set upon the values specified in the <i>data_coding</i> field?	5.2.19	No.

5.1.1.3. Message Types

Item	Functional Unit/Description	SMPP REF.	Support	
			YES	NO
TYPE-1	Are normal data messages transmitted?	2.11	•	
TYPE-2	Can SMSC Registered Message be requested and obeyed?	2.11	•	

5.1.1.3.1 Registered Messages

When a message enters the SMS network, it is forwarded to the mobile network for delivery. As the message passes through the network it change states – these states reflect the progress of message delivery. At a later date the SMSC will return a message (or final state notification), including the MessageID, to the source address that originally submitted the message – the following notifications are applicable:

State	Description
Delivered	The message has been successfully sent to a mobile phone (for Telstra Mobile services) or has reached a final state (for non-Telstra Mobile services).
Undeliverable	A condition exists that prevents message delivery – that is, the SMSC does not know how to route the message to its destination (e.g. invalid mobile number).
Deleted	The message has been deleted by Telstra Mobile – for example, the PDU-CANCEL has been sent or the message has been manually deleted.
Accepted	The message has been marked by Telstra Mobile as sent.
Unknown	The message is in an invalid state.
Rejected	The message is in a rejected state.
Expired!	The message validity period has expired.

While a final state notification can be supported within the Telstra Mobile network, it may not be supported where the messages terminate on another network. In this regard, the full extent of functionality is limited, as Telstra Mobile is not responsible for the configuration and architecture of the terminating network.

Upon receipt of the final state notification, the onus is on the customer's application to match the notification message with the message originally submitted to the SMS network. Please note, for this to be effective the following conditions apply:

- the source address must be a legitimate routable number (eg. 614xxx);
- the customer's application must have a continuous receiver bind into the SMS network.

5.1.1.4. Telstra Mobile SMSC Specific

Item	Functional Unit/Description	SMPP REF.	Support	
			YES	NO
SMSC-1	Can a Store and Forward method of final delivery be used?	2.10	•	
SMSC-2	Can a Datagram method of final delivery be used?	2.10		•
SMSC-3	Can a Transaction mode method of final delivery be used?	2.10		•
SMSC-4	Can this initiate a session by using the outbind operation sequence?	2.2.1		•
SMSC-5*	What is the maximum length of <i>message_id</i> supported in operations?	5.2.23	Not Supported	

Item	Functional Unit/Description	SMPP REF.	Support	
			YES	NO
IMP-SMSC-1	Is information in a bind PDU used for access control?		•	
IMP-SMSC-2	Can the information in the bind PDU be used for routing messages to the ESME?		•	
IMP-SMSC-3	In a cancel_sm received from an ESME, must the <i>service_type</i> field be set to the same value as the original message which is being canceled?	5.2.12	•	
IMP-SMSC-4*	In a replace_sm received from an ESME, must the <i>service_type</i> field be set to the same value as the original message which is being replaced?	5.2.12	•	

5.1.1.4.1 SMS Numbering Requirements

Item	Functional Unit/Description	SMPP REF.	Support	
			YES	NO
SMSC-Num-1	SMPP Originating Address/TPOA. This must be a valid ACIF assigned number. ACIF numbers assigned to Telstra must be in the standard E164 format (eg 614xxx).			
SMSC-Num-2	Alpha Codes – Source and Destination Addresses. This is an address containing non-numeric characters – '*' and '#' are considered non-numeric characters.			•
SMSC-Num-3	Short Codes – Source and Destination Addresses. This is a number not in any of the assigned ACIF number ranges.			•
SMSC-Num-4	Extra Digits – Source and Destination Address. This is an ACIF number with up to 4 additional numeric digits on the end. This is only supported for sources and destinations within Telstra's network.			•

5.1.2. SMPP Toolkit

Telstra can provide a commercial SMPP toolkit.

This toolkit is available under certain Terms and Conditions for the following platforms:

- Linux
- HP Unix 11
- Sun Solaris 2.7 & 2.8
- Microsoft Windows 95
- Microsoft Windows NT 4.0

5.1.3. Other SMPP Toolkits

Other toolkits are available at:

- <http://www.telstra.com.au/mobilenet/services/wddzone.htm>

5.2. Consultancy Services

Telstra does not offer consultancy services to help with the development of your application. However, Telstra can provide an SMPP Toolkit to assist you with your implementation. In addition, Telstra may provide access to an SMSC test environment for you to test your implementation.

Glossary

The following words, acronyms and abbreviations are referred to in this document.

Term	Definition
ACIF	Australian Communications Industry Forum. An industry body overseeing agreements and standards between carriers within Australia.
ADSL	Asynchronous Data Subscriber Link. A method for high-speed data transfer over PSTN lines.
CIR	Committed Information Rate. Represents bandwidth allocated to a Frame Relay connection.
DLCI	Data Link Connection Identifier. Used to identify a connection point within a Frame Relay endpoint.
FNN	Full National Number. Used to identify a communications service.
Frame Relay	A permanent, circuit switched network
F/W	Firewall
GSM	Global System for Mobiles. One of the networks used in Australia to provide mobile phone services.
Internet registered address	An Internet Address which is registered on the Internet but never actually used on the Internet.
Internet routable address	An Internet Address which is used across the Internet.
IP	Internet Protocol
ISDN	Integrated Services Digital Network. The network used for data traffic.
MT	Mobile Termination
POP	Point of Presence
PSTN	Public Switched Trunk Network. The network used for conventional voice and data traffic.
PVC	Permanent Virtual Circuit.
SIM	Subscriber Identity Module. A small card inserted into a device connecting to the GSM network to identify the owner.
SMPP	Short Message Peer to Peer. A protocol for sending and receiving SMS messages over a session link.
SMS	Short Message Service.
SMSC	Short Message Service Centre. A component of the SMS network.
TAP	Telocator Alphanumeric Protocol. A protocol for sending SMS messages using a dial up terminal.
TCP	Transmission Control Protocol.
VPN	Virtual Private Network.

For information visit the website:
www.telstra.com/info/smsaccess