



mBalance wireless network solutions

TextPass™

FIREWALL

White Paper

Version V01.00

CONFIDENTIAL



Executive Summary

Interoperability between operator's SMS networks has been one of the keys to success of SMS. The downside of interoperability is the danger of SMS fraud, commonly known as SMS spamming. The possibilities of abusing SMS have been identified by the GSMA (GSMA SMS fraud White Paper (FF Doc 29/009)) under the four types of SMS fraud: spamming, flooding, faking and spoofing.

In today's SMS networks, protection from hostile SMS spam attacks is getting increasingly difficult as fraud techniques are becoming more advanced. For example, by spoofing, (changing the SMSC SCCP address in the SMS message), spammers make it very difficult to distinguish a spam message from a legitimate message from a partner network. Two things are required to defy the high-tech international SMS spammers. First, basic screening and filtering on SMS (MAP and SCCP) fields is needed. Second, advanced anti-spoofing and anti-faking technology as well as effective spam and flooding-detection technology are required.

A Mobile Network Operator must be able to cope with the ever increasing resourcefulness of spammers from all over the world. This depends on the ability to respond quickly to changing tactics and spam techniques. With the increasing threat of SMS spam, a solid spam protection is an essential customer care asset. The TextPass™ Firewall has a powerful rule-based routing and filtering engine that allows for immediate response to new spam methods. This can be done on-line, without any service interruption, by using a web-based GUI.

The highlights of the TextPass™ SMS firewall are:

- ▶ Powerful screening; extreme performance of 1000SM/s per device with SS.7 and SIGTRAN.
- ▶ Highly flexible rule-based filtering with on-line configurable SMS fields as condition.
- ▶ SMS MO screening towards SMSCs and towards applications.
- ▶ SMS MT screening from foreign SMSCs and applications towards mobile subscribers.
- ▶ Advanced anti-spoofing/anti-faking with verification of the originating network and detection of false SMSC addresses.
- ▶ Flooding detection?
- ▶ Fully configurable logging with all message details, suspect messages and blocked messages.
- ▶ Message correction through message field modifiers and replace fields.
- ▶ Throughput regulation and overload protection.
- ▶ Weighted, prioritised and adaptive load balancing for SS.7, SIGTRAN and IP.
- ▶ Real-time statistics with user defined counters and web interface.
- ▶ Intuitive web interface for operation and maintenance.
- ▶ Rack mounted 19-inch architecture for unlimited scalability.



Firewall Introduction

The persistence of SMS spam is a growing concern for mobile network operators worldwide. Measures taken over the last few years have significantly reduced the amount of spam. Yet mobile network operators still suffer from regular attacks. New threats are on the horizon as the capabilities and flexibility of mobile terminals increase.

This White Paper provides background information on SMS spam. It also discusses (new) potential threats. In addition it describes how a mobile network operator can protect its network and minimize fraud against the ever changing nature of SMS spam.

Implementation of SMS Firewall functionality to protect and optimize the SS.7 network is an attractive alternative compared to investing in legacy SS.7 equipment. It provides network operators with a technically superior, future-proof and cost-effective solution.

The **TextPass™** FIREWALL, based on the market leading **TextPass™** ROUTER offers advanced spam detection and filtering capabilities for all MO and MT messages. This includes content filtering on specific or malicious content. Detection triggers and filter settings can be adapted real-time. This enables network operators to react very quickly on newly emerging threats.



Addressing SMS Threats

Introduction

The **TextPass™** Firewall is designed to protect Mobile Subscribers and Mobile Operator Equipment from SMS related network operations such as:

- ▶ Spoofed Mobile Originated SMS
- ▶ Spoofed Mobile Terminated SMS (Faking)
- ▶ Spam messages
- ▶ SS.7 Protocol Violations
- ▶ Flooding

The risks of the above mentioned network operations are described on the following sections.

Spoofed Mobile Originated SMS

It is possible that an SME connected to an external SS.7 network is able to present itself to the SMSC and MSC components as a mobile handset roaming in the foreign network. Then it is able to send SMS messages assuming the identity of this handset. This will result in two undesired events:

1. The spoofed party will be charged for an SMS message which was not sent by him/her.
2. The receiving party will hold the spoofed party responsible for the message.

When the spoofed party understands that he paid for something he/she did not initiate, it is likely that this will affect the trust-level in the billing-relationship. This will then put a lot more attention on the invoices. Further it will degrade the trust-level that subscribers inherently have in the SMS communication medium.

Spoofed Mobile Terminated SMS

When an SME or network element in an external SS.7 network is able to send SMS traffic into the home network thereby pretending that these messages originate from another external network, it can cause accounting and accountability issues in the interconnect-revenue balancing.

For example, a network-component in network A is able to originate Mobile Terminated SMS traffic into network B while pretending to be network C. When network B and network C attempt to reconcile their SMS interconnect bill, they will find that network C has sent less SMSs than what was registered in network B. Naturally these messages are actually originated from network A, who will not be invoiced for the relevant messages.

Spam Messages

Spam messages are unsolicited short messages with commercial or malicious content directly targeted at mobile subscribers.

Spam messages can originate from SMS applications, national interconnect networks, international interconnect networks or home-network subscribers. Examples of Spam are applications which pretend to be a bank, a lottery, or chain-mail messages which have a viral effect. Spam messages typically enter the network through valid interfaces and can only be detected by deep content inspection or statistical analysis.

Spam messages will negatively affect customer satisfaction and also lower the level of trust associated with SMS as a communication medium.

Protocol Violations

Protocol violations are usually the result of badly configured network elements. This enables discrepancies in the SCCP / MAP addressing details and other protocol elements in various parts of the SS.7 stack.

Protocol violations are a risk, as it is not clearly defined how network elements will deal with those. This can cause billing and/or other operational issues. Protocol violations are also an indication of unprofessional attempts of spoofing. Some implementations of spoofing software incorrectly adjust the parameters in the stack.

Flooding

SMS Flooding takes place when a message with the same or similar content is sent to a large number of subscribers in a short period of time. The source of the message can be the same for all messages (one Application Provider) or the source address may vary. In the latter case, it is likely that SMS Spoofing or even SMS Impersonation is applied to the SMSC address and/or originator address of the SMS message. These flooding attack can take place on both SCCP and MAP level.

This means that methods that look only at multiple messages from one source may miss the spoofed cases. Therefore, the **TextPass™** SMS Firewall covers multiple flooding cases and provides a way to detect flooding in order to be able to take appropriate measures.

Please note that in combination with the very strong anti-spoofing capabilities of **TextPass™** it is possible to uniquely identify the source (SMSC) responsible for the flooding.

Firewall Advantages

Power and Reliability

A single **TextPass™** Firewall unit can already handle 1000SM/sec (including logging). Using multiple units in a redundant configuration, the system performance can be scaled up to a virtually unlimited system throughput. This unprecedented performance allows you to process unexpected peak traffic before it overloads your network. Now you can introduce SMS security without compromising on the Quality of Service of your network.



Innovation and Flexibility

The **TextPass™** Firewall is based on mBalance's advanced **TextPass™** SMS Router. Therefore it is built on proven technology and provides an extremely flexible and highly efficient SMS routing and filtering solution. This enables mobile network operators to grow and manage their SMS security and market opportunities. The intuitive web-based configuration tool enabled instant responses to changing spam threats and service requirements. At the same time the highest possible quality standards can be maintained.

Simple Integration and Ease of Use

TextPass™ integrates flexibility with existing network environments and all available interfaces:

- ▶ SS.7 interfaces: ITU-T/ANSI/CDMA/China, over normal signalling (64 kbps) and high speed signalling (2Mbps over ATM);
- ▶ SIGTRAN interface: M3UA and SUA;
- ▶ Message logging formats: CSV, ASN.1 and SMSC CDRs;
- ▶ External condition interface, enabling advanced message screening;
- ▶ SMSC white list, offering full operator control on SMS screening.
- ▶ OAM interfaces: SNMP for statistics, configuration and alarming;
- ▶ Provisioning interfaces: SNMP and easy web-based configuration;
- ▶ Statistical interfaces: Providing full real-time traffic details, graphically presented on a web page.

Firewall Abilities

The **TextPass™** Firewall provides the following advantages and use cases to mobile operators:

- ▶ The ability to protect subscribers from spam will increase customer satisfaction.
- ▶ The ability to detect MO-spoofing shields subscribers from fraud messages and prevents wrong phone bills, thereby protecting the subscribers trust in their mobile operator.
- ▶ The ability to detect and prevent MT-spoofed messages from international SMSCs prevents sending incorrect invoices to the wrong interconnect parties.
- ▶ The ability to detect irregularities in the SMS traffic via statistical analysis, which can dramatically reduce SPAM.
- ▶ The ability to detect irregularities in the SMS content via statistical analysis which can significantly reduce SPAM.
- ▶ The ability to prevent any message which has been caught by any of the detection methods above from actually reaching its intended destination.

Return on investment

The **TextPass™** SMS Firewall provides a quick return on investment:

- ▶ Any ability for external parties to use operator network resources without paying for these resources accordingly, can be considered a loss of revenue, or a loss of revenue-opportunity.

- ▶ Spoofed MT messages are an annoyance to subscribers. By being able to prevent these spoofed messages, the customer satisfaction KPI can be increased significantly.
- ▶ Spoofed MO messages are a risk to subscribers, as it affects the direct security of their account with the mobile operator. Once a single case is made public where a subscriber successfully challenges a mobile phone bill, it will have a huge cost impact on the perceived reliability of the mobile operator, and on the additional challenged mobile phone bills.
- ▶ When the interconnect billing-relationship is compromised, a significant part of the mobile operator revenue cannot be recognized until it is certain that no additional claims can be made. This can have a dramatic (temporary) impact on the perceived/accounted profitability of a mobile operator.

An **TextPass™** SMS Firewall provides extreme security and control on SMS traffic, to the benefit of the subscriber and the mobile operator. The **TextPass™** SMS Firewall enables a mobile operator to address all of these aspects.

TextPass™ FIREWALL is based on the proven **TextPass™** ROUTER, commonly recognized in the mobile industry as the most powerful SMS Router available on the market today. The **TextPass™** FIREWALL offers simple integration and ease of use for network operators, and integrates flexibly with existing network environments and all available interfaces:

- ▶ Application (ESME) interfaces: SMPP, UCP, CIMD2, OIS and SMAP;
- ▶ SS.7 interfaces: ITU-T, ANSI, China, over normal signalling (64 kbps), high speed signalling (2 Mbps over ATM), IP (SUA/M3UA);
- ▶ Billing interfaces: supporting any required CDR format, using configurable mediation;
- ▶ OAM interfaces: SNMP for statistics, configuration and alarming;
- ▶ Provisioning interfaces: SNMP and easy web-based configuration from remote terminals;
- ▶ Statistical interfaces: SNMP, providing full real-time traffic details, graphically presented on a web page.

The **TextPass™** FIREWALL offers unprecedented filtering and screening capacity. Maximum reliability is ensured through a N+1 or N+N redundancy scheme. Multiple units can be scaled up to a virtually unlimited system throughput. This kind of performance allows network operators to process unexpected peak traffic before it overloads the network. The **TextPass™** FIREWALL supports weighted load distribution and guaranteed throughput control, as well as overload protection for all SS.7 and IP destinations.

SMS Firewall Technology

The Home Network

Spam initiated via the Home Network usually originates from SMS Service Providers with direct connectivity to the SMSC of the network operator. As this connectivity is fully under the control of the operator, spam can easily be prevented by contractual agreements between operator and Service Provider.

Large scale spam attacks have been reduced significantly in many European countries. Strict enforcement of the agreements mentioned above has substantially contributed to this. Also the preventing of pay-out of kickback from premium-rate phone numbers (which is often the source of income from spam) has helped enormously.

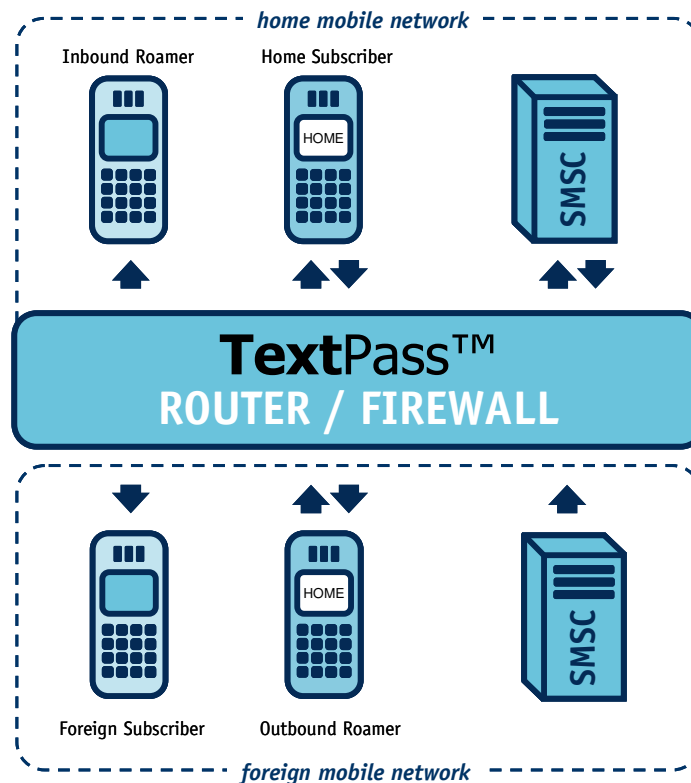


Fig 1. The firewall is an integral part of the home mobile network.

The National and International SS.7 Network

National SS.7 Network

Introduction of termination fees for the delivery of SMS messages on a network is an effective way to reduce spam entering the network via the national and international SS.7 network. Due to the increased costs of sending an SMS message, large-scale spam is no longer commercially attractive. This is commonplace in many European countries, where SMS spam originating from other national mobile operators has virtually been eliminated. In regions or between networks where termination fee arrangements are not in place, there is no financial barrier for the originating SS.7 network to prevent spam. In such a case, state-of-the-art SMS technology will be required to detect and block spam messages.

International SS.7 Network

These days, the focus of operators looking at spam prevention is the international SS.7 network. Spam entering the mobile network directly or indirectly via international SS.7 links is complex to eliminate as the parties are numerous and sometimes anonymous. A rudimentary measure usually taken is to create a 'White List' of SS.7 networks which are allowed to terminate SMS messages on a network, in combination with termination fee agreements. While this method works, it has a major drawback: customers of networks which are not on the White List cannot send SMS messages to subscribers and roamers on the destination network. Also network operators who do not own their own SS.7 equipment have limited capability to control incoming SS.7 traffic.

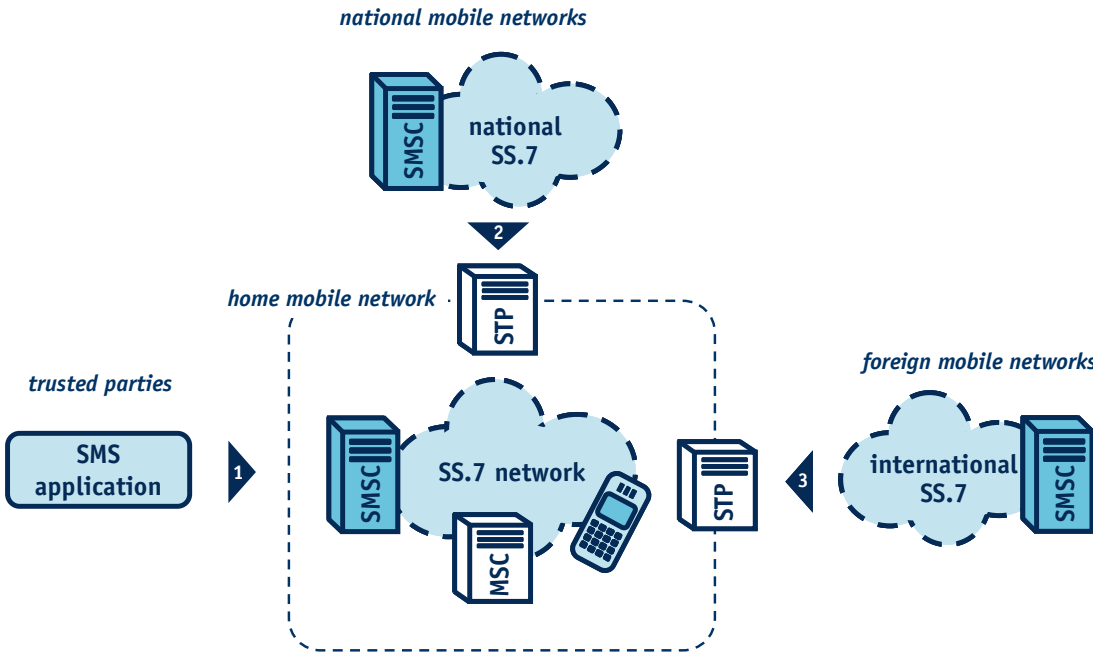


Fig 2. Mobile network relationships.

Providing full subscriber security requires the following interception points:

- 1) Mobile Terminated international originated traffic.
- 2) Mobile Originated international roaming traffic.
- 3) Mobile Originated local traffic.
- 4) Mobile Terminated national, and Mobile Originated national roaming traffic.
- 5) Application Originated traffic

SMS Filtering

TextPass™ FIREWALL will screen and filter the SMS messages based not only on SCCP and MAP fields, but also on message content. The SMS Firewall capabilities of TextPass™ are based on user definable rules that block and pass an incoming message. It is also possible to store a copy of all or a selection of messages, for example for off-line analysis of incoming message traffic. The filter criteria can be changed real-time via a simple GUI, and can be applied to all or a (fully configurable) selection of originators and/or recipients.

The diagram below depicts the network architecture including the **TextPass™** FIREWALL. The incoming MAP traffic entering the network on an STP is routed by the STP (using MAP Screening or similar features) to the **TextPass™** FIREWALL. Alternatively, if the SS.7 traffic enters the network directly on a **TextPass™** FIREWALL, all non-SMS traffic is passed to the STP for further routing.

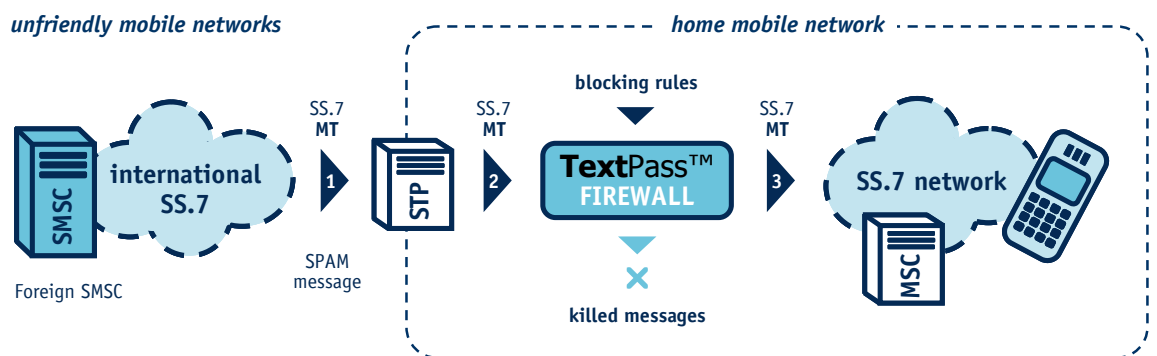


Fig 3. Firewall inbound MT screening.

Spoofing Detection

In many cases SMS spoofing techniques are applied to SPAM messages to try to avoid termination fees and circumvent basic originating network based traffic blockades. It can be categorically stated that spoofed SMS messages are very harmful and extremely undesired.

The RTR can be optionally enable with firewall functions that can be configured to detect SMS spoofing for incoming MO and incoming MT SMS messages. SMS spoofing can be defined as: "the act of one SME impersonating another SME".

SMS spoofing is generally done by replacing the SCCP addresses with forged addresses, usually real addresses of different networks. SMS spoofing is done at both the SCCP and MAP level for all relevant SMS operations:

- ▶ SendRoutingInfoForSm,
- ▶ MtForwardSm and MoForwardSM.

The **TextPass™** FIREWALL is able to detect perfectly spoofed Mobile Originated messages which contain the correct IMSI and MSC pairs.

Flooding Detection

The following flooding situations are covered by the SMS Firewall:

- ▶ **Out-of-profile message quantity from a single source.** The amount of messages from a specific source is significantly more than the expected defined amount (*the profile*) for this source. Note that the source is typically an Application, Country or Network.
Example: Normally, on Wednesday morning between 10h00 and 11h00 between 500 and 1400 message are received from France (profile is: 1400 +50%), when on Wednesday morning at 10h15 suddenly 3600 messages are received from France this is potential flooding and an alarm is raised.
- ▶ **Similar messages from a single source.** Identical or similar messages are sent from the same source. Note that in most cases this is a legal activity of for example an SMS Application Provider (“authorized flooding”).
Example: 15000 messages with the same content are coming from a specific foreign GSM network.
- ▶ **Similar messages to many destinations.** Identical or similar messages are sent to a significant amount of subscribers.
Example: The message “Buy cheap phones, call (0900) 12345” is sent to 5000 subscribers.
- ▶ **Similar messages to sequential destinations.** Identical or similar messages are sent to subscribers with sequential MSISDNs, indicating that the sender is trying out destination MSISDNs.
Example: The message “Buy cheap phones, call (0900) 12345” is sent to 100,000 subscribers with MSISDN in range xxxxx00000 to xxxxx99999.
- ▶ **Similar messages to invalid destinations.** Identical or similar messages are sent to non-existing subscribers (MSISDN not in HLR), indicating that the sender is trying out destination MSISDNs.
Example: The message “Buy cheap phones, call (0900) 12345” is sent to 38 unknown subscribers (not registered in HLR).



About TextPass™

The mBalance **TextPass™** messaging solution platform comprises a series of products for SMS routing & security(SS.7/SIGTRAN and applications), real-time message statistics and generic network Querying products.

To date **TextPass™** is deployed in many mobile networks throughout the world.

About mBalance

mBalance provides mobile network operators, system integrators and OEMs with various products and services related to SS.7 and mobile messaging.

As the telecom industry technology partner for message security and routing, as well as network querying in wireless networks, mBalance provides advanced solutions for GSM, UMTS, CDMA and TDMA networks.

Our core network products offer the innovation, versatility and performance that is required in today's wireless world.

For more information contact mBalance at: www.mbalance.com