International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1242

(02/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Short message service (SMS) spam filtering system based on user-specified rules

Recommendation ITU-T X.1242

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	**X.1230–X.1249**
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1242

Short message service (SMS) spam filtering system based on user-specified rules

Summary

Recommendation ITU-T X.1242 describes the realization of the SMS spam filtering system based on user-specified rules. It defines the structure of SMS spam filtering system, SMS spam filtering functions, users' service management, communication protocols and basic functional requirements of terminals with SMS functions.

Source

Recommendation ITU-T X.1242 was approved on 20 February 2009 by ITU-T Study Group 17 (2009-2012) under the WTSA Resolution 1 procedure.

Keywords

Filtering system, SMS, SMS spam, SMS spam filtering system based on user-specified rules.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Introduction

With the increasing popularization of mobile services, SMS has become one of the most profitable value-added services due to low price, excellent flexibility and easy usage. However, at the same time, SMS spam is growing rapidly and is bringing the following serious influences:

– reducing users' satisfaction about SMS

– wasting network resources

– increasing social instability

– bringing other negative influences.

Therefore, it is very important to find an effective and efficient solution to counter SMS spam while maintaining the operational efficiency of SMS. However, the following principles should be taken into account:

– minimize changes to the user SMS interface

– improve the users' confidence in the SMS

– be easy to implement and deploy

– minimize changes to the existing network system

Based on the above principles, the SMS spam filtering system based on user-specified rules is an effective and efficient way to counter SMS spam. It means to establish a SMS spam filtering system, in which users can manage SMS filtering rules and entrust the system that belongs to the service provider or the network operator to block the correlative short messages.

The system has the following merits:

– protect the users' privacy through user-specified rules

– meet the users' requirements on countering SMS spam

– implement easily without changing the existing network systems

– run as a value-added service which can bring profits for service providers

This Recommendation is suitable for the design, deployment and evaluation of SMS spam filtering system based on user-specified rules in mobile networks and fixed networks.

Recommendation ITU-T X.1242

Short message service (SMS) spam filtering system based on user-specified rules

1 Scope

This Recommendation describes the realization of the SMS spam filtering system based on user-specified rules (hereafter referred to as the SMS spam filtering system or the filtering system). It defines:

- the structure of the filtering system
- the SMS spam filtering functions
- users' service management
- communication protocols
- functional requirements of the terminal

This Recommendation is suitable for the design, deployment and evaluation of SMS spam filtering system based on user-specified rules in mobile networks and fixed networks.

NOTE – Some filtering mechanisms described in this Recommendation may affect the privacy of telecommunication traffic. Therefore, implementations of SMS spam filtering systems have to take care to be in alignment with the applicable legislations. This Recommendation or parts of it may not be applicable in Germany due to German legislation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ETSI TR 101 632] ETSI TR 101 632 V7.0.0 (2000-06), *Digital cellular telecommunications system (Phase 2+) (GSM); Interface protocols for the connection of Short Message Service Centres (SMSCs) to Short Message Entities (SMEs) (GSM 03.39 version 7.0.0 Release 1998).* <http://pda.etsi.org/exchangefolder/tr-101632v070000p.pdf>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 mobile station (MS): Entity capable of accessing a set of UMTS services via one or more radio interfaces. This entity may be stationary or in motion within the UMTS service area while accessing the UMTS services, and may simultaneously serve one or more users. [b-ETSI TR 125 990].

3.1.2 short message: Information that is conveyed from a sending user to a receiving user via an SMSC. [b-ETSI TS 102 507].

3.1.3 short message entity (SME): The SME is an entity that composes and decomposes short messages. A SME may or may not be located within, and be indistinguishable from, an HLR, MC, VLR, MS, or MSC. [b-ITU-T Q.1742.3].

3.1.4 short message service centre (SMSC): Function unit, which is responsible for the relaying and store-and-forwarding of a short message (SM) between two SM-TEs or SME and an MS. The SMSC can functionally be separated from or integrated in the network. [b-ETSI ES 201 986].

3.1.5 SMS-DELIVER: Short message transfer protocol data unit containing user data (the short message), being sent from an SC to an MS. [b-ETSI TS 100 901].

3.1.6 SMS-STATUS-REPORT: Short message transfer protocol data unit informing the receiving MS of the status of a mobile originated short message previously submitted by the MS, i.e., whether the SC was able to forward the message or not, or whether the message was stored in the SC for later delivery. [b-ETSI TS 100 901].

3.1.7 SMS-SUBMIT: Short message transfer protocol data unit containing user data (the short message), being sent from an MS to an SC. [b-ETSI TS 100 901].

3.1.8 status report: SC informing the originating MS of the outcome of a short message submitted to an SME. [b-ETSI TS 100 901].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Internet short message gateway (ISMG): The entity between the SP and SMSC, implementing the transportation of short messages from the SP to the SMSC and from the SMSC to the SP, while implementing protocol conversion of interactive information between the SP and the SMSC.

3.2.2 short message service (SMS): The services in telecommunication networks, which provide mobile phones, telephones and other SMEs to transfer and receive text messages through SMSCs that store messages if the receiving terminal cannot be contacted.

3.2.3 spam: The electronic information delivered from senders to recipients by terminals such as computers, mobile phones, telephones, etc., which is usually unsolicited, unwanted, and harmful for recipients.

3.2.4 SMS spam: Spam sent via SMS.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

FMD Filtered Messages Database

ISMG Internet Short Message Gateway

MS Mobile Station

SC Service Centre

SCM Service Control Module

SM MO Short Message Mobile Originated Point-to-Point

SM MT Short Message Mobile Terminated Point-to-Point

SME Short Message Entity

SMPP Short Message Point-to-Point

SMS Short Message Service

SMSC Short Message Service Centre

SP Service Provider

SS Secretary Station

SSFM SMS Spam Filtering Module

SSFS SMS Spam Filtering Service

URD User-specified Rules Database

USMM User Service Management Module

5 Conventions

None.

6 System description

SMS spam filtering system based on user-specified rules refers to a filtering system attached to SMSCs, in which users can configure (add, delete and edit) filtering rules, and at the same time, all short messages to such users can be filtered according to those filtering rules. In addition, users can manage (query, delete and restore) filtered short messages by specified methods.

Filtering rules can be based on address (phone number), time, content, etc. In addition, specific filtering rules can be used individually or in combination with other filtering rules. If filtering rules are used in combination with other filtering rules, prioritization of the filtering rules is one of the necessary steps implicit in setting the rules. In order to be used easily and practically for this service, at least one of the following management methods for users should be provided: SMS, Web and secretary station.

7 System structure

7.1 General structure

The SMS spam filtering system includes the following logical modules: service control module (SCM), SMS spam filtering module (SSFM), user service management module (USMM), user-specified rules database (URD) and filtered messages database (FMD). The structure of the SMS spam filtering system is shown in Figure 1:

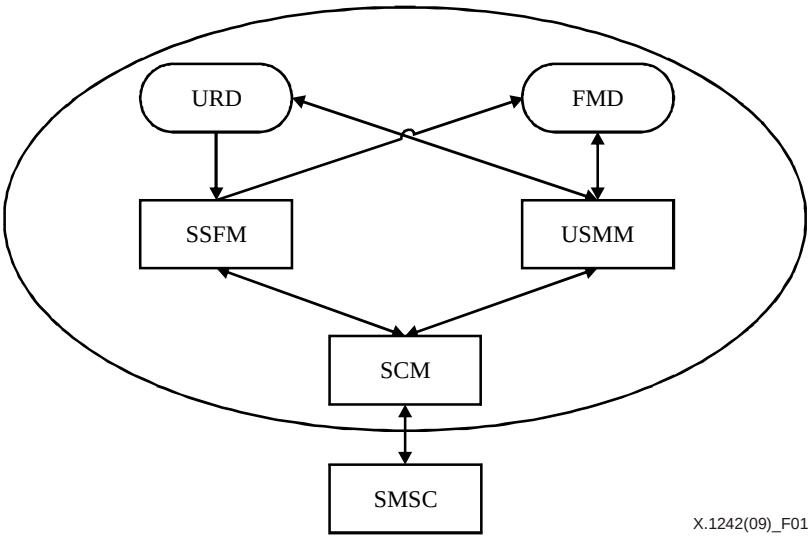

Figure 1 – Structure of the SMS spam filtering system

According to the locations, the above 5 modules in Figure 1 can be put into 3 layers: the access layer, the service layer and the data layer. The access layer includes the SCM; the service layer includes the USMM and the SSFM; the data layer includes the URD and the FMD.

7.2 Module requirements

7.2.1 Access layer

The access layer, the outer layer, is connected to the SMSC directly and is mainly responsible for external entities (including users) accessing the filtering system.

7.2.1.1 Service control module (SCM)

SCM is an integrated service management platform of the filtering system, which includes the following functions:

- Query of service subscription: SMS spam filtering is a kind of optional services for users. Therefore, any short message should be queried in the SCM before being transferred to determine whether the recipient has the service subscription for SMS spam filtering service or not. If so, the short message will be delivered to the SSFM to continue the following filtering processes; otherwise, the short message will be transferred using the normal (non-filtering) process.
- Delivery of management instruction: the short message including service management instructions (management of service states, filtering rules and filtered short messages) should be recognized and delivered by the SCM to the USMM.

The SCM is a relatively independent module, which can be integrated with other value-added services to form an integrated service platform in order to be implemented and deployed easily. In practice, the SCM usually has accounting functions.

7.2.2 Service layer

The service layer implements the core functions of the filtering system: SMS spam filtering, management of filtering rules and management of filtered short messages. In practice, the service layer includes 2 modules at least: SMS spam filtering module (SSFM) and user service management module (USMM). The SSFM implements SMS spam filtering, while the USMM implements management of the filtering rules and management of the filtered short messages.

7.2.2.1 SMS spam filtering module (SSFM)

The SSFM, the core element of the filtering system, processes filtering requests from the SCM, determines whether the short message is spam or not according to the filtering rules stored in the user-specified rules database (URD) and then responds to the SMSC with the decision. If the short message is spam, then it will be stored into the filtered messages database (FMD) for future management (query, delete and restore); otherwise, the short message will be delivered to the recipient normally.

In addition, interface protocols between the SCM, the URD, the FMD and the SSFM should be taken into consideration in this module.

Interface protocol between SSFM and SCM: The SSFM receives the authentication message including the original short message from the SCM and responds to the SCM with authentication results.

Interface protocol between SSFM and URD: The SSFM gets user-specified filtering rules from the URD.

Interface protocol between SSFM and FMD: The SSFM stores the filtered short messages in the FMD to determine if it is spam.

7.2.2.2 User service management module (USMM)

The USMM is used by users to manage filtering rules and filtered short messages. Through the USMM, users can add, delete, edit and query filtering rules. At the same time, through the USMM, users can query, delete and restore filtered short messages. The USMM should support at least one of the following management methods: the SMS management method; the web management method and the SS management method.

In addition, interface protocols between the SCM, the URD, the FMD and the USMM should be taken into consideration in this module.

Interface protocol between USMM and SCM: the USMM receives the short message including management instructions about filtering rules and the filtered short messages from users through the SCM and responds with the results to users through the SCM.

Interface protocol between USMM and URD: the USMM sends management instructions (addition, deletion, modification or query of filtering rules) to the URD and obtains relative information from the URD.

Interface protocol between USMM and FMD: the USMM sends management instructions (restoration, deletion or query of filtered short messages) to the FMD and obtains relative information from the FMD.

7.2.3 Data layer

The data layer is mainly responsible for storing filtering rules and filtered short messages. These data should be stored to permanent media such as disks, tapes, etc., as database-format or text-format. In addition, the data can be transferred and deleted. When the size of data files exceeds the storage threshold, the filtering system should remind operators immediately, even while backing up the data automatically.

7.2.3.1 Filtered messages database (FMD)

FMD is used for storing short messages filtered out as spam by the SSFM. Storage time can be specified by users. Without clear specification of storage time, filtered short messages should be stored for at least 3 months.

Interface protocols should be taken into consideration from the FMD to the SSFM and the USMM.

7.2.3.2 User-specified rules database (URD)

The URD is used for storing user-specified filtering rules. User-specified filtering rules can be based on address, time and content. Blacklists based on address are compulsory, and whitelists based on address are optional.

Interface protocols should be taken into consideration from URD to SSFM and USMM.

7.3 Device requirements

SCM, SSFM, USMM, FMD and URD are all logical modules of the filtering system. They can be not only installed independent devices, but also combined into one device or several devices. For a large-scale short message service centre (SMSC), the first form is recommended to improve performance and expansibility. In addition, as a complete system, the system management function and the logging audit function are also very important.

8 SMS spam filtering function

8.1 SMS working modes

Short message point-to-point services comprise two basic services:

- SM MT (short message mobile terminated point-to-point);
- SM MO (short message mobile originated point-to-point).

SM MT denotes the capability to transfer a short message submitted from the SMSC to the recipient's MS, and to provide information about the delivery of the short message either by a delivery report or a failure report with a specific mechanism for later delivery; see Figure 2.

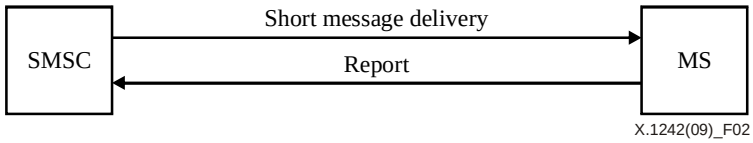

Figure 2 – Short message service mobile terminated, point-to-point

SM MO denotes the capability to transfer a short message submitted by the sender's MS to one SME via an SMSC, and to provide information about the delivery of the short message either by a delivery report or a failure report. The message must include the address of that SME to which the SMSC shall eventually attempt to relay the short message; see Figure 3.

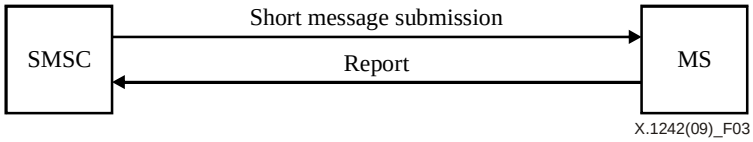

Figure 3 – Short message service mobile originated, point-to-point

However, after SM MO, SMS delivery to the recipient's MS can be realized in 2 modes. In the first mode, after SM MO, the short message will be delivered to the recipient's MS directly. In the second mode, the short message will be transferred to SMSC at the recipient's side by some communication mechanism (i.e., through SMPP protocol implemented in IP network) after SM MO, and then be delivered to the recipient's MS. Although users have the same feeling about SMS working in the different working modes, yet the practical realizations of the filtering system in both

of the modes have tremendous differences. For the sake of simplicity, the first working mode is called the delivery mode at the sender's side and the second working mode is called as the delivery mode at the recipient's side.

8.2 Realization of SMS spam filtering

The SMS spam filtering is a kind of subscription services for recipients, which provides recipients with configuration capabilities of user-specified filtering rules and management capabilities of filtered short messages. User-specified filtering rules and filtered short messages are usually stored in the URD and the FMD installed at the recipient's side.

In the delivery mode at the recipient's side, management of filtering rules, management of filtered short messages and delivery of short messages are all implemented at the recipient's side. Therefore, the realization of the filtering system in the delivery mode at the recipient's side will be easy because only devices at the recipient's side need to be modified.

In the delivery mode at the sender's side, delivery of short messages is implemented at the sender's side SMSC while management of filtering rules and filtered short messages is implemented in the URD and the FMD installed at the recipient's side. Therefore, the synchronization mechanisms between SMS spam filtering systems at the sender's side and at the recipient's side are required. Usually, short messages will be transferred to the filtering system at the recipient's side before the filtering process. Generally speaking, the realization of a filtering system in the delivery mode at the sender's side is harder than in the delivery mode at the recipient's side, due to the synchronization mechanisms.

8.2.1 Realization of SMS spam filtering in the delivery mode at the recipient's side

In the delivery mode at the recipient's side, the SCM, the SSFM and the USMM can be deployed at the recipient's side without the participation of devices or modules at the sender's side; see Figure 4.

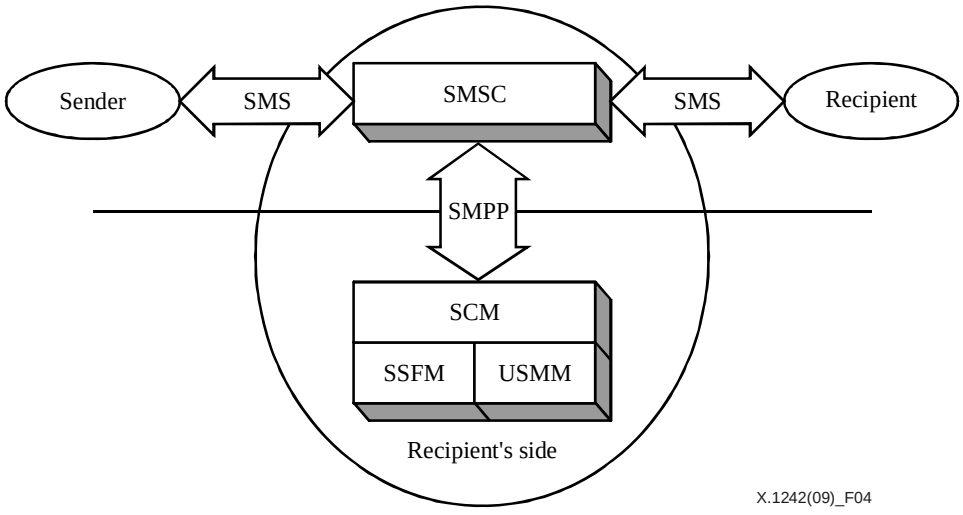

Figure 4 – SMS spam filtering in the delivery mode at the recipient's side

The working process is shown in Figure 5:

- The SMSC will send a SMPP authentication containing the original short message to the SCM, after receiving the short message from the sender;
- The SCM will query the service subscription of the recipient of the short message. If the recipient has service subscription, the short message will be transferred to the SSFM; otherwise, the short message will be delivered normally;

- The SSFM will check whether the short message is valid according to the recipient's filtering rules. If the short message is legitimate, the filtering system should deliver the short message to the recipient and respond to the SMSC with a successful SMPP response; if the short message is invalid, the SMS spam filtering system should block the short message and store it in the FMD for future management (query, deletion and restoration).

Because the number of SMSs to be processed simultaneously may be big and the filtering process may need a long time, it is necessary to set a timer in the SMSC to prevent the SMS from being lost or delayed. If the SMSC could not receive the SMPP response within a certain time specified by the timer, the short message will be delivered normally. Usually, the network operator or the service operator sets the timer.

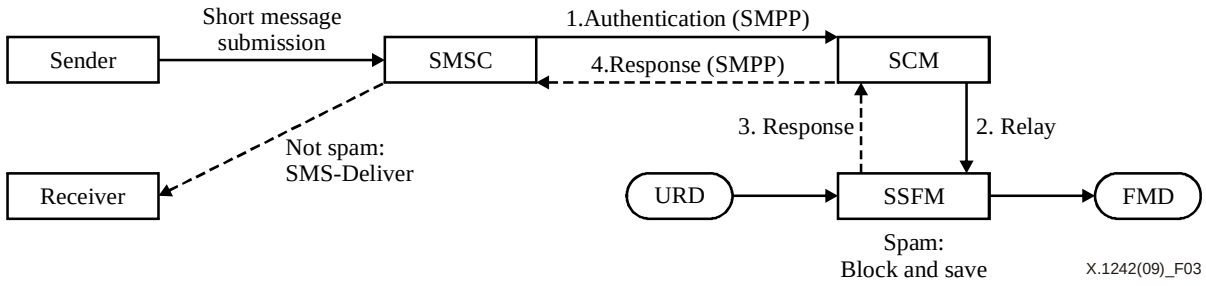

Figure 5 – Process of SMS spam filtering system in the delivery mode at the recipient's side

8.2.2 Realization of SMS spam filtering in the delivery mode at the sender's side

In the delivery mode at the sender's side, the SCM, the SSFM and the USMM can be deployed only at the sender's side, while the delivery of short messages is implemented at the sender's side. Therefore, some synchronization mechanisms between SMS spam filtering systems at the sender's side and the recipient's side should be taken into consideration. Usually, short messages will be transferred to the filtering system at the recipient's side to continue the following filtering process; see Figure 6.

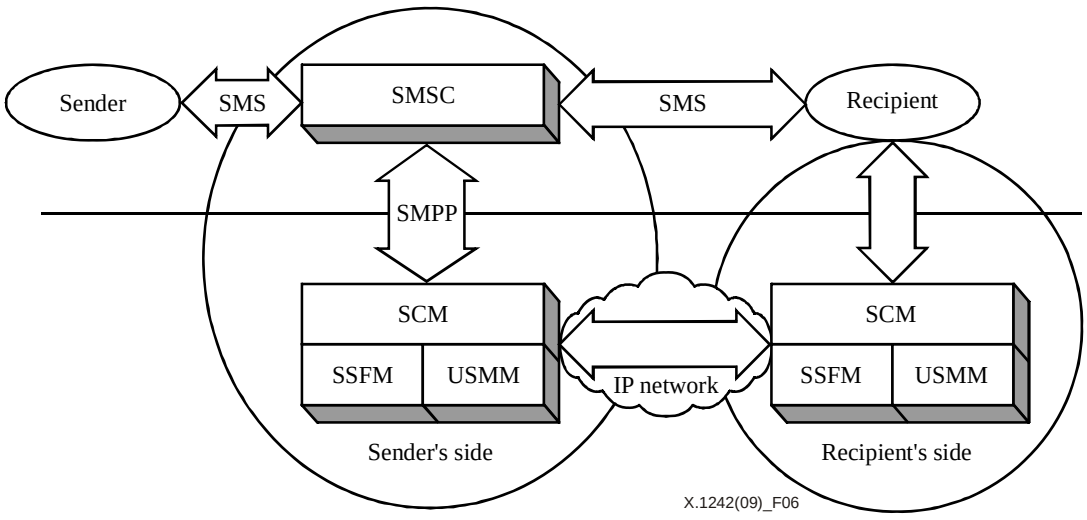

Figure 6 – SMS spam filtering in the delivery mode at the sender's side

The working process is as in Figure 7:

- After receiving the short message from the sender, the SMSC will send a SMPP authentication containing the original short message to the SCM at the sender's side;
- The SCM at the sender's side will query the service subscription status of the recipient of the short message. If the recipient has a service subscription, the short message will be transferred to the SSFM at the sender's side; otherwise, the short message will be delivered to the recipient normally;
- The SSFM at the sender's side will transfer the short message to the SSFM at the recipient's side. Then, the SSFM at the recipient's side will determine whether the short message is valid or not according to the recipient's filtering rules stored in the URD. If the short message is legitimate, the filtering system will deliver the short message to the recipient and respond to the SMSC with a successful SMPP response; if the short message is not legitimate, the SMS spam filtering system should block the short message and store it in the FMD at the recipient's side for future query.

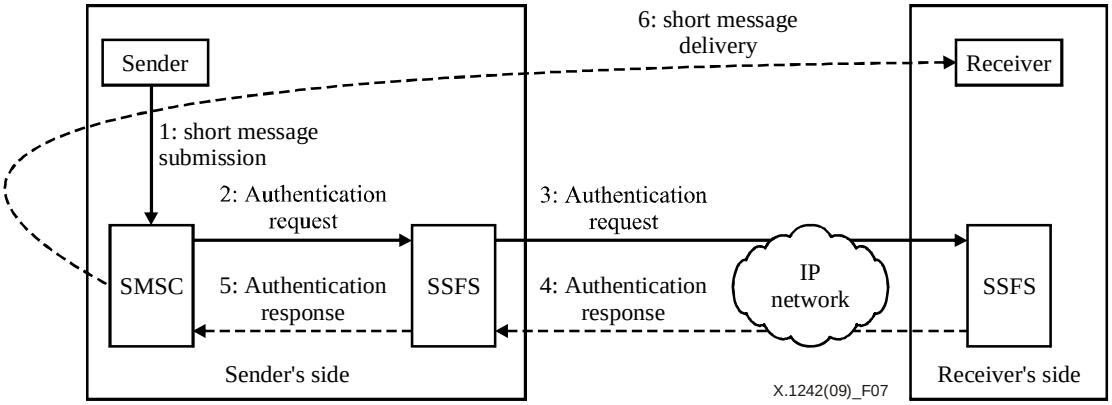

Figure 7 – Processes of SMS spam filtering in the delivery mode at the sender's side

Because the number of SMSs to be processed simultaneously may be big and the filtering process may need a long time, it is necessary to set a timer in the SMSC to prevent the SMS from being lost or delayed. If the SMSC could not receive the SMPP response within a certain time specified by the timer, the short message will be delivered normally. Usually, the network operator or the service operator sets the timer.

9 User's service management

9.1 Management methods

The SMS spam filtering system should provide the SMS management method and the web management method for users. In addition, the secretary station management method can be provided depending on the practical network environment, for example, whether there are enough trained people who can do the job.

9.1.1 Short message management method

Users can manage the user-specified filtering rules and the filtered short messages by SMS through the short message entity (SME) added to the USMM as a service provider (SP).

On the one hand, the SME can receive and recognize the SMS that includes the management instructions; on the other hand, the SME can send the management instructions to the USMM, and the USMM can manage the user-specified filtering rules and the filtered short messages according to the management instructions of the users. This is shown in Figure 8:

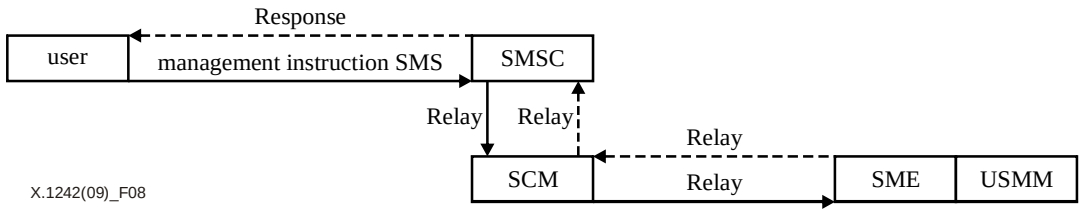

Figure 8 – Management by short message

If the users want to manage the user-specified filtering rules and the filtered short messages, the only thing that users need to do is to send a SMS, including management instructions, to a specific access number of the SME. Then the SME should do the following tasks.

The size of the short message is too limited (typically maximum 160 characters) to contain enough information. In addition, almost all of the SMS terminals are mobile phones which are usually small. It is very difficult to enter data through a keypad or to see voluminous data on the screen because of the limited space of the screen. Therefore, it is hard to manage filtering rules and filtered short messages on SMS terminals. Nonetheless, because SMS terminals are usually carried about by users, there is an advantage to allowing users to use that terminal also to manage user-specified filtering rules and filtered short messages while sending and receiving short messages.

9.1.2 Web management method

Users can manage the user-specified filtering rules and the filtered short messages by the web, through the web server added to the USMM.

On the one hand, the web server can receive the management instructions; on the other hand, the web server can send the management instructions to the USMM, and the USMM can manage the user-specified filtering rules and the filtered short messages according to the management instructions. This is shown in Figure 9:

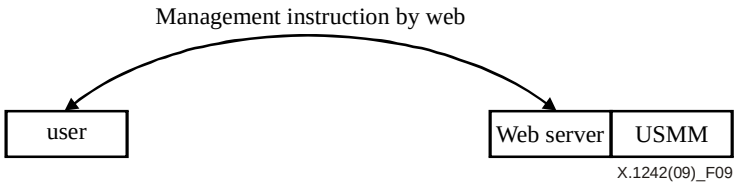

Figure 9 – Management by web

The operation process is similar to normal web operation. However, the web management method supports more management instructions than the short message management method. Taking security into consideration, the web management method should support SSL/TLS to authenticate the web server and the client, and then use it to encrypt messages between the authenticated parties. In fact, it is more powerful to use the web management method than the SMS management method; however, it is limited to Internet access points.

9.2 Management capability

9.2.1 Types of user-specified filtering rules

Because the filtering system is working based on user-specified filtering rules; therefore, filtering rules are very important for the filtering system. In practice, filtering rules can be based on address, time and content.

- *Address-based filtering rule*

Address-based filtering rules determine whether a short message is spam or not based on its source address (phone number). There are two kinds of filtering rules based on address: the whitelists of acceptable senders and the blacklists of suspected spammers. In practice, all the short messages from the whitelists will be delivered normally without further judgment; all the short messages from the blacklists will be blocked immediately. The item of whitelists/blacklists can be not only an independent phone number, but also a phone number segment. However, whitelists/blacklists, especially blacklists, will inevitably contain inaccuracies, known as false positive problems and false negative problems. However, address-based filtering is the most effective and most convenient way for countering SMS spam. Therefore, although the whitelists/blacklists approach is often a too drastic solution to be acceptable by most users, yet address-based filtering is the most important filtering rule in the filtering system.

- *Time-based filtering rule*

Time-based filtering rules restrict delivering the short messages in the specified time. Therefore, short messages blocked in the FMD may not be spam. Generally, users do not want to receive short messages at night, in some meetings or at any important time, so they can use the time-based filtering rule. In the time-based filtering rule, users can specify the time span when they do not want to receive any short messages. However, users can choose the option how to deal with the short messages blocked due to the time-based filtering rule after the time span: retransmission or non-retransmission.

- *Content-based filtering rule*

Content-based filtering is the most reasonable filtering method. However, the accuracy of content-based filtering is usually lower than the other filtering methods because of the challenges of language processing used by the content-based filtering. In fact, keyword-based filtering is the most useful filtering method of content-based filtering. In the filtering system, keyword-based filtering rules are compulsory. At the same time, the filtering system should support the following matching methods for the keyword-based filtering rules: accurate matching and fuzzy matching.

- *Combined filtering rule*

In fact, filtering rules are always used in combination. Therefore, the prioritization of the filtering rules should be considered seriously. In practice, the prioritization can be decided by the basic regulation of service operators and the practical requirements of the users.

9.2.2 Management of user-specified filtering rules

Users can perform the following management filtering rules:

- Load and unload predefined filtering rules made by service operators:

  In order to simplify the operation of filtering rules for users, service operators should establish or cite well-known blacklists. Therefore, users can use such predefined filtering rules.

- Manage filtering rules based on address, time and content:

  Users can add, modify, delete and query filtering rules. However, users have different experiences in different management methods. In the SMS management methods, users can only manage filtering rules with one short message for one management instruction, which is usually difficult to operate; while in the web management method, users can manage the filtering rules very easily.

9.2.3 Format of filtered short messages

Any filtered short messages should be stored in the FMD with a detailed record. The record should include, at least the following fields:

- Sender: phone number of sender
- Receiver: phone number of recipient
- Time: sending time of short message
- Content: content of short message
- Filtering type: address-based, keyword-based, time-based

9.2.4 Management of filtered short messages

Users can manage the filtered short messages. They can do the following operations:

- Make statistics of the filtered short messages
- See the details of the filtered short messages
- Query filtered short messages
- Restore some filtered short messages
- Delete specified filtered short messages

10 Communication protocols

10.1 Structure of communication protocols

There are 8 protocol interfaces in the filtering system (the last one is only used for the filtering system in the delivery mode at the sender's side):

- The interface between the SMSC and the SCM
- The interface between the SCM and the SSFM
- The interface between the SCM and the USMM
- The interface between the SSFM and the URD
- The interface between the SSFM and the FMD
- The interface between the USMM and the URD
- The interface between the USMM and the FMD
- The interface between the SSFM at the sender's side and the recipient's side

The first 3 interface protocols are outside interfaces, mainly used for interconnection between the different modules in the same network or the different networks. The last 5 interface protocols are inner interfaces and can be developed according to the practical requirement of service providers, which are usually invisible for the outside.

Generally, SMPP, the authentication protocol, can be used between the SMSC and the SCM. The ISMG protocol can be used between the SCM and the SSFM, and the SCM and USMM.

In addition, the SMS interconnection should be taken into consideration.

10.2 Authentication protocol

The authentication protocol should be based on extended SMPP (see [ETSI TR 101 632]). There are two messages used in the SMS spam filtering system: DELIVER_SM, and DELIVER_SM_RESP. The working process is shown in Figure 10.

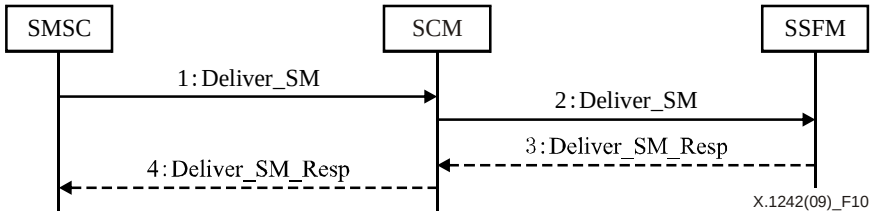

Figure 10 – SMPP authentication protocol

DELIVER_SM is issued by the SMSC or the SCM. Using this command, the SMSC or the SCM may submit a short message to the SCM or SSFM for delivery.

DELIVER_SM_RESP is issued as the response of DELIVER_SM, note whether the delivery is successful or not. The status value in DELIVER_SM_RESP represents different meaning: 0 represents successful to delivery; other values represent failed to delivery.

10.3 ISMG protocol

The ISMG protocol enables users to configure user-specified filtering rules and manage filtered short messages. The short message entity (SME) is added to the user service management module (USMM) through which users can manage the filtering rules and the filtered short messages stored in the FMD. The SMS gateway protocol is used between the SMSC and the SME. The working process is shown in Figure 11.

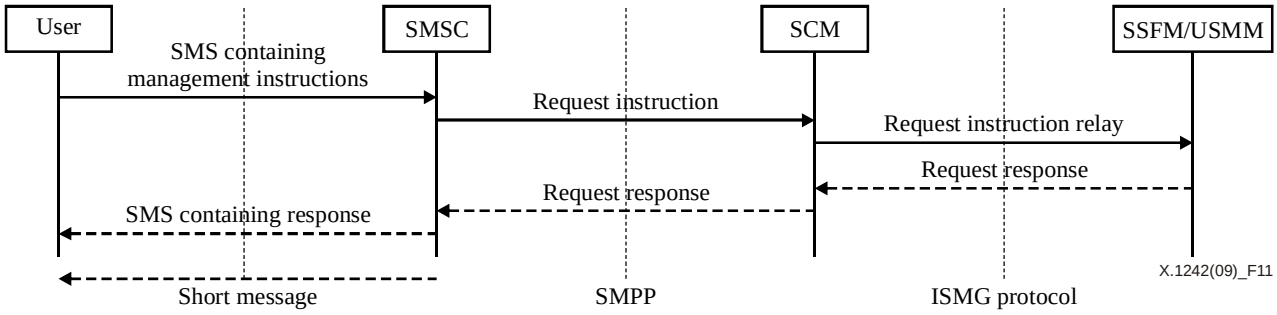

Figure 11 – ISMG protocol

Appendix I

Requirements of terminal software supporting the SMS spam filtering

(This appendix does not form an integral part of this Recommendation)

This appendix is applicable for intelligent terminals.

I.1 General aspects

Almost all of the SMS terminals are mobile phones which are usually small, especially with a limited screen space and a small keypad. Therefore, it is hard for users to manage filtering rules and filtered short messages through text commands. In order to facilitate management, based on intelligent terminals, terminal software supporting the SMS spam filtering is developed. In general, the software provides users with an operation menu where management instructions are mapped into the menu items. However, the terminal software should satisfy the two following basic requirements:

- Fully management of filtering rules and filtered short messages
- Friendly and convenient man-machine interface for users to operate

In practice, there are two types of terminal software:

- Basic software for SMS spam filtering:

  The filtering function is implemented in the SMS spam filtering system connected to the SMSC. The terminal software only provides the man-machine interface for users.
- Enhanced software for SMS spam filtering:

  The terminal software has all the functional modules of the SMS spam filtering system, which can filter SMS spam independently. Usually, the enhanced software includes all functions of basic software.

I.2 Basic software for SMS spam filtering

I.2.1 Configuration of filtering rules

The following operation functions should be provided, see Table I.1.

Table I.1 – Management of filtering rules

Predefined filtering rules	Load predefined filtering rules
	Unload predefined filtering rules
Address-based filtering rules	Add whitelist items
	Delete whitelist items
	Add blacklist items
	Delete blacklist items
	Query filtering rules based on address
Keyword-based filtering rules	Add keywords
	Delete keywords
	Query filtering rules based on keyword
Time-based filtering rules	Add time rules
	Delete time rules
	Query filtering rules based on time

Table I.1 – Management of filtering rules

Query all filtering rules
Delete all user-specified filtering rules
Start and stop SMS spam filtering

I.2.2 Configuration of filtering rules

Table I.2 – Management of filtered short messages

Make statistics of the filtered short messages
See the detail of filtered short messages
Query filtered short messages
Restore some filtered short messages
Delete specified filtered short messages

I.3 Enhanced software for SMS spam filtering

If intelligent terminals have enough resources (i.e., processing capabilities, storage space, etc.), all functional modules can be installed and implemented in intelligent terminals. In this case, the software installed on intelligent terminals is usually called SMS firewalls. However, intelligent terminals still need to access the Internet to update the software and the predefined filtering rules.

Bibliography

[b-ITU-T Q.1742.3] Recommendation ITU-T Q.1742.3 (2004), *IMT-2000 references (approved as of 30 June 2003) to ANSI-41 evolved core network with cdma2000 access network.*

[b-ETSI TS 100 901] ETSI TS 100 901 V7.5.0 (2001-12), *Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) (3GPP TS 03.40 version 7.5.0 Release 1998).* http://pda.etsi.org/exchangefolder/ts_100901v070500p.pdf

[b-ETSI TS 102 507] ETSI TS 102 507 V1.1.1 (2006-03), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Fixed network Short Message Service (F-SMS) for IP networks; Service description.* http://pda.etsi.org/exchangefolder/ts_102507v010101p.pdf

[b-ETSI TR 125 990] ETSI TR 125 990 V3.0.0 (2000-01), *Universal Mobile Telecommunications System (UMTS); Vocabulary*. http://pda.etsi.org/exchangefolder/tr_125990v030000p.pdf

[b-ETSI ES 201 986] ETSI ES 201 986 V1.1.2 (2002-01), *Services and Protocols for Advanced Networks (SPAN); Short Message Service (SMS) for PSTN/ISDN; Service description.* http://pda.etsi.org/exchangefolder/es_201986v010102p.pdf

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009