ICS 33 070
M 37

YD

中华人民共和国通信行业标准

YD/T 1775-2008

基于用户设置规则的短消息过滤系统技术要求

Technical Specification
for Filtering System of Short Messages Based on User's Rules

2008-03-28 发布　　2008-06-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本标准是消息业务安全系列标准之一。该系列标准的名称预计如下：

1. 基于用户设置规则的消息过滤业务技术要求
2. 基于用户设置规则的短消息过滤系统技术要求
3. 消息类业务内容分类技术要求

本标准在制定过程中，还参考了以下标准：

1. GB 4943-2001	信息技术设备的安全
2. GB/T 5271.8-2001	信息技术 词汇 第8部分:安全
3. GB/T 18336.2-2001	信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求
4.YD/T 1039.1-2005	900/1800MHz TDMA数字蜂窝移动通信网短消息中心设备技术要求 第一部分：点对点短消息业务部分
5.YD/T 1040.1-2005	900/1800MHz TDMA数字蜂窝移动通信网短消息中心设备测试方法 第一部分：点对点短消息业务部分
6.YD/T 1094-2000	900/1800MHz TDMA数字蜂窝移动通信网扩展短消息实体与短消息业务中心间的接口协议规范
7.YD/T 1290.1-2003	点对点短消息网间互通总体技术要求 第一部分 固定网与移动网之间互通
8.YD/T 1290.2-2005	点对点短消息网间互通总体技术要求 第二部分 固定网和固定网之间互通
9.YD/T 1364-2005	点对点短消息网间互通设备技术要求
10.ETSI GSM 03.38（1996）	欧洲数字蜂窝通信系统（阶段2+）：字符和特定语言信息
11.ETSI GSM 03.39（1996）	欧洲数字蜂窝通信系统：短消息中心和短消息实体间连接的接口协议
12.ETSI GSM 03.40（1996）	欧洲数字蜂窝通信系统（阶段2+）：短消息业务技术实现
13.ETSI GSM 03.47（1996）	欧洲数字蜂窝通信系统:短消息中心与移动交换中心间互联协议栈举例
14.3GPP TS 23.040（2004）	短消息业务的技术实现
15.TIA/EIA/IS-637（1995）	宽带扩频蜂窝通信系统的短消息业务

本标准的附录A是规范性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院、北京汉铭无线网络有限公司、中国移动通信集团公司、中国联合通信有限公司、国家计算机网络应急技术处理协调中心、华为技术有限公司、中兴通讯股份有限公司

本标准起草人：何桂立、落红卫、张　薇、胡　岗、文登敏、黄元飞

引　言

随着移动用户的迅猛增长和移动业务的日益普及，消息业务作为一项移动增值业务，借助于其使用方便、收费低廉和随时随地收发等优点在短时期内得到大规模普及，成为人们日常工作生活中沟通和交流的重要方式。但是，消息业务收发自由、难于控制等客观原因也带来了诸多安全问题和社会问题，严重影响了消息业务健康发展。如今，垃圾消息问题备受社会重视。如何在保持消息业务活力的同时限制有害消息的传播成为一个棘手的问题，而该问题的核心是没有统一标准来判断垃圾短信，而由用户自己判定是非常有效的判定方法。因此，非常有必要开展基于用户设置规则的消息过滤业务。

基于用户设置规则的消息过滤业务，是通过由用户设置消息过滤规则从而把判断垃圾消息的权力交给用户，让用户自己决定是否过滤消息，这样一方面可以解决垃圾消息判定标准的问题，另外一方面也提高了用户的业务满意度，进而可以保证消息业务的健康快速发展。

本标准主要对当前急需的基于用户设置规则的短消息过滤系统进行规范。

基于用户设置规则的短消息过滤系统技术要求

1 范围

本标准规定了基于用户设置规则的短消息过滤系统（以下简称短消息过滤系统）的系统架构、过滤功能实现、用户业务管理、采用的通信协议、系统管理、扩展功能、安全要求以及性能指标。

本标准适用于基于用户设置规则的短消息过滤系统。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD/T 1774-2008　　基于用户设置规则的消息过滤业务技术要求

YD/T 1291-2003　　点对点短消息网间互通协议要求

3 术语和定义

下列术语和定义适用于本标准。

短消息业务 Short Message Service

短消息业务是通信系统提供的通信终端之间，或者通信终端与其他短消息实体之间进行文字信息收发的业务。

短消息业务中心 Short Message Service Center

在短消息业务网络中，完成短消息发送、接收、转发和存储等处理功能的系统。

短消息终端 Short Message Terminal

从短消息业务中心接收或者向短消息业务中心发送短消息的终端设备。

短消息用户 Short Message User

可以通过短消息终端使用短消息业务的用户。

互联网短消息网关 Internet Short Message Gateway

业务提供商与短消息业务中心之间的中介实体。互联网短消息网关一方面负责接收业务提供商发送给移动用户的短消息并且提交给短消息中心。另一方面，移动用户点播业务提供商的信息将由短消息中心通过互联网短消息网关发给业务提供商。另外，互联网短消息网关还应根据路由原则将业务提供商提交的信息转发到相应的互联网短消息网关。

漏报 False Negatives

漏报是指非法短消息未被短消息过滤系统检测到而造成的错误。

误报 False Positives

误报是指短消息过滤系统把合法短消息判断为非法短消息，或者把一种非法短消息判断为另一种非法短消息而导致的错误。

防火墙 Firewall

在网络之间执行安全访问控制策略的一个或一组设备。

4 缩略语

下列缩略语适用于本标准。

ACL	Access Control List	访问控制列表
FSD	Filtered SMS Database	过滤短信数据库
SFM	SMS Filtering Module	短信过滤模块
HTTP	Hypertext Transfer Protocol	超文本传输协议
IP	Internet Protocal	互联网协议
ISMG	Internet Short Message Gateway	互联网短消息网关
MS	Mobile Station	移动台
SCM	Service Control Module	业务控制模块
SM MO	Short Message Mobile Originated Point-to-Point	点对点短消息发起
SM MT	Short Message Mobile Terminated Point-to-Point	点对点短消息终止
SME	Short Message Entity	短消息实体
SMC	Short Messaging Center	短消息中心
SMS	Short Messaging Service	短消息业务
SMPP	Short Message Peer to Peer	短消息点对点协议
SMT	Short Message Terminal	短消息终端
SS	Secretary Station	秘书台
TCP	Transmission Control Protocol	传输控制协议
UMM	User Management Module	用户管理数据库
URD	User Rules Database	用户规则数据库

5 总体要求

5.1 系统描述

基于用户设置规则的短消息过滤系统既由用户设置短消息过滤规则，并且可以根据以上用户设置的过滤规则而进行短消息过滤的系统。该系统可以是与短消息业务中心相连独立的系统，也可以作为短消息中心的一个部分。

短消息过滤规则可以是基于号码、关键词、时间等独立的过滤规则也可以是若干规则的组合。过滤掉的短消息存储在被叫归属的短消息过滤系统。用户可以通过短消息、Web、秘书台等多种管理方式设置管理短消息过滤规则和查询管理被过滤掉的短消息。

5.2 系统架构

在系统架构上，短消息过滤系统在逻辑上至少涉及五个功能模块：业务控制平台（SCP）、短信过滤模块（SFM）、用户管理模块（UMM）、用户规则数据库（URD）和过滤短信数据库（FSD）。系统示意图如图1所示。

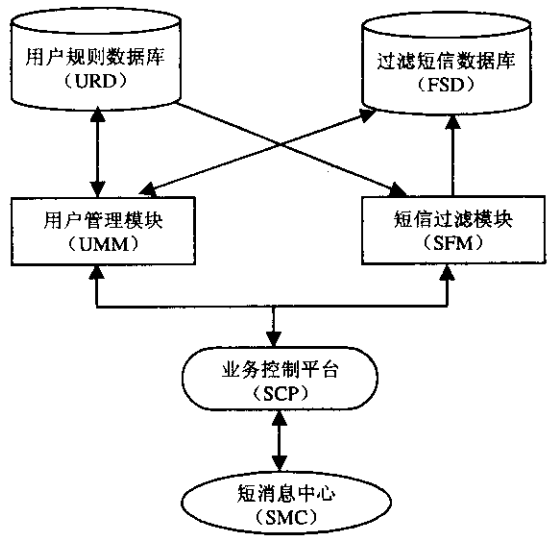

图 1　基于用户设置规则的短消息过滤系统

根据体系架构位置不同，短消息过滤系统的 5 个模块在逻辑上可划分为3个层面：接入层、业务层和数据层。

5.2.1　接入层

处于短消息业务中心和短消息过滤系统业务实体之间（属于短消息过滤系统），主要用于用户或者短消息中心（SMC）接入短消息过滤系统以及对短消息过滤业务本身的管理控制。短消息过滤系统接入层主要包括业务控制平台（SCP）。

5.2.1.1　业务控制平台（SCP）

业务控制平台（SCP）是基于用户设置规则的短消息过滤的综合管理控制平台，主要包括如下功能：

业务订购关系查询：业务控制平台（SCP）可以针对短消息进行短消息过滤业务订购关系的查询，根据业务订购关系查询的结果，对于发往有业务订购关系用户的短消息，短消息过滤系统进行下一步“短消息转发”处理；而对于没有业务订购关系用户的短消息，该短消息按照常规流程正常下发，不进行短消息过滤处理。

短消息转发：把发往有业务订购关系用户的短消息转发到短消息过滤模块（SFM）并把处理结果返回到短消息中心（SMC）；把包括用户设置规则的短消息转发到用户业务管理模块（UMM），而把用户业务管理模块处理的结果返回给用户。

业务控制平台（SCP）是多个业务处理单元的集合，每个业务处理单元负责处理特定功能，由于业务控制平台（SCP）独立于特定业务，业务控制平台（SCP）接收到短消息后可以根据业务特征把该短消息分发到对应的业务处理单元，作相应处理。

5.2.2　业务层

业务层是基于用户设置规则的短消息过滤系统的核心，主要负责具体短消息的鉴别过滤和用户过滤规则的设置管理，主要包括短消息过滤模块（SFM）、用户业务管理模块（UMM）和计费管理管理模块。

5.2.2.1　短消息过滤模块（SFM）

在接到业务控制模块传输过来的需要鉴别的短消息后，短消息过滤模块可以根据用户设定的过滤规则对该短消息进行鉴别过滤：对于合法短消息，正常下发，并返回状态报告；对于非法短消息，在过滤掉该段消息以后还要将该段消息保存到被叫归属所在的过滤短信数据库（FSD）。

对于短消息过滤模块（SFM），需要具备与业务控制平台（SCP）、用户规则数据库（URD）、过滤短信数据库（FSD）相应的协议接口：

- 短消息过滤模块（SFM）与业务控制平台（SCP）的协议接口主要作用是接收业务控制平台（SCP）发来的鉴别请求和向业务控制平台（SCP）返回鉴别响应；
- 短消息过滤模块（SFM）与用户规则数据库（URD）的协议接口主要作用是提取用户设置的短消息过滤规则以作为判断短消息的过滤依据；
- 短消息过滤模块（SFM）与过滤短信数据库（FSD）的协议接口主要作用是短消息过滤模块（SFM）向过滤短信数据库（FSD）存储已经过滤掉的短消息以备用户查询和管理。

具体短消息过滤实现规定参见第6章，具体接口协议要求参见第8章。

5.2.2.2 用户业务管理模块（UMM）

用户业务管理模块（UMM）用于支持用户查看和管理用户过滤规则和过滤掉短消息。用户业务管理至少支持Web方式和短消息方式，另外也可以支持秘书台方式（SS）。

系统应该支持更新提示，用户可以根据实际需要选择相应的提示方式，至少系统应提供短消息更新提示方式，在短消息更新提示方式中，用户可以开启自动更新并设置更新提示时间长度，如果到更新提示时间用户还没有查阅或者更新规则，则系统可以自动通过短消息方式提示用户查阅或者更新。

系统应该支持定期自动删除无效过滤规则。用户可以设置提示删除，也可以设置自动删除。

对于用户管理模块（UMM），需要提供与业务控制平台（SCP）、用户规则数据库（URD）、过滤短信数据库（FSD）相应的协议接口：

- 用户管理模块（UMM）与业务控制平台（SCP）的协议接口主要作用是接收业务控制平台（SCP）发来的用户对过滤规则以及已过滤短消息的SMS管理指令，和向业务控制平台（SCP）返回鉴别响应；
- 用户管理模块（UMM）与用户规则数据库（URD）的协议接口主要用于用户设置短消息过滤规则；
- 用户管理模块（UMM）与过滤短信数据库（FSD）的协议接口主要用于用户查询和管理保存在过滤短信数据库（FSD）的已经过滤掉的短消息。

用户业务管理实现规定参见第7章，具体接口协议要求参见第8章。

5.2.2.3 计费管理模块

根据既定的计费策略对有短消息过滤业务订购关系的用户进行计费管理。该模块具体设置与具体业务网络有关，在此不做具体规定。

5.2.3 数据层

数据层主要用于存储用户设置的过滤规则和被过滤掉的短消息。相应数据可以以文本或者数据库的形式存储于磁带、磁盘等永久性存储介质中，要求做相应的冗余备份，并支持过滤短消息数据的转储和备份。当系统内的数据超过预定义的域值时，系统应及时通知进行外部备份，从而确保数据的安全可靠。数据层主要包括用户规则数据库（URD）和过滤短信数据库（FSD）。

5.2.3.1 用户规则数据库（URD）

用于保存用户设置的过滤规则，过滤规则至少包含基于地址的黑白名单规则、基于关键词的关键词规则和基于时间的时间规则。需要提供到短消息过滤模块（SFM）和用户业务管理模块（UMM）的协议接口，具体接口协议要求参见第8章。

5.2.3.2 过滤短信数据库（FSD）

用于保存拦截掉的短消息，存储时间应能够满足用户的要求，原始被拦截掉的短消息至少应该保存3个月。需要提供到短消息过滤模块（SFM）和用户业务管理模块（UMM）的协议接口，具体接口协议要求参见第8章。

5.3 系统要求

短消息过滤系统中，业务控制平台（SCP）、短消息过滤模块（SFM）、用户业务管理模块（UMM）、规则设置数据库（URD）和过滤短消息数据库（FMD）都是逻辑实体，可以是独立的设备，也可以根据具体需要，将若干模块合成一个设备来实现。对于较大的短消息中心，建议尽量采用独立的设备，以提高系统的性能和可扩展能力。另外，作为一个完整的短消息过滤系统，系统管理和系统安全也是非常重要的。系统管理完成对系统的操作与配置，而日志审计是任何安全系统必须具备的功能。

系统管理要求参见第9章，系统安全要求参见第10章。

6 短消息过滤功能要求

6.1 短消息工作方式

点对点短消息业务由两种基本业务组成：SM MO（点对点移动台发起短消息）、SM MT（点对点移动台终结短消息）。SM MO表示要从移动台（MS）向短消息中心（SMC）递交的短消息，并且通过一种特定的机制来提供关于递交报告或者错误报告的信息，SM MO流程如图2所示；SM MT表示要从短消息中心（SMC）到移动台（MS）下发的短消息，并且通过一种特定的机制来提供关于下发报告或者错误报告的信息，如图3所示。

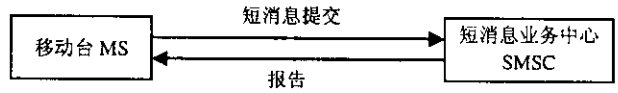

图 2 点对点移动发起短消息（SM MO）

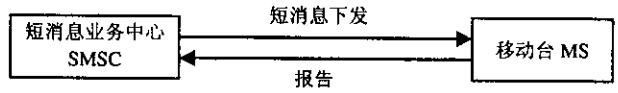

图 3 点对点移动下发短消息（SM MT）

但是在短消息下发却有不同的实现方式：有的短消息业务是在主叫归属的短消息中心（SMC）直接下发到移动台（MS）；有的短消息业务是主叫归属的短消息中心（SMC）通过某些通信机制（例如IP专网）转发到被叫归属的短消息中心（SMC）以后，再由被叫归属的短消息中心下发短消息到移动台（MS）。因此，产生了两种短消息工作方式：短消息主叫归属下发模式和短消息被叫归属下发模式。虽然两种方式实现的短消息过滤系统在使用过程没有明显差异，但是在短消息过滤功能具体实现却有巨大的差别。

6.2 短消息过滤流程要求

由于短消息过滤业务属于被叫签约业务，用户设置的过滤规则以及要查询管理的被过滤短消息只能存储在被叫归属地。对于采用被叫归属短消息下发模式的短消息业务，由于用户规则设置、被过滤短消息管理与短消息下发都是在被叫归属地完成，因此仅需要在被叫归属地的短消息过滤系统即可，相对而言，实现比较简单；而对于采用主叫归属短消息下发模式的短消息业务，由于用户规则设置、被过滤短消息管理与短消息下发只能被叫归属地完成，而短消息下发在主叫归属地完成，因此需要主被叫系统之

间的同步或者短消息转移，使短消息的下发过滤与用户设置过滤规则和被过滤短消息关联同步起来，相对而言，实现复杂。

6.2.1 被叫归属短消息下发模式的短消息过滤流程要求

基于被叫归属短消息下发模式的短消息过滤流程的具体步骤如下：

（1）被叫归属短消息中心接收到普通用户提交的短消息后，发送一个SMPP鉴别请求消息到业务控制平台（SCP）；

（2）业务控制平台（SCP）首先判断接收方是否是业务订购用户，如果是则转发该鉴别请求到短消息过滤模块（SFM），否则直接鉴别响应合法，进行正常短消息下发；

（3）短消息过滤模块（SFM）收到发往有业务订购关系用户的短消息，短消息过滤模块（SFM）根据用户在系统中设置的过滤规则对短消息进行判断。如果短消息合法，短消息过滤模块（SFM）把合法的判断结果返回业务控制模块；如果短消息非法，则首先把该短消息存储到本地过滤短消息数据库以供用户将来查询管理，同时把非法的判断结果返回业务控制模块，由业务控制模块返回SMPP鉴别失败响应消息；

（4）对于合法短消息，短消息中心（SMC）下发该短消息，如图4所示。

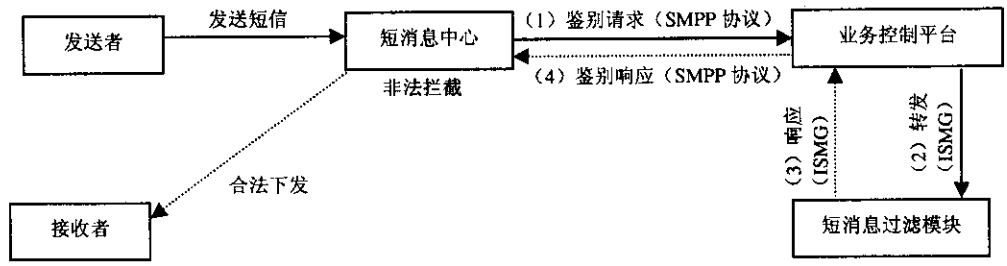

图 4 被叫归属短消息下发模式的短消息过滤流程

另外，短消息中心设定有短消息定时，如果在定时之内没有SMPP鉴别消息返回，则短消息也将发送，不影响短消息正常下发。

6.2.2 主叫归属短消息下发模式的短消息过滤流程要求

基于主叫归属短消息下发模式的短消息过滤流程的具体步骤如下：

首先，主叫归属短消息中心接收到普通用户提交的短消息后，发送一个SMPP鉴别请求消息到主叫归属业务控制平台（SCP）；

其次，主叫归属业务控制平台（SCP）通过业务订购关系查询确定接收方是否是业务订购用户，如果是则转发该鉴别请求到主叫归属短消息过滤模块（SFM），否则直接鉴别响应合法，进行正常短消息下发；

然后，主叫归属短消息过滤模块（SFM）把短消息鉴别请求转发到被叫归属短消息过滤模块（SFM），被叫归属短消息过滤模块（SFM）根据被叫归属用户规则数据库（URD）保存过滤规则对该短消息进行鉴别，如果短消息非法，则被叫归属短消息过滤模块（SFM）把该短消息存储下来，并向主叫归属短消息过滤模块返回鉴别失败响应，不下发短消息；如果短消息合法，则向主叫归属短消息过滤模块（SFM）返回鉴别成功响应，正常下发该短消息，如图5所示。

另外，主叫归属短消息中心设置对每条短消息都有定时器，超过定时没有鉴别响应则使用正常流程下发短消息，从而保证短消息业务中心正常使用。

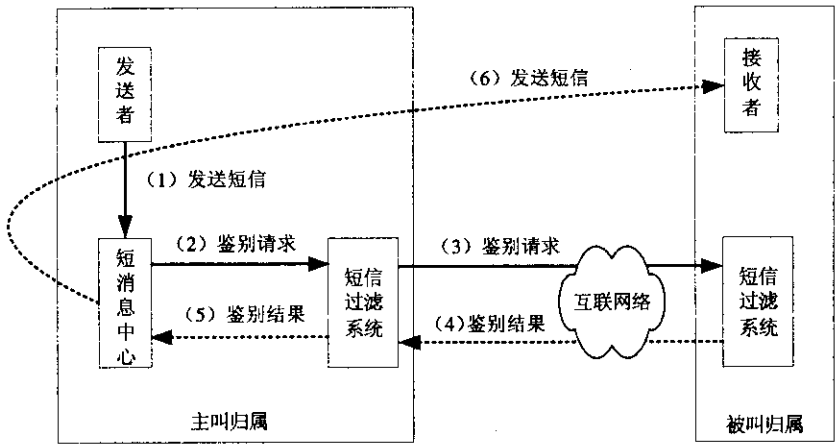

图 5　主叫归属短消息下发模式的短消息过滤流程

7　用户业务管理

用户可以通过多种方式来连接用户管理模块（UMM），从而对存储在用户规则数据库（URD）中的过滤规则进行管理和对存储在过滤短信数据库（FSD）中已被过滤掉的短消息进行统计查询和管理。

7.1　业务管理方式

短消息过滤系统至少支持短消息管理方式和Web管理方式，同时可以根据实际运营需要支持秘书台设置（SS）等方式。

7.1.1　短消息设置方式

在用户管理模块（UMM）内增设短消息实体（SME），由用户通过发送短消息到用户业务管理模块（UMM）的方式来进行短消息过滤规则的设置和被过滤掉短消息的查询管理，如图6所示。

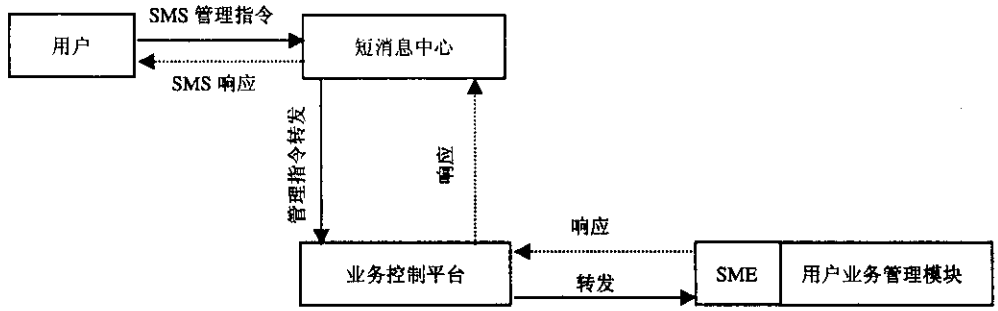

图 6　短消息管理方式

具体操作方式：利用短消息终端（SMT）通过短消息（SMS）的形式发送管理指令（包括过滤规则设置指令和被过滤短消息查询统计指令）到短消息过滤业务接入号即可。具体定制指令要求参见YD/T 1774-2008 《基于用户设置规则的消息过滤业务技术要求》。

由于短消息本身传输容量小以及终端文本管理不便，故短消息过滤规则设置或被过滤短消息管理受到一定的限制。但优点是用户可以随时随地进行相应短消息过滤规则的设置或被过滤短消息的查询及管理，故此尽管操作相对困难，但是使用十分方便，要求系统必须支持。随着终端越来越智能，操作困难的问题也会日渐减少。

7.1.2　Web 设置方式

需要在用户业务管理模块（UMM）中增加Web服务器模块，用户可以基于HTTP或者HTTPS的来进行短消息过滤业务管理，如图7所示。处于安全目的考虑，需要采纳以下建议：

- 具备安全可靠的用户鉴别机制；
- 支持HTTPS协议。

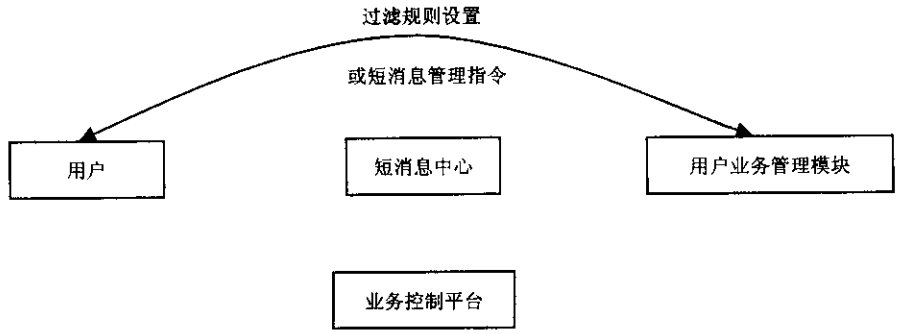

图7 Web设置方式

具体操作方式：同普通Web页面管理。由于Web操作本身具备信息量大、操作方便等优势，基于Web业务管理内容不仅要包括所有基于短消息业务管理内容，还要具备更多短消息业务管理无法或者不便实现的管理内容。

7.2 业务管理内容

7.2.1 短消息日志管理

短消息用户可以经过认证后查询、统计和删除发给自己的已经被过滤的短消息。

- 统计功能，可以对当前所有已经过滤掉的短消息进行统计；
- 查看功能，可以查看已经过滤掉的短消息的具体内容；
- 查询功能，可以根据查询特征来搜索已经被过滤掉的短消息；
- 删除功能，可以单独或者批量删除指定的被过滤短消息。

相应内容参见YD/T 1774-2008 《基于用户设置规则的消息过滤业务技术要求》

7.2.2 过滤规则管理

短消息过滤规则管理：

- 黑白名单规则设置，包括单条或者成组添加黑白名单、单条或者成组删除黑白名单，并且支持黑白名单查询统计。
- 关键词规则设置，包括单条或者成组添加关键词、单条或者成组删除关键词，支持关键词的查询。
- 时间段规则设置，包括添加、删除过滤短消息时间段，并支持过滤短消息时间段查询。

相应内容参见YD/T 1774-2008 《基于用户设置规则的消息过滤业务技术要求》

8 通信协议

8.1 总体协议接口要求

为了满足不同运营商或者同一运营商不同网络之间的互联互通要求，短消息过滤系统模块之间应尽量采用标准协议接口。目前存在的协议接口有8个（其中1个只适用于基于主叫归属下发模式的短消息过滤系统）。

（1）短消息中心（SMC）与业务控制平台（SCP）；

（2）业务控制平台（SCP）与短消息过滤模块（SFM）之间的协议接口；

（3）业务控制平台（SCP）与用户管理模块（UMM）之间的协议接口；

（4）短消息过滤模块（SFM）与用户规则数据库（URD）的协议接口；

（5）短消息过滤模块（SFM）与过滤短信数据库（FSD）；

（6）用户管理模块（UMM）与用户规则数据库（URD）的协议接口；

（7）用户管理模块（UMM）与过滤短信数据库（FSD）的协议接口；

（8）主被叫短消息过滤系统之间通信的协议接口。

其中，涉及互联互通要求的主要是前3个协议接口；后5个协议接口属于运营商同网络内部的实现协议接口，可以根据运营商实际需要自行开发，出于自身网络发展要求最好也进行标准规范，在此不对此5个协议接口进行规范。

前3个接口，短消息中心（SMC）与业务控制平台（SCP）之间短消息鉴别接口采用标准的短消息点对点协议（SMPP）（参见第8.2节）；业务控制平台（SCP）与短消息过滤模块（SFM）之间接口和业务控制平台（SCP）与用户管理模块（UMM）之间接口采用互联网短消息网关协议（参见第8.3节）。

8.2 短消息鉴别接口协议

短消息鉴别接口协议主要基于扩展的短消息点对点协议（SMPP），具体采用协议流程如图8所示。

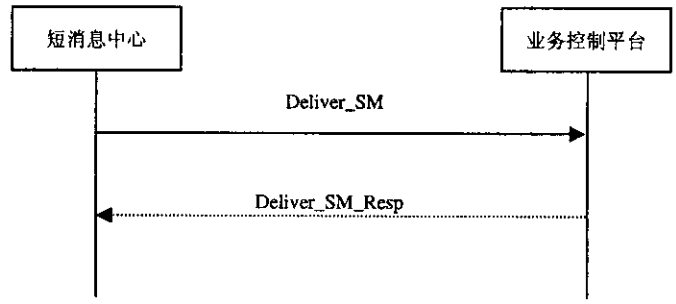

图 8 SMPP 短消息鉴别协议

8.2.1 描述

SMSC在接收到短消息时，向过滤模块发送鉴别请求消息，过滤模块处理完后，向SMSC发送鉴别响应消息。

方向：SMSC↔过滤模块

8.2.2 鉴别请求消息 （DELIVER_SM）的参数

方向：SMSC→过滤模块

参数说明：所有的参数延续SMPP标准协议中的DELIVER _SM参数。

8.2.3 鉴别响应消息 （DELIVER _SM_RESP）的参数

操作结果

方向：SMSC←过滤模块

说明：操作结果为长度为4字节的整数，目前取值为：

0—正常发送；

1—不发送短消息。

注：根据运营商实际运营需求，该取值范围将来可能扩充。

8.2.4 错误处理

SMPP层的错误在Command_status中统一定义，应用层的错误不处理。

SMSC等待响应消息，如果响应时间≥5s（参考，一般60s。可配置项），则SMSC记录日志不必重发，正常下发信息。

如果错误是SMPP层的错误或操作超时，则SMSC应该按照正常流程处理（发送短消息）。

8.3 互联网短消息网关协议

互联网短消息网关协议主要用于用户通过短消息方式进行短消息过滤规则管理以及过滤掉的短消息统计查询。短消息中心增设用户业务管理短消息实体（SME），由用户通过短消息方式来进行短消息过滤规则的设置和被过滤短消息的统计查询。短消息中心与该用户业务管理短消息实体（SME）之间采用短消息网关协议。由于各个运营商都有各自的互联网短消息网关协议，故采取相应的互联网短消息网关协议。

具体相关协议应用如图9所示。

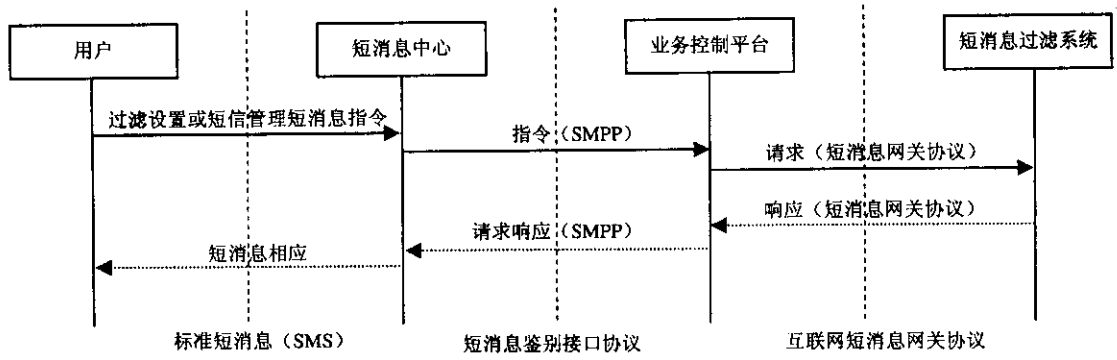

图9 短消息网关协议

在实际短消息过滤系统中，要根据具体采用的互联网短消息网关协议进行实际部署。

8.4 网间互通协议要求

对于不同网络之间短消息过滤需要考虑网间互通。不同运营商之间短消息采用点对点前转方式，通过互通网关以后，进入被叫所在的运营网络，之后即可采用第6章两种短消息过滤方式，即采用主叫归属短消息下发模式的短消息过滤和采用被叫归属短消息下发模式的短消息过滤。建议把短消息前转到被叫归属短消息中心（SMC），然后采用被叫归属下发模式的短消息过滤。

网间互通协议参见YD/T 1291-2003 《点对点短消息网间互通协议要求》。

9 系统管理

短消息过滤系统需要必须提供本地和远程管理控制手段（例如互联网或专用网）进行管理策略配置和系统日志接收访问，远程通信采用加密方式，并且系统本身要提供管理终端软件以验证此管理和控制手段。系统管理至少应包括角色管理、设备管理和业务管理。

9.1 角色管理

为了安全可靠，短消息过滤系统至少应该提供3种管理角色：用户管理角色、系统管理角色和审计管理角色。

- 用户管理角色：可以生成、修改和删除系统管理员账号，调整系统管理员对应账号的具体管理权限，但用户管理角色不能调整自身和审计管理角色对应账号的管理权限；

- 系统管理角色：具有对短消息过滤系统的管理权限，如：系统平台管理、查看过滤短消息日志等权限，但无用户管理和系统操作日志审计权限；
- 审计管理角色：仅具有对系统操作日志的查看、备份、删除的权限，并可以进行可选的用户审计配置、审计日志的完整性检查及登陆失败处理。

对于所有权限的管理角色，都应有详细的登录记录和操作记录，以备参看。

9.2 设备管理

具有系统管理角色的实体可以管理、配置和控制短消息过滤设备的运行。设备管理主要包括如下功能：

- 查看短消息过滤系统的网络接口状态、组件的工作状态、当前的日志文件大小、CPU占用率、内存占用率、存储器占用率，以及软硬件版本信息；
- 配置短消息过滤系统的网络接口和组件的工作参数与工作状态；设置管理接口的通信参数；启动或者停止系统运行；备份和转储系统日志和用户日志；

具体具有系统管理角色的实体所对应的管理权限可以由具有用户管理角色的实体来设置。

9.3 业务管理

管理和控制短消息过滤业务运行。业务管理主要包括如下功能：

- 配置业务运行参数，启动或者停止业务运行；
- 加载预定义过滤规则，以方便用户选择过滤规则集；
- 查询和统计短消息过滤业务数据。

9.4 计费管理

9.4.1 计费方式

短消息过滤系统计费支持多种计费方式：

- 预付费/后付费方式；
- 包月/按条付费方式。

若要对被拦截短消息的源号码计费，就需要短消息过滤系统的计费网关生成计费话单，提交营账系统进行计费。具体的计费格式，以局方话单格式为准。

9.4.2 计费流程

短消息过滤系统计费网关针对不同的业务，分别配置计费参数，由业务系统发起扣费请求，计费网关根据配置信息生成正式扣费信息，发送到计费系统进行计费。具体计费流程以运营商或者业务提供商实际计费策略为准。

10 安全要求

和其他系统一样，短消息过滤系统也可能存在安全漏洞。若对该系统攻击成功，则会导致其工作失灵。因此短消息过滤系统首先要保证自身的安全。

10.1 网络安全

鉴于短消息过滤系统的重要性，建议在网络安全方面采取以下措施：

- 短消息过滤系统与现有短消息系统进行网络隔离，可以采用VLAN技术；
- 在短消息过滤系统所处局域网与外网之间建议增加防火墙设备，局域网内部建议增加入侵检测设备（IDS）；

- 重要设备需要采用双机热备；
- 系统除了管理端口可以配置有效IP地址以外，其他端口都不设IP地址；
- 系统不允许启用任何Internet 服务（远程管理除外）。

10.2 数据库安全

对数据库系统所管理的数据和资源提供安全保护主要包括以下几点：

- 物理安全，对数据库要求采用Raid磁盘阵列，并有明确的备份机制，避免物理方面破坏的问题；
- 逻辑安全，对于用户数据采用严格的加密机制，没有一定授权不能访问；
- 用户鉴别，确保每个用户被正确识别，避免非法用户入侵；
- 可获得性，指用户一般可访问数据库和所有授权访问的数据；
- 可审计性，能够追踪到谁访问过数据。

10.3 日志审计

日志审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。审计信息对于确定问题和攻击源很重要，同时，系统事件的记录能够更迅速和系统地识别问题，并且它是后面阶段事故处理的重要依据。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便发现或对可能产生的破坏性行为提供有力的证据，从而避免针对系统的攻击以及系统本身存在的问题。

短消息过滤系统至少应包括系统操作日志和系统运行日志。

10.3.1 系统操作日志

针对系统的所有登录以及操作事件，系统都要有详细的记录，应包括如下字段：

- 操作者；
- 操作时间；
- 操作内容；
- 是否成功。

系统操作日志的存储时间应能够满足用户的要求，系统操作日志数据库原始数据最低存储时间不低于3个月。

10.3.2 系统运行日志

主要是记录系统运行状况，具体格式根据实际需求而定。

10.3.3 审计功能

短消息过滤系统必须支持操作日志和系统日志的转储和备份。当系统内的日志数据超过预定义的域值时，系统应及时通知进行外部备份。

短消息过滤系统应严格保护操作日志和运行日志，只有具有审计管理角色的实体可以查询和审阅操作日志和运行日志，并可以在确认后删除日志数据。

10.4 管理安全

短消息过滤系统应具备严格的访问控制机制，一般采用身份认证形式确保具有管理角色实体的身份，非授权人员不能登录短消息过滤系统。

具有管理角色的实体在一定时限内失败的登录次数超过设定限值，系统应阻止该实体的进一步的登录或在设定时间内无法登录。

具有管理角色的实体在设定时间内没有任何操作，则自动退出。如要进行进一步的操作，必须重新登录。

对于远程管理应采用加密信道对传输信息进行处理，保证数据的机密性、完整性和不可否认性。

系统必须严格按照操作日志格式记录所有的登录事件与操作事件。

11 扩展功能实现

11.1 过滤规则分析功能

短消息过滤系统可以具备对用户设置规则的统计分析功能，即对用户设置的黑名单进行统计分析，如果出现达到一定比例，则系统提炼为怀疑地址，然后分析相关过滤掉的短消息，如果达到一定阈值，则自动进入公共过滤后备库，从而可以有两个用途：

- 形成公共过滤黑名单条目提供给用户自行选择；
- 形成安全部门公共过滤后备条目以便进一步确认；

过滤规则分析功能只能通过短消息过滤系统自动分析实现。

11.2 对公共过滤投诉支持

短消息过滤系统可以支持公共过滤投诉平台，用户可以把自认为具有共性的黑名单和关键词标识为怀疑条目。系统自动进行统计，达到一定阈值，则自动进入公共过滤后备库，可以有两个用途：

- 形成公共过滤黑名单条目提供给用户自行选择；
- 形成安全部门公共过滤后备条目以便进一步地确认。

公共过滤投诉功能只能通过用户自己发指定格式的投诉短消息或者在Web界面操作实现。

12 性能指标

性能指标是业务系统的重要评价手段，对基于用户设置规则的短消息过滤系统也非常重要。但是对于短消息过滤系统，由于性能指标除了取决于系统本身以外，还与测试环境、测试样本有关，因此，本标准对短消息过滤系统的具体性能指标数值不作统一规范，只作为重要的性能指标供比较。基于用户设置规则的短消息过滤系统的性能指标主要包括3类：准确性指标、效率指标和系统指标。具体规定参见附录A——基于用户设置规则的短消息过滤系统的性能指标。

附 录 A
（规范性附录）
基于用户设置规则的短消息过滤系统的性能指标

本附录的目的是提供对短消息过滤系统性能评价的指标体系。短消息过滤系统的指标主要包括3类：准确性指标、效率指标和系统指标。

A.1 准确性指标

准确性指标在很大程度上取决于测试时采用的样本集和测试环境。样本集和测试环境不同，准确性也不相同。因此，本标准对检测率、误报率和漏报率的准确性数值不作统一规定，只作为重要的性能指标供比较。

A.1.1 检测率

检测率是指系统能够正确识别非法短消息的概率。通常利用已知非法短消息的实验数据集合来测试系统的检测率。

检测率=检测出的非法短消息的数量/实际非法短消息的数量

A.1.2 误报率

误报率是指系统把合法短消息作为非法短消息的概率和把一种非法短消息报告为另一种非法短消息的概率。

误报率=错误识别短消息的数量/（总体合法短消息数量+总体非法短消息数量）

A.1.3 漏报率

漏报率是指接收到非法短消息时，系统不能正确识别的概率。通常利用已知非法短消息的实验数据集合来测试系统的漏报率。

漏报率=不能识别的非法短消息的数量/非法短消息的数量

A.2 效率指标

效率指标是短消息过滤系统本身具备的处理能力。效率指标和系统软硬件都有关系。效率指标与准确性指标一样，只作为重要的性能指标供比较。主要技术指标是过滤速度。

A.2.1 过滤速度

过滤速度是短消息过滤系统在保障检测率的条件下的最大处理能力。

A.3 系统指标

系统指标是短消息过滤系统本身具备的存储能力。系统指标主要和系统设备硬件和系统设置有关，往往根据用户系统的实际需求，选取不同的设备级别。系统指标与准确性指标一样，只作为重要的性能指标供比较。主要技术指标包括最大账户数、系统最大规则数和用户最大规则数。

A.3.1 最大账户数

系统可以支持的最大个性化账户数目。

A.3.2 系统最大规则数

系统可以具有地址规则（黑白名单）、关键词规则和时间规则的最大数目。

A.3.3 用户最大规则数

系统允许用户具有地址规则（黑白名单）、关键词规则和时间规则的最大数目。

参 考 文 献

1. GB 4943-2001	信息技术设备的安全
2. GB/T 5271.8-2001	信息技术 词汇 第8部分：安全
3. GB/T 18336.2-2001	信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求
4. YD/T 1039.1-2005	900/1800MHz TDMA数字蜂窝移动通信网短消息中心设备技术要求 第一部分：点对点短消息业务部分
5. YD/T 1040.1-2005	900/1800MHz TDMA数字蜂窝移动通信网短消息中心设备测试方法 第一部分：点对点短消息业务部分
6. YD/T 1094-2000	900/1800MHz TDMA数字蜂窝移动通信网扩展短消息实体与短消息业务中心间的接口协议规范
7. YD/T 1290.1-2003	点对点短消息网间互通总体技术要求 第一部分 固定网与移动网之间互通
8. YD/T 1290.2-2005	点对点短消息网间互通总体技术要求 第二部分 固定网和固定网之间互通
9. YD/T 1364-2005	点对点短消息网间互通设备技术要求
10. ETSI GSM 03.38（1996）	欧洲数字蜂窝通信系统（阶段2+）：字符和特定语言信息
11. ETSI GSM 03.39（1996）	欧洲数字蜂窝通信系统：短消息中心和短消息实体间连接的接口协议
12. ETSI GSM 03.40（1996）	欧洲数字蜂窝通信系统（阶段2+）：短消息业务技术实现
13. ETSI GSM 03.47（1996）	欧洲数字蜂窝通信系统：短消息中心与移动交换中心间互联协议栈举例
14. 3GPP TS 23.040（2004）	短消息业务的技术实现
15. TIA/EIA/IS-637（1995）	宽带扩频蜂窝通信系统的短消息业务