国 际 电 信 联 盟

ITU-T X.1248

(09/2017)

国际电信联盟
电信标准化部门

X系列：数据网，开放系统通信和安全性

网络空间安全 – 反垃圾信息

打击手机垃圾短信的技术框架

ITU-T X.1248建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
报文处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
PITV安全	X.1180–X.1199
网络空间安全	
计算网络安全	X.1200–X.1229
反垃圾信息	**X.1230–X.1249**
身份管理	X.1250–X.1279
安全应用和服务	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1339
PKI相关建议书	X.1340–X.1349
网络安全信息交换	
网络安全综述	X.1500–X.1519
脆弱性/状态信息交换	X.1520–X.1539
事件/事故/探索法信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
探索法和信息要求	X.1560–X.1569
标示和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全综述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳实践和指导原则	X.1640–X.1659
云计算安全实现	X.1660–X.1679
其他云计算安全	X.1680–X.1699

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1248建议书

打击手机垃圾短信的技术框架

摘要

ITU-T X.1248建议书定义了垃圾即时消息的特征，并详述了打击垃圾即时消息（SPIM）的技术要求。随着即时通讯（IM）的普及，垃圾即时消息扩散的问题日益严重。即时通讯的特点（例如基于网际协议（IP）、应用广泛、免费使用）很大程度上导致了垃圾即时消息广泛地、肆无忌惮地传播。如果垃圾即时消息问题未得以认真解决，可能会对即时消息服务本身的使用产生负面影响

历史沿革

版本	建议书	批准日期	研究组	唯一ID*
1.0	ITU-T X.1248	2017-09-06	17	11.1002/1000/13262

关键词

打击垃圾信息、手机垃圾短信、技术框架

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

简介

随着网络以及移动互联网的飞速发展，即时通讯（IM）已从一个简单的聊天工具发展为集通信、信息、娱乐、搜索、电子商务、商务合作、企业客户服务于一体的综合信息平台。即时通讯价格低廉、使用便捷，因此越来越多的人改用即时通讯，这也对传统通讯领域造成了很大影响。目前，电信运营商正在提供更多的即时通讯服务，但同时，即时通讯在很大程度上已成为垃圾邮件在音频和短消息服务上传播的介质。各国的电信运营商均不同程度地意识到和/或受到了垃圾即时消息（SPIM）的影响。垃圾即时消息不仅浪费网络资源，而且浪费用户的时间、降低用户的工作效率。另外，垃圾即时消息被用于网络欺诈、传播网络病毒、蠕虫病毒、间谍软件以及传播各种形式的恶意软件，甚至会携带对用户造成损害的信息。因此，垃圾即时消息降低了用户对使用即时通讯的满意程度，已成为阻碍用户使用即时通讯的重要因素。

虽然我们已在即时通讯系统上实施了很多反垃圾邮件的对策，但即时消息系统里的许多弱点仍会造成垃圾即时消息，这些弱点例如：无限制注册率、未经认证接收信息、不安全的网络传输机制、缺乏用户信息发送率控制以及即使通讯系统中不可避免的漏洞。

为防止垃圾即时消息的产生和蔓延，本建议书针对即时信息系统的功能，详述了打击垃圾即时消息的技术要求。例如，应当设计出注册机制，该种注册机制能够防止大量自动化注册，并要求即时通讯系统为使用者提供一种功能来选择是接收还是阻拦来自经授权的/未经授权的实体的所有信息，以及当使用者发送超场量的信息时，限制使用者发送率。

ITU-T X.1248建议书

打击垃圾即时消息的技术要求

1 范围

此建议书确认了打击垃圾即时消息系统的类型和特征。为减缓垃圾即时消息的产生和蔓延，本建议书规定了打击垃圾即时消息的技术要求（涉及即时消息客户端和服务器两方面）。本建议书主要说明即时消息系统层面的反垃圾即时消息措施，适用于即时通讯服务运营商。

2 参考文献

无。

3 定义

3.1 在其他处规定的术语

本建议书使用以下在其它文献中规定的术语：

3.1.1 即时通讯（instant messaging）（IM）[b-IETF RFC 3428]：在接近实时的一组参与者之间交换内容。一般来说，内容是短文本消息，尽管情况并非如此。

3.1.2 垃圾信息（spam）[b-ITU-T X.1240]：“垃圾信息”一词的含义取决于各国根据其国家技术、经济、社会和实际情况对隐私和垃圾信息构成的看法。值得一提的是，随着技术的发展，其含义不断变化并拓宽，为滥用电子通信创造了新的可乘之机。尽管在全球范围内没有有关垃圾信息的一致定义，但该术语一般用来描述为推销商业化产品或服务通过电子邮件或移动消息批量传送的推介性电子通信。

3.1.3 垃圾即时消息（spam over instant messaging）（SPIM）：目标是即时消息业务用户的垃圾信息。

3.1.4 垃圾散播者（spimmer）[b- ITU-T X.1244]：SPIM的散播者。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用以下缩写词和首字母缩略语：

ID 身份

IM 即时消息

IP 网际协议

SMS 短消息业务

SPIM 垃圾即时消息

5 惯例

无。

6 垃圾即时消息的特征及产生方式

垃圾即时消息，指使用者接收到的不想看到的或者对用户产生破坏的消息。因此，垃圾即时消息具有以下特征：

– 垃圾即时消息经常实时出现。当发送者和接收者都在线时，一般发送者刚发出消息接收者就能看到。即使接收者当时不在线，接收者刚上线时也能立即收到垃圾即时消息。

– 垃圾即时消息经常以大量的消息及相同的内容被发送。

– 垃圾即时消息散播者是用来称呼未经授权向即时消息接收者发送垃圾即时消息的人。然而，有时好友的账户也会由于感染病毒或者泄露个人账户信息而被强制发送垃圾软件。朋友发来的垃圾即时消息其实更危险，尤其是邮件中包含恶意网站或包含接收者可点击的可操作的文件，这样接收者的系统也更有可能感染病毒。

– 因为账户可以随意申请，垃圾即时消息不容易被追踪，并且即使追踪到了也并非是真实信息。

垃圾即时消息的产生和即时信息系统功能（详见附件1）密切相关，能产生垃圾即时消息的情况如下：

– 垃圾即时消息散播者可利用自动注册软件来注册大量账户，从而利用这些账户来传播垃圾即时消息。

– 不良用户可能利用假的即时消息账户，并利用利用假的即时消息账户来传播垃圾软件。

– 如果黑客已经获得账户的合法使用权，他/她将修改用户信息，如密码或其他验证信息，来用这个账户发垃圾即时消息（经常会持续很长一段时间）。

– 如果即时消息客户的接受条件被改为无需认证，就可任意无限制接收垃圾即时消息了。

– 即时消息在传送的过程中被篡改。广告或者病毒可能被嵌入即时消息中将它转变成垃圾即时消息。

– 由于缺乏验证机制，垃圾即时消息制造者能随意加好友，然后给这些好友发送垃圾即时消息。

为拦截垃圾即时消息，必须考虑垃圾即时消息的特点和造成垃圾即时消息出现的可能情况，尽可能全面地提出阻拦方案。

7 打击垃圾即时消息结构功能图

7.1 概述

打击垃圾即时消息结构功能图如下图7-1。

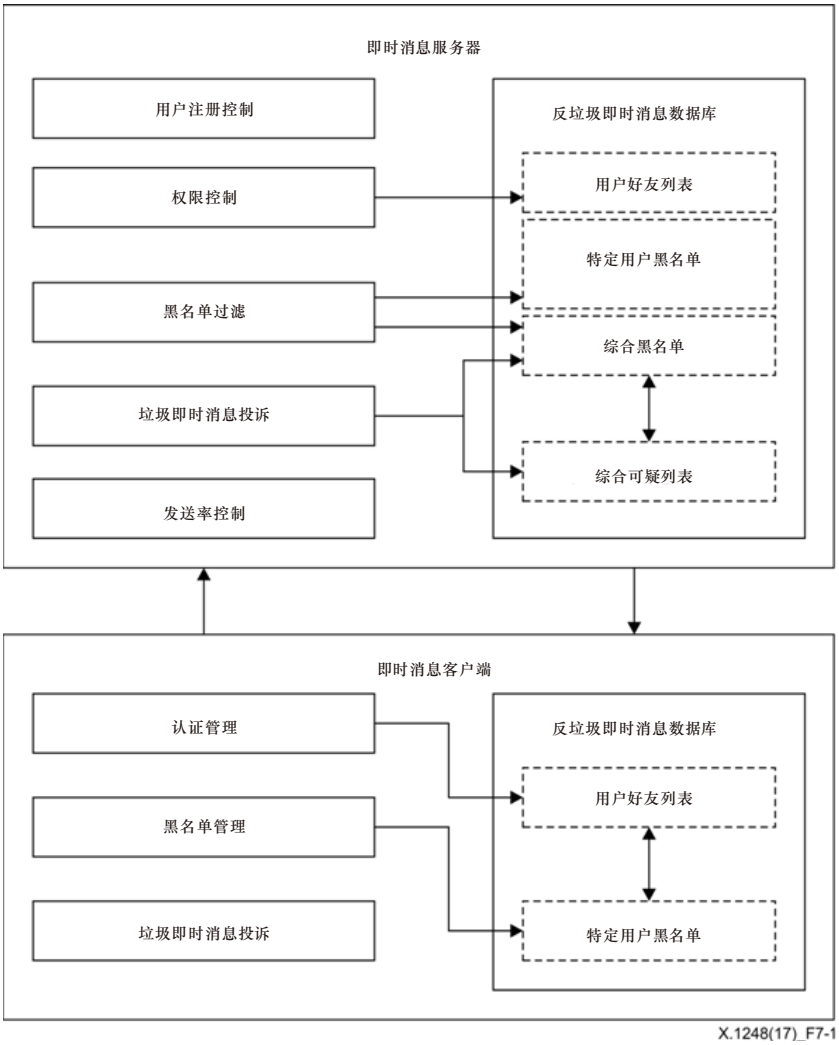

图7-1 – 打击垃圾即时消息结构功能图

这个结构图融合了打击垃圾即时消息的功能，包括黑名单过滤器、用户注册控制、垃圾即时消息投诉。更重要的是，该结构支持限制即时消息发送率的过滤、即时消息发送者的权限控制。

附录I更详尽地描述了即时消息客户端和即时消息服务器功能，即时消息发送者、即时消息接收者和即时消息散播者的角色。

7.2 组件功能

7.2.1 即时消息服务器

即时消息服务器组件功能包含以下六个因素：

1) 用户注册控制

用户注册控制需要人工确认，如验证码、邮件验证、短信验证码来防止用户自动注册。这能防止有大量电子注册账号的垃圾即时消息传播者发送垃圾即时消息。

2） 权限控制

当加好友的时候它需要发送一个申请请求，根据即时消息客户端的回馈来给是否加好友权限。

3） 黑名单过滤

即时消息服务器过滤器通过综合黑名单和特殊用户黑名单来过滤。

4） 垃圾即时消息投诉

用户的投诉机制可接到垃圾即时消息然后决定是否将这些账户加入到可疑黑名单或者综合黑名单里。要求结合外部的垃圾即时消息处理举报系统来输入或输出到综合黑名单里。

5） 发送率控制

要求在一段时间里同一个账户所发送的消息的数量要得到控制。当即时消息发送超量时就会被控制。

6） 反垃圾即时消息数据库

- 用户好友列表：它包含了所有受即时消息服务器管理的用户好友列表。要求即时消息服务器和用户的好友列表是同步的。
- 特定用户黑名单：它包含了所有受即时消息服务器管理的特定用户黑名单。要求即时消息服务器和用户的特定黑名单是同步的。
- 综合黑名单：它包含了被用户所举报的账户和被即时消息服务器发现的账户。例如，当即时消息发送率超出设置底线时，发送者的账户就会被即时消息服务器归结到综合黑名单。综合黑名单也包含了从其他途径（如其他即时消息处理器）归结到这里的账户。
- 综合可疑黑名单：它由所有的被即时消息处理器处理的可疑账户组成。综合可疑名单包含了被用户举报的账户、其他系统处理的可疑用户等等。

7.2.2 即时消息客户端

即时消息客户端功能构成包括以下四部分：

1） 权限管理

两大重要成分为即时消息用户的可见控制和对来自未经授权的实体的请求的管理控制。对于即时消息身份可见控制，用户决定是否应允许未经授权的用户查看本人消息（如即时消息用户账号、昵称、位置）。对来自未经授权的实体的请求管理控制，需要用户本人能选择一个适当的方式来处理这些请求。对私人问题用户应认为求证一个精准的答案或者屏蔽所有请求。更进一步来说，用户应该有能力来设定好友，在即时消息客户上管理这些好友列表。

2） 黑名单管理

用户能自我管理他们的特殊用户黑名单列表，所有在特殊用户黑名单列表账户的消息都被拦截。用户也可以从黑名单里加减人员甚至可以分享他们的特殊用户黑名单。

3） 垃圾即时消息投诉

即时消息用户应有投诉发送垃圾即时消息的账户的功能。被投诉的账户可能是户好友列表里的联系人，甚至未经授权的账户（该账户发送经授权的消息）。

4） 反垃圾即时消息数据库

- 用户好友列表：需要通过用户认证的好友列表。
- 特殊用户黑名单：用户自定义想屏蔽哪些账户的消息。

即时消息客户的数据库需要自动上传到即时消息处理器。

8 工作流程

8.1 发送率控制的工作流程

即时消息账户在一段时间能发送最大限制的消息数应该由即时消息处理器控制。

这个限制应对用户消息进行大量数据研究如机器研究、深层研究等。该限制应考虑到各种不同情况（包括但不限于以下情况）：

– 把即时消息发送给一批人，发送者是该组中的一位成员；

– 把即时消息发送给一批人，但发送者不是该组中的一位成员；

– 把即时消息被发送给用户的一个或更多好友；

– 把即时消息发送给非用户好友的人；

当收到的即时消息是从一个特定的账户发来的，即时消息处理器应根据以下步骤向发送率控制发送指令，如图表8-1所示：

– 统计特定时间内用户发送的消息数量；

– 和设定最小值相比，如果超出最小值，即时消息处理器进一步决定这属于哪种情况，看这种情况是否超出了某一特定情况。如果没有超出，那么即时消息处理器发送消息；

– 如果超出特定值，即时消息处理器查看该用户是否在综合可疑列表里。如果在，即时消息处理器屏蔽掉这些消息；如果不是，发送消息要计数超时间消息。如果这些超时消息超出给定值，即时消息处理器会把这个账户发送到可疑列表里。

执行发送率控制率步骤如下图表8-1所示：

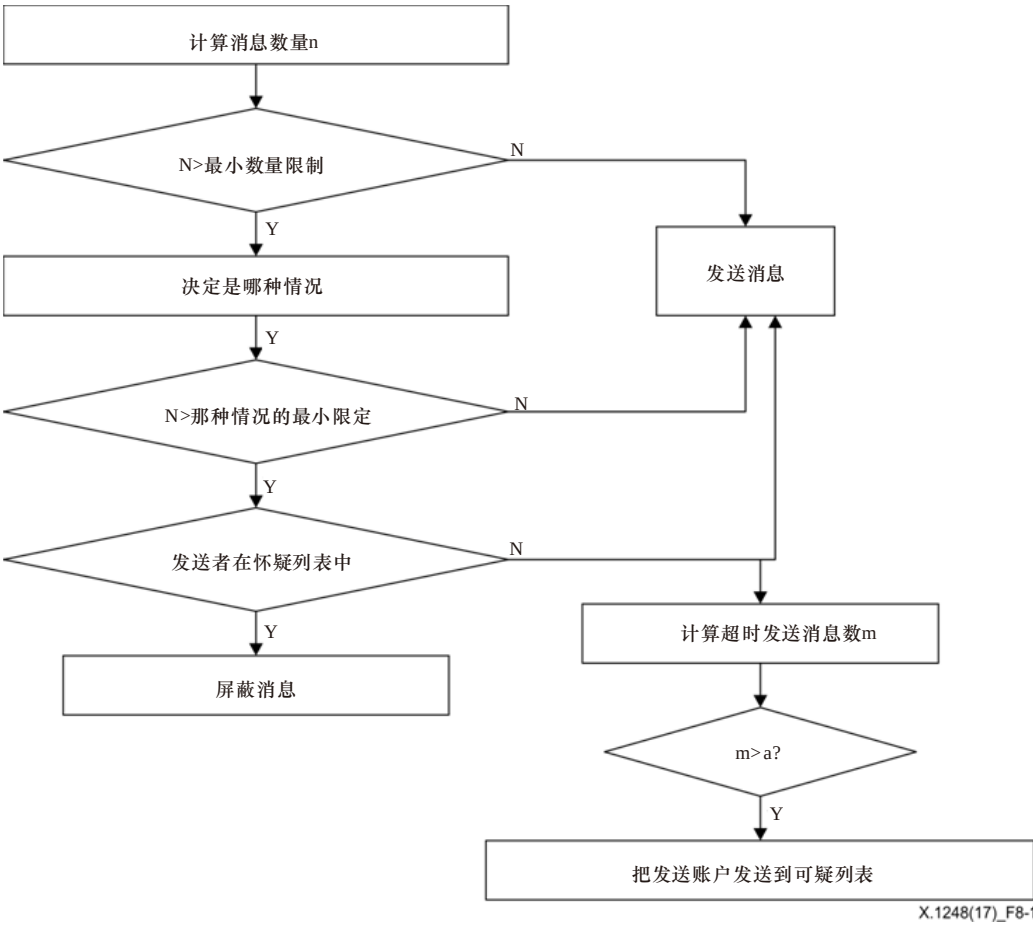

图8-1 – 执行发送率控制率步骤

8.2 黑名单工作流程

即时消息系统相对来说是独立的，因此即时消息服务提供者需要为即时消息处理器建立自主的综合黑名单。再者，出于考虑用户的利益，需要把特殊用户黑名单提供到即时消息用户里。

在即时消息系统里的各种黑名操作单流程如下：

– 用户在即时消息客户里编辑其特殊用户黑名单。当用户黑名单发生变化时，即时消息处理器及时更新管理特殊用户黑名单；

– 即时消息处理器多次跟踪过同一个账户（该账户被发送到特殊用户黑名单里）。如果次数超出了限制，即时消息处理器就会把它发送到综合黑名单里；

– 如果账户既不在综合可疑名单里又不在综合黑名单里，即时消息处理器就会把用户投诉里的名单放到综合可疑名单里。即时消息处理器会记录对于账户投诉的次数；如果账户超出限定次数，就会被添加到综合黑名单里。

黑名单过滤消息的步骤如下：

– 当即时消息处理器收到消息时，处理器会查看发送账户是否在综合黑名单里；如果在，处理器屏蔽该消息；

– 如果该账户不在综合黑名单里，处理器进一步查看是否放在用户的特殊用户黑名单里，如果在，处理器屏蔽消息。如果不在，处理器发送消息。

8.3 权利管理流程

这需要即时消息客户端拥有允许用户来设定哪种类型的消息是可以接收的功能，即时消息处理器也需要有根据用户需求来过滤消息的能力，来阻截非未被授权的发送者（如，非好友，非群好友，其他即时消息系统的好友，电话联系人）发送的消息。许可情况包括但不限于以下步骤：

1) 在即时消息客户里设置仅接受好友消息。当即时消息收到来自用户B给用户的消息时，即时消息处理器就会在A的好友列表里看用户B是否是其好友。如果不是，处理器会屏蔽其消息。

2) 在即时消息客户里设置接收来自群的消息。当即时消息处理器接收到来自群B的消息，处理器将会查看用户是否加入该群。如果没有，处理器会屏蔽该消息。另外，当即时消息处理器收到来自B群成员的邀请，用户A加入群B前会进行授权允许。

3) 在即时消息客户里设置接受既是好友又是群好友的消息，当即时消息处理器接受到来自群A的用户B发来的消息，处理器讲查看用户B是否在该用户的好友列表。如果不是，处理器屏蔽该消息。

4) 在即时消息用户里设置为只接收来自其它即时消息系统和电话联系人账户授权为朋友时的消息。当即时消息处理器接收到相关账户B的消息时，处理器将会查看账户B是否在该用户的好友列表。如果不在，处理器屏蔽该消息。另外，当即时消息处理器收来自用户B的加好友的请求，处理器把用户B放到好友列表前要经过该用户的许可。

5) 在即时消息处理客户里设置为仅限好友间的点对点连接。当即时消息处理器接受到来自用户A建立点对点请求，处理器将会查看用户B在该用户的好友列表里。如果在，即时消息处理器将会对该用户发送用户B的请求，并帮助该用户和用户B建立点对点连接。如果不是，处理器将会屏蔽用户B的请求。

用户A、用户B、A群、B群、账户B的关系如图表8-2。

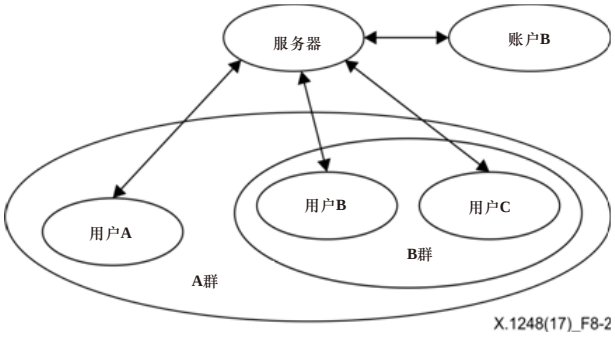

图8-2 – 用户和群的关系

8.4 用户注册管理流程

为防止用户自动注册，即时消息系统应执行一步或多步确认措施，如验证码、验证邮件、短信验证码。

当用户在即时消息客户、即时消息用户注册网提交注册信息（如用户名、密码、手机号、邮箱）时，即时消息处理器发送一个注册认证给用户，如验证码、短信验证码、注册确认邮件。

当用户发送确认信息到即时消息处理器后，即时消息处理器会确认由用户提交上来的消息。如果是实时认证，即时消息处理器会发送认证成功消息，并在数据库储存用户注册信息。如果没有，会发送认证失败消息。

即时消息系统应与消息网关或邮件服务器相联系来实现给用户发送消息验证码或注册消息确认邮件的功能。

8.5 垃圾即时消息投诉流程

两项垃圾即时消息投诉流程应如下：

1) 通过即时消息客户举报。用此方法，举报处理步骤应实施如下：

接收垃圾即时消息以后即时消息用户在即时消息客户里标记这个账户；投诉会被发送到即时消息处理器。即时消息处理器应有一个投诉确认设定。当收到用户的投诉，及时消息处理器先确认该账户是否在综合可疑名单里，同时计算该账户被投诉的次数。如果该数量超出审核限定，即时消息处理器将此账户添加到综合黑名单。如果此账户已经在综合可疑名单里，即时消息处理器累计其投诉次数。如果在限定时间里超出审核限定，即时消息处理器将这个账户发送到综合黑名单。如果此账户已经在综合黑名单里，即时消息处理器就不做处理。之后这个账户发送的消息就会被即时消息处理器屏蔽。

2) 通过外部举报处理系统举报。用此方法，投诉处理步骤实施如下：

收到垃圾即时消息后用户向外部垃圾即时消息处理系统投诉。外部垃圾即时消息处理系统掌管分析用户投诉决定是否将被该账户加入黑名单。即时消息处理器和外部垃圾即时消息投诉处理系统相连接来决定黑名单。黑名单账户消息会被即时消息处理器屏蔽。

8.6 垃圾即时消息过滤流程

当即时消息处理器接收到即时消息，处理器根据综合黑名单和特殊用户黑名单设置过滤；此步骤在条款8.2中解释。

如果即时消息发送者不在综合黑名单和特殊用户黑名单，接着即时消息处理器将根据权限控制过滤，分析发送者是否有权发送消息给接收者（被接收者设定的）。如果没有，消息会被屏蔽。授权情况在条例8.3中解释。

如果是，即时消息会根据发送率限制来进行过滤；此步骤在条例8.1中解释。

附录I

即时消息系统的角色与功能

（此附录不构成该建议书的一部分）

基本即时消息系统模式如图1.1。

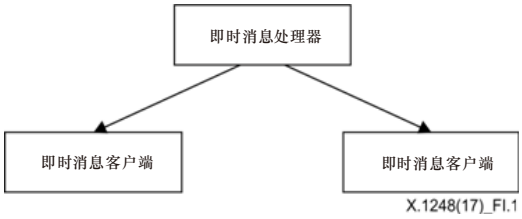

图1.1 – 即时消息基本模式

即时消息基本系统包括即时消息处理器和大量客户端。即时消息处理器用于接收和发送客户发的消息。即时消息客户端有两个角色：即时消息发送者和即时消息接收者。即时消息发送者发送即时消息给即时消息接收者转送器，即时消息处理器传送消息给即时消息接收者。如果即时消息发送者发送垃圾信息，那么该用户就被认定为垃圾即时消息传播者。

即时消息系统的功能需要被即时消息服务器、即时消息客户和两者之间的联系所完善。

即时消息处理器的主要功能如下：

– 用户管理，如用户注册、用户登录和注销、用户账户编辑；
– 即时消息管理，如消息发送、消息接收、消息转换；
– 好友管理，如好友查找、好友列表管理；
– 系统管理，如参数结构、系统更新、系统开启/重启/退出。

即时消息客户端主要功能如下：

– 用户管理，如用户注册、用户登录注销；
– 即时消息管理，如消息发送、消息接收；
– 好友管理，如添加好友、删除好友、好友查找；
– 客户管理，如参考结构、客户更新、客户端开启/重启/退出。

参考文献

[b-ITU-T X.1231] ITU-T X.1231建议书（2008），反垃圾信息技术策略。

[b-ITU-T X.1240] ITU-T X.1240建议书（2008），用于打击垃圾电子邮件的技术。

[b- ITU-T X.1244] ITU-T X.1244建议书（2008），打击IP多媒体应用中垃圾信息的概述。

[b-IETFRFC2778] IETF RFC2778（2000），即时通讯和空间的模型。

[b-IETF RFC 3428] IETF RFC 3428（2002），用于即时通讯的会话启动协议（SIP）扩展。

ITU-T 系列建议书

系列 A	ITU-T 工作安排
系列 D	一般关税原则
系列 E	整体网络运营、电话业务、服务运营和人为因素
系列 F	非电话电信服务
系列 G	传输系统和媒体、数字系统和网络
系列 H	视听和多媒体系统
系列 I	综合服务数字网络
系列 J	有线电视网络和电视的传播，合理的计划和其他多媒体信号
系列 K	干扰防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理、包括电信管理网和网络维护
系列 N	维护：国际广播节目和电视传输电路
系列 O	测量设备说明书
系列 P	终端和主观及客观的评价方法
系列 Q	交换和信令
系列 R	电报传输
系列 S	终端服务终端设备
系列 T	远程信息处理服务终端
系列 U	电报交换
系列 V	电话网络之上的数据通信
系列 X	**数据网络、开放系统通信和安全**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	电信系统的语言和通用软件方面

瑞士印刷
2017年，日内瓦