[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04W 4/14 (2009.01)
H04W 12/04 (2009.01)
H04W 12/06 (2009.01)
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610099083.X

[45] 授权公告日 2009 年 12 月 23 日

[11] 授权公告号 CN 100574524C

[22] 申请日 2006.7.19

[21] 申请号 200610099083.X

[73] 专利权人 王李琰

地址 518048 广东省深圳市福田区益田路福乐雅园 2－304

[72] 发明人 程朝辉 王李琰

[56] 参考文献

CN1645789A 2005.7.27

CN1394032A 2003.1.29

CN1697379A 2005.11.16

US2006/0095521A1 2006.5.4

US6356935AB1 2002.3.12

EP1653696A1 2006.5.3

Internet 中使用安全数字证书——加密与数字签名. 祁飚，石中锁. 电脑开发与应用，第 16 卷第 3 期. 2003

《电子签名法》与数字签名的技术实现. 关振胜. 电子商务，第 1 期. 2006

巧用数字签名为电子邮件护航. 李晓昀，余颖. 福建电脑，第 5 期. 2006

审查员 李彦琴

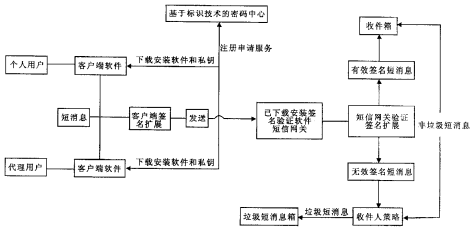
权利要求书 2 页 说明书 11 页 附图 2 页

[54] 发明名称

一种基于标识的密码技术的短消息认证及可靠分类传递方法

[57] 摘要

一种基于标识的密码技术的短消息认证及可靠分类传递方法，包括：用户向密码中心以代表自己身份的、合法、有效标识申请注册，密码中心向用户提供私钥和客户软件，对发送的短消息进行签名，用户收到短消息后，判断是否是带签名的短消息，验证签名成功，该短消息将作为有效短消息。本发明具有方法简单、易于实施、工作准确、可靠、效率高、便于大面积推广等优点。



1．一种基于标识的密码技术的短消息认证及可靠分类传递方法，其过程包括用户申请服务过程；签名发送短消息过程；签名验证/短消息分类过程；其特征在于：

1）用户申请服务过程

①用户向密码中心以代表自己身份的、合法、有效标识申请注册，所说的密码中心为基于标识技术的密码中心，

②密码中心对用户的申请进行认证，确定其提供的标识合法、有效后，将该标识作为该用户的基本标识，

③用户认证通过后，密码中心确定该用户完整的用户标识，包括至少三个部分：密码中心系统标识、认证时使用的基本标识和服务有效期限，

④密码中心根据选择的标识签名算法和系统参数生成对应用户完整的用户标识的私钥并向用户提供客户软件，

⑤用户将密码中心提供的私钥和客户软件安装到手机终端或计算机上，

2）签名发送短消息过程

①确定要签名的内容信息

②通过密码中心提供的用户私钥和客户软件中设定的签名算法，对要签名的内容信息生成签名，

③组装带签名的短消息，在短消息中至少要添加用户的完整的用户标识和签名信息，包括被签名内容确定方法，签名算法和签名结果，然后发送短消息，

3）签名验证/短消息分类过程

用户收到短消息后，判断是否是带签名的短消息，对有签名的短消息进行如下处理：

①获取签名用户的完整的用户标识和签名信息，包括被签名内容确定方法，签名算法和签名结果，

②验证服务有效期限，如果服务有效期到期，则不验证签名，而以未签名短消息方式对待该短消息，

③确定被签名内容，并采用基于标识的密码技术验证签名，

④如果验证签名成功，该短消息将作为有效短消息处理而不进行短消息过滤。

2．如权利要求 1 所述的基于标识的密码技术的短消息认证及可靠分类传递方法，其特征在于对有签名的短消息进行处理时，验证该用户标识是否在标识黑名单中，如在黑名单中，则作为垃圾短消息处理。

3．如权利要求 1 或 2 所述的基于标识的密码技术的短消息认证及可靠分类传递方法，其特征在于对不带签名的短消息、超过服务有效期的短消息、签名有效性未通过验证的短消息，按照普通短消息进行短消息过滤处理。

4．如权利要求 1 或 2 所述的基于标识的密码技术的短消息认证及可靠分类传递方法，其特征在于还包括有标识黑名单的更新过程：

1）用户认为某封通过签名认证的短消息为垃圾短消息，将整封短消息发送到密码中心，举报该短消息，

2）密码中心验证被举报短消息的签名的真实性后，并按照规则决定是否将用户标识列入黑名单。

5．如权利要求 3 所述的基于标识的密码技术的短消息认证及可靠分类传递方法，其特征在于还包括有标识黑名单的更新过程：

1）用户认为某封通过签名认证的短消息为垃圾短消息，将整封短消息发送到密码中心，举报该短消息，

2）密码中心验证被举报短消息的签名的真实性后，并按照规则决定是否将用户标识列入黑名单。

一种基于标识的密码技术的短消息认证及可靠分类传递方法

技术领域

本发明属于网络技术领域，具体地说是一种基于标识的密码技术对短消息发送方认证并实现可靠分类传递的方法。短消息包括手机短信、即时通信 QQ、MSN 等

背景技术

随着无线通信及互联网的发展，手机短信、QQ、MSN 等已经成为人们重要的通信工具，而且手机短信与 MSN 等逐渐在融合互通。由此也产生了许多的问题，其中一个严重的问题是垃圾短信的泛滥。作为一个信息传播的媒体，没有有效的监督方法，必然带来很多的有害信息，给社会带来危害，在 SARS 肆虐期间，有很多无稽的谣言就是通过短信传播的，其传播速度之快传播面之广出乎人们的意料，因此必须建立一个严密、高效的短消息过滤平台，确保有害信息被及时拦截。运营商也纷纷表示要用技术手段遏制有害短信，努力为短信业务的发展创造一个持续、有序、健康的发展环境。

随着移动网络和智能手机平台的快速发展，信息病毒已开始登录手机平台从而在移动网络中传播开来，而手机短信是病毒传播的一个重要通道。保障手机移动网络的信息安全，消除手机蠕虫病毒所带来的短信流量对移动网络资源的有害占用，维护手机移动网络安全高效的运行，也已成为移动运营商急需解决的一个问题。

另一方面，许多有用的短信又被当成垃圾短信处理，对经济生活带来不利的影响。为了解决垃圾短信的问题，现有技术主要是在汇聚网关通过使用短信过滤系统去实现，通常使用的方法有：

1. 过滤器：通过缺省规则，用户设置过滤规则，从用户行为学习规则等方式，建立过滤规则库，比如通过关键字搜索。从而对收到短信按照规则进行分类为垃圾短信和非垃圾短信。
2. 黑名单：不接受来自黑名单上的短信或者根据病毒库特征拒收。

3．白名单：只接受来自白名单上的短信。

由于短消息内容、形式的多样性和每日不断出现的新的网站和服务商，采用以上技术的垃圾短信过滤技术都不可能实现完全正确的短消息分类。从而使得一些有用的短信被作为垃圾短信过滤掉了。另一方面，由于所有的处理都要在汇聚网关集中处理，对处理中心的每秒要求的处理能力非常高，在节假日或短信高峰期，就会有处理不及的情况，造成正常短信堵塞或收不到。

为了保证短消息的可靠送达，降低短消息汇聚网关集中处理的压力，本发明基于标识的密码技术实行数字签名认证，保证对注册用户短消息的可靠分类，同时基于该方法在短消息的处理上能实现分布式处理，减轻了汇聚网关的处理压力，提高了分类处理的效率及可靠性，同时，实现了一种好的商业模式和管理模式，对许多公司的业务至关重要。下面就基于标识的密码技术背景做简单介绍。

为了解决传统不对称密钥系统的缺点，在1984年以色列科学家Shamir提出了基于标识的密码系统的概念（IBC）。在基于标识的系统中，每个实体具有一个标识。该标识可以是任何有意义的字符串。但和传统公钥系统最大的不同是，在基于标识的系统中，实体的标识本身就是实体的公开密钥。由于标识本身就是实体的公钥，这类系统就不再依赖证书和证书管理系统如PKI，从而极大地简化了管理密码系统的复杂性。基于标识的数字签名与验证过程如下：

- 密码中心生成系统参数（包括公开的系统参数和主密钥）。
- 用户申请密码服务。用户向密码中心认证自己后，密码中心用公开的系统参数，主密钥和用户标识计算并分发对应于用户标识的签名私钥。
- 发送方用（从密码中心获取的）签名私钥与系统参数对需要签名的消息进行签名运算取得数字签名。发送方将被签名消息与数字签名一起发送给接收方；
- 接收收方验证签名，即用发送方的标识，系统参数和声明的被签名消息验证发送方的签名。

当密码中心是诚实时，如果接收方对发方数字签名验证成功，就可以说明以下实质性的问题：

（1） 该电子文件确实是由签名者的发方所发出的，电子文件来源于该发送者。

（2） 接收方收到的电子文件在传输中没有被篡改，保持了数据的完整性，因为，签署后对电子签名的任何改动都能够被发现。

以上均可参见现有技术 1 ISO. Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms. ISO-14888-3.

发明内容

本发明的目的在于针对短消息发送方提供一种高效的用户身份认证方法，进而实现一种短消息可靠分类传达方法，该方法能简单高效并可靠地解决短消息发送方的身份认证问题，进而解决一类短消息的准确分类问题。同时基于该方法在短信息的处理上能实现分布式处理，减轻了汇聚网关的处理压力，提高了分类处理的效率及可靠性，同时，实现了一种好的商业模式和管理模式。

本发明的目的是通过采用基于标识的密码技术实现的，其核心思想是将基于标识的密码技术应用于短消息分类领域。包括以下组成部分：第一用户申请服务过程；第二签名发送短消息过程；第三签名验证/短消息分类过程；还可以包括，第四标识黑名单的更新过程。系统有三个基本组成部分：密码中心，客户端签名扩展，短消息服务器验证签名扩展。密码中心根据选择的标识签名算法生成系统参数，包括主密钥。该过程与具体选择的标识签名算法有关（示例见具体实施部分）。客户（包括两类客户：个人用户和用户代理）向密码中心进行身份认证。该过程（1） 明确用户使用的基本标识；（2）验证用户确实拥有该标识；（3）生成对应用户标识的私钥；（4）用户安装私钥和客户端签名扩展软件。具体过程见下面的用户申请服务过程。客户申请服务成功后，即可用获得的私钥和签名软件发送签名的短消息（具体过程见下面的签名发送短消息过程）。短消息服务器在接收用

户的短消息时，如果短消息有签名则使用服务器验证签名扩展软件（该软件可从密码中心网站公开下载）验证签名。如果签名有效，则认为该短消息不是普通短消息，因而将该短消息直接放置到用户的收件箱。如果短消息签名无效或无签名，则短消息将进入短消息过滤程序进行过滤，其分类结果取决于过滤规则，具有不确定性（可被分类为正常短消息，也可能被判定为垃圾短消息）。通过该发明的实施，用户使用申请的服务发送的短消息将被准确地分类为有效短消息，将被确保放置到接收用户的收件箱中，而不会被作为垃圾短消息处理。

本发明的技术方案具体包括：用户申请服务过程；签名发送短消息过程；签名验证/短消息分类过程；其特征在于：

1）用户申请服务过程

①用户向密码中心以代表自己身份的、合法、有效标识申请注册，所说的密码中心为基于标识技术的密码中心，

②密码中心对用户的申请进行认证，确定其提供的标识合法、有效后，将该标识作为该用户的基本标识，

③用户认证通过后，密码中心确定该用户完整的用户标识，包括至少三个部分：密码中心系统标识、认证时使用的基本标识和服务有效期限，

④密码中心根据选择的标识签名算法和系统参数生成对应用户完整的用户标识的私钥并向用户提供客户软件，

⑤用户将密码中心提供的私钥和客户软件安装到手机终端或计算机上，

2）签名发送短消息过程

①确定要签名的内容信息

②通过密码中心提供的用户私钥和客户软件中设定的签名算法，对要签名的内容信息生成签名，

③组装带签名的短消息，在短消息中至少要添加用户的完整的用户标识和签名信息，包括被签名内容确定方法，签名算法和签名结果，然后发送短消息，

3）签名验证/短消息分类过程

用户收到短消息后，判断是否是带签名的短消息，对有签名的短消息进行如下处理：

①获取签名用户的完整的用户标识和签名信息，包括被签名内容确定方法，签名算法和签名结果，

②验证服务有效期限，如果服务有效期到期，则不验证签名，而以未签名短消息方式对待该短消息，

③确定被签名内容，并采用基于标识的密码技术验证签名，

④如果验证签名成功，该短消息将作为有效短消息处理而不进行短消息过滤。

本发明的进一步特征在于对有签名的短消息进行处理时，验证该用户标识是否在标识黑名单中，如在黑名单中，则作为垃圾短消息处理。

本发明的进一步特征还在于对不带签名的短消息、超过服务有效期的短消息、签名有效性未通过验证的短消息，按照普通短消息进行短消息过滤处理。

本发明还可以包括标识黑名单的更新过程，其特征在于：

1）用户认为某封通过签名认证的短消息为垃圾短消息，将整封短消息发送到密码中心，举报该短消息，

2）密码中心验证被举报短消息的签名的真实性后，并按照规则决定是否将用户标识列入黑名单。

概括地说，本发明是通过采用标识密码技术实现大用户量的短消息发送方认证，从而实现一类短消息的准确分类，近而实现对该类短消息的可靠传递。由于使用了基于标识的密码技术，免去了签名、验签的证书验证过程，免去了传统 PKI 技术所需要的巨大花费和复杂管理，从而能够支持海量用户；并且基于该方法在短信息的处理上能实现分布式处理，减轻了汇聚网关的处理压力，提高了分类处理的效率及可靠性，同时，实现了一种好的商业模式和管理模式。具有方法简单、易于实施、工作准确、可靠、效率高、便于大面积推广等优点。

附图说明

本发明有如下附图

图 1 系统结构示意图

图 2 签名发送短消息过程示意图

图 3 签名验证/短消息分类过程示意图

图 4 用户软件程序示意图

具体实施方式

本发明的核心是使用基于标识的密码技术,对信息发送、信息代理、信息接受实现基于一定规则的签名和验签，从而能够对信息实现明确有效的分类确认。由于使用了基于标识的密码技术，免去了签名、验签的证书验证过程，免去了传统 PKI 技术所需要的巨大花费和复杂管理，从而能够支持海量用户，而且简单、易用、准确、高效，便于大面积推广。下面以短消息为例，叙述具体的实施方式：

图 1 为发明系统结构示意图，本文中的用户，既可以是发件人，也可以是收件人，还可以是代理方，包括个人、公司、团体、ISP，还包括短信中心、汇聚网关等，同时用户包括防病毒软件供应商（比如瑞星、诺盾等）。

本发明的方法包括：

1）用户申请服务过程

A. 用户认证。系统支持两类用户，即有两种不同的认证方式：

- 个人用户：个人将签名从自己拥有的短消息地址发送的短消息。该类用户使用短消息地址作为基本部分标识，短消息地址包括手机号或 MSN 地址或 QQ 号等。该类用户的申请先要进行用户的认证，以确定其对声明短消息地址的拥有权，可以是任何认证方法，只要能确认该用户拥有该短消息地址（比如，可以采用“一种基于标识的密码技术的公共网络安全通信服务用户身份的认证方法”（专利号 200510077335.4）进行认证）。
- 签名代理用户：该类用户可签名其他委托人发送的短消息。该类用户可以使用约定的字符串如公司名，服务器名，IP 地址等作为基本部分标识（不局限于某个短消息

地址)。该类用户可以使用更强的认证方式：如书面合同，电子合同等。

B. 当用户通过用户认证后，确定完整的用户标识。完整的用户标识包括至少三个部分：系统标识（该标识可以唯一确定密码中心的系统参数)，在认证步骤 A 中使用的基本标识和服务有效期限。服务有效期至少包括服务的到期时间，一般还包括开始时间。完整用户标识还可包括其他信息，如国家名，城市名，公司名，部门名，姓名，身份证号码等信息。

C. 生成对应用户完整的用户标识的私钥。生成私钥方法决定于具体的标识签名算法,如可用现有技术 1 所述的算法及方法。

D. 用户获取并安装私钥。私钥的获取和认证的方法有关。如果采用“一种基于标识的密码技术的公共网络安全通信服务用户身份的认证方法”中的认证方法，则私钥由用户在认证时设置的保护口令加密后，用户从密码中心的网站上下载并安装。如果采用人工验证，则私钥可以使用 USB 钥匙等物理介质人工安全传递。用户的私钥文件包含私钥对应的完整的用户标识。

E. 用户获取并安装客户软件。客户软件可以从密码中心的网站公开下载。客户软件参见图 4，至少包括短消息签名功能。

2）签名发送短消息过程，参见图 2

A. 确定签名内容。用户可以签名整封短消息，也可以签名短消息的某些部分：如基本短消息头加短消息的前 12 字节。

B. 使用安装的私钥和客户软件中的签名算法生成签名。系统不局限于某种标识签名算法,如可用现有技术 1 所述的算法及方法。

C. 组装带签名的短消息。短消息中至少需要添加两条信息：

1)用户的完整的用户标识（至少三个部分：系统标识，在认证步

骤使用的标识和服务有效期限）；2)签名信息（包括被签名内容确定方法，签名算法和签名结果）。将这些信息和短消息原文一起组装发送，可以有多种组装方式，比如以扩展的短消息头域方式发送.

3）签名验证/短消息分类过程，参见图 3

A. 对无签名的短消息，以正常过滤方式分类处理。对有签名短消息：

B. 获取签名用户的完整的用户标识和签名信息。

C. 验证标识是否在标识黑名单中。该黑名单主要是用于防止某些申请服务通过认证的用户，以带认证的方式发送垃圾短消息给其他用户。该黑名单的维护见操作：标识黑名单更新过程。

D. 验证服务有效期限，如果服务有效期到期，则不验证签名，而以未签名短消息方式对待该短消息，进入正常过滤方式分类处理。

E. 确定签名内容。

F. 验证签名。用户，包括个人用户和短消息服务提供商，收到短消息后，个人用户的客户软件或短消息服务器的服务扩展软件，判断是否是带签名的短消息。短消息服务商并不一定要申请私钥才能使用这个服务的部分功能。短消息服务商只需要下载安装短消息服务器验证签名扩展软件（这是公开可下载的）后，就可以验证短消息的基于标识的签名。由于采用基于标识的密码技术，无证书验证过程，从而加快签名验证过程，进而支持海量用户。

G. 如果验证签名成功，则以正常短消息对待，不进入过滤程序。如果签名验证失败，则记录日志。

4）标识黑名单的更新过程。维护标识黑名单主要是为了防止个别用户通过申请短消息认证及可靠分类传递服务来发送垃圾短消息。

A. 如果用户认为某封通过签名认证的短消息为垃圾短消息，则将举报该短消息（发送整封短消息到提供服务的密码中心指定位置来举报发件人）。

B. 密码中心验证被举报短消息的签名的真实性后，并按照规则决定是否将用户标识列入黑名单。

以下是本发明的一个具体实施例：

本发明的密码中心是采用基于标识的密码技术建立的，（1）要确定使用标识签名算法，如现有技术 1 中的 IBS-2 算法；（2）生成系统参数（包括主密钥）。示例见技术 1 中附录。

用户申请服务过程。首先，用户要向密码中心申请注册，个人用户一般以自己的短消息地址作为标识，其他用户可以以自己拥有的合法标识作为注册标识，比如 IP 地址、域名等，也可是短消息地址，密码中心可以采用任何注册认证方法，例如 CN1697379 公开的“一种基于标识的密码技术的公共网络安全通信服务用户身份的认证方法”，进行注册认证，只要能有效证明该标识为该用户所拥有即可。例如，MSN 用户李三、公司 abc.com(该用户没有自己的短信网关)、短信 ISP 用户 soohu.com（可代理签名）、手机用户张五、短信中心、汇聚网关分别到密码中心去申请注册，个人用户一般以自己的手机号、MSN 标识或 QQ 号等作为标识，其他用户可以以自己拥有的合法标识作为注册标识（比如 IP 地址、域名等，也可是手机号、MSN 标识等），李三以自己的 MSN 标识 myibe@hotmail.com作为标识，到基于标识技术的密码中心去申请注册，该密码中心确认该短消息地址为用户李三所拥有，该密码中心根据李三的标识生成李三的私钥，并将相关的软件下发给李三，李三安装相关的软件和私钥。同样的过程，同样的过程，ISP 用户 soohu.com 就以自己的域名www.soohu.com 作为标识到密码中心申请得到自己的私钥及相关软件，并完成软件及私钥的安装。手机用户可通过无线上网安装下载私钥、软件或通过人工服务申请安装，其他用户类推。

签名短消息的发送过程。用户李三以自己的 MSN 地址

myibe@hotmail.com.给个人手机用户张五1269898118发一个短信，为了让短信网关能确认这封信的确是合法用户李三发出的，李三对信进行数字签名。假定事先约定的签名内容是短信内容的前12字节，李三通过从密码中心得到安装的软件，先提取所要发送短消息的基本信头及前12字节作为要签名的内容（也可以约定其它签名内容），然后用自己的私钥对要签名内容进行签名，将数字签名和李三的标识（电子短消息地址）以及其他可能需要的信息（如服务有效期）以某种方式组合（比如以扩展短消息头的方式），再和短消息正文一起发送给张五。

短消息验签/分类过程。李三的短消息先到短信中心，短信中心由于已在密码中心注册，获得自己的私钥和具有签名验证功能的软件，短信中心收到李三的签名短消息后，首先提取组合在短消息里的标识和签名，根据该标识和系统公钥参数验证签名，如果验证成功则证明该短消息是李三发送的；如果不成功，说明不是李三发送的。如果被签名内容为整个短消息，则有效的签名保证了电子短消息原文内容是完整的，没有被篡改。短消息中心经过确认是有效用户李三发送的，短消息中心将该信息作为有效用户传递给汇聚中心，汇聚中心反馈直接下发给张五，而且可告诉张五这是李三发来的。由于采用基于标识的密码系统，任意两个注册用户之间可以迅速进行认证，不需要像传统PKI密码体系一样事先要交换证书，不需要维护庞大的证书管理系统。因为这一显著的特点，使得基于标识的短消息认证技术可以支持海量用户，而且在管理和运营流程上更方便，让所有想用的用户都能方便的使用。

由于该方法有效的解决了大用户量的短消息认证难题，再结合一定的规则，就可以有效的实现短消息的分类及分类传递，比如我们事先约定使用标识密码技术签名的用户，发送的短消息是有效短消息（除非是在黑名单上），因为数字签名技术能解决身份认证问题，再结合黑名单原则，就可以高效的区分非垃圾短消息，从而实现短消息的分类传递，解决防垃圾短消息软件的分类识别问题。

在以上所述的基于标识的密码技术的短消息认证及可靠分类传递方法的基础上，本发明给出了以下进一步的实施方案：

对有签名的短消息进行处理时，验证该用户的标识是否在标识黑名单中，如在黑名单中，则作为垃圾短消息处理；

对不带签名的短消息、超过服务有效期的短消息、签名有效性未通过验证的短消息，按照普通短消息进行短消息过滤处理；

本发明还可以包括标识黑名单的更新过程：用户认为某封通过签名认证的短消息为垃圾短消息，可将整封短消息发送到密码中心，举报该短消息；密码中心验证被举报短消息的签名的真实性后，按照公知的规则确定被举报短消息是否为垃圾短消息，并确定是否将其用户标识列入黑名单。

本发明所说的基于标识的密码技术及生成公钥、私钥的方法、算法等均可参见现有技术 1：ISO. Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms. ISO-14888-3，2006

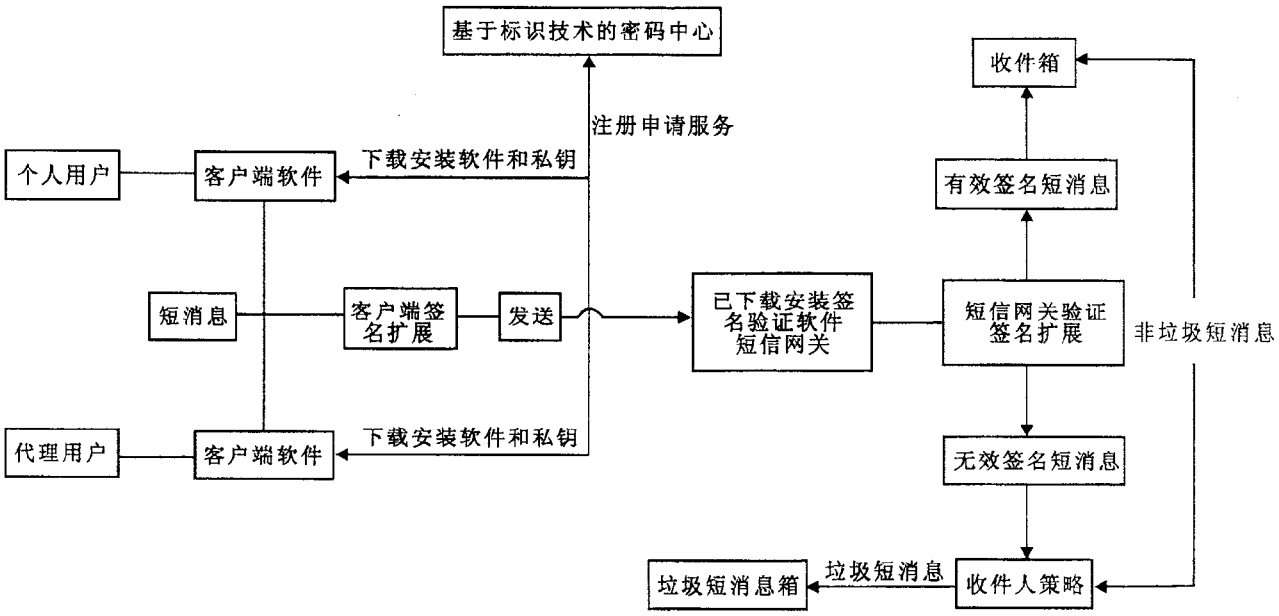

基于标识技术的密码中心
注册申请服务
收件箱
个人用户
客户端软件
下载安装软件和私钥
有效签名短消息
短消息
客户端签名扩展
发送
已下载安装签名验证软件短信网关
短信网关验证签名扩展
非垃圾短消息
代理用户
客户端软件
下载安装软件和私钥
无效签名短消息
垃圾短消息箱
垃圾短消息
收件人策略

图1

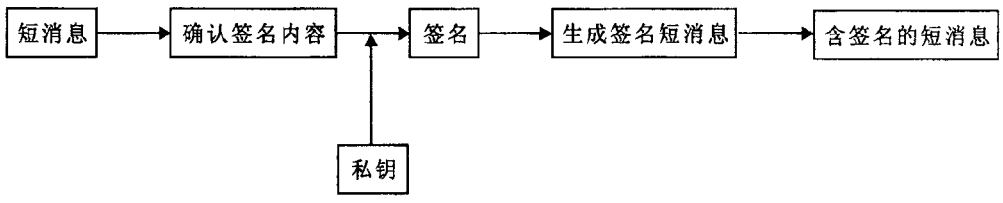

短消息
确认签名内容
签名
生成签名短消息
含签名的短消息
私钥

图2

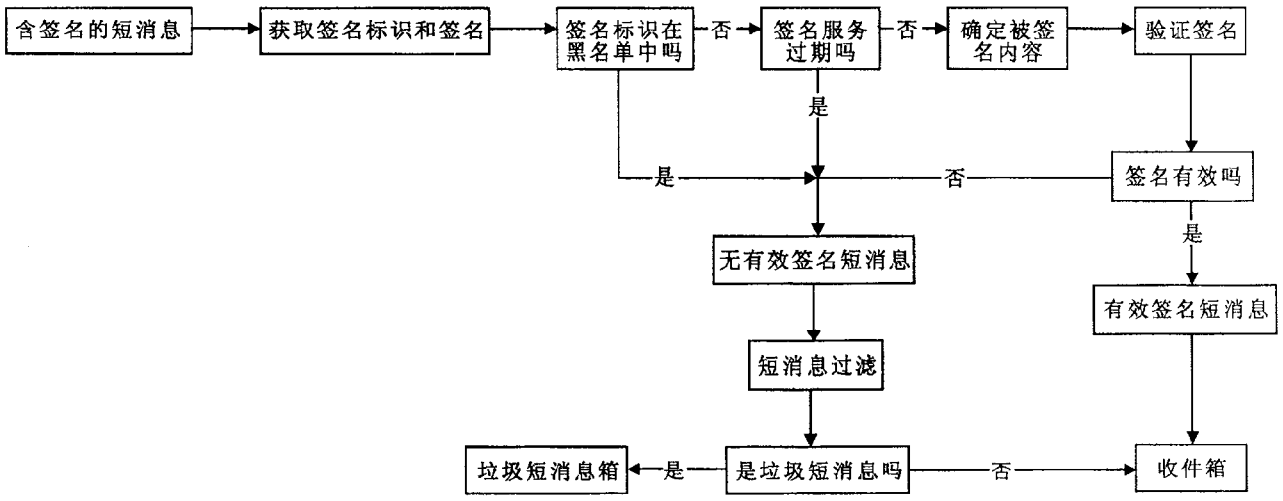

含签名的短消息
获取签名标识和签名
签名标识在黑名单中吗
否
签名服务过期吗
否
确定被签名内容
验证签名
是
是
否
签名有效吗
是
无有效签名短消息
有效签名短消息
短消息过滤
垃圾短消息箱
是
是垃圾短消息吗
否
收件箱

图3

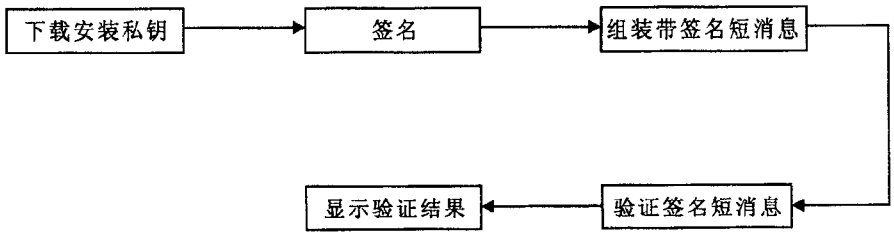

下载安装私钥
签名
组装带签名短消息
显示验证结果
验证签名短消息

图4