(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2008 年4 月24 日 (24.04.2008)

PCT

(10) 国际公布号
WO 2008/046246 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2006/002745

(22) 国际申请日: 2006 年10 月18 日 (18.10.2006)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人及
(72) 发明人: **黄金富(WONG, Kamfu)** [CN/CN]; 中国香港特别行政区沙田径口路3号金富台, Hong Kong (CN)。

(74) 代理人: **中国专利代理（香港）有限公司(CHINA PATENT AGENT (H. K.) LTD.)**; 中国香港特别行政区湾仔港湾道23号鹰君中心22字楼, Hong Kong (CN)。

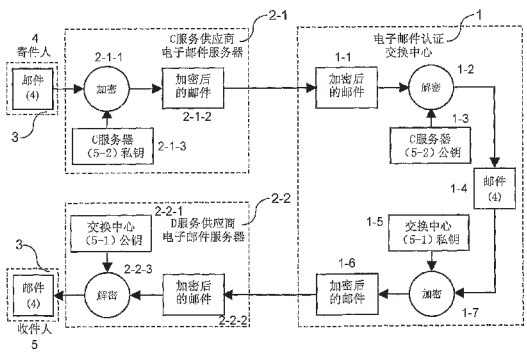
(81) 指定国（除另有指明，要求每一种可提供的国家保护）: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR),

[见续页]

(54) Title: SYSTEM AND METHOD FOR PREVENTING SPAM BY USING PAY-CHARGE-CONTRIBUTION AND AUTHENTICATION MEANS

(54) 发明名称: 用付费收费捐款和认证手段来防止垃圾电邮的系统和方法



1 E-MAIL AUTHENTICATION SWITCHING CENTER
1-1 ENCRYPTED E-MAIL
1-2 DECRYPTING
1-3 C-SERVER (5-2) PUBLIC KEY
1-4 E-MAIL(4)
1-5 SWITCHING CENTER (5-1) PRIVATE KEY
1-6 ENCRYPTED E-MAIL
1-7 ENCRYPTING
2-1 C-SERVICE PROVIDER E-MAIL SERVER
2-1-1 ENCRYPTING
2-1-2 ENCRYPTED E-MAIL
2-1-3 C-SERVER (5-2) PRIVATE KEY
2-2 D-SERVICE PROVIDER E-MAIL SERVER
2-2-1 SWITCHING CENTER (5-1) PUBLIC KEY
2-2-2 ENCRYPTED E-MAIL
2-2-3 DECRYPTING
3 E-MAIL(4)
4 SENDER
5 RECEIVER

(57) Abstract: A system and method for preventing Spam by using pay-charge-contribution and authentication means, adopting a method of a sender pays a addressee for the sent E-mail, and authenticates the E-mail server by using digital certificate, encrypts the sent E-mail by private key of the server's own digital certificate, then decrypts the E-mail by public key of the digital certificate, thereby authenticating whether the sending server is right of not, and it could prevent the E-mail from the imitated identity.

(57) 摘要:

一种用付费收费捐款和认证手段来防止垃圾电邮的系统和方法,采用了由寄件人付费用给收件人以寄出电邮的方法,以及采用数字证书认证电邮服务器,将寄出的电邮以服务器自己的数字证书的私钥进行加密,由接收方以该数字证书的公钥将电邮进行解密,从而认证寄出电邮的服务器的真伪,可防止以假冒身分发出电邮。

WO 2008/046246 A1

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

用付费收费捐款和认证手段来防止垃圾电邮的系统和方法

【技术领域】

本发明涉及互联网通讯技术领域，特别是涉及互联网中电子邮件通讯技术的系统和方法。

【背景技术】

随着互联网的普及，越来越多人使用电子邮件，电子邮件在本发明中也简称为电邮或邮件，电子邮件已经成为人们主要的通讯方法之一，是现今一种不可缺少的通信工具，尤其是在商业上的应用，由于电子邮件差不多取代了以前由使用传真机传送资料的方法，由于电子邮件的传送速度快，通信成本比传真低，无论传到世界上任何地方的电邮服务器，都不用付长途通话费用。由于现时发电子邮件是不用付费用的，所以有些人利用这漏洞，从各种不同渠道大量收集别人的电子邮件地址，然后将一些商业广告、个人广告甚至成人信息，在未经用户同意就强行发送到这些电子邮件地址。收件人收到这些电子邮件，看到是一些不认识的人寄给自己的电子邮件，内容一般都是一些没有用的广告信息，是所谓的垃圾邮件，所以一般用户都会将这些垃圾邮件删除不看，但由于垃圾邮件的数量越来越多，甚至比正常有用的电子邮件还要多，有些还会带有电脑病毒，打开这些垃圾邮件可能令用户的电脑感染电脑病毒。

垃圾邮件带来的主要影响是生产力的损失，当每天都收到大量的垃圾邮件时，用户要花不少时间去删除垃圾邮件，而且垃圾邮件还会浪费网路频宽和服务器储存空间。此外，当用户删除这些垃圾邮件时，匆忙之间还可能将重要的邮件也一并删除，这样严重影响了人们正常的通信，如何防止垃圾电邮，减低垃圾电邮的影响，是一个极需解决的迫切问题。

【发明内容】

本发明的目的，在于提供一种可防止垃圾电邮的电子邮件系统和相应的方法。

本发明的目的是这样实现的，即，采用这样一种用付费收费捐款和认证手段来防止垃圾电邮的系统和方法，所述系统主要包括：

电子邮件认证交换中心（1）、电子邮件服务器（2）、用户终端（3）、电子邮件（4）、互联网络（6）；

或还包括数字证书（5），

其中，

电子邮件认证交换中心（1）是一电子邮件服务器加上相应的账户管理和认证程式，并储存有各电子邮件服务器（2）的数字证书（5-2）的公钥，及电子邮件认证交换中心（1）自己的数字证书（5-1）的私钥，负责将从寄件人的电子邮件服务器（2）传送来的加密邮件（4），以该寄件人的电子邮件服务器（2）的数字证书（5-2）的公钥进行解密，然后重新以电子邮件认证交换中心（1）本身的数字证书（5-1）的私钥对邮件（4）进行加密，然后将加密后邮件（4）传送给收件人的电子邮件服务器（2），

电子邮件服务器（2）是一电子邮件服务器加上数字证书，并储存有本身的数字证书（5-2）的私钥和电子邮件认证交换中心（1）的数字证书（5-1）的公钥，负责将从用户终端（3）传送来的邮件（4）使用电子邮件服务器（2）本身的数字证书（5-2）的私钥进行加密，然后将加密后邮件传送到电子邮件认证交换中心（1），以及将从电子邮件认证交换中心（1）传送来的加密邮件使用电子邮件认证交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后才将邮件（4）储存到用户的电子邮箱内，再由用户通过用户终端（3）查看该邮件（4），

用户终端（3）是用户用来接收和发送电子邮件（4）的终端，是可以上网连线到电子邮件服务器（2）的电脑、PDA 或手机等设备，用户终端（3）设有收发电子邮件的程式，用户使用用户终端（3）上网连线登入到电子邮件服务器（2），使用收发电子邮件的程式查阅或下载用户自己电子邮箱内的邮件（4），和通过电子邮件服务器（2）寄出邮件（4），

数字证书（5）是由认证中心所发出的 PKI 数字证书，PKI 数字证书包括一对互相匹配的密钥，即数字证书（5）的公钥和私钥。

以及，采用了由寄件人付费用给收件人才能发出电子邮件（4）的方法，采用如上所述系统，特别是，所述方法采用数字证书（5）认证电子邮件服务器（2）的步骤。

这样就实现了本发明。

本发明的优点是，可以有效防止垃圾电邮，而且由于发出电邮（4）者要付出费用给收件人，增加了发电邮（4）的成本，令滥发电子邮件（4）者要为所发出的电子邮件（4）付出相当的成本代价，就可大幅减少垃圾电邮。而一般人与人之间的电邮（4）通信，商业上公司与公司之间的电邮（4）通信，一般都是互有往来的，也就是会互相付

费用给对方，所付出的费用和所收取的费用两者相差不会很大，所以不会对使用正常的电子邮件（4）通信的人造成负担和影响。

【附图说明】

图 1 是本发明的电邮认证系统的结构说明图。

图 2 是使用本发明的系统和方法时，通过电子邮件服务器（2）和电子邮件认证交换中心（1）使用电子邮件（4）通信的说明图。

图 3 是使用本发明的系统和方法时，公司与公司之间使用电子邮件（4）通信的说明图。

图 4 是是使用本发明的系统和方法的另一实施例的说明图。

图 5 是本发明的系统使用了收费机制的实施例的步骤的说明图。

图 6 是本发明的系统使用了收费机制的实施例的结构示意图。

图 7 是本发明的增加了邮件收费查询网站（9）的实施例说明图。

图 8 是本发明应用在知名人士的收费电子邮件的实施例的步骤说明图。

图中的各附号表示相同或相应的系统，装置，或部件，其中，电子邮件认证交换中心（1），简称交换中心（1），电子邮件服务器（2）包括寄件服务器（2-1）和收件服务器（2-2），数字证书（5）包括交换中心（1）自己的数字证书（5-1）和电子邮件服务器（2）的数字证书（5-2）及某公司的数字证书（5-3），以及，用户终端（3），电子邮件（4），互联网络（6），支付网关（7），银行账户电脑系统（8），收费查询网站（9），银行卡中心（88），收费电子邮件服务器（22）。

【具体实施方式】

下面结合附图，对本发明作进一步详细说明。

参阅图 1，图 1 是本发明的用付费收费捐款和认证手段来防止垃圾电邮的系统和方法的结构说明图，说明系统的构成。

在发明内容中，已说明了本发明系统的基本构成，继续参阅图 1，交换中心（1）是电子邮件认证交换中心（1）的简称，交换中心（1）是一电子邮件服务器加上相应的账户管理和认证程式，并储存有各电子邮件服务器（2）的数字证书（5-2）的公钥，及交换中心（1）自己的数字证书（5-1）的私钥，交换中心（1）将从电子邮件服务器（2）寄来的已加密邮件，以该电子邮件服务器（2）对应的数字证书（5-2）的公钥将邮件解

密，解密成功后将邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到该邮件（4）的收件人的电子邮件服务器（2）。

电子邮件服务器（2）是一电子邮件服务器加上相应的处理加密和解密程式，并储存有本身的数字证书（5-2）的私钥和交换中心（1）的数字证书（5-1）的公钥，当用户将要寄出的电子邮件（4）传送到电子邮件服务器（2）时，电子邮件服务器（2）将用户所传送来的邮件（4）使用本身的数字证书（5-2）的私钥进行加密，然后传送到交换中心（1）；以及当有邮件从交换中心（1）传送来时，电子邮件服务器（2）使用交换中心（1）的数字证书（5-1）的公钥将邮件解密，解密成功后才将该解密后的邮件（4）储存到该邮件（4）的收件人的电子邮箱，等待收件人上网查阅该邮件（4），

用户终端（3）是可以上网的电脑、PDA 或手机等设备，并设有收发电子邮件的程式，用户使用用户终端（3）上网连线登入到电子邮件服务器（2），使用收发电子邮件的程式查阅或下载用户自己电子邮箱内的邮件（4），和通过电子邮件服务器（2）寄出邮件（4），

电子邮件（4）是指通过电子通讯系统进行发送和接收的信件即邮件（4），包括通过互联网（6）传送的邮件（4），或通过其他通讯网络传送的邮件（4），都是属于本发明的保护范围，为了方便说明，在本说明书内即使只写电邮（4）或邮件（4），也表示是电子邮件（4）。

互联网络（6）是 Internet 互联网络、区域网络、电脑网络等的通讯网络，在本发明中用于传送电子邮件（4）。

数字证书（5）包括交换中心（1）的数字证书（5-1）和电子邮件服务器（2）的数字证书（5-2），数字证书（5）采用 PKI 技术(Public Key Infrastructure-公钥基础设施)的公钥和私钥对邮件进行加密和解密，PKI 技术是现有的技术，以发出信息者以数字证书（5）的私钥对信息进行加密，加密后的信息只能使用该数字证书（5）的公钥才能将信息进行解密，这就可以保证信息的真实性和完整性，同时也确认了信息发出方的身份。

本发明的一个主要特征是交换中心(1)利用电子邮件服务器(2)的数字证书(5-2)，来认证所接收到的邮件是从该电子邮件服务器（2）所发出的，以及电子邮件服务器（2）利用交换中心（1）的数字证书（5-1），来认证所接收到的邮件是从交换中心（1）所发出的。

其中，系统的设置方法是：

首先，设置一个交换中心（1），和多个电子邮件服务器（2），可以在一些现有的电子邮件服务器加上相应的处理加密和解密程式，就成为本发明的电子邮件服务器（2），交换中心（1）要向有关数字证书认证中心申请一份数字证书（5-1），而各电子邮件服务器（2）也要各自向有关数字证书认证中心申请一份数字证书（5-2），并且各电子邮件服务器（2）要将自己的数字证书（5-2）的公钥和电子邮件服务器（2）的网域名称等资料，预先在交换中心（1）登记储存，交换中心（1）同时设立一个发垃圾电邮的电子邮件服务器的黑名单，交换中心不会处理黑名单上所列出的电子邮件服务器（2）的邮件（4）。

当用户通过电子邮件服务器（2）发出电邮（4）时，电子邮件服务器（2）就会将用户的电邮（4）以电子邮件服务器（2）本身的数字证书（5-2）的私钥进行加密，然后将加密后的邮件传到交换中心（1），交换中心（1）将该加密邮件以该电子邮件服务器（2）的数字证书（5-2）的公钥对邮件进行解密，解密成功后就可确定该加密邮件是从电子邮件服务器（2）所发出的，并查核该电子邮件服务器（2）并非垃圾电子邮件服务器的黑名单上的服务器，查核无误后，交换中心（1）就将该邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后将加密后的邮件传送到收件人的电子邮件服务器（2），收件人的电子邮件服务器（2）将收到的邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所传送来的，就将该解密后的邮件（4）存到收件人的电子邮箱内。

当交换中心（1）收到没有使用数字证书（5-2）加密的邮件，或收到垃圾电子邮件服务器的黑名单上的服务器所发出的邮件，就会立即将该邮件弃置，也就是说交换中心（1）只会处理从已登记了电子证书的电子邮件服务器（2）所发出的邮件（4），而且在黑名单上并没有该电子邮件服务器（2）的名字，当有服务器被人投诉发出大量垃圾电邮时，如果交换中心（1）调查后发现投诉属实，就会取消该被投诉的电子邮件服务器（2）的账户，并将该服务器的名字等资料写到黑名单上，以后该电子邮件服务器（2）就不能通过交换中心（1）传送邮件（4）。

至于电子邮件服务器（2）方面，当电子邮件服务器（2）收到不是从交换中心（1）传送来的邮件，即没有使用交换中心（1）的数字证书（5-1）加密的邮件，电子邮件服

务器（2）会立即将该邮件存放到用户的另一个电子邮箱，即杂件邮箱，这杂件邮箱内所储存的邮件可能包含有大量垃圾电邮，用户可选择是否查阅这些电邮。

当大部份或所有的电子邮件服务器（2）都在交换中心（1）登记，并且使用数字证书（5）认证身份，所有正常的电子邮件（4）都会通过交换中心（1）传送到收件人的电子邮件服务器（2）内的收件人电子邮箱，而垃圾电邮是不能通过交换中心（1）传送，只能直接传送到收件人的电子邮件服务器（2）内收件人的杂件邮箱，由于正常的电子邮件（4）都会储存在收件人的电子邮箱，收件人也就无需花时间去查阅包含有大量垃圾电邮的杂件邮箱。再进一步，电子邮件服务器（2）可以将用户的杂件邮箱取消，所有不是从交换中心（1）传来的邮件都会直接弃置，可大量节省储存空间。

这就实现了本发明的目的。

参阅图 2，图 2 是使用本发明的系统和方法时，电子邮件服务器（2）通过交换中心（1）传送电子邮件的步骤的说明图，图中示出的是以寄件人向收件人发电子邮件（4）为例，进行说明，其中寄件人是通过 C 服务供应商（即 ISP）的电子邮件服务器（2）收发邮件（4），而收件人是通过 D 服务供应商的电子邮件服务器（2）收发邮件（4），为了方便说明，在本说明书中，用于将寄件人发出邮件（4）所使用的电子邮件服务器（2），即 C 服务供应商（即 ISP）的电子邮件服务器（2）简称为寄件服务器（2-1），而用于为收件人接收邮件（4）的电子邮件服务器（2），即 D 服务供应商（即 ISP）的电子邮件服务器（2）简称为收件服务器（2-2）。图 2 示出的实施例包括如下 A 组步骤：

A1. 当寄件人要向收件人发送电子邮件（4）时，电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1）；

A2. 寄件服务器（2-1）以自己的数字证书（5-2）的私钥将该电子邮（4）件进行加密，然后将加密后的邮件传送到交换中心（1）；

A3. 交换中心（1）将收到的加密邮件以寄件服务器（2-1）的数字证书（5-2）的公钥进行解密，解密成功后就可确定该邮件是从寄件服务器（2-1）所发出的，就立即将该邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到收件服务器（2-2）；

A4. 收件服务器（2-2）将收到的加密邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所发出的，就

立即将该解密后的邮件（4）储存在收件人的电子邮箱内，等待收件人上网查阅该邮件（4）。

参阅图 3，图 3 是使用本发明的系统和方法时，公司与公司之间使用电子邮件（4）通信的步骤的说明图，图中示出的是以某 A 公司的寄件人向某 B 公司的收件人发电子邮件（4）为例，进行说明，某 A 公司要按系统预定程序，预先申请一份某 A 公司的数字证书（5-3），并将该数字证书（5-3）的公钥在交换中心（1）登记储存，及将数字证书（5-3）的私钥储存在寄件服务器（2-1）内，类似地，B 公司也要预先申请一份 B 公司的数字证书（5-3），并将该数字证书（5-3）的公钥在交换中心（1）登记储存，及将数字证书（5-3）的私钥储存在收件服务器（2-2）内。图 3 示出的实施例包括如下 B 组步骤：

B1. 当 A 公司的寄件人要向 B 公司的收件人发送电子邮件（4）时，电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1）；

B2. 寄件服务器（2-1）以 A 公司的数字证书（5-3）的私钥将该电子邮件（4）进行加密，然后将加密后的邮件传送到交换中心（1）；

B3. 交换中心（1）将收到的加密邮件以 A 公司的数字证书（5-3）的公钥进行解密，解密成功后就可确定该邮件是从 A 公司所发出的，就立即将该邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到收件服务器（2-2）；

B4. 收件服务器（2-2）将收到的加密邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所发出的，就立即将该解密后的邮件（4）储存在 B 公司的收件人的电子邮箱内，等待收件人上网查阅该邮件（4）。

在本实施例里，使用了 A 公司的数字证书（5-3）来代替寄件服务器（2-1）的数字证书（5-2），也就是说如果当 A 公司向外发出大量的垃圾电邮，交换中心（1）就可以将 A 公司的名字加到黑名单内，以后 A 公司都不能通过交换中心（1）传送电邮（4），这样即使有人采用开设空壳公司然后申请公司的数字证书（5-3）的方法来发垃圾电邮，交换中心（1）可以使用行政手段，就可杜绝这些行为，例如申请这些公司的数字证书（5-3）或在交换中心（1）登记时，要交一定的手续费用或保证金，如果被发现发出大量垃圾电邮，就可立即将这些公司列入黑名单并没收保证金，加重了发垃圾电邮的成本，就可减少垃圾电邮的出现。

参阅图 4，图 4 是使用本发明的系统和方法的另一实施例，本实施例是图 3 实施例的简化版本，本实施例里没有交换中心（1），认证的工作由各公司的电子邮件服务器（2）互相直接认证，每一公司的电子邮件服务器（2）要预先登记与该公司有电子邮件（4）往来的其他公司的电子邮件服务器（2）的名字，并储存这些公司的电子邮件服务器（2）的数字证书（5-3）的公钥，当公司的电子邮件服务器（2）收到由这些已登记的电子邮件服务器（2）发来的电子邮件时，就会将该邮件以发出邮件的电子邮件服务器（2）的数字证书（5-3）的公钥进行解密，解密成功后就可确定该邮件是从已登记的电子邮件服务器（2）所发出的，就立即将解密后的邮件（4）储存到收件人的电子邮箱，而从其他电邮服务器传来的电邮就会储存在收件人的杂件邮箱，由于将邮件分类存放，公司的职员查看电邮时，就可先看电子邮箱里的电邮（4），这些通常是一些比较重要的电邮（4），有时间才看杂件邮箱的电邮，这样就可以减少发生用户在删除垃圾邮件时，匆忙之间将重要的邮件（4）也一并删除的事件。图 4 示出的实施例包括如下 C 组步骤：

C1. 当 A 公司的寄件人要向 B 公司的收件人发送电子邮件（4）时，电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1）；

C2. 寄件服务器（2-1）以 A 公司的数字证书（5-3）的私钥将该电子邮件（4）进行加密，然后将加密后的邮件传送到收件服务器（2-2）；

C3. 收件服务器（2-2）将收到的加密邮件以 A 公司的数字证书（5-3）的公钥进行解密，解密成功后就可确定该邮件是从 A 公司的寄件服务器（2-1）所发出的，就立即将该解密后的邮件（4）储存在 B 公司的收件人的电子邮箱内，等待收件人上网查阅该邮件（4）。

本发明更进一步的改进，是加入收费机制，由发件人付钱给收件人，即在图 3 的实施例中增加步骤 B5，发件人每发一封电邮（4）都要向收件人支付一指定金额费用，这些费用由交换中心（1）于每月的结算日向寄件服务器（2-1）的公司收取，扣除手续费后将钱存到收件服务器（2-2）的公司的银行账户内，然后由寄件服务器（2-1）的公司向寄件人收回有关的费用，以及由收件服务器（2-2）的公司将有关费用返还给收件人。

首先交换中心（1）登记各电子邮件服务器（2）的银行账户号码，各电子邮件服务器（2）同时要与交换中心（1）签订合约，双方同意按邮件（4）数量计费，电子邮件服务器（2）通过交换中心（1）寄到其他电子邮件服务器（2）的每一封邮件（4），都

要支付指定金额费用，由寄件人的电子邮件服务器（2）即寄件服务器（2-1）支付给收件人的电子邮件服务器（2）即收件服务器（2-2），这些收发邮件（4）的费用，可以即时结算，即在发邮件（4）时立即从寄件服务器（2-1）的银行账户转钱到收件服务器（2-2）的银行账户内，也可以定期结算，例如每日、或每星期、或每月等结算一次，在结算时才计算出各电子邮件服务器（2）的应付费用及应收款项，然后是由交换中心（1）通过支付网关（7）从电子邮件服务器（2）的银行账户内转账支付或存入款项，交换中心（1）可从这些收发邮件（4）的费用中收取一定比例或定额的手续费用。一般的电子邮件（4）通信，通常都是互有往来的，也就是互相会付费用给对方，所付出的费用和所收取的费用两者相差不会很大，所以大多数情况下用户不会付出很多费用。

参阅图 5，图 5 是本发明的系统使用了收费机制的实施例的步骤的说明图，包括如下 D 组步骤：

D1. 当寄件人要向收件人发送电子邮件（4）时，电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1）；

D2. 寄件服务器（2-1）以自己的数字证书（5-2）的私钥将该电子邮件（4）进行加密，然后将加密后的邮件传送到交换中心（1），并且在该寄件人账户记录内，记下该笔发邮件的账项；

D3. 交换中心（1）将收到的加密邮件以寄件服务器（2-1）的数字证书（5-2）的公钥进行解密，解密成功后就可确定该邮件是从寄件服务器（2-1）所发出的，就立即在该寄件服务器（2-1）的账户记录内记下该笔发邮件的支出账项，并将该解密后的邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到收件服务器（2-2），同时在该收件服务器（2-2）的账户记录内记下该笔收邮件的收入账项；

D4. 收件服务器（2-2）将收到的加密邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所发出的，就立即将该解密后的邮件（4）储存在收件人的电子邮箱内，等待收件人上网查阅该邮件（4），并且在该收件人账户记录内，记下该笔收邮件的收入账项；

D5. 到结算时，交换中心（1）以各电子邮件服务器（2）的账户记录，扣除手续费用后计算出该电子邮件服务器（2）的应付费用或应收款项，然后通过支付网关（7）及银行账户电脑系统（8），在该电子邮件服务器（2）的银行账户内

转账收款或存入款项，再由各电子邮件服务器（2）即寄件服务器（2-1）和收件服务器（2-2），向其用户收回款项或将款项返还给用户。

参阅图 6，图 6 是本发明的系统使用了收费机制的实施例的结构示意图，图中示出的是在不同地区各自设置定一个交换中心（1），为了方便说明，图中只示出了其中两个地区即甲地和乙地的交换中心（1），每一交换中心（1）负责处理当地的电子邮件服务器（2）的电子邮件（4）交换和收费结算等工作，当有电子邮件（4）从甲地传送到乙地时，邮件（4）会通过寄件人的寄件服务器（2-1）、甲地的交换中心（1），乙地的交换中心（1）才传送到收件服务器（2-2）的收件人电子邮箱。到结算时，双方的交换中心（1）才按邮件（4）的收发量进行结算，然后通过支付网关（7）和银行账户电脑系统（8）进行转账。只要在世界各地都设置了交换中心（1），所有正常邮件（4）都会通过交换中心（1）才传送到收件人的电子邮箱，这样一般用户只要使用已在交换中心（1）登记的电子邮件服务器（2）收发电邮（4），就不会再受垃圾邮件的困扰，而垃圾邮件一般都是单向由垃圾邮件制造者寄给收件人，如果垃圾邮件通过交换中心（1）传送，就要要付出相当大的费用，令发垃圾邮件者无法负担，如果将垃圾邮件通过其他的服务器发出，则这些邮件可能会被收件人的电子邮件服务器（2）弃置，或者将邮件存入收件人的杂件邮箱，由于正常的邮件（4）已经存到收件人的电子邮箱，很少收件人会查看杂件邮箱，令发垃圾电邮的人无法将垃圾电邮的内容信息传达给收件人，这样以后就很少人会发垃圾电邮。利用向发电子邮件（4）者收费的方法，是最有效的防止垃圾电邮的方法，更进一步，交换中心（1）可以将所有从发件者收取的费用，扣除成本后全部捐至慈善机构，例如捐给无国界医生组织、奥比斯眼科医院等慈善志愿机构，帮助有需要的人，相信大部份的电邮用户都不会反对，这有助推广本发明的系统和方法的实施。

各地政府也可以通过交换中心（1）对发电邮者征收税项，可增加政府的收入，由于征税的对像是发电邮者，不会加重市民的负担，不会影响当地的经济，是增加政府收入的一个好方法。

参阅图 7，图 7 是本发明的增加了邮件收费查询网站（9）的实施例说明图，本实施例采用的是在定额收费上加入自定捐款收费额机制，自定捐款收费额是由电子邮件地址的拥有者自己设定捐款收费水平，本实施例和图 6 的实施例的结构相比，增加了邮件收费查询网站（9），其中，所述邮件收费查询网站（9）用于提供有关世界各地的各个

电子邮件服务器（2）的电邮地址的捐款收费金额资料，只要上网到邮件收费查询网站（9）输入所要查询的电子邮件地址，就可找到有关该电子邮件地址的自定捐款收费金额。各个电子邮件服务器（2）要将其电邮用户划分为两类，其中一类为普通电邮用户，只需支付定额费用就可成功将邮件（4）寄到这些电邮用户的电子邮箱，另一类为自定捐款收费电邮用户，将邮件（4）寄到这类电邮用户的电子邮箱时，除了要收取定额费用外，还要支付该电邮用户所设定的自定捐款收费金额的费用，电子邮件服务器（2）还会将这类自定捐款收费电邮用户的电子邮件地址和捐款收费金额等资料预先储存到邮件收费查询网站（9），电子邮件地址的拥有者可以随时通过发电邮（4）到邮件收费查询网站（9）更改自定捐款收费金额，只要以自己的电邮账户通过寄件服务器（2-1）寄一个电邮（4）到邮件收费查询网站（9），该电邮的内容就是新的自定捐款收费金额，就可以变更自定捐款收费金额，有些电邮用户希望少接收一些电邮（4），可以设定一个较高的自定捐款收费金额，例如某公司的董事长将他的电子邮件地址的自定捐款收费金额设定为 100 美元，这样只有肯捐款 100 美元的人才可成功将电邮（4）传送到该董事长的电子邮箱内。图 7 示出的实施例包括如下 E 组步骤：

E1. 当寄件人要寄电子邮件（4）给收件人前，可上网到邮件收费查询网站（9），输入收件人的电邮地址，就可找到该收件人的电邮地址的自定捐款收费金额；

E2. 如寄件人同意该自定捐款收费金额，就将电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1）；

E3. 寄件服务器（2-1）以自己的数字证书（5-2）的私钥将该电子邮件（4）进行加密，然后将加密后的邮件传送到交换中心（1），并且在该寄件人账户记录内，记下该笔发邮件的账项；

E4. 交换中心（1）将收到加密邮件，以寄件服务器（2-1）的数字证书（5-2）的公钥进行解密，解密成功后就可确定该邮件是从寄件服务器（2-1）所发出的，就立即在该寄件服务器（2-1）的账户记录内记下该笔发邮件的支出账项，并将该解密后的邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到收件服务器（2-2），同时在该收件服务器（2-2）的账户记录内记下该笔收邮件的收入账项；

E5. 收件服务器（2-2）将收到的加密邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所发出的，就

立即在该收件人账户记录内，记下该笔收邮件的收入账项，并且收件服务器（2-2）会核对收件人的电邮地址是普通电邮用户或是自定捐款收费电邮用户，如果该收件人是普通电邮用户，就立即将该解密后的邮件（4）储存在收件人的电子邮箱内，等待收件人上网查阅该邮件（4），并转到步骤 E15；如果该收件人是自定捐款收费电邮用户，立即将邮件（4）暂时储存，并转到步骤 E6；

E6. 收件服务器（2-2）向交换中心（1）发出请求支付自定捐款金额费用信息，信息内容包括该邮件（4）的寄件人电子邮件地址、收件人电子邮件地址、标题及寄件日期和时间等资料；

E7. 交换中心（1）收到请求支付自定捐款金额费用信息后，从信息内容找到收件人电子邮件地址，立即向邮件收费查询网站（9）查询该电子邮件地址的捐款收费金额；

E8. 邮件收费查询网站（9）从所储存的记录内，找出该电子邮件地址的捐款收费金额资料，并立即将捐款收费金额资料传送到交换中心（1）；

E9. 交换中心（1）立即将捐款收费金额资料暂时储存起来，并回复一个以交换中心（1）本身的数字证书（5-1）的私钥加密的邮件给寄件人，邮件内容是通知寄件人有关的捐款收费金额及一个捐款参考号码，请他在指定期限内（例如一星期内）上网到交换中心（1）的网站，通过网上付款缴交有关的捐款收费，所述捐款参考号码是用来在接收捐款时分辨不同的电邮（4）的一个编号；

E10. 寄件人的电子邮件服务器（2）将回复给寄件人的邮件，以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件（4）是从交换中心（1）所发出的，从内容知道是一个请用户支付捐款费用的邮件，就将该回复邮件储存到寄件人的电子邮箱内；

E11. 寄件人上网查看自己的电子邮箱，看到有关的回复邮件的内容，同意捐款就在指定时间内上网到交换中心（1）的网站，输入寄件人自己的电邮地址和付款参考号码，就可在交换中心（1）的网站内找出之前在步骤 E2 传送到寄件服务器（2-1）的邮件（4）的收件人电邮地址，核对无误后寄件人在交换中心（1）的付款网页内输入自己的付款资料，包括信用卡卡号、信用卡有效期等网上付款所必需的资料，或借记卡卡号、密码等网上付款所必需的资料；

E12. 交换中心（1）将付款资料和金额通过支付网关（7）传送到银行账户电脑系统（8），请求转账付款；

E13. 银行账户电脑系统（8）核对付款资料和账户结余等资料无误后，从寄件人的所输入的付款资料的账户内转钱到交换中心（1）的银行账户内，并通知交换中心（1）转账付款成功；

E14. 交换中心（1）将已收到转账付款成功信息传送到收件服务器（2-2），收件服务器（2-2）将在步骤 E5 中暂时储存的解密后邮件（4），储存在收件人的电子邮箱内，等待收件人上网查阅该邮件（4）；

E15. 到结算时，交换中心（1）以各电子邮件服务器（2）的账户有关定额收费的电邮收发记录，扣除手续费用后计算出该电子邮件服务器（2）的应付费用或应收款项，然后通过支付网关（7）及银行账户电脑系统（8），在各电子邮件服务器（2）的银行账户内转账收款或存入款项，再由各电子邮件服务器（2）即寄件服务器（2-1）和收件服务器（2-2），向其用户收回款项或将款项返还给用户，以及将在步骤 E13 中收到的捐款，扣除手续费后全部捐给当地的公益慈善机构。

本实施例中，交换中心（1）所收到的捐款，扣除手续费后全部捐给当地的公益慈善机构，同时邮件收费查询网站（9）会做一个收到最多捐款的电邮地址的排名榜的网页，只要上网到这网页就可以看到那一个电邮地址收到最多捐款，也就是最多人愿意捐钱寄电邮给他。本实施例的系统和方法，不但可以防止垃圾电邮，更可减少一些不重要的电邮，只要设定较高的自定捐款收费金额，就可保证所收到的都是一些重要的电邮（4），既可做善事，又可防止垃圾电邮，一举两得。

参阅图 8，图 8 示出的是本发明的另一实施例的步骤示意图，本例子与上述的例子不同的地方是，本例子没有交换中心（1）和没有邮件收费查询网站（9），而且只有一个电子邮件服务器，即收费电子邮件服务器（22），本实施适合一些跨国公司的高层人员，社会知名人士等的电子邮件账户，现时由于垃圾电邮的泛滥，大部份社会知名人士和商业机构的高级管理人员，都不敢公开自己的电子邮件地址，因为公开了就会每天收到大量的邮件，其中主要是垃圾邮件，而电子邮件（4）又是他们必需的通信工具之一，大量的垃圾邮件会严重影响他们的工作，所以他们都会将自己的电子邮件地址保密，一般都是内部使用，外面的人很难会知道他们的电子邮件地址。他们虽然都是社会上的知

名人士，但如果有人有要发邮件（4）给这些知名人士，是非常困难的，往往是无从入手，如果建一个收费电子邮件服务器（22）的网站，每位知名人士分配一个电子邮箱和电邮地址，而且将这些电邮地址全部公开，谁要发邮件（4）给这些知名人士，首先要上网到收费电子邮件服务器（22）的网站支付一定金额的费用，例如 1,000 元，才能将电邮（4）发送到知名人士的邮箱，收费电子邮件服务器（22）所收到的钱扣除成本开支后，全部捐给慈善机构，由于发件人是捐了钱才能发电邮（4）到知名人士的邮箱，一般知名人士都会对这些做善事的人予以善意的回应，会细心阅读邮件（4）内容，这样对社会和知名人士都有好处。图 8 示出的实施例包括如下 F 组步骤：

F1. 当寄件人要向知名人士发送电子邮件（4）前，寄件人首先上网到收费电子邮件服务器（22）的网站开设寄件人账户，并且在网站购买积分，寄件人在网站输入自己的信用卡卡号等付款资料和要购买的积分的金额，例如每 1 元代表 1 分，寄件人要买 1,000 分就要付出 1,000 元；

F2. 收费电子邮件服务器（22）将收寄件人的付款资料包括信用卡卡号和金额等传送到银行卡中心（88），请求转账付款；

F3. 银行卡中心（88）核对付款资料和账户结余无误后，从寄件人的信用卡账户转钱到收费电子邮件服务器(22)的银行账户内，并通知收费电子邮件服务器(22)转账付款成功；

F4. 收费电子邮件服务器（22）通知寄件人申请账户成功，并且已经从他的信用卡账户内收取购买积分的款项；

F5. 寄件人在收费电子邮件服务器（22）的网站上查找出所选的知名人士的电邮地址，及发电邮（4）给该知名人士的授权码所需的费用（即积分），例如发给微软 Bill Gates 的授权码的费用为 500 分，于是使用刚才所购买的积分，在网站内购买这授权码；

F6. 收费电子邮件服务器（22）核对寄件人的积分账户结余无误后，从寄件人的账户扣取该授权码所需的费用（即积分），并且向该寄件人发出一个随机产生的授权码，这授权码编号是唯一的，而且是一次过使用的，请寄件人在指定期限（例如一星期）内，将这授权码放到电邮（4）的标题内，然后将电邮（4）寄给所选的知名人士 Bill Gates 在收费电子邮件服务器（22）的电邮地址；

F7. 寄件人在指定期限内，以授权码为电邮（4）的标题写一个电邮（4），寄给所选的知名人士 Bill Gates 在收费电子邮件服务器（22）的电邮地址，收费电子邮件服务器（22）收到邮件（4）后，将邮件（4）的标题内的授权码与步骤 F6 中所发出的授权码相核对，核对无误后，将该邮件（4）储存到该知名人士 Bill Gates 的电子邮箱内，并将该授权码的记录删除，如果收费电子邮件服务器（22）收到的电邮的标题内没有对应该收件人的有效授权码，收费电子邮件服务器（22）会将邮件弃置，并发电邮回复寄件人，通知他要购买有关的授权码后才能成功发电邮（4）的详细资料；

F8. 知名人士 Bill Gates 上网登入收费电子邮件服务器（22）查看邮件（4）；

F9. 收费电子邮件服务器（22）将寄件人所寄给知名人士 Bill Gates 的邮件（4），传送给知名人士 Bill Gates 阅看。

本发明的实施，可彻底解决垃圾电邮泛滥的问题，减少因垃圾电邮而引起生产力的损失，本发明的一个主要特征就是所有电子邮件服务器（2）与交换中心（1）的邮件传送，都使用了 PKI 技术数字证书来认证，只要电子邮件服务器（2）通过认证，就等于该电子邮件服务器（2）的所有用户的邮件（4）都可通过认证，这比现时一般以用户个人为认证单位的方法更有效推广 PKI 数字证书技术，现时一般使用数字证书的用户，很多人都不完全明白有关数字证书的安装和使用步骤，经常会犯错，不能发挥数字证书应有的效用，使用本发明的方法，一般邮件（4）的认证工作由电子邮件服务器（2）处理，用户无需作任何设定，可以像平常一样操作来收发电邮（4），所以能有效地应用 PKI 数字证书技术，适合绝大部份的用户。对于要求数字签名和保密的用户，他们仍然可以由发件人将邮件（4）签名和加密，然后通过本发明的系统和方法，将邮件传送给收件人，再由收件人将邮件解密和核对数字签名，这样就更安全可靠。

权 利 要 求

1. 一种防止垃圾电子邮件的系统，所述系统包括电子邮件服务器（2）、用户终端（3）、电子邮件（4）、互联网络（6）；特别是，所述系统还包括数字证书（5），以及数字证书（5）包括用于对电子邮件（4）进行认证加密和认证解密的数字证书（5）的公钥和私钥。

2. 如权利要求 1 所述系统，其特征在于，所述系统还包括电子邮件认证交换中心（1）。

3. 如权利要求 2 所述系统，其中，

电子邮件认证交换中心（1）是一电子邮件服务器加上相应的账户管理和认证程式，并储存有各电子邮件服务器（2）的数字证书（5-2）的公钥，及电子邮件认证交换中心（1）自己的数字证书（5-1）的私钥，负责将从寄件人的电子邮件服务器（2）传送来的加密邮件，以该寄件人的电子邮件服务器（2）的数字证书（5-2）的公钥进行解密，然后重新以电子邮件认证交换中心（1）本身的数字证书（5-1）的私钥对邮件（4）进行加密，然后将加密后邮件（4）传送给收件人的电子邮件服务器（2），电子邮件服务器（2）是一电子邮件服务器加上数字证书，并储存有本身的数字证书（5-2）的私钥和电子邮件认证交换中心（1）的数字证书（5-1）的公钥，负责将从用户终端（3）传送来的邮件（4）使用电子邮件服务器（2）本身的数字证书（5-2）的私钥进行加密，然后将加密后邮件传送到电子邮件认证交换中心（1），以及将从电子邮件认证交换中心（1）传送来的加密邮件使用电子邮件认证交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后才将邮件（4）储存到用户的电子邮箱内，再由用户通过用户终端（3）查看该邮件（4），

用户终端（3）是用户用来接收和发送电子邮件（4）的终端，是可以上网连线到电子邮件服务器（2）的电脑、PDA 或手机等设备，用户终端（3）设有收发电子邮件的程式，用户使用用户终端（3）上网连线登入到电子邮件服务器（2），使用收发电子邮件的程式查阅或下载用户自己电子邮箱内的邮件（4），和通过电子邮件服务器（2）寄出邮件（4），

数字证书（5）是由认证中心所发出的PKI数字证书，PKI数字证书包括一对互相匹配的密钥，即数字证书（5）的公钥和私钥。

4. 一种防止垃圾电子邮件的方法，采用如权利要求1或2或3所述系统，以及，采用了用数字证书（5）对电子邮件（4）进行认证加密和认证解密的步骤。

5. 一种防止垃圾电子邮件的方法，采用如权利要求1或2或3所述系统，以及，采用了交换中心（1）利用电子邮件服务器（2）的数字证书（5-2），来认证所接收到的邮件是从该电子邮件服务器（2）所发出的，以及电子邮件服务器（2）利用交换中心（1）的数字证书（5-1），来认证所接收到的邮件是从交换中心（1）所发出的步骤。

6. 如权利要求4或5所述方法，所述方法采用如下步骤，

首先，设置一个交换中心（1），和多个电子邮件服务器（2），可以在一些现有的电子邮件服务器加上相应的处理加密和解密程式，就成为本发明的电子邮件服务器（2），交换中心（1）要向有关数字证书认证中心申请一份数字证书（5-1），而各电子邮件服务器（2）也要各自向有关数字证书认证中心申请一份数字证书（5-2），并且各电子邮件服务器（2）要将自己的数字证书（5-2）的公钥和电子邮件服务器（2）的网域名称等资料，预先在交换中心（1）登记储存，交换中心（1）同时设立一个发垃圾电邮的电子邮件服务器的黑名单，交换中心不会处理黑名单上所列出的电子邮件服务器（2）的邮件（4）；

当用户通过电子邮件服务器（2）发出电邮（4）时，电子邮件服务器（2）就会将用户的电邮（4）以电子邮件服务器（2）本身的数字证书（5-2）的私钥进行加密，然后将加密后的邮件传到交换中心（1），交换中心（1）将该加密邮件以该电子邮件服务器（2）的数字证书（5-2）的公钥对邮件进行解密，解密成功后就可确定该加密邮件是从电子邮件服务器（2）所发出的，并查核该电子邮件服务器（2）并非垃圾电子邮件服务器的黑名单上的服务器，查核无误后，交换中心（1）就将该邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后将加密后的邮件传送到收件人的电子邮件服务器（2），收件人的电子邮件服务器（2）将收到的

邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所传送来的，就将该解密后的邮件（4）存到收件人的电子邮箱内；

当交换中心（1）收到没有使用数字证书（5-2）加密的邮件，或收到垃圾电子邮件服务器的黑名单上的服务器所发出的邮件，就会立即将该邮件弃置，也就是说交换中心（1）只会处理从已登记了电子证书的电子邮件服务器（2）所发出的邮件（4），而且在黑名单上并没有该电子邮件服务器（2）的名字，当有服务器被人投诉发出大量垃圾电邮时，如果交换中心（1）调查后发现投诉属实，就会取消该被投诉的电子邮件服务器（2）的账户，并将该服务器的名字等资料写到黑名单上，以后该电子邮件服务器（2）就不能通过交换中心（1）传送邮件（4）；

至于电子邮件服务器（2）方面，当电子邮件服务器（2）收到不是从交换中心（1）传送来的邮件，即没有使用交换中心（1）的数字证书（5-1）加密的邮件，电子邮件服务器（2）会立即将该邮件存放到用户的另一个电子邮箱，即杂件邮箱，这杂件邮箱内所储存的邮件可能包含有大量垃圾电邮，用户可选择是否查阅这些电邮。

7. 如权利要求 6 所述方法，寄件人利用其用户终端（3）通过某 C 服务供应商的电子邮件服务器（2）收发邮件（4），而收件人是利用其用户终端（3）通过 D 服务供应商的电子邮件服务器（2）收发邮件（4），其中，寄件人发出邮件（4）所使用的电子邮件服务器（2）即 C 服务供应商的电子邮件服务器（2）称为寄件服务器（2-1），用于为收件人接收邮件（4）的电子邮件服务器（2）即 D 服务供应商的电子邮件服务器（2）称为收件服务器（2-2），所述方法采用如下 A 组步骤：

A1. 当寄件人要向收件人发送电子邮件（4）时，电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1），

A2. 寄件服务器（2-1）以自己的数字证书（5-2）的私钥将该电子邮（4）件进行加密，然后将加密后的邮件传送到交换中心（1）

A3. 交换中心（1）将收到的加密邮件以寄件服务器（2-1）的数字证书（5-2）的公钥进行解密，解密成功后就可确定该邮件是从寄件服务器（2-1）所发出的，就立即将该邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到收件服务器（2-2），

A4. 收件服务器（2-2）将收到的加密邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所发出的，就立即将该解密后的邮件（4）储存在收件人的电子邮箱内，等待收件人上网查阅该邮件（4）。

8. 如权利要求 6 所述方法，所述方法特别适用于公司与公司之间使用电子邮件（4）通信，当某 A 公司的寄件人向某 B 公司的收件人发电子邮件（4）时，某 A 公司要按系统预定程序，预先申请一份某 A 公司的数字证书（5-3），并将该数字证书（5-3）的公钥在交换中心（1）登记储存，及将数字证书（5-3）的私钥储存在寄件服务器（2-1）内，类似地，B 公司也要预先申请一份 B 公司的数字证书（5-3），并将该数字证书（5-3）的公钥在交换中心（1）登记储存，及将数字证书（5-3）的私钥储存在收件服务器（2-2）内，以及采用如下 B 组步骤：

B1. 当 A 公司的寄件人要向 B 公司的收件人发送电子邮件（4）时，电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1），

B2. 寄件服务器（2-1）以 A 公司的数字证书（5-3）的私钥将该电子邮件（4）进行加密，然后将加密后的邮件传送到交换中心（1），

B3. 交换中心（1）将收到的加密邮件以 A 公司的数字证书（5-3）的公钥进行解密，解密成功后就可确定该邮件是从 A 公司所发出的，就立即将该邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到收件服务器（2-2），

B4. 收件服务器（2-2）将收到的加密邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所发出的，就立即将该解密后的邮件（4）储存在 B 公司的收件人的电子邮箱内，等待收件人上网查阅该邮件（4）。

9. 一种防止垃圾电子邮件的方法，采用如权利要求 1 所述系统，以及，采用了认证的工作由各公司的电子邮件服务器（2）互相直接认证的方法，每一公司的电子邮件服务器（2）要预先登记与该公司有电子邮件（4）往来的其他公司的电子邮件服务器（2）的名字，并储存这些公司的电子邮件服务器（2）的数字证书（5-3）的公钥，当公司的电子邮件服务器（2）收到由这些已登记的电子邮件服务器（2）发来的电

子邮件时，就会将该邮件以发出邮件的电子邮件服务器（2）的数字证书（5-3）的公钥进行解密，解密成功后就可确定该邮件是从已登记的电子邮件服务器（2）所发出的，就立即将解密后的邮件（4）储存到收件人的电子邮箱，而从其他电邮服务器传来的电邮就会储存在收件人的杂件邮箱，以及，包括采用如下 C 组步骤：

C1. 当 A 公司的寄件人要向 B 公司的收件人发送电子邮件（4）时，电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1），

C2. 寄件服务器（2-1）以 A 公司的数字证书（5-3）的私钥将该电子邮件（4）进行加密，然后将加密后的邮件传送到收件服务器（2-2），

C3. 收件服务器（2-2）将收到的加密邮件以 A 公司的数字证书（5-3）的公钥进行解密，解密成功后就可确定该邮件是从 A 公司的寄件服务器（2-1）所发出的，就立即将该解密后的邮件（4）储存在 B 公司的收件人的电子邮箱内，等待收件人上网查阅该邮件（4）。

10. 如权利要求 8 所述方法，其特征在于，增加了步骤 B5，即，发件人每发一封电邮（4）都要向收件人支付一指定金额费用，这些费用由交换中心（1）于每月的结算日向寄件服务器（2-1）的公司代收，扣除手续费后将钱存到收件服务器（2-2）的公司的银行账户内，然后由寄件服务器（2-1）的公司向寄件人收回有关费用，以及由收件服务器（2-2）的公司将有关费用返还给收件人。

11. 如权利要求 6 所述方法，所述方法还包括了设置支付网关（7）及利用银行账户电脑系统（8）收取费用的步骤，由交换中心（1）通过支付网关（7）从电子邮件服务器（2）的银行账户内转账支付或存入款项，交换中心（1）可从这些收发邮件（4）的费用中收取一定比例或定额的手续费用，以及，采用如下 D 组步骤：

D1. 当寄件人要向收件人发送电子邮件（4）时，电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1），

D2. 寄件服务器（2-1）以自己的数字证书（5-2）的私钥将该电子邮件（4）进行加密，然后将加密后的邮件传送到交换中心（1），并且在该寄件人账户记录内，记下该笔发邮件的账项，

D3. 交换中心（1）将收到的加密邮件以寄件服务器（2-1）的数字证书（5-2）的公钥进行解密，解密成功后就可确定该邮件是从寄件服务器（2-1）所发出的，就立即在该寄件服务器（2-1）的账户内记下该笔发邮件的支出账项，并将该解密后的邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到收件服务器（2-2），同时在该收件服务器（2-2）的账户内记下该笔收邮件的收入账项，

D4. 收件服务器（2-2）将收到的加密邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所发出的，就立即将该解密后的邮件（4）储存在收件人的电子邮箱内，等待收件人上网查阅该邮件（4），并且在该收件人账户记录内，记下该笔收邮件的收入账项，

D5. 到结算时，交换中心（1）以各电子邮件服务器（2）的账户记录，扣除手续费用后计算出该电子邮件服务器（2）的应付费用或应收款项，然后通过支付网关（7）及银行账户电脑系统（8），在该电子邮件服务器（2）的银行账户内转账收款或存入款项，再由各电子邮件服务器（2）向其用户收回款项或将款项返还给用户。

12. 如权利要求 6 所述方法，所述方法还包括了设置支付网关（7）及利用银行账户电脑系统（8）收取费用的步骤，以及，增设了邮件收费查询网站（9），所述邮件收费查询网站（9）用于提供有关世界各地的各个电子邮件服务器（2）的电邮地址的捐款收费金额资料，只要上网到邮件收费查询网站(9)输入所要查询的电子邮件地址，就可找到有关该电子邮件地址的自定捐款收费金额，各个电子邮件服务器（2）要将其电邮用户划分为两类，其中一类为普通电邮用户，只需支付定额费用就可成功将邮件（4）寄到这些电邮用户的电子邮箱，另一类为自定捐款收费电邮用户，将邮件（4）寄到这类电邮用户的电子邮箱时，除了要收取定额费用外，还要支付该电邮用户所设定的自定捐款收费金额的费用，电子邮件服务器（2）还会将这类自定捐款收费电邮用户的电子邮件地址和捐款收费金额等资料预先储存到邮件收费查询网站（9），电子邮件地址的拥有者可以随时通过发电邮（4）到邮件收费查询网站（9）更改自定捐款收费金额，只要以自己的电邮账户通过寄件服务器（2-1）寄一个电邮（4）到邮件收费查询网站（9），该电邮的内容就是新的自定捐款收费金额，就可

以变更自定捐款收费金额，有些电邮用户希望少接收一些电邮（4），可以设定一个较高的自定捐款收费金额，以及，包括采用如下E组步骤：

E1. 当寄件人要寄电子邮件（4）给收件人前，可上网到邮件收费查询网站（9），输入收件人的电邮地址，就可找到该收件人的电邮地址的自定捐款收费金额，

E2. 如寄件人同意该自定捐款收费金额，就将电子邮件（4）通过用户终端（3）传送到寄件服务器（2-1），

E3. 寄件服务器（2-1）以自己的数字证书（5-2）的私钥将该电子邮件（4）进行加密，然后将加密后的邮件传送到交换中心（1），并且在该寄件人账户记录内，记下该笔发邮件的账项，

E4. 交换中心（1）将收到加密邮件，以寄件服务器（2-1）的数字证书（5-2）的公钥进行解密，解密成功后就可确定该邮件是从寄件服务器（2-1）所发出的，就立即在该寄件服务器（2-1）的账户内记下该笔发邮件的支出账项，并将该解密后的邮件（4）以交换中心（1）的数字证书（5-1）的私钥进行加密，然后传送到收件服务器（2-2），同时在该收件服务器（2-2）的账户内记下该笔收邮件的收入账项，

E5. 收件服务器（2-2）将收到的加密邮件以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件是从交换中心（1）所发出的，就立即在该收件人账户记录内，记下该笔收邮件的收入账项，并且收件服务器（2-2）会核对收件人的电邮地址是普通电邮用户或是自定捐款收费电邮用户，如果该收件人是普通电邮用户，就立即将该解密后的邮件（4）储存在收件人的电子邮箱内，等待收件人上网查阅该邮件（4），并转到步骤E15；如果该收件人是自定捐款收费电邮用户，立即将邮件（4）暂时储存，并转到步骤E6，

E6. 收件服务器（2-2）向交换中心（1）发出请求支付自定捐款金额费用信息，信息内容包括该邮件（4）的寄件人电子邮件地址、收件人电子邮件地址、标题及寄件日期和时间等资料，

E7. 交换中心（1）收到请求支付自定捐款金额费用信息后，从信息内容找到收件人电子邮件地址，立即向邮件收费查询网站（9）查询该电子邮件地址的捐款收费金额，

E8. 邮件收费查询网站（9）从所储存的记录内，找出该电子邮件地址的捐款收费金额资料，并立即将捐款收费金额资料传送到交换中心（1），

E9. 交换中心（1）立即将捐款收费金额资料暂时储存起来，并回复一个以交换中心（1）本身的数字证书（5-1）的私钥加密的邮件给寄件人，邮件内容是通知寄件人有关的捐款收费金额及一个捐款参考号码，请他在指定期限内（例如一星期内）上网到交换中心（1）的网站，通过网上付款缴交有关的捐款收费，所述捐款参考号码是用来在捐款时分辨不同的电邮（4）的一个编号，

E10. 寄件人的电子邮件服务器（2）将回复给寄件人的邮件，以交换中心（1）的数字证书（5-1）的公钥进行解密，解密成功后就可确定该邮件（4）是从交换中心（1）所发出的，从内容知道是一个请用户支付捐款费用的邮件，就将该回复邮件储存到寄件人的电子邮箱内，

E11. 寄件人上网查看自己的电子邮箱，看到有关的回复邮件的内容，同意捐款就在指定时间内上网到交换中心（1）的网站，输入寄件人自己的电邮地址和付款参考号码，就可在交换中心（1）的网站内找出之前在步骤E2传送到寄件服务器（2-1）的邮件（4）的收件人电邮地址，核对无误后寄件人在交换中心（1）的付款网页内输入自己的付款资料，包括信用卡卡号、信用卡有效期等网上付款所必需的资料，或借记卡卡号、密码等网上付款所必需的资料，

E12. 交换中心（1）将付款资料和金额通过支付网关（7）传送到银行账户电脑系统（8），请求转账付款，

E13. 银行账户电脑系统（8）核对付款资料和账户结余等资料无误后，从寄件人的所输入的付款资料的账户内转钱到交换中心（1）的银行账户内，并通知交换中心（1）转账付款成功，

E14. 交换中心（1）将已收到捐款信息传送到收件服务器（2-2），收件服务器（2-2）将在步骤E5中暂时储存的解密后邮件（4），储存在收件人的电子邮箱内，等待收件人上网查阅该邮件（4），

E15. 到结算时，交换中心（1）以各电子邮件服务器（2）的账户有关定额收费的电邮收发记录，扣除手续费用后计算出该电子邮件服务器（2）的应付费用或应收款项，然后通过支付网关（7）及银行账户电脑系统（8），在各电子邮件服务器（2）的银行账户内转账收款或存入款项，再由各电子邮件服务器（2）向

其用户收回款项或将款项返还给用户，以及将在步骤E13中收到的捐款，扣除手续费后全部捐给当地的公益慈善机构。

13. 一种防止垃圾电子邮件的方法，所述方法 特别适合于用付费方法发电邮给知名人士等， 采用如权利要求1所述系统，以及，增设一收费电子邮件服务器（22）的网站，每位知名人士分配一个电子邮箱和电邮地址，而且将这些电邮地址全部公开，谁要发邮件（4）给这些知名人士，首先要上网到收费电子邮件服务器（22）的网站支付一定金额的费用，才能将电邮（4）发送到知名人士的邮箱，所述方法包括如下F组步骤：

F1. 当寄件人要向知名人士发送电子邮件（4）前，寄件人首先上网到收费电子邮件服务器（22）的网站开设寄件人账户，并且在网站购买积分，寄件人在网站输入自己的信用卡卡号等付款资料和要购买的积分的金额，

F2. 收费电子邮件服务器（22）将收寄件人的付款资料包括信用卡卡号和金额等传送到银行卡中心（88），请求转账付款，

F3. 银行卡中心（88）核对付款资料和账户结余无误后，从寄件人的信用卡账户转钱到收费电子邮件服务器(22)的银行账户内，并通知收费电子邮件服务器(22)转账付款成功，

F4. 收费电子邮件服务器（22）通知寄件人申请账户成功，并且已经从他的信用卡账户内收取购买积分的款项，

F5. 寄件人在收费电子邮件服务器（22）的网站上查找出所选的知名人士的电邮地址，及发电邮（4）给该知名人士的授权码所需的费用（即积分），于是使用刚才所购买的积分，在网站内购买这授权码，

F6. 收费电子邮件服务器（22）核对寄件人的积分账户结余无误后，从寄件人的账户扣取该授权码所需的费用（即积分），并且向该寄件人发出一个随机产生的授权码，这授权码编号是唯一的，而且是一次过使用的，请寄件人在指定期限内，将这授权码放到电邮（4）的标题内，然后将电邮（4）寄给所选的知名人士在收费电子邮件服务器（22）的电邮地址，

F7. 寄件人在指定期限内，以授权码为电邮（4）的标题写一个电邮（4），寄给所选的知名人士在收费电子邮件服务器（22）的电邮地址，收费电子邮件服务器

（22）收到邮件（4）后，将邮件（4）的标题内的授权码与步骤F6中所发出的授权码相核对，核对无误后，将该邮件（4）储存到该知名人士的电子邮箱内，并将该授权码的记录删除，如果收费电子邮件服务器（22）收到的电邮的标题内没有对应该收件人的有效授权码，收费电子邮件服务器（22）会将邮件弃置，并发电邮回复寄件人，通知他要购买有关的授权码后才能成功发电邮（4）的详细资料，

F8. 知名人士上网登入收费电子邮件服务器（22）查看邮件（4），

F9. 收费电子邮件服务器（22）将寄件人所寄给知名人士的邮件（4），传送给知名人士阅看。

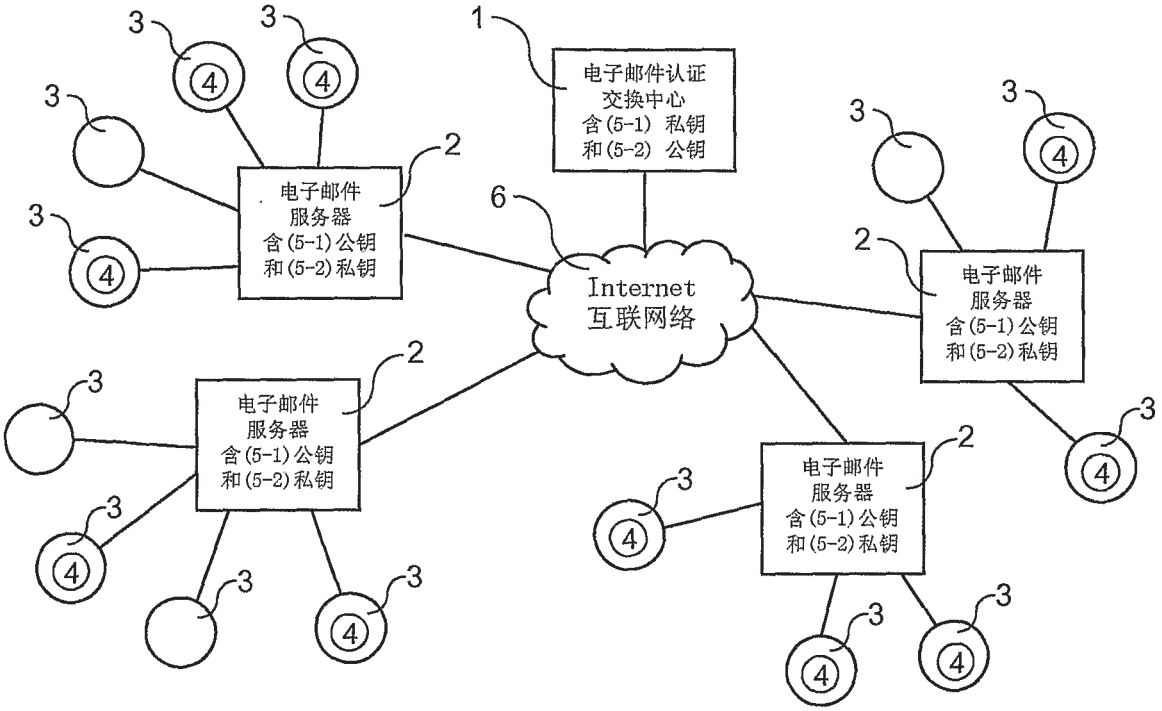

1
电子邮件认证
交换中心
含(5-1) 私钥
和(5-2) 公钥
2
电子邮件
服务器
含(5-1)公钥
和(5-2)私钥
6
Internet
互联网络
3
4

图 1

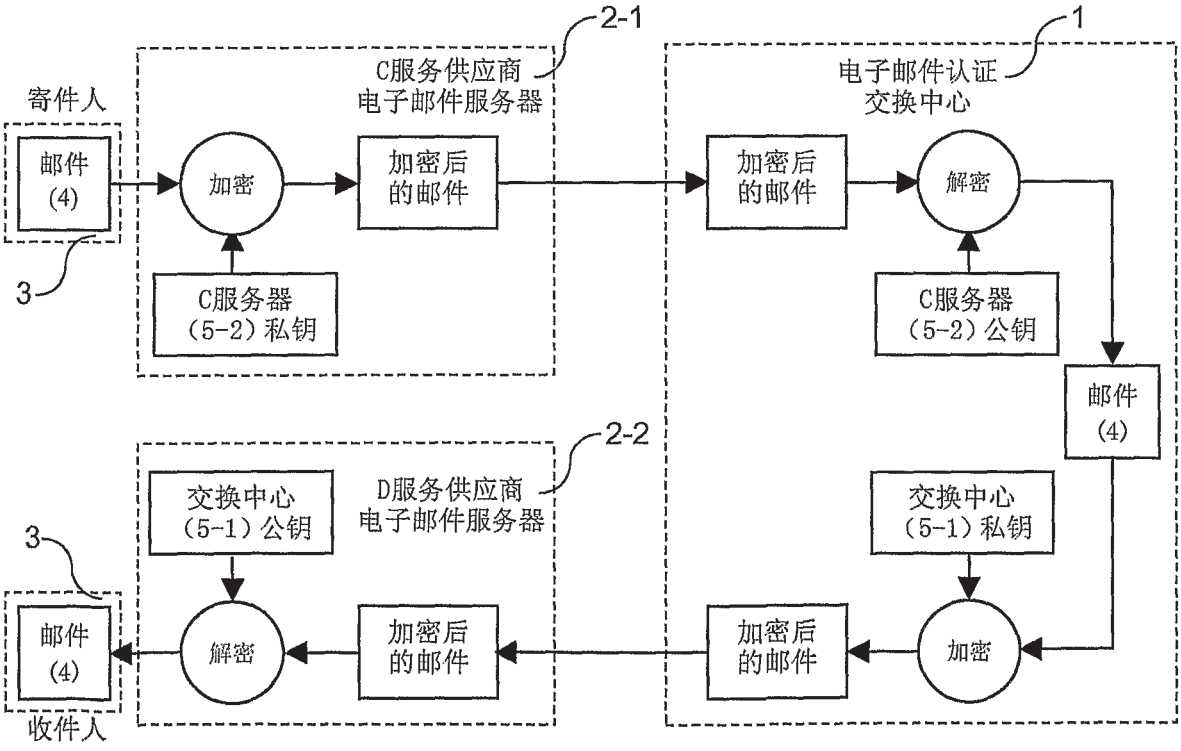

2-1
C服务供应商
电子邮件服务器
1
电子邮件认证
交换中心
寄件人
邮件
(4)
加密
加密后
的邮件
C服务器
(5-2) 私钥
C服务器
(5-2) 公钥
解密
邮件
(4)
2-2
D服务供应商
电子邮件服务器
交换中心
(5-1) 公钥
交换中心
(5-1) 私钥
加密
解密
收件人

图 2

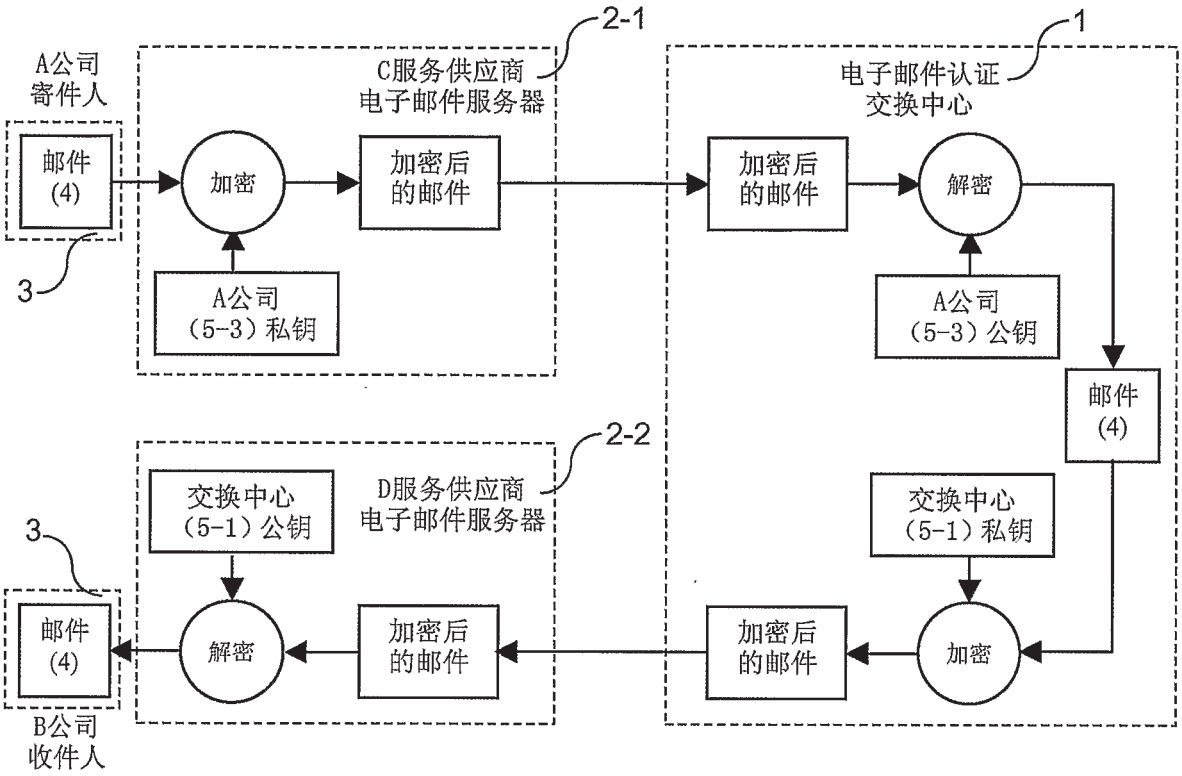

2-1
1
A公司
寄件人
C服务供应商
电子邮件服务器
电子邮件认证
交换中心
邮件
(4)
加密
加密后
的邮件
加密后
的邮件
解密
3
A公司
(5-3) 私钥
A公司
(5-3) 公钥
邮件
(4)
2-2
交换中心
(5-1) 公钥
D服务供应商
电子邮件服务器
交换中心
(5-1) 私钥
3
邮件
(4)
解密
加密后
的邮件
加密后
的邮件
加密
B公司
收件人

图 3

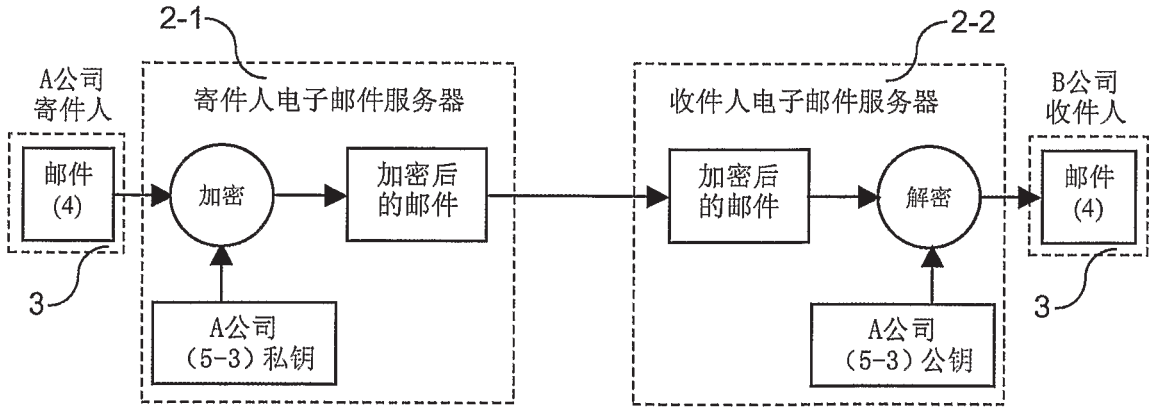

2-1
2-2
A公司
寄件人
寄件人电子邮件服务器
收件人电子邮件服务器
B公司
收件人
邮件
(4)
加密
加密后
的邮件
加密后
的邮件
解密
邮件
(4)
3
A公司
(5-3) 私钥
A公司
(5-3) 公钥
3

图 4

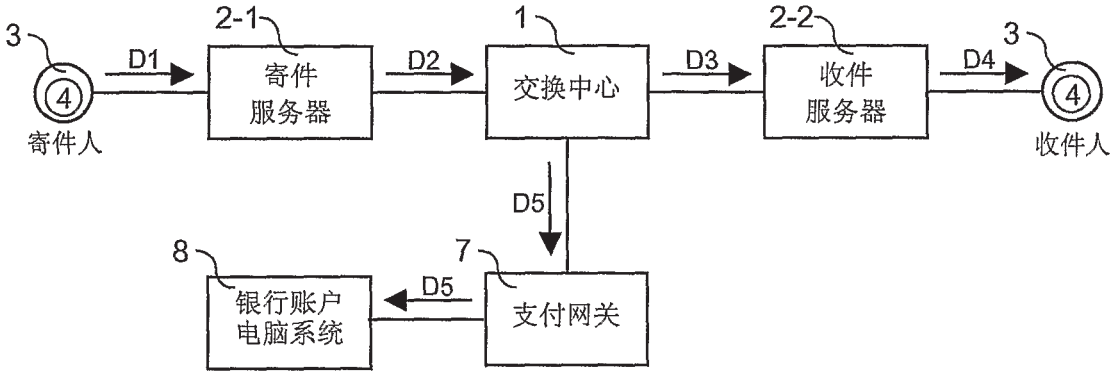

3
2-1
1
2-2
3
D1
D2
D3
D4
寄件
服务器
交换中心
收件
服务器
寄件人
收件人
D5
8
7
D5
银行账户
电脑系统
支付网关

图 5

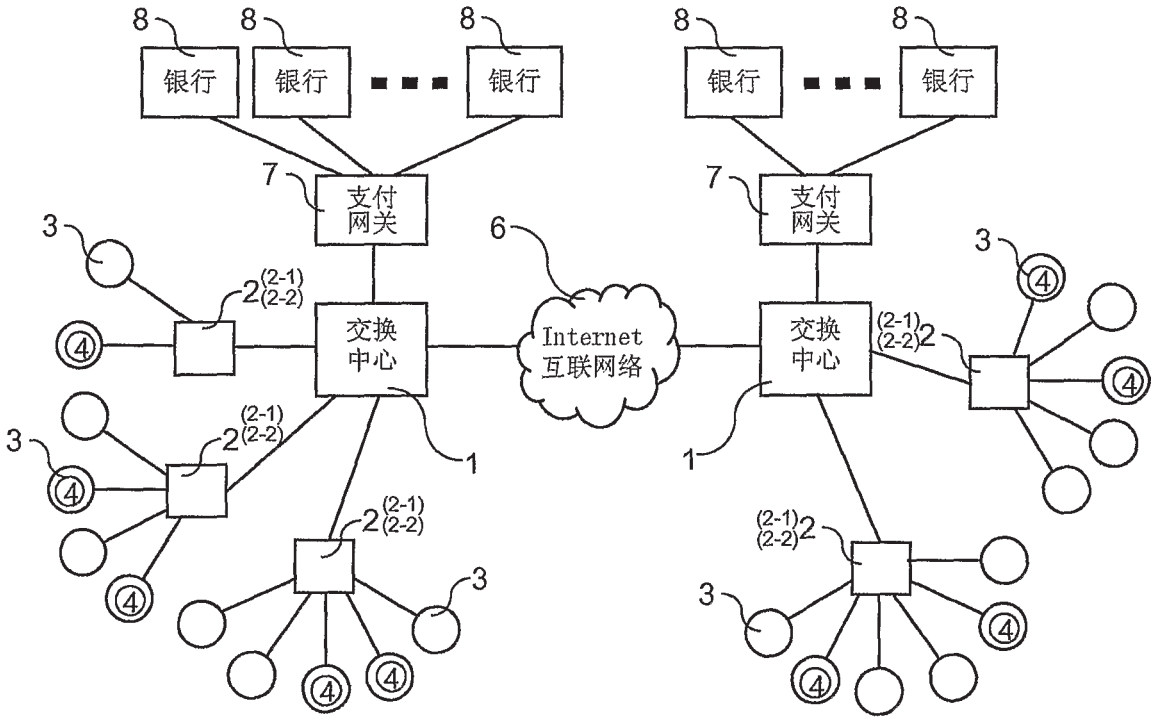

8
8
8
8
8
银行
银行
银行
银行
银行
7
7
支付
网关
支付
网关
3
6
3
2(2-1)(2-2)
交换
中心
Internet
互联网络
交换
中心
(2-1)(2-2)2
1
1
3
2(2-1)(2-2)
(2-1)(2-2)2
3
2(2-1)(2-2)
3
3

图 6

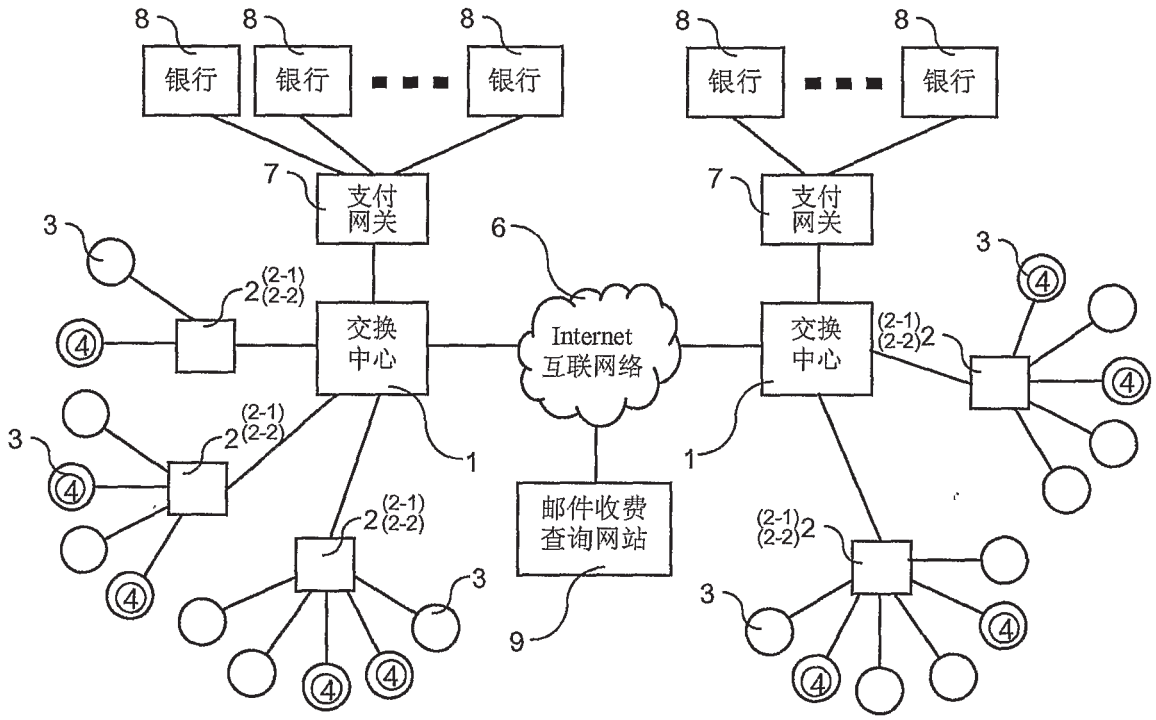

8
银行
银行
银行
银行
银行
7
支付网关
支付网关
6
Internet
互联网络
3
2(2-1)(2-2)
交换中心
交换中心
1
邮件收费查询网站
9
4

图 7

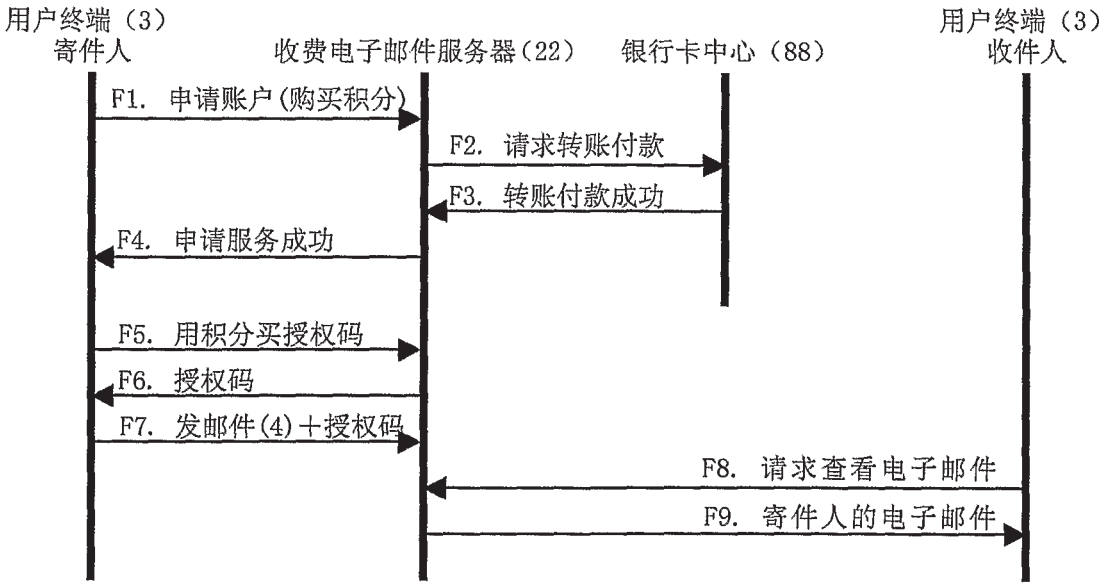

用户终端（3）
寄件人
收费电子邮件服务器(22)
银行卡中心（88）
用户终端（3）
收件人
F1. 申请账户(购买积分)
F2. 请求转账付款
F3. 转账付款成功
F4. 申请服务成功
F5. 用积分买授权码
F6. 授权码
F7. 发邮件(4)＋授权码
F8. 请求查看电子邮件
F9. 寄件人的电子邮件

图 8