[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32

[12] 发明专利说明书

[21] ZL 专利号 98800992.7

[45] 授权公告日 2003 年 12 月 17 日

[11] 授权公告号 CN 1131621C

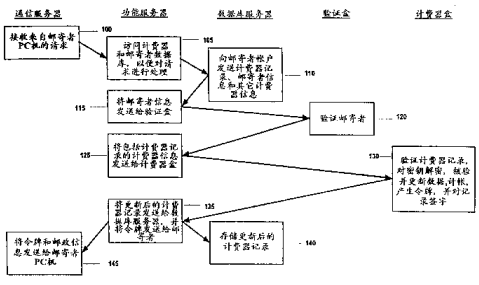
[22] 申请日 1998.6.12 [21] 申请号 98800992.7
[30] 优先权
[32] 1997. 6.12 [33] US [31] 60/049,518
[86] 国际申请 PCT/US98/12276 1998.6.12
[87] 国际公布 WO98/57304 英 1998.12.17
[85] 进入国家阶段日期 1999.3.16
[71] 专利权人 皮特尼鲍斯股份有限公司
地址 美国康涅狄格州
[72] 发明人 罗伯特·A·考德里
福兰克·M·迪普利托
盖瑞·M·海登 大卫·K·李
审查员 朱 骥
[74] 专利代理机构 上海专利商标事务所
代理人 钱慰民

权利要求书 2 页 说明书 11 页 附图 4 页

[54] 发明名称 保密邮资分配系统和证明邮资已付的方法

[57] 摘要

一种证明邮资已付的系统和方法包括具有存储有多条计费器记录的数据库的数据中心。每条计费器记录包括对应于分配给多个远程用户装置中每一个的计费器帐户的计费器信息，远程用户装置被授权请求邮资已付证明。当在数据中心接收到邮资请求时，数据中心中的保密协处理器装置获取合适的计费器记录，并通过核验计费器记录中的签名以及将计费器记录中的新数据与保密装置中的新数据比较，来验证计费器记录的真实性。如果核验通过，保密装置对要证明的邮资金额计帐，产生邮资已付证明并更新计费器信息，包括计费器记录中的新数据。然后，保密装置对更新的计费器信息签名，并将签名存储在计费器记录中。然后，保密装置将更新的计费器记录送回数据库。



ISSN1008-4274

1. 一种保密邮资分配系统，其特征在于，包括：

数据中心，用于响应于来自多个远程用户装置的邮资请求进行邮资分配，所述数据中心包括：

数据库服务器，用于存储数据记录，所述数据记录包括关于个人计费器帐户的用户信息和计费器信息，每个所述计费器帐户分配给所述多个远程用户装置中的每一个；

用于从多个远程用户装置接收邮资证明请求的通信服务器；

用所述用户信息和所述计费器信息验证每一条邮资证明请求的装置，其中所述用户信息和所述计费器信息对应于发出邮资证明请求的远程用户装置的计费器帐户；和

用于分配所述被请求的邮资证明的装置，所述分配装置至少包括一个第一保密装置，所述第一保密装置包括处理器和存储器，它从所述数据库服务器获得所述计费器信息，核验所述计费器信息的真实性， 产生所请求的邮资证明，更新所述计费器信息，对更新后的计费器信息进行数字签字，并且将经签字的、更新后的计费器信息送回所述数据库服务器。

2. 如权利要求 1 所述的系统，其特征在于，所述数据库服务器包括计费器记录数据库，每条计费器记录包括计费器信息以及计费器信息的签名，其中所述计费器信息对应于供多个远程用户装置使用的计费器帐户中的一个。

3. 如权利要求 2 所述的系统，其特征在于，所述计费器信息包括升值和降值寄存器，经加密的令牌密钥和新数据。

4. 如权利要求 3 所述的系统，其特征在于，所述新数据包括一记录更新计数器，它对应于由所述保密装置处理的邮资证明事务的数目。

5. 如权利要求 2 所述的系统，其特征在于，所述第一保密装置包括用于存储第一和第二加密密钥的装置，所述第一密钥用于核验每条计费器记录中的签名并在将每条计费器记录送回数据库服务器之前对更新后的计费器信息签字，所述第二密钥用于对计费器记录中被加密的令牌密钥解密，所述保密装置用所述令牌密钥产生所请求的邮资证明。

6. 如权利要求 5 所述的系统，其特征在于，由功能服务器处理所述通信服

务器接收到的每个请求，从所述数据库服务器获取合适的用户信息和计费器信息，并将用户信息和计费器信息发送给验证装置和分配装置。

7. 如权利要求 5 所述的系统，其特征在于，所述验证装置包括第二保密盒，所述第二保密盒包括处理器、存储器和用于存储第三加密密钥的装置，所述第三密钥用于核验与正被处理的计费器帐户之所述用户信息相关的签名。

8. 如权利要求 7 所述的系统，其特征在于，还包括一密钥管理系统服务器，用于产生和保留所述验证装置和所述分配装置所用的加密密钥。

9. 一种证明邮资已付的方法，其特征在于，所述方法包括以下步骤：

提供多条计费器记录，每条计费器记录都包括计费器信息，所述计费器信息对应于分配给多个远程用户装置中的每一个的计费器帐户，而所述远程用户装置被授权对邮资已付证明提出请求；

将所述多个计费器记录存储在数据中心的数据库中；

当数据中心接收到邮资已付证明请求时，获取第一计费器记录；

通过核验第一计费器记录中的签名，验证第一计费器记录的真实性；

对被证明的邮资金额计帐；

产生数字令牌，作为邮资已付的证明；

更新第一计费器记录中的计费器信息；

对更新后的计费器信息签字，以更新第一计费器记录的签名；以及

将第一计费器记录送回数据库。

10. 如权利要求 9 所述的方法，其特征在于，所述获取、核验、计帐、产生、更新、签字和回送步骤都在一保密装置中进行。

11. 如权利要求 10 所述的方法，其特征在于，所述验证第一计费器记录之真实性的步骤包括下述步骤：

将第一计费器记录中的新数据与存储在所述保密装置中的新数据比较。

12. 如权利要求 10 所述的方法，其特征在于，所述更新计费器信息的步骤包括下述步骤；

更新存储在保密装置和第一计费器记录中的新数据。

保密邮资分配系统和证明邮资已付的方法

本申请是美国临时专利申请第60/049,518号的部分连续申请，其中临时专利申请第60/049,518号于1997年6月13日提出，并已转让给本发明的受让人。

技术领域

本发明总体上涉及一种在开放系统中证明邮资已付的邮资计费系统和方法，尤其涉及一种在虚拟计费结构中证明邮资已付的邮资计费系统和方法。

相关申请

本发明与以下国际专利申请有关(律师档案号E－731，E－733，E－734，E－735和E－736)，这些申请同时提交，并都被转让给本发明的受让人，所有申请通过引用全部包括在此。

背景技术

已开发了各种邮资计费系统，这些系统将加密信息印刷在邮件上，作为证明邮资已付的邮戳的一部分。加密信息包括邮件的邮资以及其它与邮件和印刷邮戳的邮资计费器相关的邮政数据。加密信息一般称为数字令牌或数字签名，它可以验证并保护信息的完整性，包括印在邮件上的邮资值，供日后核验邮资已付之用。由于数字令牌包含与证明邮资已付有关的加密信息，所以通过标准的核验程序可以检测出改变邮戳之印刷信息的行为。美国专利第4,725,718号、第4,757,537号、第4,775,246号和第4,873,645号描述了几例产生并印刷这类邮戳的系统，这些专利都已转让给本发明的受让人。

目前，存在两种类型的邮资计费装置，一类是封闭系统，另一类是开放系统。在封闭系统中，系统功能专用于计费活动。封闭系统的计费装置也称为邮资证明装置，例子包括传统的数字和模拟(机械的和电子的)邮资计费器，在这种系统中，将专用打印机与一计费或计帐功能安全地耦合。在封闭系统中，一般将打印机与计费器安全地耦合，并专供计费器使用，并且在邮资证明未计帐的情况下，

不打印邮资证明。在开放系统中，打印机并不供计费活动专用，除计费活动之外，系统功能还可以自由地适应多种不同的应用。开放系统计费装置的例子包括带有单/多任务操作系统、多用户应用程序和数字打印机的基于个人计算机(PC)的装置。开放系统计费装置是具有非专用打印机的邮资证明装置，打印机不与保密计帐模块安全地耦合。通过连续核验打印于邮件上的加密邮资证明中包含收件人的信息，使得由非专用打印机打印的开放系统邮戳安全可靠。参见美国专利第4,725,718号和第4,831,555号，这些专利都已转让给本发明的受让人。

美国邮政部门(“USPS”)已提议使用一种**基于信息的邮戳程序(“IBIP”)**，它是一种分布式的信托系统，用新的称为基于信息之邮戳的邮资已付证明来更新和扩充现有的邮资计费器。该邮戳程序利用数字签名技术为每张信封产生一邮戳，邮戳的发源地可以验证，但内容不可以改变。除了目前一般靠邮资计费器在邮件上打印邮戳的方法外，能期望IBIP支持新的应用邮资的方法。IBIP要求在邮件上打印一个较大的、高密度的两维(“2－D”)条形码。2－D条形码对信息编码，并用数字签名签字。

USPS已公布了IBIP的草案。于1996年6月13日公布并于1997年7月23日修订的**基于信息的邮戳程序(IBIP)邮戳规定(“IBIP”邮戳规定)**确定了关于用IBIP产生的、将被加盖在邮件上的新邮戳的推荐性要求。于1996年6月13日公布并于1997年7月23日修订的**基于信息的邮戳程序邮政保密装置规定**确立了关于邮政保密装置(“PSD”)的推荐性要求，该邮政保密装置是一种基于处理器的保密计帐装置，可以对存储其中的邮资值进行分配和计帐，以支持产生一种新的“基于信息的”邮资邮政标记或邮戳，加到采用IBIP进行处理的邮件上。于1996年10月9日公布的**基于信息的邮戳程序主系统规定**确立了关于IBIP主系统单元的推荐性要求(“IBIP主规定”)。IBIP包括与用户连接、邮政和卖家的基础结构，它们是程序的系统单元。于1997年4月25日公布的**基于信息的邮戳程序密钥管理计划规定**确立了USPS产品/服务提供器和PSD所用的加密密钥的产生、分布、使用和替换(称“IBIP KMS规定”)。各项规定在此统称为“IBIP规定”。

IBIP规定确立了一种独立开放计费系统，这里称为PC计费器，它包括与个人计算机(“PC机”)耦合的PSD，该计算机作为主系统运行，有一打印机与之相连(“主PC机”)。主PC运行计费应用软件和相关的库(这里统称为“主应用程序”)，并与一个或多个相连的PSD通信。PC计费器只能访问与主PC机耦合的

PSD。PC 计费器不能访问远程的 PSD。

PC 计费器在主 PC 上处理有关分配邮资、登记以及再注入的事务。处理在主 PC 机和与之耦合的 PSD 之间局域地完成的。例如，对于登记和再注入事务。与数据中心的连接是从主 PC 机通过本地或网络调制解调器/互联网连接局域地完成的。将借贷计帐入 PSD 也是局域地进行的，将事务记录在主 PC 机上。主 PC 机可以容纳不止一个 PSD，例如每个串行口支持一个 PSD。在主 PC 机上运行的几个应用程序，诸如字处理程序或信封设计程序，可以访问主应用程序。

IBIP 规定不访问在网络环境上的 BIP 开放计费系统。但是，规定并不禁止这种基于网络的系统。一般情况下，在网络环境中，网络服务器控制在网络上的客户 PC 机请求的远程打印。当然，客户 PC 机控制任何本地的打印。

一种版本的网络计费系统称为“虚拟计费器”，它具有许多主 PC 机，但不耦合任何 PSD。主 PC 机运行主应用程序，但是所有 PSD 功能都在位于数据中心的一个或多个服务器上实现。数据中心处的 PSD 功能可以在连接数据中心计算机的保密装置中完成，或者在数据中心计算机本身内完成。各主 PC 机必须与数据中心相连，以便处理诸如邮资分配、计费登记或计费再注入等事务。由主 PC 机提出事务请求，并将其发送至数据中心进行远程处理，在数据中心集中处理事务，并且将结果返回给主 PC 机。资金计帐和事务处理集中在数据中心。例如，参见美国专利第 5,454,038 号和第 4,873,645 号，该专利已转让给本发明的受让人。

虚拟计费器不符合 IBIP 规定的所有的现行要求。特别是，IBIP 规定不允许 PSD 功能在数据中心完成。但是，应该理解，使每个邮寄者的 PSD 都放置于数据中心的虚拟计费器结构可以提供与 IBIP 规定所要求的相等的保密等级。

在常规的封闭系统机械和电子邮资计费器中，在打印和计帐功能之间需要一条保密链路。对于在单个保密盒内完成打印和计帐功能的邮资计费器，通过对计费器进行周期性检查来监视保密盒的完整性。 新近，数字打印邮资计费器一般包括一种与计费(计帐)装置耦合的数字打印机，此处称它为邮政保密装置(PSD)。数字打印邮资计费器通过加密方式使计帐和打印机构之间的链路保密，从而不需要实际的检查。实质上，新的数字打印邮资计费器在 PSD 和打印头之间产生一条保密的点对点通信链路。例子参见颁发给 Christopher B. Wright 等人的美国专利第 4,802,218 号，该专利现已转让给本发明的受让人。进行打印头保密通信的数字打印邮资计费器的一个例子是由 Connecticut,Stamford 的 Pitney

Bowes 股份有限公司制造的个人邮局™。

在美国专利第 4,873,645 号和第 5,454,3,038 号中，揭示了一种虚拟计费系统和方法，在该系统和方法中，邮政计帐和令牌产生发生在远离邮资证明打印机的数据中心。尽管数据中心可能是一保密装置，但仍存在一些固有的保密性问题，因为计帐和令牌产生功能不是在靠近邮资打印机的保密装置中发生的。虚拟邮资计费系统包括一计算机，计算机与一非保密的打印机和一远程数据计费系统耦合。邮政计帐和令牌产生发生在数据中心。

数据中心是由诸如 Pitney Bowes 或邮政部门等计费器卖家控制的集中化的设施。因此，与客户直接处理计费器的环境相比，这被认为是安全的。但是，数据中心的全体人员都可访问存储在数据中心的数据，因此最低限度，至少这类人员会进行无意地更改。对存储在数据中心的用户和计费数据进行任何未授权的更改都会损害虚拟计费系统的完整性。

发明内容

本发明涉及一种保密邮资分配系统，它包括数据中心，用于响应于来自多个远程用户装置的邮资请求进行邮资分配，所述数据中心包括：数据库服务器，用于存储数据记录，所述数据记录包括关于个人计费器帐户的用户信息和计费器信息，每个所述计费器帐户分配给所述多个远程用户装置中的每一个；用于从多个远程用户装置接收邮资证明请求的通信服务器；用所述用户信息和所述计费器信息验证每一条邮资证明请求的装置，其中所述用户信息和所述计费器信息对应于发出邮资证明请求的远程用户装置的计费器帐户；和用于分配所述被请求的邮资证明的装置，所述分配装置至少包括一个第一保密装置，所述第一保密装置包括处理器和存储器，它从所述数据库服务器获得所述计费器信息，核验所述计费器信息的真实性， 产生所请求的邮资证明，更新所述计费器信息，对更新后的计费器信息进行数字签字，并且将经签字的、更新后的计费器信息送回所述数据库服务器。

本发明还涉及一种证明邮资已付的方法，所述方法包括以下步骤：提供多条计费器记录，每条计费器记录都包括计费器信息，所述计费器信息对应于分配给多个远程用户装置中的每一个的计费器帐户，而所述远程用户装置被授权对邮资已付证明提出请求；将所述多个计费器记录存储在数据中心的数据库中；当数据

中心接收到邮资已付证明请求时，获取第一计费器记录；通过核验第一计费器记录中的签名，验证第一计费器记录的真实性；对被证明的邮资金额计帐；产生数字令牌，作为邮资已付的证明；更新第一计费器记录中的计费器信息；对更新后的计费器信息签字，以更新第一计费器记录的签名；以及将第一计费器记录送回数据库。

附图概述

结合附图阅读以下详细描述，将清楚本发明的上述和其它目的和优点，在所有附图中，相同的标号表示相同的部件，附图有：

图 1 是一方框图，示出了应用本发明原理的用于分配邮资的虚拟邮资计费系统；

图 2 是一方框图，示出了关于图 1 中虚拟邮资计费系统的数据中心数据库服务器和保密盒；

图 3 是一流程图，示出了用图 1 虚拟邮资计费系统证明邮资的过程；以及

图 4 是一流程图，示出了在图 1 虚拟邮资计费系统的保密计费器盒中所进行的过程。

实施本发明的最佳方式

以下参照附图，描述本发明。由图 1 可见，虚拟邮资计费系统一般用标号 10 表示。虚拟邮资计费系统 10 包括多个个人计算机(PC)系统(图中仅画出一个)，一般用标号 20 表示。每个个人计算机系统可以连接一个打印机 22，用于在信封或标签上打印邮资证明。PC 20 与事务处理数据中心 30 相连，而事务处理数据中心 30 则履行邮资的邮政计帐和邮资证明。虚拟邮资计费系统 10 根据需要允许每个邮寄者用常规的 PC 机获取远距离处的邮资已付证明。与传统的邮资计费系统不同的是，虚拟邮资计费系统 10 在邮寄者一侧不包括任何计费器硬件。在邮寄者一侧也不存储任何邮政资金。所有资金计费和计帐都发生在使用功能性软件和数据库记录的数据中心 30 中，其中数据库记录代表每个邮寄者的“邮资计费器”，这里称为“计费器帐户”

虚拟邮资计费系统 10 的计帐方法可以是传统的预付或后付系统。较佳的方法是预付法，该方法要求每个邮寄者将最小数额的钱存入邮寄者的虚拟计费器帐

户中。当帐户资金低于规定水平时，会要求把钱再存入邮寄者的帐户。另一种适用于虚拟邮资计费系统的计帐方法是实时付费方法，在该方法中，当发生事务时，事务额被记入邮寄者的信用卡帐户内。由于邮寄者直到准备打印邮件时才对邮件付费，所以这里将该方法称为“涓流补充”邮资支付法，

在虚拟邮资计费系统中，“计费器”的卖家(诸如 Pitney Bowes 股份有限公司)为邮寄者提供在 PC 20 上运行的客户软件，例如，可以从卖家的互联网服务器上下载客户软件。另一方面，客户软件可以是基于互联网浏览器的主页，用户可以借此与数据中心 30 交互作用。计费器卖家还对数据中心 30 进行管理。客户软件起动与数据中心 30 的通信，数据中心 30 进行计费事务，为单个邮件和批量邮件提供邮资证明。在较佳实施例中，客户软件建立至数据中心的连接，并通过提供与诸如，邮资金额、收件人信息以及(可选的)每个邮件的积存地等所请求的事务相关的邮政信息来要求邮资。数据中心 30 接收邮政信息，确定邮件积存地的邮政编码，完成计帐功能，并产生关于邮资已付的加密证明(诸如，令牌或数字签名)，然后将包含该令牌的邮戳信息发送给 PC 20。PC 20 接收邮戳信息，产生邮戳位图，邮戳位图可以显示在 PC 监视器(未示出)上，并且由打印机 22 将邮戳位图打印在邮件上。然后，PC 20 中断与数据中心 30 的连接，或者请求另一次事务。PC 20 与数据中心 30 之间的连接可以通过诸如互联网上的网络服务提供器，或者用 PC 的调制解调器直接拨打来实现。

虚拟邮资计费系统 10 不需要在每个邮寄者一侧保留和构成传统的计费装置，为每个邮寄者从多个积存地发出的处理请求提供灵活性。虚拟邮资计费系统 10 还提供了传统计费装置没有的增值服务，诸如实时地址清理(address hygiene)、直销服务和涓流补充邮资支付等。虚拟邮资计费系统 10 通过数据中心 30 为用户提供验证，以便用有效帐户识别邮寄者。当用例如用户姓名、密码或其它常规方法就每个请求对邮寄者作出验证时，数据中心 30 为该请求服务，并将邮戳信息返回 PC 20，然后 PC 20 产生邮戳并将其打印在邮件上。

再参照图 1，邮寄者通过运行 PC 20 中的客户软件，起动邮资证明事务，这时 PC 20 与数据中心 30 接触。在数据中心 30，通信服务器 32 支持来自各种通信技术和协议的连通性。通信服务器合并所有输入的通信量，并且将其传送到功能服务器 34。功能服务器 34 包括支持邮寄者签字、邮资分配和邮政报告的应用软件。可以从数据库服务器 36 中访问所有的邮寄者信息和计费器信息，如下所述，

这些信息是通过保密加密过程和协议安全地存储在数据库服务器 36 中的。数据中心 30 为数据库服务器 36 中的每个计费器帐户保留加密密钥。加密密钥用来进行邮资证明和核验，并对存储在数据库服务器 36 中的记录保密。密钥管理系统 38 管理虚拟邮资计费系统 10 中使用的所有加密密钥。加密密钥可以分配给远处的核验器。美国专利申请第 08/553812 号描述了这样一种密钥管理系统，该申请于 1995 年 10 月 23 日提出，并且已转让给本发明的受让人。

邮寄者可以通过与数据中心 30 发生的联机签约过程，建立计费器帐户。在签约过程中，邮寄者用 PC 20 输入诸如用户姓名、密码和支付方式等帐户信息。任何登记费都可在此时收取。数据中心 30 最好由计费器卖家(例如，Pitney Bowes 股份有限公司)来管理，数据中心 30 在其邮寄者和邮局之间安排所有的计费器许可证和协议。

在本发明中，不存在 PSD，即没有与请求支付邮资的 PC 机耦合的计费装置。虚拟邮资计费系统 10 用 PC 20 中的计费软件以及在数据中心 30 中执行和更新的邮寄者帐户信息代替了 PSD 的计帐和计费功能。虚拟邮资计费系统 10 为每个邮寄者提供一计费系统，该系统具有从多个积存地起动事务的能力。例如，参见上面提及的国际专利申请(律师档案号 E－735)。

可以用各种方法确定所请求的事务积存地。例如，美国专利申请第 08/775,818 号揭示了一种方法，该方法用来自电话呼叫的呼叫者 ID 确定积存地的邮政编码，上述专利申请是于 1996 年 12 月 31 日提出的，并已转让给本发明的受让人，该申请通过引用作为整体包括在此。

依照本发明，在数据中心 30 内放置一个或多个加密模块，这里称为保密“盒”，用于加密处理。每个保密盒是一个保密的、对窜改敏感并能响应窜改的装置，它包括处理器和存储器，用于存储加密密钥并用该装置中保密边界内的密钥进行加密操作。数据中心 30 包括以下描述的几种类型的保密盒。在较佳实施例中，数据中心 30 包括每种类型的多个盒，以便冗余和运行。

密钥管理系统 38 包括一制造盒(未示出)，它提供的高级密钥用于产生随机数据，以便加入其余每一个保密盒中。通过共享一个公用加密密钥，保密盒可以在数据中心 30 内安全通信。密钥管理系统 38 还包括一“钢”盒(未示出)，它与计费器盒 44(在下面描述)共享一个公用密钥，以便就每个计费器帐户的邮资证明事务对主令牌密钥进行加密/解密。钢盒将卖家密钥和邮政密钥合并成密码文本

中的一条记录。对于每个计费器帐户，数据中心 30 通过以下方式在数据库服务器 36 中产生一个逻辑计费器，即一条计费器记录，即用卖家密钥和邮政密钥产生一令牌密钥，启动计费寄存器(升值和降值)、计费器新数据(以下将作描述)和其他邮政信息作为计费器记录的一部分，然后将计费器记录存储在数据库服务器 36 中。

数据中心 30 还包括计费器盒 44，它与钢盒共享一秘密密钥，用于对在计费器记录中加密的令牌密钥解密。计费器盒 44 还持有用于事务记录数字签名的密钥。存储在计费器盒 44 中的另一唯一的信息是关于由计费器盒 44 处理的每条计费器记录的新数据。对于每次邮政事务，计费器盒 44 至少产生一个数字令牌或对邮政事务签字，并且更新与该事务对应的计费器记录。数据库服务器 36 中的每条计费器记录包括邮政资金以及密码文本中的令牌密钥。计费器盒 44 用令牌密钥产生令牌，更新计费器记录中的邮政资金，并对更新后的计费器记录签名。用这种方式，计费器盒执行和控制对每次事务的保密计帐。计费器盒 44 还可用来核验令牌或事务签名，从而证实事务的邮资证明。

数据中心 30 还包括一验证盒 40，它与钢盒共享一个不同的秘密密钥，以便对用密码文本存储在数据库服务器 36 中的用户验证密钥进行解密。验证盒 40 还用解密后的验证密钥进行验证运算，以对邮寄者进行验证。可以对密钥管理系统 38 的钢盒增加该功能，从而避免在数据中心 30 使用一个分立的盒。

最后，数据中心 30 包括一事务盒 42，它与钢盒共享另一个秘密密钥，以便对诸如注册和注册史记录等用户事务记录签名而不是由计费器盒 44 进行的计费器记录签名。之后，当请求下一次事务时，事务盒 42 要核验该事务记录签名。

现在参照图 2，该图示出了数据服务器 36 的结构，它包括计费器数据库 60、邮寄者数据库 62 和计费器记录数据库 64。计费器数据库 60 包括与每个计费器帐户相关的计费器信息，诸如计费器序号、记录更新计数、升值寄存器、降值寄存器和其它邮政值。邮寄者数据库 62 包括邮寄者信息以及将邮寄者与计费器帐户相联系的信息。

在工作过程中，通信服务器 32 从邮寄者的 PC 20 接收到一条计费器事务的请求。功能服务器 34 中的应用软件控制对事务请求的处理。功能服务器 34 访问邮寄者数据库 62 和计费器数据库 60，以获得包括适当计费器记录 64 的各种记录，这些记录对应于发出请求的邮寄者的计费器帐户。功能服务器 34 将来自邮

寄者数据库 62 的邮寄者记录发送给验证盒 40，然后验证盒 40 对请求事务的邮寄者进行验证。一旦验证了邮寄者，那么功能服务器 34 将合适的计费器记录 64 发送给计费器盒 44，计费器盒 44 对记录的签名和新数据进行核验。计费器盒 44 对存储在计费器记录 64 内的加密密钥解密，在计费器记录 64 中的升值和降值寄存器上完成计帐功能，并用密钥为所请求的事务产生一令牌。然后，计费器盒 44 产生邮戳数据，并再次对计费器记录 64 签名。然后，将更新后和经签名的记录发送回数据库服务器 36，将其作为计费器数据库 60 的一部分存储起来。

在数据中心 30，在明码文本中不能获得验证密钥，但必须将其分配给邮寄者。可以使用常规的为每位邮寄者分配和更新验证密钥的方法。例如，参见上述美国专利申请第 08/553,812 号，该申请描述了一种用于向保密盒和邮寄者 PC 机分配和更新加密密钥的密钥管理系统。

密钥管理系统 38 的重要任务之一是，获得邮政密钥并将其与卖家密钥相联系。在密钥管理系统 38 中，钢盒为每个计费器帐户在一个计费器记录 64 中产生一个计费器序号、制造号、卖家和邮政密钥。

对于加密/解密运算，用一组三个 DES 密钥对加密密钥加密，从而产生邮戳的令牌或签名。用另一组三个 DES 密钥对计费器记录签字。计费器盒 44 安全地存储这两组三个 DES 密钥。为了避免只使用一个密钥来对整个计费器密钥组加密而生成邮戳的令牌或签名，可以使用一个导出密钥。第一组三个 DES 密钥通过对每条计费器记录中的计费(计帐)序号加密来导出三个 DES 密钥。然后，被导出的三个 DES 密钥对将被存储在数据库服务器 36 中的邮戳的加密密钥加密。用于签字的第二组三个 DES 密钥使用类似的方案，以类似方式导出签名密钥，即把计费序号当作数据来导出密钥。应该理解，可以用一组三个 DES 密钥来实现两个目的。但是，希望每组密钥只用于一个目的。

在本发明的较佳实施例中，可用一个公用密钥对要求数字签名的所有事务和记录签字，诸如计费器记录、邮政事务、资金转帐记录、主计帐记录等。将每个盒中的多个盒用于冗余，并用于分担事务数量增长时的工作量。诸如计费器盒 44 或验证盒 40 等签字盒还将核验记录的签名。

关于计费器记录 64 的签名运算，可以用消息验证代码(MAC)为敏感的虚拟计费器记录提供消息的完整性。该 MAC 包括数据加密标准(DES)的多个应用。用当前的年月更新签名密钥。在制造期间，把两个初始的主密钥输入计费器盒 44 的

非易失性存储器(NVM)中。NVM 用于永久存储和防止外界获取密钥信息两个方面。可以用诸如上面描述的常规方式导出邮戳密钥和签名密钥。虚拟计费器记录签名核验运算简单地用计费器记录 64 内的签名运算和数据重新计算计费器记录 64 的签名，并将计算得到的签名与计费器记录 64 中的签名比较。

现在参照图 3，描述在虚拟邮资计费系统中安全地进行邮资证明事务的过程。在步骤 100，通信服务器 32 从邮寄者 PC 20 接收邮资证明请求，在步骤 105，功能服务器 34 请求访问存储在数据库服务器 36 中的邮寄者帐户信息。在步骤 110，数据库服务器 36 发送邮寄者信息和计费器信息(包括与发出请求的邮寄者有关的计费器记录)。在步骤 115，功能服务器 34 将邮寄者信息发送给验证盒 40。当在步骤 120 对邮寄者验证时，然后在步骤 125，功能服务器 34 将包括计费器记录的计费器信息发送给计费器盒 44。在步骤 130，计费器盒 44 验证计费器记录，对作为记录一部分的加密令牌密钥解密，核验记录的新度，进行计帐，产生令牌，更新新数据并对计费器记录签名，然后将其送回功能服务器 34。在步骤 135，功能服务器 34 将更新后的、经签名的计费器记录发送给数据库服务器 36，并将产生邮戳所需的令牌和相关邮政信息发送给通信服务器 32。在步骤 140，数据库服务器 36 存储更新后的、经签名的计费器记录。在步骤 145，通信服务器 32 将令牌和邮政信息发送给邮寄者 PC 20。

现在参照图 4，描述在虚拟邮资计费系统的保密计费器盒内执行的过程。在步骤 200，计费器盒 44 接收经签名的计费器记录。在步骤 205，核验计费器记录的签名。如果在步骤 210 未被核验通过，那么在步骤 215，计费器盒终止事务，并向功能服务器 34 报警可能有窜改。如果签名被核验通过，那么在步骤 220，计费器盒将为每个计费器帐户存储在计费器盒中的新数据与作为计费器记录一部分存储起来的新数据比较。选择用于该比较的新数据必须是每次事务的专用数据。在较佳实施例中，使用记录更新计数器，但也可以使用随机数、时间标记或其它现时标志。步骤 220 进行的比较过程防止在虚拟邮资计费事务期间无意或故意地用当前计费器记录代替旧的计费器记录。

在步骤 225，如果被比较的新数据不一致，那么在步骤 230，计费器盒终止事务，并向功能服务器 34 报警可能有窜改。如果存储在计费器记录中的新数据与存储在计费器盒中的与计费器记录相关的新数据一致，那么在步骤 235，计费器盒对作为计费器记录一部分并按加密形式接收到的令牌密钥解密。在步骤

240，计费器盒完成对事务的计帐功能，诸如使升值寄存器增加，降值寄存器减小，并使记录更新计数器增加。在步骤 245，更新计费器记录中的新数据。在步骤 250，更新存储在计费器盒 44 中的新数据。在步骤 255，计费器盒用经解密的令牌密钥产生令牌。在步骤 260，计费器盒通过把新的寄存器值和记录更新计数存储在计费器记录中，对计费器记录进行更新，然后用存储在计费器记录盒中的密钥对更新后的记录签字。在步骤 265，计费器盒将更新后的、经签字的计费器记录发送给数据库服务器 36，用于存储，直至该计费器帐户的下一次事务分配给计费器记录。

不用说，尽管将本发明的实施例描述为邮资计费系统，但本发明适用于包括事务证明的任何计值系统，诸如货币事务、项目事务和信息事务等。

尽管已参照实施例描述和揭示了本发明，但如上所述，显然可以进行各种改变和变化，诸如用公开密钥代替私人密钥。因此，意图是使以下的权利要求书覆盖每一种落在本发明真实精神和范围内的变化和修改。

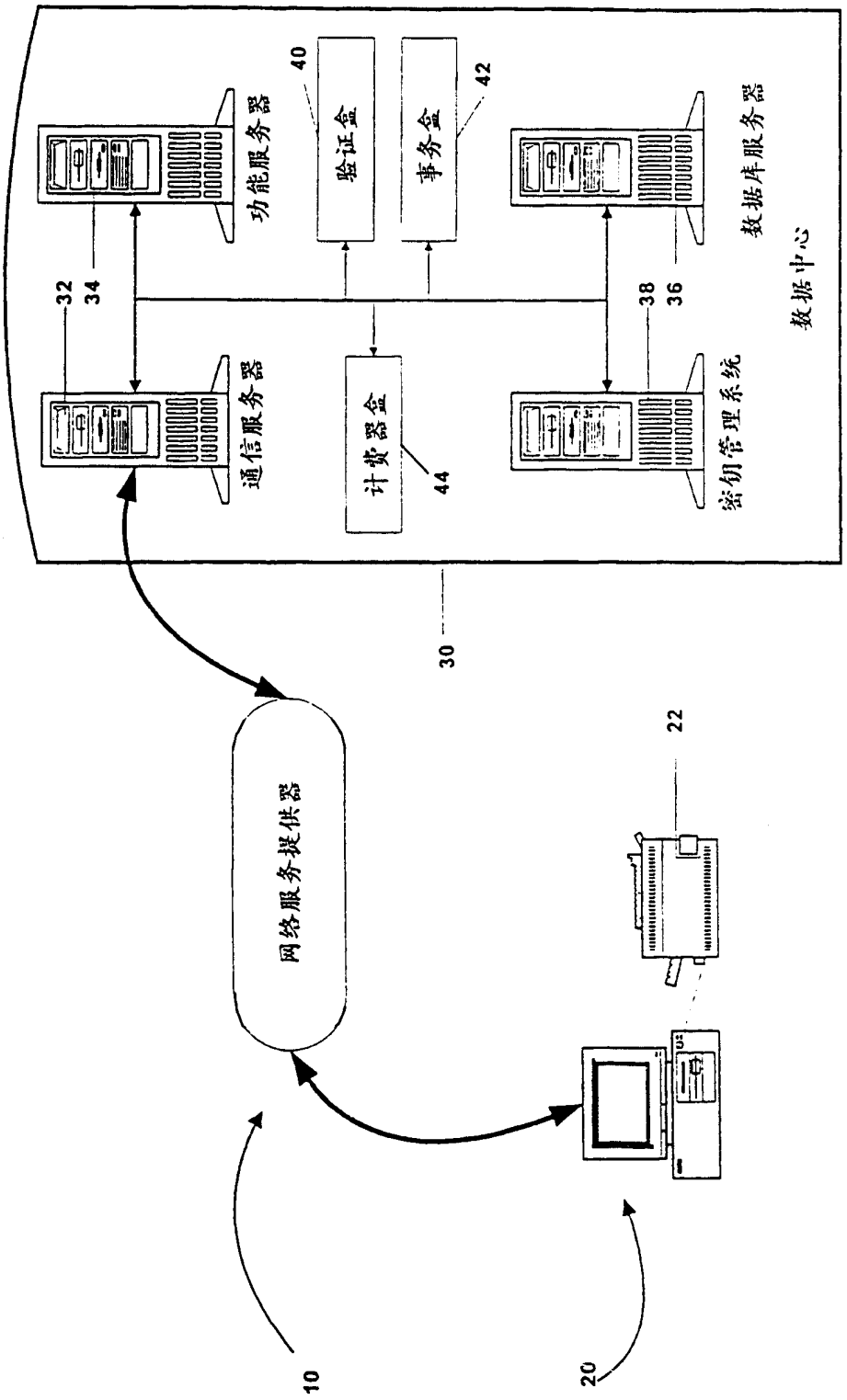

数据中心
功能服务器
通信服务器
验证盒
事务盒
计费器盒
数据库服务器
密钥管理系统
网络服务提供器
10
20
22
30
32
34
36
38
40
42
44

图 1

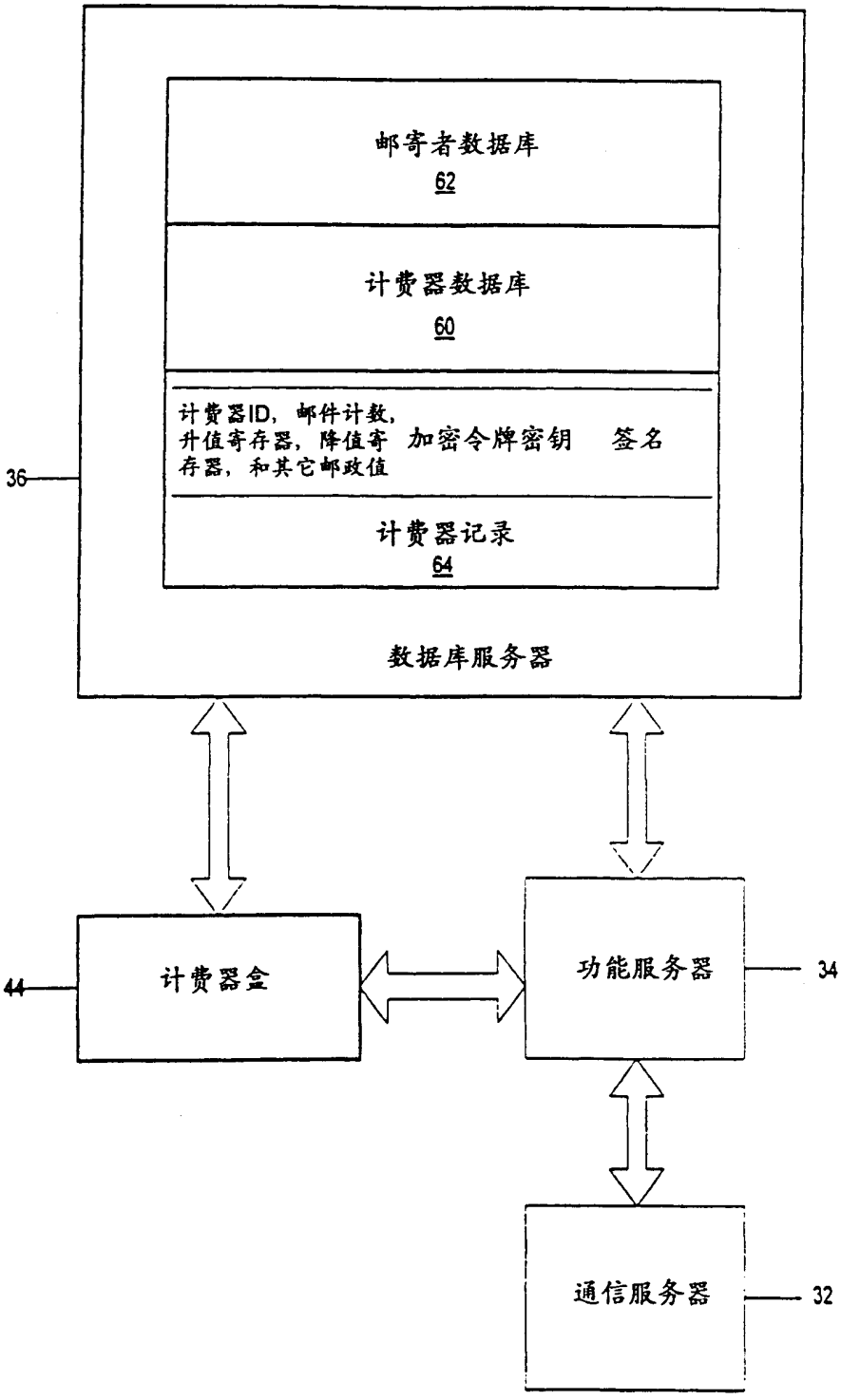

邮寄者数据库
62
计费器数据库
60
计费器ID，邮件计数，
升值寄存器，降值寄存器，和其它邮政值
加密令牌密钥
签名
计费器记录
64
36
数据库服务器
计费器盒
44
功能服务器
34
通信服务器
32

图 2

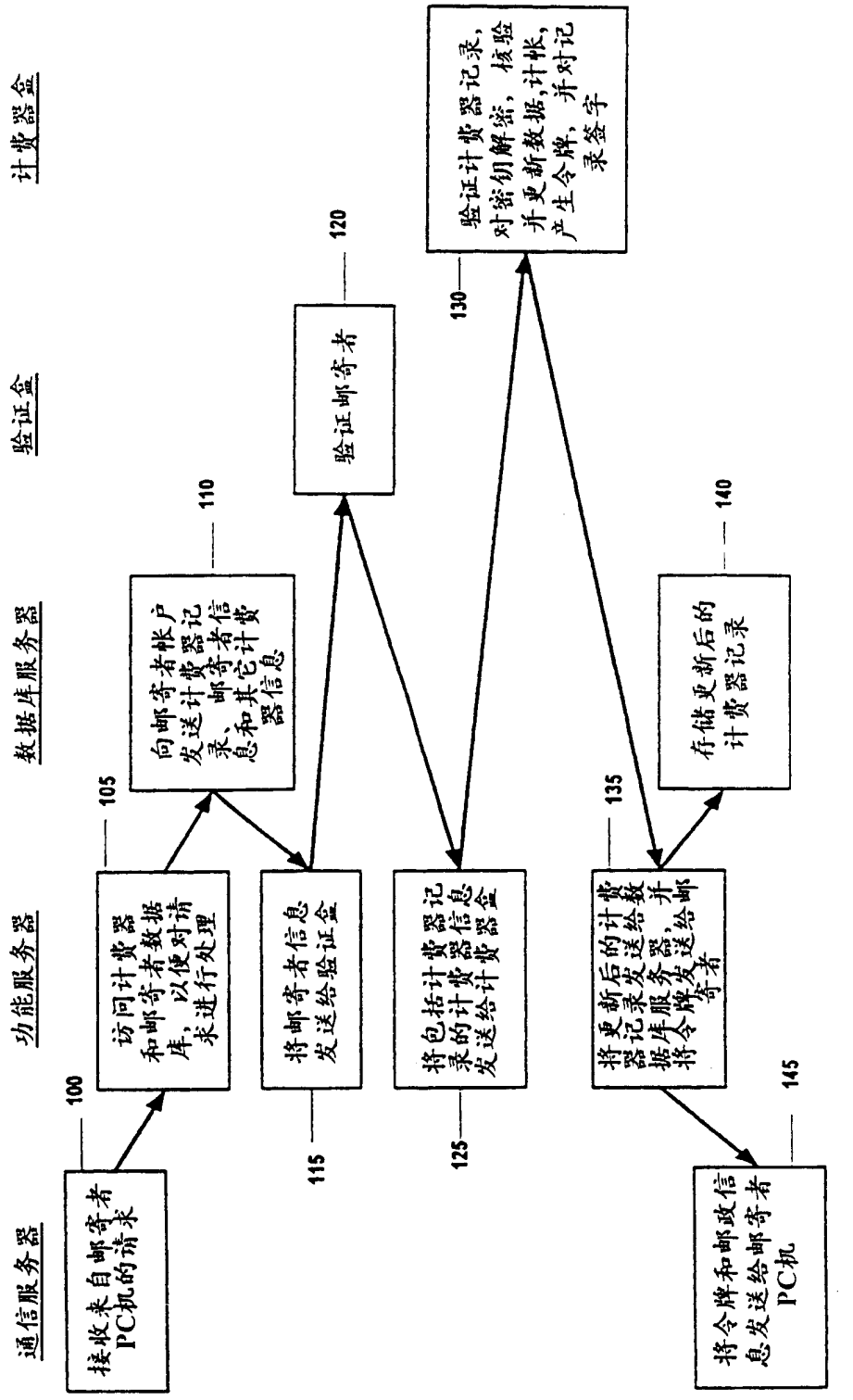

通信服务器
功能服务器
数据库服务器
验证盒
计费器盒
接收来自邮寄者PC机的请求
100
访问计费器和邮寄者数据库，以便对请求进行处理
105
向邮寄者帐户发送计费器记录、邮寄者信息和其它计费器信息
110
将邮寄者信息发送给验证盒
115
验证邮寄者
120
将包括计费器记录的计费信息发送给计费器盒
125
验证计费器记录，对密钥解密，核验并更新数据，计帐，产生令牌，并对记录签字
130
将更新后的计费器记录发送给数据库服务器，并将令牌发送给邮寄者
135
存储更新后的计费器记录
140
将令牌和邮政信息发送给邮寄者PC机
145

图 3

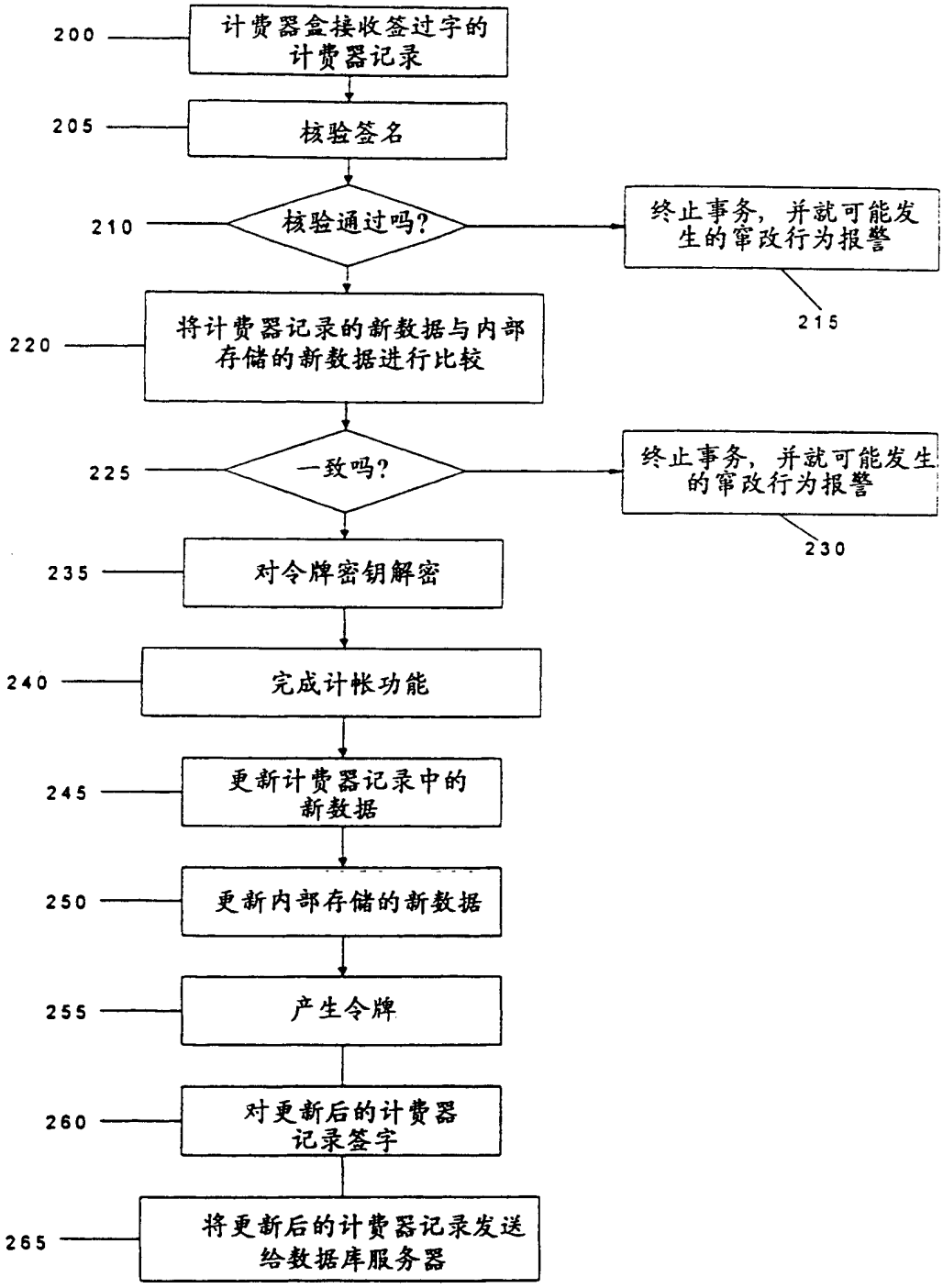

200
计费器盒接收签过字的计费器记录
205
核验签名
210
核验通过吗?
终止事务，并就可能发生的窜改行为报警
215
220
将计费器记录的新数据与内部存储的新数据进行比较
225
一致吗?
终止事务，并就可能发生的窜改行为报警
230
235
对令牌密钥解密
240
完成计帐功能
245
更新计费器记录中的新数据
250
更新内部存储的新数据
255
产生令牌
260
对更新后的计费器记录签字
265
将更新后的计费器记录发送给数据库服务器

图 4