[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06Q 10/00 (2006.01)
G06Q 30/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610138600.X

[43] 公开日 2008 年 5 月 21 日

[11] 公开号 CN 101183439A

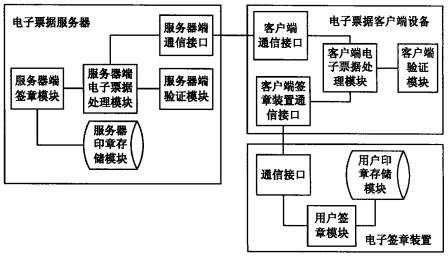
[22] 申请日 2006.11.14
[21] 申请号 200610138600.X
[71] 申请人 中国民生银行股份有限公司
地址 100031 北京市西城区复兴门内大街 2 号
[72] 发明人 宋 涛
[74] 专利代理机构 北京同立钧成知识产权代理有限公司
代理人 刘 芳
权利要求书 8 页 说明书 11 页 附图 4 页

[54] 发明名称

电子票据处理系统及处理方法

[57] 摘要

本发明涉及电子票据服务器、客户端设备、电子签章装置、电子票据处理系统及处理方法，在生成电子印章时，根据印章图样数据生成印章信息及印章标识；获取数字证书；将印章信息与数字证书进行绑定；在签章时，记录用户电子印章在电子票据上的位置信息，使用杂凑函数对电子票据、电子印章信息及位置信息进行杂凑，利用数字证书对杂凑结果进行签名。 本发明实现了电子票据的可视化电子签章，在实现了票据电子签章的同时，具有直观的签章效果，具有完整性、不可否认性以及直观的可视化效果，真正实现了票据的电子签章。



1、 一种电子票据服务器，其中包括:

服务器端通信接口，用于与电子票据客户端设备进行信息交互;

服务器端电子票据处理模块，与所述服务器端通信接口连接，用于生成及管理电子票据;

服务器印章存储模块，用于存储服务器电子印章信息;

服务器端签章模块，与所述服务器端电子票据处理模块及服务器印章存储模块连接，用于对电子票据进行电子签章操作;

服务器端验证模块，与所述服务器端电子票据处理模块连接，用于对电子票据进行验证。

2、 根据权利要求 1 所述的电子票据服务器，其中还包括:

电子印章生成模块，与所述服务器印章存储模块连接，用于生成服务器电子印章及用户电子印章。

3、 根据权利要求 2 所述的电子票据服务器，其中还包括: 服务器端签章装置通信接口，与所述电子印章生成模块连接，用于将用户电子印章存储至与该服务器端签章装置通信接口连接的电子签章装置。

4、 根据权利要求 1 所述的电子票据服务器，其中还包括: 认证模块，用于用户身份认证及安全认证; 所述服务器端通信接口通过该认证模块与服务器端电子票据处理模块连接。

5、 根据权利要求 1 所述的电子票据服务器，其中所述服务器端电子票据处理模块包括:

服务器端数据处理模块，与所述服务器端通信接口、服务器端签章模块以及服务器端验证模块连接，用于根据服务器端通信接口接收的业务请求生成电子票据，通过服务器端签章模块对电子票据进行电子签章操作，以及通过服务器端验证模块对电子票据进行验证;

服务器端电子票据数据库，与所述服务器端数据处理模块连接，用于存

储电子票据模版以及已签章的电子票据;

电子票据查询模块，与所述服务器端电子票据数据库连接，用于查询已签章的电子票据。

6、 一种电子票据客户端设备，其中包括:

客户端通信接口，用于与电子票据服务器进行信息交互;

客户端签章装置通信接口，用于与连接的电子签章装置进行信息交互;

客户端电子票据处理模块，与所述客户端通信接口及客户端签章装置通信接口连接，用于生成业务请求、处理电子票据，对电子签章装置中的电子印章进行验证，以及使用电子签章装置对电子票据进行电子签章操作;

客户端验证模块，与所述客户端电子票据处理模块连接，用于对电子票据进行验证。

7、 根据权利要求 6 所述的电子票据客户端设备，其中所述客户端电子票据处理模块包括:

客户端数据处理模块，与所述客户端通信接口、客户端签章装置通信接口以及客户端验证模块连接，用于生成业务请求，处理电子票据，通过客户端签章装置通信接口使用电子签章装置对电子票据进行电子签章操作，以及通过客户端验证模块对电子票据进行验证;

印章验证模块，与所述客户端数据处理模块连接，用于对电子印章进行验证;

客户端电子票据数据库，与所述客户端数据处理模块连接，用于存储已签章的电子票据。

8、 一种电子签章装置，其中包括:

通信接口，用于连接到电子票据客户端设备，并与电子票据客户端设备进行信息交互;

用户印章存储模块，用于存储用户的电子印章信息;

用户签章模块，与所述通信接口及用户印章存储模块连接，用于对电子

票据进行电子签章操作。

9、一种电子票据处理系统，其中包括:

电子票据服务器，用于提供电子票据服务，生成及管理电子票据，对电子票据进行电子签章操作，以及验证电子签章；该电子票据服务器包括:

服务器端通信接口，用于与电子票据客户端设备进行信息交互;

服务器端电子票据处理模块，与所述服务器端通信接口连接，用于生成及管理电子票据;

服务器印章存储模块，用于存储服务器电子印章信息;

服务器端签章模块，与所述服务器端电子票据处理模块及服务器印章存储模块连接，用于对电子票据进行电子签章操作；以及

服务器端验证模块，与所述服务器端电子票据处理模块连接，用于对电子票据进行验证;

电子票据客户端设备，与所述电子票据服务器连接，用于使用电子票据服务器提供的电子票据服务；该电子票据服务器包括:

客户端通信接口，用于与电子票据服务器进行信息交互;

客户端签章装置通信接口，用于与连接的电子签章装置进行信息交互;

客户端电子票据处理模块，与所述客户端通信接口及客户端签章装置通信接口连接，用于生成业务请求、处理电子票据，对电子签章装置中的电子印章进行验证，以及使用电子签章装置对电子票据进行电子签章操作;

客户端验证模块，与所述客户端电子票据处理模块连接，用于对电子票据进行验证;

电子签章装置，与所述电子票据客户端设备连接，用于存储用户电子印章以及使用用户电子印章对电子票据进行电子签章操作；该电子签章装置包括:

通信接口，用于连接到电子票据客户端设备，并与电子票据客户端设备进行信息交互；

用户印章存储模块，用于存储用户电子印章；

用户签章模块，与所述通信接口及用户印章存储模块连接，用于使用用户电子印章对电子票据进行电子签章操作。

10、 根据权利要求 9 所述的电子票据处理系统，其中所述电子票据服务器还包括：

电子印章生成模块，与所述服务器印章存储模块连接，用于生成服务器电子印章及用户电子印章。

11、 根据权利要求 10 所述的电子票据处理系统，其中所述电子票据服务器还包括：服务器端签章装置通信接口，与所述电子印章生成模块连接，用于将用户电子印章存储至与该服务器端签章装置通信接口连接的电子签章装置。

12、 根据权利要求 9 所述的电子票据处理系统，其中所述电子票据服务器还包括：认证模块，用于用户身份认证及安全认证；所述服务器端通信接口通过该认证模块与服务器端电子票据处理模块连接。

13、 根据权利要求 9 所述的电子票据处理系统，其中所述服务器端电子票据处理模块包括：

服务器端数据处理模块，与所述服务器端通信接口、服务器端签章模块以及服务器端验证模块连接，用于根据服务器端通信接口接收的业务请求生成电子票据，通过服务器端签章模块对电子票据进行电子签章操作，以及通过服务器端验证模块对电子票据进行验证；

服务器端电子票据数据库，与所述服务器端数据处理模块连接，用于存储电子票据模版以及已签章的电子票据；

电子票据查询模块，与所述服务器端电子票据数据库连接，用于查询已签章的电子票据。

14、 根据权利要求 9 所述的电子票据处理系统，其中所述客户端电子票据处理模块包括:

客户端数据处理模块，与所述客户端通信接口、客户端签章装置通信接口以及客户端验证模块连接，用于生成业务请求，处理电子票据，通过客户端签章装置通信接口使用电子签章装置对电子票据进行电子签章操作，以及通过客户端验证模块对电子票据进行验证;

印章验证模块，与所述客户端数据处理模块连接，用于对电子印章进行验证;

客户端电子票据数据库，与所述客户端数据处理模块连接，用于存储已签章电子票据。

15、 一种电子票据处理方法，其中包括:

电子票据服务器生成电子印章的步骤;

电子票据服务器生成电子票据的步骤; 以及

电子票据服务器和/或电子票据客户端设备对电子票据进行电子签章操作的步骤。

16、 根据权利要求 15 所述的电子票据处理方法，其中所述的生成电子印章的步骤包括: 生成用户电子印章的步骤以及生成服务器电子印章的步骤。

17、 根据权利要求 16 所述的电子票据处理方法，其中所述的生成用户电子印章的步骤具体包括:

根据印章图样数据生成印章信息及印章标识的步骤;

为用户分配数字证书的步骤;

根据用户数字证书密钥标识号、用户识别名、印章信息、印章标识生成认证信息的步骤;

将所述印章信息、印章标识、认证信息以及用户的数字证书保存为用户电子印章并存储到用户的电子签章设备的步骤。

18、 根据权利要求 17 所述的电子票据处理方法，其中所述的根据用户

数字证书密钥标识号、用户识别名、印章信息、印章标识生成认证信息的步骤为：使用系统私钥对用户数字证书密钥标识号、用户识别名、印章信息、印章标识进行签名生成认证信息。

19、 根据权利要求 15 所述的电子票据处理方法，其中所述的电子票据客户端设备对电子票据进行电子签章操作的步骤包括：

电子票据客户端设备验证用户电子印章的有效性的步骤；

当用户电子印章有效时，电子票据客户端设备使用用户电子印章对电子票据进行电子签章操作的步骤。

20、 根据权利要求 19 所述的电子票据处理方法，其中所述的验证用户电子印章的有效性的步骤具体为：解开签名，判断电子印章是否为电子票据服务器生成的；从用户电子印章中提取印章信息、印章标识、用户数字证书密钥标识号及用户识别名，进行杂凑运算，将杂凑结果与揭开签名得到的结果进行比对，如果一致，则用户电子印章有效，否则，用户电子印章无效。

21、 根据权利要求 19 所述的电子票据处理方法，其中所述的使用用户电子印章对电子票据进行电子签章操作的步骤具体为：记录用户电子印章在电子票据上的位置信息，使用杂凑函数对电子票据、用户电子印章及位置信息进行杂凑，利用用户数字证书对杂凑结果进行签名。

22、 根据权利要求 21 所述的电子票据处理方法，其中还包括：电子票据服务器接收电子票据客户端设备发送的进行了电子签名的电子票据，生成包含有用户电子印章信息和签名信息的已签章电子票据，保存并发送至电子票据客户端设备。

23、 根据权利要求 16 所述的电子票据处理方法，其中所述的生成服务器电子印章的步骤具体包括：

根据印章图样数据生成印章信息及印章标识的步骤；

获取服务器数字证书的步骤；

分配印章编号的步骤；

保存印章编号、印章信息、印章标识、服务器数字证书及密钥的步骤。

24、 根据权利要求 23 所述的电子票据处理方法，其中还包括电子票据服务器记录生成的服务器电子印章的数目。

25、 根据权利要求 24 所述的电子票据处理方法，其中所述的根据印章图样数据生成印章信息及印章标识的步骤具体为：判断已生成的服务器电子印章的数目是否已达到预先设定的阈值，若未达到，则根据印章图样数据生成印章信息及印章标识。

26、 根据权利要求 15 所述的电子票据处理方法，其中所述的电子票据服务器对电子票据进行电子签章操作的步骤包括：

提取服务器电子印章信息的步骤；

使用服务器电子印章对电子票据进行电子签章操作的步骤。

27、 根据权利要求 26 所述的电子票据处理方法，其中所述的提取服务器电子印章信息的步骤具体为：根据电子票据的类型确定印章编号，根据印章编号，提取服务器电子印章。

28、 根据权利要求 26 所述的电子票据处理方法，其中所述的使用服务器电子印章对电子票据进行电子签章操作的步骤具体为：记录服务器电子印章在电子票据上的位置信息，使用杂凑函数对电子票据、服务器电子印章及位置信息进行杂凑，利用服务器数字证书对杂凑结果进行签名。

29、 根据权利要求 26 所述的电子票据处理方法，其中所述的生成服务器电子印章的步骤还包括：对服务器数字证书进行加密操作，生成加密的服务器数字证书及密钥的步骤。

30、 根据权利要求 29 所述的电子票据处理方法，其中所述的电子票据服务器对电子票据进行电子签章操作的步骤还包括，电子票据服务器对服务器数字证书及密钥进行解密。

31、 根据权利要求 17-30 任一所述的电子票据处理方法，其中所述的根据印章图样数据生成印章信息及印章标识的步骤包括：

根据印章图样数据生成印章信息的步骤；以及

根据印章信息生成印章标识的步骤。

32、 根据权利要求 31 所述的电子票据处理方法，其中所述的根据印章图样数据生成印章信息的步骤具体为：对印章图样数据进行压缩或/和加密生成印章信息。

33、 根据权利要求 31 所述的电子票据处理方法，其中所述的根据印章信息生成印章标识的步骤具体为：使用杂凑函数对所述印章信息进行杂凑，将得到的杂凑结果作为印章标识。

34、 根据权利要求 17-30 任一所述的电子票据处理方法，其中还包括：电子票据服务器和/或电子票据客户端设备对已签章电子票据的完整性进行验证的步骤，具体包括：电子票据服务器和/或电子票据客户端使用杂凑函数对电子票据、电子印章及位置信息进行杂凑，使用数字签名携带的公钥对签名解密，比对杂凑结果及解密结果，若二者一致，则该已签章电子票据是完整的。

35、 根据权利要求 17-30 任一所述的电子票据处理方法，其中还包括：电子票据服务器和/或电子票据客户端设备对已签章电子票据的电子印章有效性进行验证的步骤，具体包括：解开电子印章签名，判断电子印章是否为电子票据服务器生成的；从用户电子印章中提取印章信息、印章标识、用户数字证书密钥标识号及用户识别名，进行杂凑运算，将杂凑结果与解开签名得到的结果进行比对，如果一致，则用户电子印章有效，否则，用户电子印章无效。

36、 根据权利要求 17-30 任一所述的电子票据处理方法，其中还包括：电子票据客户端设备向电子票据服务器查询电子票据的步骤。

电子票据处理系统及处理方法

技术领域

本发明涉及电子票据处理技术，尤其涉及能够进行电子签章的电子票据处理系统及电子票据处理方法。

背景技术

现有的票据普遍以纸质、实物化的物理形式存在，这造成一些困扰着票据使用者的问题难以得到解决，例如：票据真伪辨别困难；票据查询效果不佳、效率低下；票据流转和保管过程的风险控制成本高；二级市场交易效率低，无法实现信息透明的集中交易，公平价格难以形成；票据托收环节多、资金回收周期难以确定，等等。这些问题直接限制了票据业务的发展，也与信息时代的科技发展水平不相适应。

现在出现了一些电子票据系统，业务人员可以通过计算机输入数据信息，电子化的票据信息存储于系统中，并可通过与计算机直接连接的打印机或通过网络与计算机连接的打印机将电子票据打印出来。利用这种电子票据系统，相关人员不必再手工填写票据，在向系统输入数据的同时就可完成票据填写，可有效提高工作效率，避免重复劳动。但这种电子票据系统仍然存在一些问题：它只是实现了票据在系统内部的电子化，当需要将票据需要在两方或多方间流转时，仍需将票据打印出来进行签章，然后将纸质票据传送给他方。

随着信息技术的发展，人们开始使用数字签名技术对电子文件进行迅速的、远距离的签名。目前的数字签名技术的研究主要是基于公钥密码体制，比较著名的数字签名算法包括RSA、ElGmal、Schnorr等。密钥主要是通过可信机构，如认证中心（Certificate Authority，以下简称CA），以证书的方

式颁发给用户。

一般来说，数字签名是用户用自己的私钥对原始数据的杂凑（hash）摘要进行加密所得的数据。信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后获得杂凑摘要，并通过与自己用收到的原始数据产生的杂凑摘要对照，便可确信原始信息是否被篡改，保证了数据的完整性。另外，由于在理论上只有发送者才唯一拥有私钥，只有发送者才可能产生该数字签名，因此可保证发送者的真实性；也由于只有发送者才可能产生该数字签名，所以只要数字签名通过验证，发送者就不能否认曾发送过该消息，这样数字签名后的数据具有不可否认性。数字签名在电子商务、电子政务等方面有着广泛的应用，但是，目前的数字签名还不具备类似传统手工签名的直观视觉效果，若利用现有的数字签名技术对电子票据进行电子签章操作，虽然可以对电子票据数据的完整性、真实性以及不可否认性进行验证，但是操作人员在浏览相关电子文件时并不能直观方便地看到票据是否已被执行电子签章操作，亦即签章者是谁。

发明内容

本发明的目的在于针对现有技术所存在的问题，提供电子票据服务器、电子票据客户端、电子签章装置、电子票据处理系统及电子票据处理方法，实现电子票据的电子化签章，并且具有直观的签章效果，从而真正实现票据的电子化。

为了实现上述目的，本发明提供了电子票据服务器，电子票据客户端设备，电子签章装置，由所述电子票据服务器、电子票据客户端设备、电子签章装置构成的电子票据处理系统，以及电子票据处理方法。

本发明的电子票据服务器包括：服务器端通信接口，用于与电子票据客户端设备进行信息交互；服务器端电子票据处理模块，与所述服务器端通信接口连接，用于生成及管理电子票据；服务器印章存储模块，用于存储服务

器电子印章信息；服务器端签章模块，与所述服务器端电子票据处理模块及服务器印章存储模块连接，用于对电子票据进行电子签章操作；服务器端验证模块，与所述服务器端电子票据处理模块连接，用于对电子票据进行验证。

本发明的电子票据客户端设备包括：客户端通信接口，用于与电子票据服务器进行信息交互；客户端签章装置通信接口，用于与连接的电子签章装置进行信息交互；客户端电子票据处理模块，与所述客户端通信接口及客户端签章装置通信接口连接，用于生成业务请求、处理电子票据，对电子签章装置中的电子印章进行验证，以及使用电子签章装置对电子票据进行电子签章操作；客户端验证模块，与所述客户端电子票据处理模块连接，用于对电子票据进行验证。

本发明的电子签章装置包括：通信接口，用于连接到电子票据客户端设备，并与电子票据客户端设备进行信息交互；用户印章存储模块，用于存储用户的电子印章信息；用户签章模块，与所述通信接口及用户印章存储模块连接，用于对电子票据进行电子签章操作。

本发明的电子票据处理方法包括：

电子票据服务器生成电子印章的步骤；

电子票据服务器生成电子票据的步骤；以及

电子票据服务器和/或电子票据客户端设备对电子票据进行电子签章操作的步骤。

在生成用户电子印章时，根据印章图样数据生成印章信息及印章标识；为用户分配数字证书；根据用户数字证书密钥标识号、用户识别名、印章信息、印章标识生成认证信息；将所述印章信息、印章标识、认证信息以及用户的数字证书保存为用户电子印章并存储到用户的电子签章设备。

在生成服务器电子印章时，根据印章图样数据生成印章信息及印章标识；获取服务器数字证书；分配印章编号的步骤；保存印章编号、印章信息、印章标识、服务器数字证书及密钥。

在进行电子签章时，记录电子印章在电子票据上的位置信息，使用杂凑函数对电子票据、服务器电子印章及位置信息进行杂凑，利用服务器数字证书对杂凑结果进行签名。

本发明实现了电子票据的可视化电子签章，在实现了票据电子化的同时，具有直观的签章效果，从而真正实现票据的电子化签章。

下面通过附图和实施例，对本发明的技术方案做进一步的详细描述。

附图说明

图 1 为本发明的电子票据处理系统的结构示意图；

图 2 为本发明的电子票据处理方法流程图；

图 3 为本发明的电子票据服务器一具体实施例结构示意图；

图 4 为本发明的电子票据处理方法的生成用户电子印章的方法流程图；

图 5 为本发明的电子票据处理方法的生成服务器电子印章的方法流程图；

图 6 为本发明的电子票据服务器的再一具体实施例结构示意图；

图 7 为本发明的电子票据服务器的服务器端电子票据处理模块结构示意图；

图 8 为本发明的电子票据客户端设备的客户端电子票据处理模块结构示意图。

具体实施方式

本发明中的电子票据包括电子合同、票据凭证等各种电子化的需要签章的电子文件。

如图 1 所示，为本发明的电子票据处理系统的结构示意图，包括电子票据服务器、电子票据客户端设备以及电子签章装置。其中，电子票据服务器用于提供电子票据服务，即生成及管理电子票据，对电子票据进行电子签章

操作，以及验证电子签章；电子签章装置用于存储用户电子印章以及使用用户电子印章对电子票据进行电子签章操作；电子票据客户端设备用于使用电子票据服务器提供的电子票据服务，验证电子签章装置中的电子印章的有效性，并将需要使用用户电子印章进行签章的电子票据发送至电子签章装置，由电子签章装装置进行签章操作。

电子票据服务器包括：服务器端通信接口，用于通过互联网络或专用网络与电子票据客户端设备进行信息交互；服务器端电子票据处理模块，与服务器端通信接口连接，用于生成及管理电子票据；服务器印章存储模块，用于存储服务器电子印章信息；服务器端签章模块，与服务器端电子票据处理模块连接，用于对电子票据进行电子签章操作；服务器端验证模块，与服务器端电子票据处理模块连接，用于对电子票据进行验证。

电子票据客户端设备包括：客户端通信接口，用于与电子票据服务器进行信息交互；客户端签章装置通信接口，用于与连接的电子签章装置进行信息交互；客户端电子票据处理模块，与客户端通信接口及客户端签章装置通信接口连接，用于生成业务请求、处理电子票据，对电子签章装置中的电子印章进行验证，以及使用电子签章装置对电子票据进行电子签章操作；客户端验证模块，与客户端电子票据处理模块连接，用于对电子票据进行验证。

电子签章装置包括：通信接口，用于连接到电子票据客户端设备，并与电子票据客户端设备进行信息交互；用户印章存储模块，用于存储用户电子印章；用户签章模块，与所述通信接口及用户印章存储模块连接，用于使用用户电子印章对电子票据进行电子签章操作。数字签名在电子签章装置内部进行，从而可保证电子印章及数字证书的安全性。

如图 2 所示，为本发明的电子票据处理方法流程图，包括如下步骤：

步骤 1、电子票据服务器生成电子印章；

步骤 2、电子票据服务器生成电子票据；

步骤 3、电子票据服务器和/或电子票据客户端设备对电子票据进行电子

签章操作。

如图 3 所示，为本发明的电子票据服务器一具体实施例结构示意图，进一步加入了用于生成电子印章的电子印章生成模块，该模块与服务器印章存储模块连接，可生成服务器进行电子签章所用的服务器电子印章，以及用户进行电子签章是所用的用户电子印章。

如图 4 所示，为本发明的电子票据处理方法的生成用户电子印章的方法流程图，包括如下步骤:

步骤 111、根据印章图样数据生成印章信息及印章标识;

印章图样数据，可以是用户印鉴的图样数据，也可以是用户手写签名的图样数据等。用户提交的图样信息，往往采用扫描的方式获得，图样数据较大，图像精度较高，而在电子印章中，有时并不需要高精度的图片显示并且印章图样信息未加密容易被攻击者读取或篡改，所以需要对印章图样数据进行压缩和加密处理，生成印章信息。印章标识唯一标识该印章，可利用杂凑函数对印章信息进行杂凑运算（以下简称 Hash 运算），将运算结果作为印章标识。印章信息包含印章的图样数据，用于直观显示印章。

步骤 112、为用户分配数字证书;

数字证书的分配可以通过已有的认证中心实现，如中国金融认证中心（China Financial Certification Authority，以下简称 CFCA）、北京 CA、天津 CA 等; 也可以是为实现本发明而建设认证中心。

步骤 113、根据用户数字证书密钥标识号、用户识别名、印章信息、印章标识生成认证信息;

认证信息用于标识该电子印章的合法性。使用系统私钥对用户数字证书密钥标识号、用户识别名、印章信息、印章标识进行签名生成认证信息，即将用户数字证书中的密钥的标识号、用户识别名、印章信息及印章标识整体作为 Hash 函数的输入，输入产生一个 Hash 值，用系统私钥对此 Hash 值进行签名，生成认证信息。数字证书中的密钥标识号以及用户识别名是可以标识

该密钥和数字证书的特征信息，即，对于每一个密钥来说密钥的标识号是唯一的，同样，对于每一个电子证书来说它的用户识别名也是唯一的，因此，将密钥的标识号以及用户识别名与印章标识以及印章信息一起进行 Hash 运算，可以对密钥标识、用户识别名、印章标识及印章信息进行绑定。由系统进行签名可以保证电子印章的颁发者为电子票据系统，从而杜绝了攻击者伪造假印章的可能。

步骤 114、将所述印章信息、印章标识、认证信息以及用户的数字证书保存为电子印章并存储到用户的电子签章装置。

用户电子印章应存储于用户的电子签章装置上，可将电子签章装置直接与电子票据服务器连接，然后将生成的用户电子印章存储于该电子签章装置上。电子签章设备可以为具有运算和存储功能任何装置，例如，具有运算功能的 USB 存储盘，该 USB 存储盘通过 USB 接口与电子票据服务器及电子票据客户端设备连接。

电子票据服务器也可保存用户电子印章的信息，以便实时掌握发送电子印章的状态，以及验证用户与电子印章的对应关系。

如图 5 所示，为本发明的电子票据处理方法的生成服务器电子印章的方法流程图，包括如下步骤:

步骤 121、根据印章图样数据生成印章信息及印章标识;

步骤 122、获取服务器数字证书;

步骤 123、分配印章编号;

根据业务的需求，服务器端可能需要多种数字证书和多个电子印章，当存在多个电子印章时，需要为印章分配可唯一标识该印章的编号，以便在电子签章时提取相应的电子印章信息。电子印章与数字证书可一一对应，即每个电子印章绑定一个数字证书；也可多对一，即多个电子印章绑定一个数字证书。

步骤 124、保存印章编号、印章信息、印章标识、服务器数字证书及密

钥。

为了控制服务器端的电子印章，电子票据服务器可预先设置一阈值，并记录生成的服务器电子印章的数目，当需要生成服务器电子印章时，先判断已生成的服务器电子印章的数目是否已达到预先设定的阈值，若未达到，则根据印章图样数据生成印章信息及印章标识。

本发明的电子票据处理系统的用户身份认证及安全认证可通过多种方式实现。在电子票据服务器中加入专门用于用户身份认证及安全认证的认证模块，各种传输的信息通过服务器端通信接口进入时，先发送直该认证模块进行身份认证健全认证，当认证通过后，再发送至服务器端电子票据处理模块进行处理。另外，可通过与现有的具有身份认证及安全认证系统连接，发送至电子票据服务器的信息可先发送至现有认证系统，在通过认证后，再发送至电子票据服务器处理。

如图 6 所示，为本发明的电子票据服务器的再一具体实施例结构示意图，在图 4 所示实施例基础上，进一步加入了服务器端签章装置通信接口及认证模块。服务器端签章装置通信接口与电子印章生成模块连接，用于将用户电子印章存储至与该服务器端签章装置通信接口连接的电子签章装置；认证模块连接服务器端通信接口与服务器端电子票据处理模块，用于用户身份认证及安全认证。

如图 7 所示，为本发明的电子票据服务器的服务器端电子票据处理模块结构示意图，包括：服务器端数据处理模块，与服务器端通信接口、服务器端签章模块以及服务器端验证模块连接，用于根据服务器端通信接口接收的业务请求生成电子票据，通过服务器端签章模块对电子票据进行电子签章操作，以及通过服务器端验证模块对电子票据进行验证；服务器端电子票据数据库，与服务器端数据处理模块连接，用于存储电子票据模版以及已签章的电子票据；电子票据查询模块，与服务器端电子票据数据库连接，用于查询已签章的电子票据。

电子票据服务器在签署电子印章时，首先提取服务器电子印章信息，若存在多个电子印章，那么可根据待签章电子票据的类型确定电子印章编号，根据印章编号提取电子印章。然后，电子票据服务器使用服务器电子印章对电子票据进行电子签章操作，记录服务器电子印章在电子票据上的位置信息，即签章的位置，使用 Hash 函数对电子票据、服务器电子印章及位置信息进行 Hash 运算，利用服务器数字证书对杂凑结果进行签名。为了保证服务器电子印章的安全性，在生成服务器电子印章时，可对服务器数字证书进行加密操作，生成加密的服务器数字证书及密钥，此时，在进行电子签章操作前，需要对服务器数字证书及密钥进行解密。

如图 8 所示，为本发明的电子票据客户端设备的客户端电子票据处理模块结构示意图，包括：客户端数据处理模块，与客户端通信接口、客户端签章装置通信接口以及客户端验证模块连接，用于生成业务请求，处理电子票据，通过客户端签章装置通信接口使用电子签章装置对电子票据进行电子签章操作，以及通过客户端验证模块对电子票据进行验证；印章验证模块，与所述客户端数据处理模块连接，用于对电子印章进行验证；客户端电子票据数据库，与所述客户端数据处理模块连接，用于存储已签章电子票据。

电子票据客户端设备对电子票据进行电子签章操作时，先验证电子签章装置中存储的用户电子印章的有效性；当用户电子印章有效时，电子票据客户端设备才使用用户电子印章对电子票据进行电子签章操作。在验证电子印章时，先解开签名，判断用户电子印章是否为电子票据服务器生成的；若是电子票据服务器生成的，则说明该用户电子印章合法；在用户电子印章合法的情况下，从用户电子印章中提取印章信息、印章标识、用户数字证书密钥标识号及用户识别名，进行 Hash 运算，将 Hash 值与解开签名得到的结果进行比对，如果一致，则用户电子印章有效，否则，用户电子印章无效。当用户电子印章有效时，可利用该用户电子印章进行电子签章操作，记录用户电子印章在电子票据上的位置信息，使用 Hash 函数对电子票据、用户电子印章

及位置信息进行 Hash 运算，利用用户数字证书对 Hash 值进行签名。电子票据服务器接收电子票据客户端设备发送的进行了电子签名的电子票据，生成包含有用户电子印章信息和签名信息的已签章电子票据，保存并发送至电子票据客户端设备。

本发明在保证传统的数字签名特性的基础上还能使签章具备类似传统签名的直观视觉效果，即在保证签名的完整性、真实性以及不可否认性的前提下还能使签章具备类似传统签名的直观视觉效果。

对于已签章的电子票据，电子票据服务器和电子票据客户端设备均可对票据的完整性及印章的有效性进行验证。在对已签章电子票据的完整性进行验证时，使用 Hash 函数对电子票据、电子印章及位置信息进行 Hash 运算；解开签名；比对 Hash 值及解开的签名，若二者一致，则该已签章电子票据是完整的。在对已签章电子票据上的用户电子印章有效性进行验证时，解开认证信息中的签名，判断电子印章是否为电子票据服务器生成的；从用户电子印章中提取印章信息、印章标识、用户数字证书密钥标识号及用户识别名，进行杂凑运算，将杂凑结果与解开签名得到的结果进行比对，如果一致，则用户电子印章有效，否则，用户电子印章无效。

电子票据服务器保存所有已签章的电子票据，电子票据客户端设备可保存预期有关的已签章电子票据。电子票据服务器提供电子票据查询功能，在电子票据客户端设备向电子票据服务器查询电子票据时，根据查询的电子票据的标识提取相应的电子票据返回客户端设备。

当系统采用浏览器/服务器结构模式时，可使用 ActiveX 控件技术。用户通过电子票据客户端设备登录电子票据服务器后，打开需要签章的 Web 页面，填写信息，在用户完成填写并确认无误后，向电子票据服务器提交 Web 页面。电子票据服务器生成不带输入域的确认页面（静态页面），并在页面中嵌入 ActiveX 控件，ActiveX 控件在页面上可体现为透明显示的样章，Active 空间在苦湖浏览器初次显示该页面时自动下载到客户端设备。页面中添加两个

隐藏域，分别用于存放客户签章图像信息和签名信息。在执行签章操作时，首先对电子签章装置中的电子印章的有效性进行验证，然后在数字签章装置中进行电子签章。签章成功后，Web 网页中相应位置显示电子印章的印章图样。签章图像信息和签名信息通过页面中的 2 个隐藏域保存并提交给电子票据服务器。电子票据服务器生成带有电子印章和认证信息的验证页面，该验证页面中也嵌入了 ActiveX 控件，包含经过了压缩和加密的用户印章图像和签名信息，并可添加自动和手动验证函数。

最后应当说明的是：以上实施例仅用以说明本发明的技术方案而非对其限制；尽管参照较佳实施例对本发明进行了详细的说明，所属领域的普通技术人员应当理解，依然可以对本发明的具体实施方式进行修改或者对部分技术特征进行等同替换；而不脱离本发明技术方案的精神，其均应涵盖在本发明请求保护的技术方案范围当中。

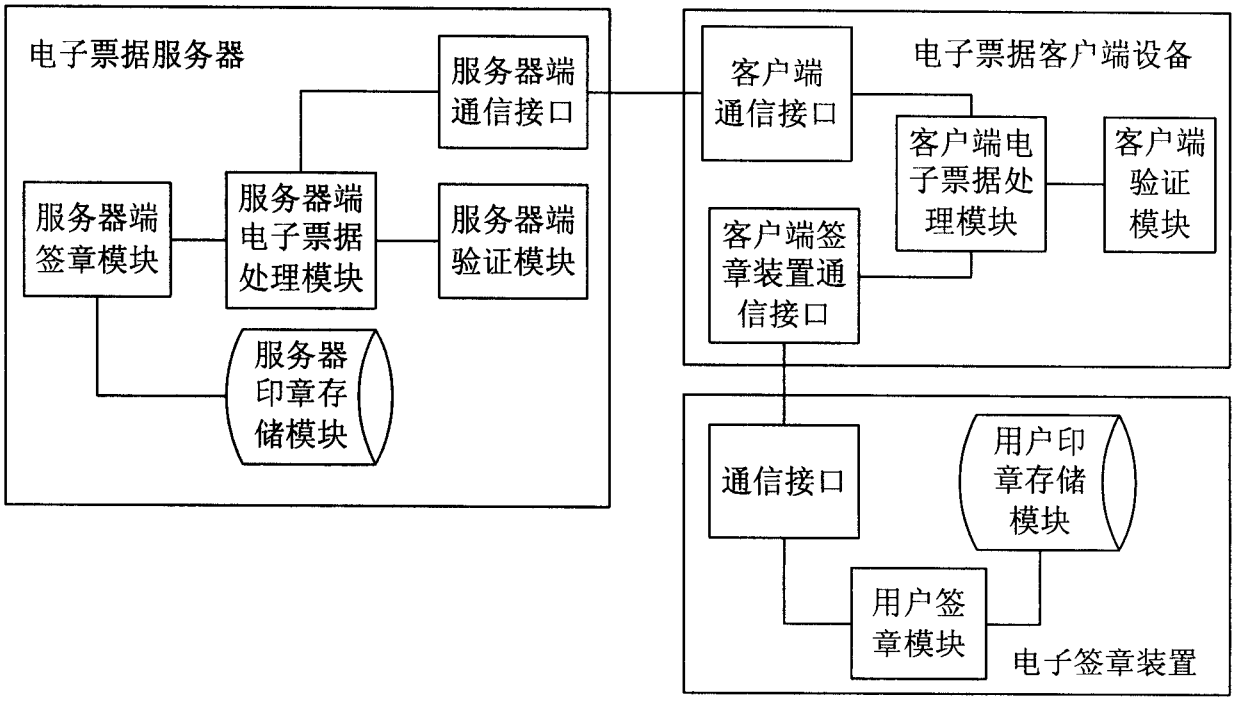

电子票据服务器
服务器端通信接口
服务器端签章模块
服务器端电子票据处理模块
服务器端验证模块
服务器印章存储模块
电子票据客户端设备
客户端通信接口
客户端电子票据处理模块
客户端验证模块
客户端签章装置通信接口
通信接口
用户印章存储模块
用户签章模块
电子签章装置

图 1

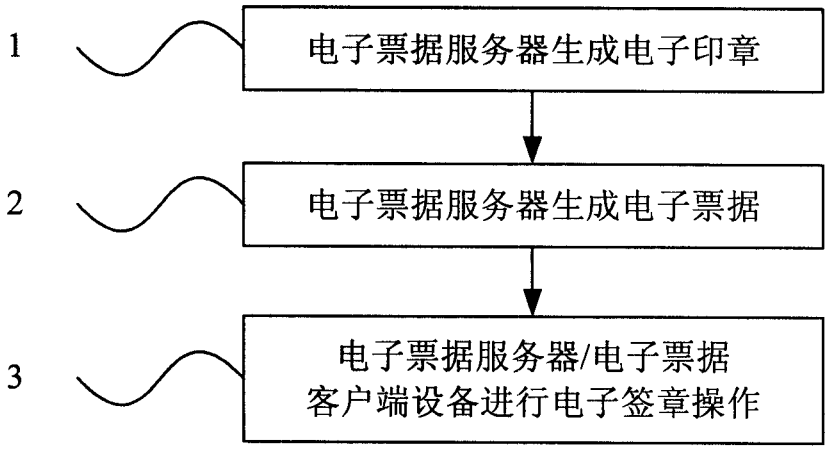

1
电子票据服务器生成电子印章
2
电子票据服务器生成电子票据
3
电子票据服务器/电子票据客户端设备进行电子签章操作

图 2

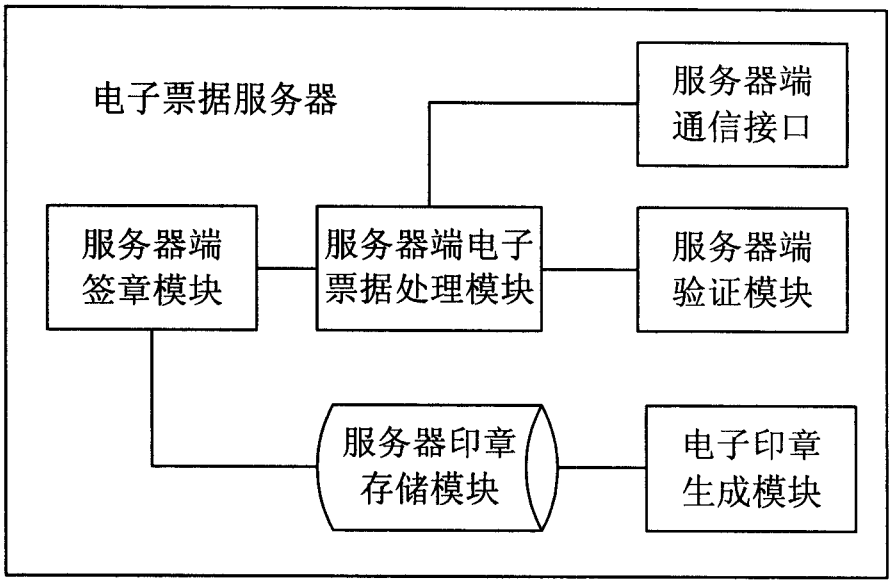

电子票据服务器
服务器端
通信接口
服务器端
签章模块
服务器端电子
票据处理模块
服务器端
验证模块
服务器印章
存储模块
电子印章
生成模块

图 3

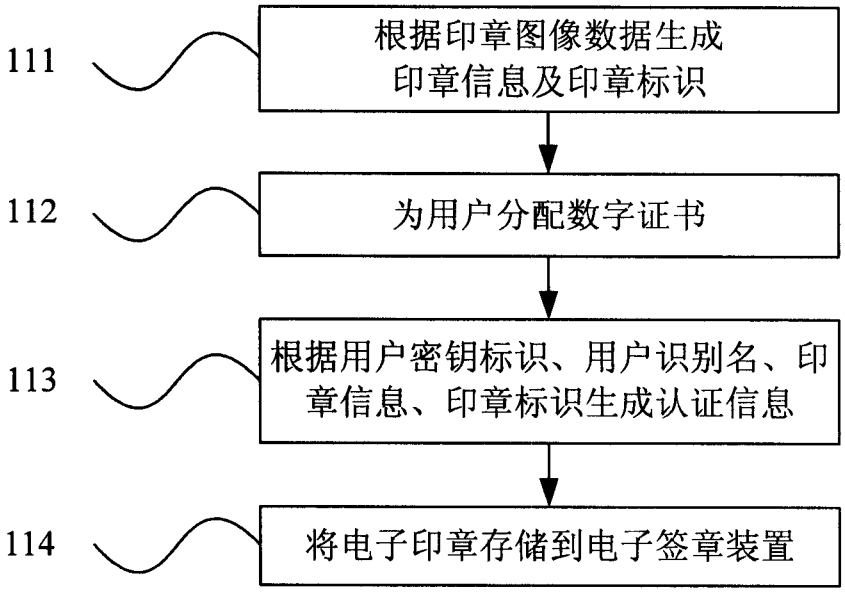

111
根据印章图像数据生成
印章信息及印章标识
112
为用户分配数字证书
113
根据用户密钥标识、用户识别名、印
章信息、印章标识生成认证信息
114
将电子印章存储到电子签章装置

图 4

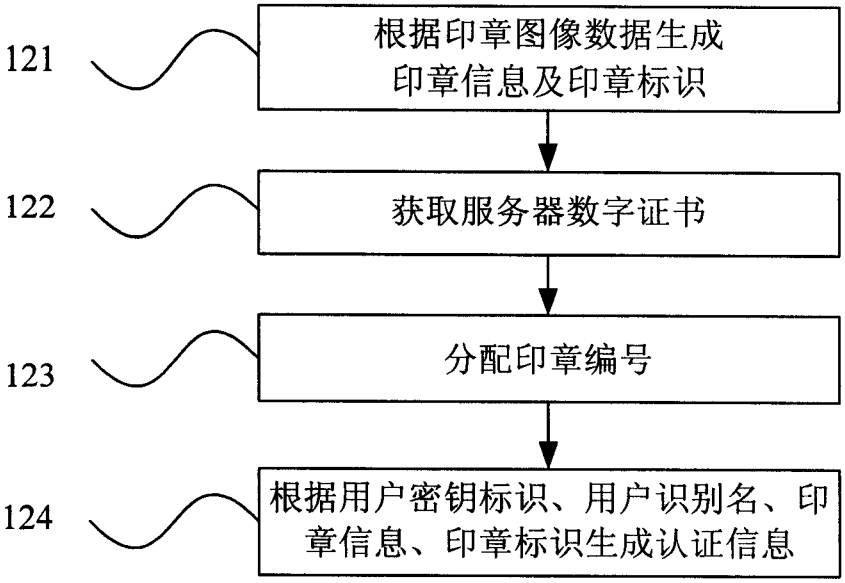

121
根据印章图像数据生成
印章信息及印章标识
122
获取服务器数字证书
123
分配印章编号
124
根据用户密钥标识、用户识别名、印
章信息、印章标识生成认证信息

图 5

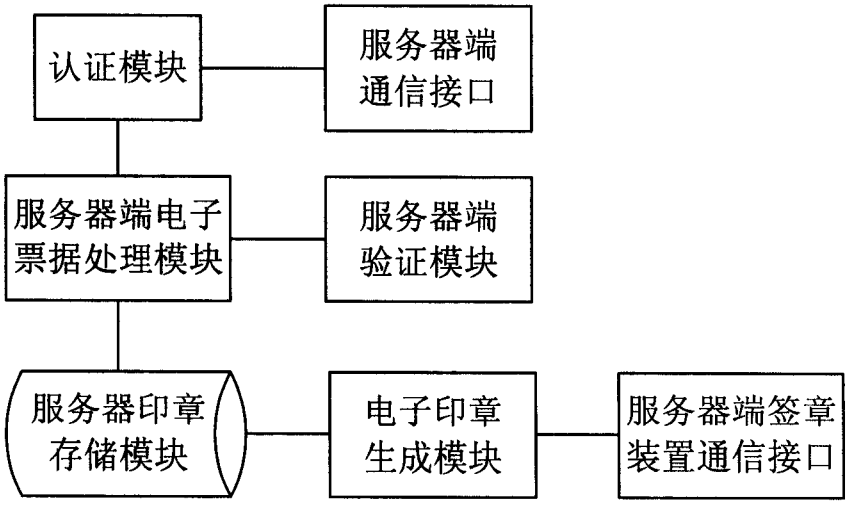

认证模块
服务器端
通信接口
服务器端电子
票据处理模块
服务器端
验证模块
服务器印章
存储模块
电子印章
生成模块
服务器端签章
装置通信接口

图 6

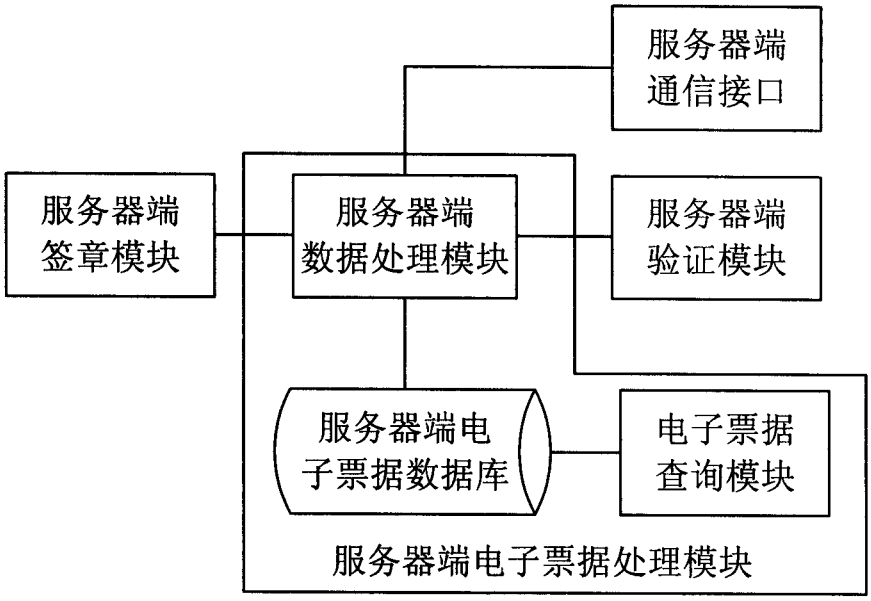

服务器端
通信接口
服务器端
签章模块
服务器端
数据处理模块
服务器端
验证模块
服务器端电
子票据数据库
电子票据
查询模块
服务器端电子票据处理模块

图 7

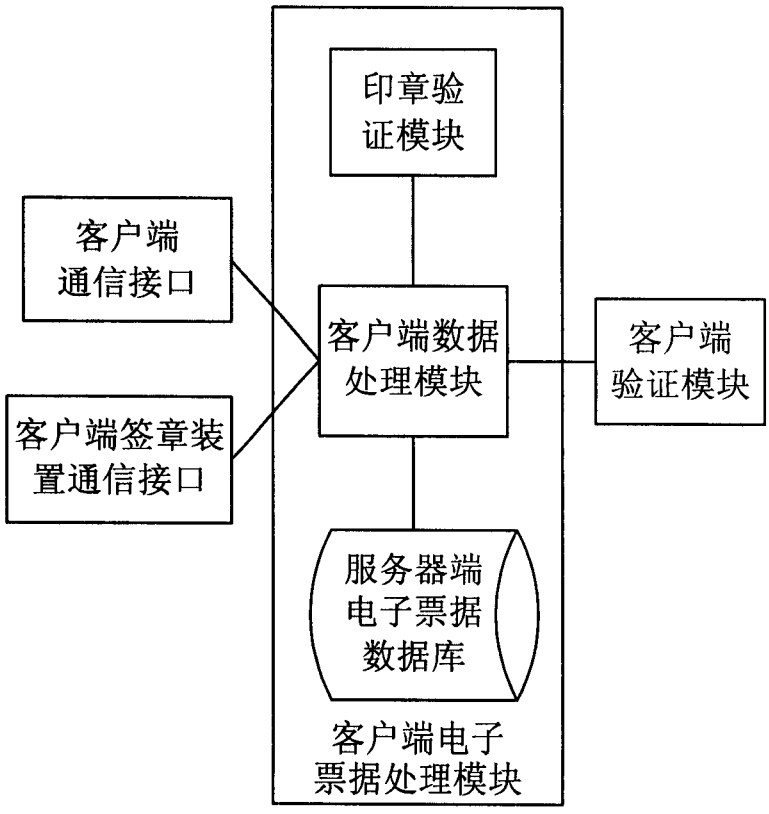

印章验
证模块
客户端
通信接口
客户端数据
处理模块
客户端
验证模块
客户端签章装
置通信接口
服务器端
电子票据
数据库
客户端电子
票据处理模块

图 8