

1、一种使用数字印章的电子商务系统，其特征在于，它包含有服务器运营端系统和客户桌面端系统，其中服务器运营端系统是配置在运营服务器端的应用装置，用于后台管理和维护工作，它包括：

- 一为交易个体进行登记、检索、保管维护数字印章图片的签章图片管理装置；
 - 一用于连接服务器运营端系统装置和客户桌面端系统装置的网站服务装置，它为客户提供的网上自助服务与桌面端系统的请求/响应；
 - 一主要完成有关数字证书申请、生成、状态查询等工作的数字证书管理装置，
 - 一用来让客户登记成为用户的客户登记装置；
 - 一用于维护管理客户资料、为网站服务装置提供客户信息，并与数字证书管理装置的证书资料相交互的客户管理装置；
- 所述客户桌面端系统是安装到桌面系统上的用于签章的应用装置，它包括：
- 一用于在客户端导入、更新印章图片和许可证，以及存储、检索印章图片和许可证的签章图片/许可证客户端管理装置；
 - 一提供客户端导入、更新、存储、检索数字证书的数字证书客户端管理装置；
 - 一自动整合到应用软件的一个插件部件、在签章控件装置被添加入电子文档并初始化前完成对签章使用许可证的验证的加盖签章控制插件装置；
 - 一自动整合到应用软件的一个插件部件、完成对签章使用许可的验证并完成打印签章的输出处理的打印签章控制插件装置；以及
 - 一由加盖签章控制插件装置添加的一个控件部件，作为一个对象控件添加到电子文档中用于管理签章操作的签章控件装置。

2、如权利要求1所述的使用数字印章的电子商务系统，其特征在于，所述签章图片管理装置，它包括：

- 一用于签章服务申请资料录入的签章图片录入装置；
- 一对于录入装置录入的签章图片生成唯一的识别编号的识别编码生成装置；
- 一为提高安全性对识别编号产生的识别编号进行加密的识别编号加密装置；
- 一对签章图片录入装置录入的签章资料进行图像处理优化并生成印章图像的签章图片生成装置；
- 一用于将加密过的识别信息嵌入到签章图片中的水印嵌入装置；
- 一用于维护签章有效性的签章有效状态维护装置；
- 一用于验证签章图片中的识别信息的水印提取装置；以及

3、如权利要求1所述的使用数字印章的电子商务系统，其特征在于，所述网站服务装置，它包括：

- 一客户申请、资料提交、服务咨询等的客户服务装置；
- 一用于查询签章图片有效性的签章状态查询装置；
- 一用于查询许可证有效性的许可证状态查询装置；以及
- 一用于网上查询数字证书有效性的数字证书状态查询装置；

4、如权利要求1所述的使用数字印章的电子商务系统，其特征在于，所述数字证书管理装置，它包括：

- 一用于给用户生成好的数字证书的数字证书生成装置；
- 一用于记录数字证书申请、使用相关资料的数字证书维护记录装置；
- 一用于验证证书有效性和用户身份的数字证书验证装置；以及

一用于存储数字证书所有数据的数字证书库装置。

5、如权利要求1所述的使用数字印章的电子商务系统，其特征在于，所述加盖签章控制插件装置，它包括：

- 一用于验证签章许可证的签章许可证验证装置；
- 一用于验证使用者身份的签章用户有效性验证装置；以及
- 一用于生成签章控件的签章控件生成装置；

6、如权利要求1所述的使用数字印章的电子商务系统，其特征在于，所述打印签章控制插件装置，它包括：

- 一用于验证签章打印许可证的打印许可证验证装置；
- 一用于获取印章图像识别码信息的签章识别信息获取装置；
- 一对原始文档的关键内容进行提取的文档提取装置；
- 一用于将电子文档的内容用签章使用者的数字证书进行签名运算的数字签名生成装置；
- 一用于打印含数字印章和二维条码文档的文档打印装置；
- 一在实际应用中为提高安全性，还有以下一些可选装置：
 - 一将从印章中提取的识别码水印信息制作成一维条码的条码生成装置
 - 一将数字签名生成装置产生的数字签名嵌入到二维水印条码中的二维水印条码生成装置；
 - 一将二维条码加入文档页眉位置的条码嵌入装置；

7、如权利要求1所述的使用数字印章的电子商务系统，其特征在于，所述签章控件装置，该装置包括：

- 一用于从本地管理容器中检索获取证书的签署者证书检索获取装置；
- 一用于从本地管理容器中检索获取签章图片获取装置；
- 一用于将水印信息嵌入到签章图片获取装置获取到的签章图片中的水印信息嵌入装置；
- 一用于保存含水印的签章图片、签章编号（明文）、签名结果、签署者数字证书、签署时间的签章信息保存装置；
- 一用于显示含水印的签章图片的签章图片显示装置；
- 一用于锁定文档禁止编辑的电子文档锁定装置；
- 以及用于验证数字印章的提取签章控件所存信息的信息提取装置；
- 一用二值图像水印算法对印章图像提取装置的印章图像进行水印信息（数字签名信息）提取的水印信息提取装置；
- 一用于验证数字签名的数字签名验证装置；
- 一当数字签名验证装置验证未通过时用于显示警告的数字签名验证警告显示装置；
- 一数字签名验证装置验证通过后进行的签章有效性验证装置；
- 一用于验证签章用户身份有效性的签章用户有效性验证装置；
- 一用于显示未通过的验证结果的存在疑问的验证报告显示装置；以及
- 一用于显示正常的验证结果的验证报告显示装置。

8、一种数字印章商务运行方法，其特征在于：

在运营商端，它包含有以下步骤：

1. 用户（客户）在数字登记中心登记成为注册用户并申请使用许可证、
2. 对用户的数字证书的申请、生成或状态进行查询；以及
3. 所述登记中心为所述用户登记的签章图片进行登记、检索、保管维；

另外，在客户桌面端，它包括以下步骤：

1. 通过公共网络与上述登记中心进行数字交换、联络：存储、检索印章图片并对许可证的签章图片进行管理；
2. 自动整合到办公软件的插件，并在加入电子文档并初始化前完成对签章使用许可证的验证；
3. 对验证的签章进行包括打印的输出处理；以及
4. 由添加的控件部件，使其作为一个对象控件添加到电子文档中。

数字印章的商务运行方法及其系统

技术领域

本发明涉及电子商务运行方法及其系统,特别涉及使用数字印章的运行方法及其系统。

背景技术

互联网的发展使得通过网络来进行电子商务活动的环境已经具备,因此,电子商务平台作为通常的商务流程之一而逐步普及,企业之间的商务活动(B2B)、企业与个人之间的商务活动(B2C)以及个人之间相互的商务活动(C2C)均得到广泛应用。

但所有的商务活动能够开始进行的前提是:

- 一、 保证每个用户都能够唯一无误地识别进行交易的另一方,就需要进行身份认证。因此电子商务交易中的身份安全认证和交易认证是实现电子商务的关键一步。
- 二、 保证用户之间往来文书的交换具有相当的安全性和权威性,即传输的电子文档是采用电子签名技术,并且经过CA认证的文档;
- 三、 保证用户之间的往来文书所附带的电子签名以国人所习惯的印章或签名形式表现。

现有的电子商务系统依靠加密技术和PKI,进行身份认证,不能实现印章的数字认证,影响了电子商务在习惯于使用印章进行交易的国家(例如中国、日本等)的普及。

发明内容

本发明所要解决的技术问题是提供一种数字印章的电子商务运行方法及其系统,它可结合用户数字证书的身份认证功能,实现电子文档(MS-Office文档、WEB 表单等)的签章功能,以印章图片结合电子签名的显示方式,来代表电子文档的真实性、完整性为目的进行商务运作。

为了解决上述技术问题,本发明提供的数字印章商务运行方法,其中:

在运营商端,它包含有以下步骤:

1. 用户(客户)在数字登记中心登记成为注册用户并申请使用许可证、
2. 对用户的数字证书的申请、生成或状态进行查询;以及
3. 所述登记中心为所述用户登记的签章图片进行登记、检索、保管维;

另外,在客户桌面端,它包括以下步骤:

1. 通过公共网络与上述登记中心进行数字交换、联络:存储、检索印章图片并对许可证的签章图片进行管理;
2. 自动整合到办公软件的插件(ADD-IN),并在加入电子文档并初始化前完成对签章使用许可证的验证;
3. 对验证的签章进行包括打印的输出处理;以及
4. 由添加的控件(ActiveX Control)部件,使其作为一个对象添加到电子文档中。

为了解决上述技术问题,本发明提供的数字印章电子商务运行系统,它包含有服务器运营端系统和客户桌面端系统,其中服务器运营端系统是配置在运营服务器端的应用装置,用于后台管理和维护工作,它包括:

- 一为交易个体进行登记、检索、保管维护数字印章图片的签章图片管理装置;
 - 一用于连接服务器运营端系统装置和客户桌面端系统装置的网站服务装置,它为客户提供的网上自助服务与桌面端系统的请求/响应;
 - 一主要完成有关数字证书申请、生成、状态查询等工作的数字证书管理装置,
 - 一用来让客户登记成为用户的客户登记装置;
 - 一用于维护管理客户资料、为网站服务装置提供客户信息,并与数字证书管理装置的证书资料相交互的客户管理装置;
- 所述客户桌面端系统是安装到桌面系统上的用于签章的应用装置,它包括:
- 一用于在客户端导入、更新印章图片和许可证,以及存储、检索印章图片和许可证的签章图片/许可证客户端管理装置;
 - 一提供客户端导入、更新、存储、检索数字证书的数字证书客户端管理装置;
 - 一自动整合到应用软件(包括 OFFICE、WPS、浏览器等)的一个 Add-in 部件、在签章控件装置被添加入电子文档并初始化前完成对签章使用许可证的验证的加盖签章控制插件装置;
 - 一自动整合到应用软件(包括 OFFICE、WPS、浏览器等)的一个 Add-in 部件、完成对签章使用许可的验证并完成打印签章的输出处理的打印签章控制插件装置;以及
 - 一由加盖签章控制插件装置添加的一个控件(如 MS - WINDOWS 平台的 ActiveX Control 部件),作为一个对象添加到电子文档中用于管理签章操作的签章控件装置。

本发明提供的数字印章电子商务系统中的数字印章是将电子文档(如 WEB 表单)内容的数字签名信息通过二值图像水印技术(中国专利:一种数字防伪方法,01132372.8)嵌入于印章图像中,此种数字印章即可在电子文档上也可在纸质文档上附加包含安全认证功能的数字印章,对两种文档可同时起到安全认证和防伪、防篡改功能。

本发明提供的数字印章商务运行方法及其系统,由于利用数字签名与数字水印技术,结合数字证书技术的确保用户身份的不可伪造、不可否认的性质,并通过网络实现企业或客户异地身份验证、文档签章,而且利用硬件保存数字证书,以达到较高的用户身份信息的安全性、和不可伪造性。另一方面,利用印章或签名的方式,即满足传统用户使用红章的习惯又使之与数字签名相结合达到法律上的认可,使的网上签发的带有电子印章的文档或合同同样具有法律效力。

附图说明

- 图 1A ~ 图 1E 为数字印章图像的示意图;
- 图 2 是一维、二维水印条码示意图;
- 图 3 是包含数字印章和水印条码(含数字签名和印章图像编码明文)的具有真伪认证功能的文档示意图;
- 图 4 为数字印章电子商务系统的总体结构示意图;
- 图 5 为数字印章服务系统登记、检索、保管维护数字印章图片的签章图片管理装置示意图;
- 图 6 为客户提供的网上服务与桌面端系统的请求/响应的网站服务装置示意图;

图 7 为申请、生成、状态查询数字证书等工作的数字证书管理装置示意图；
图 8 为服务器端其它提供客户信息，维护管理客户资料等服务的客户管理装置示意图；
图 9 为签章服务和许可证维护管理的客户管理装置示意图
图 10 为加盖签章控制插件装置添加签章控件装置流程示意图；
图 11 为验证签章使用许可证，打印签章的输出处理的打印签章处理控制插件装置示意图。
图 12A 为签章控件装置制作签章过程的示意图。
图 12B 为签章控件装置中签章验证过程示意图；

下面结合附图对本发明提供的数字印章的商务运行方法及其系统作进一步描述。

图 1A 表示一个原始的未加任何水印信息的印章图像。通常，印章图像是由用户提交的申请签章资料中获得或者通过软、硬件直接按照某种规则直接生成，再经图像软件优化，每个数字印章图片签章图片管理装置中都有一个唯一的编号。该印章图像 101 作为数字印章的母版，确保人们在使用过程的习惯性。

图 1B 表示本发明提供的数字印章系统包含数字水印信息(如印章编码识别信息)的数字印章图像。该数字印章图像 102 包含两个部分：第一部分是表征有意义的可见的印章图像，并且提供印章的初级鉴别功能；第二部分是嵌入在图像中的水印信息，用来鉴别印章的真伪，判断其完整性、非篡改性以及合法性。

图 1C 表示图 1B 的数字印章图像 102 的纸质复印版 103，即数字印章图像 102 经过打印(或印刷)设备输出到纸张上得到该复印版 103。纸张上的数字印章图像 103 同数字印章图像 102 一样，也包含有同样的两个部分：有意义的印章和嵌入到印章中的水印信息，这说明本发明提供的数字印章系统使得纸质文档也能够通过嵌入在印章中的水印信息来鉴别印章的真伪，判断其完整性、非篡改性以及合法性。

图 1D 表示用户提交的数字印章的其它表示形式，例如，一个人的签字的原始图像 104 在未加任何额外信息，可对文件做签署的标识作用，并且也作为数字印章的母版。

图 1E 是表示图 1D 所述的原始图像 104 中嵌入印章编码识别信息，并且经过打印(或印刷)设备输出到纸张上的印章图像 105。包含有印章编码识别信息的印章图像 105，除了起到文件签署的标识作用，而且还具有鉴别印章的真伪，判断其完整性、非篡改性以及合法性等功能。

图 2 是可存储少量信息的一维条码 201 和在一维条码基础上添加二维水印信息的二维水印条码 205。一维条码 201 可存储有限的数字信息，其特点是明文 204 和条码 202 并存，不但可通过明文 204 显示信息且可通过条码扫描器扫描出条码信息以方便于批量读取纸质数据信息，其读取信息的流程为：

- (1) 扫描器扫描出条码图像 202；
- (2) 条码解码装置 203 解读条码信息；
- (3) 203 解读出条码信息 204；

而二维条码 205 具有一维条码 201 的所有属性，并在这个基础上在 201 上添加水印信息，使 201 可存储更多的数据信息，205 与 201 的区别在于：

- (1) 条码图像 206 由于含有水印信息而显示成斑点状；
- (2) 205 的解码装置 207 不但要解读一维条码信息还要从条码图像中提取水印信息；

(3) 解读出的信息除了有一维条码信息 208 外还有水印信息 209

图 3 是包含数字印章部分的具有真伪认证功能的文档示意图。如图所示, 线框 310 中表示一个包含数字印章的文档, 该文档包括以下部分:

(1) 文档内容信息 311;

(2) 包含对 311 所做的数字签名信息的数字印章。

数字印章可以是普通常见图章 312 —— 图章的形状不限(如圆形、椭圆形、长方形、三角形等), 图章内部所表示的结构也不限(如公司图章、个人签章等), 图章内容不限(如有“上海阿须数码技术有限公司”字样, 或其它单位字样等);

数字印章也可以是包含数字签名的手写签名图像 315。

数字印章还可以是公司徽标 314; 数字水印条形码 316 和 313, 这些表现形式在申请号为 02110959.1 的中国专利已公开, 这里不在详细描述。

图 4 是本发明的数字印章电子商务系统的总体示意图。该系统分为两大组成部分:

数字印章商务系统中运营商端用于后台管理和维护工作的一一服务器运营商端系统装置 412;

数字印章商务系统中在客户端进行印章操作的一一客户桌面端系统装置 419;

服务器运营商端系统装置 412 包括:

(1) 签章图片管理装置 411;

(2) 网站服务装置 413;

(3) 数字证书管理装置 415;

(4) 客户管理装置 417;

(5) 服务管理装置 410;

(6) 服务统计计费装置 414;

服务器运营商端系统装置 412 在实际应用中是作为服务器为客户端提供各种服务申请或响应调用的。客户端通过浏览器登陆到网站服务装置 413 提供的网站, 413 再根据客户的申请调用签章图片管理装置 411、数字证书管理装置 415、客户管理装置 417、服务管理装置 410。服务统计计费装置 414 根据服务项目的计费规则, 记录用户的使用明细, 它主要与服务管理装置 410 和客户管理装置 417 相交互。

客户桌面端系统装置 419 包括:

(1) 签章图片/许可证客户端管理装置 420;

(2) 数字证书客户端管理装置 421;

(3) 加盖签章控制插件装置 422;

(4) 打印签章控制插件装置 416;

(5) 签章控件装置 418;

客户桌面端系统装置 419 主要用于加盖签章操作, 加盖签章操作需包括用于添加控件的加盖签章控制插件装置 422 和控件操作的签章控件装置 418。而签章图片/许可证客户端管理装置 420 是用于添加印章前验证签章图片和签章许可证时提供许可证和图片的管理器, 同样数字证书客户端管理装置 421 也是用于验证用户身份的工具, 这两个装置都需与服务器端相连接以便实时验证签章图片和许可证的有效性。打印签章控制插件装置 416 是用于打印签章文档的工具, 在打印前也需通过签章图片/许可证客户端管理装置 420 和数字证书客户端管理装置 421 验证。

图 5 是本发明的数字印章服务系统登记、检索、保管维护数字印章图片的签章图片管理装置示意图。该系统包括:

- (1) 用于录入签章图片申请资料 511 的签章图片录入装置 512;
- (2) 为签章图片生成唯一的识别编号的识别编码生成装置 513;
- (3) 签章图片生成装置 515;
- (4) 识别编号加密装置 514;
- (5) 水印嵌入装置 516;
- (6) 签章有效状态维护装置 517;
- (7) 电子签章档案库装置 518;

该系统的目的是保证数字印章的有效性和安全性, 其处理流程是:

- (1) 通过签章图片录入装置 512 录入用户提交的签章图片申请资料 511;
- (2) 一方面识别编码生成装置 513 为签章生成一个识别编号, 识别编号加密装置 514 将 513 生成识别编号加密并提交给水印嵌入装置 516 和签章有效状态维护装置 517;
- (3) 另一方面基于申请资料经签章图片生成装置 515 生成原始签章图片并交由签章图片水印嵌入装置 516, 签章图片嵌入装置 516 将 514 提交来的编信息作为水印信息加入到印章中, 并提交给签章有效状态维护装置 517;
- (4) 签章有效状态维护装置 517 将以上所有信息存入电子签章档案库装置 518, 并实时与许可证库装置、数字证书库装置、客户信息库装置进行交互;

图 6 是本发明的数字印章电子商务系统的网站服务装置示意图。该系统包括: 客户服务装置 611、签章状态查询装置 612、许可证状态查询装置 613、数字证书状态查询装置 614、网站服务装置 615、电子签章档案库装置 616、许可证库装置 617、数字证书库装置 618、客户信息库装置 619。该装置的工作过程如下:

- (1) 网站服务装置提供客户服务 611、签章状态查询服务 612、许可证状态查询服务 613、数字证书状态查询服务 614, 用户通过浏览器了解各项服务介绍、进行服务申请、以及资料提交, 且可通过许可证状态查询装置 613、数字证书状态查询装置 614 验证许可证的有效状态和数字证书的当前状态;
- (2) 网页中收集到的所有请求和资料都提交给网站服务装置 615 的服务器端, 并由网站服务装置 615 与后台电子签章档案库装置 616、许可证库装置 617、数字证书库装置 618、客户信息库装置 619 等进行交互。

另一方面网站服务装置是调用服务器端所有就用的接口, 客户桌面端的签章调用所需服务器端的服务都是通过网站服务装置进行通讯的。

图 7 是本发明中服务器运营商端系统装置 412 的数字证书管理装置示意图。该系统包括: 数字证书生成装置 712、数字证书维护记录装置 713、数字证书验证装置 714、数字证书管理装置 715、数字证书库装置 716、客户信息库装置 717。该系统的工作流程如下:

- (1) 将数字证书申请资料 711 提交给数字证书生成装置 712, 并启动数字证书维护记录装置记录证书申请相关资料;
- (2) 将上述产生的数字证书以及相关资料交由数字证书管理装置 715 处

理, 数字证书管理装置 715 再将所有数据分类存入后台数字证书库装置和客户信息库装置等后台数据库;

- (3) 对于客户端申请验证数字证书的调用, 由数字证书验证装置 714 进行验证, 714 将接收的申请提交给数字证书管理装置, 并由管理装置 715 与后台数据库交互, 将验证的结果返回给数字证书验证装置 714, 通过 714 将结果返回给客户端;

在这里数字证书的生成、维护由数据认证中心 (CA) 提供, 并由数字证书管理装置提供接口与之连接, 使系统成为一体。

图 8 是本发明的服务器运营端系统装置的组成部分之一客户管理装置示意图。其主要包括: 客户资料录入装置 812、网站服务装置 813、数字证书管理装置 814、客户管理装置 815、客户信息库装置 816、数字证书库装置 817。工作流程为:

- (1) 当客户申请注册时, 由客户资料录入装置 812 将客户资料录入进系统并交由客户管理装置处理 815;
- (2) 当网站服务申请进行客户资料查询时, 由网站服务装置 813 将申请提交给客户管理装置 815 处理;
- (3) 当数字证书服务管理需要调用客户资料时, 由数字证书管理装置 814 将所需调用提交给客户管理装置 815 处理;
- (4) 客户管理装置再将各种调用处理后与后台客户信息库装置 816 进行交互, 并同步更新数字证书库装置 817;

这里客户资料录入装置还提供用户资料更新、删除、修改、等接口, 但由于安全性考虑此类接口只面对管理员权限用户开放, 基本原理与以上流程相同这里就不过多描述。

图 9 是本发明的服务器运营端系统装置的组成部分之一的服务管理装置示意图。系统主要包括: 申请资料录入装置 912、许可证生成装置 913、签章服务项目管理装置 914、许可证管理装置 920、服务维护装置 915、签章使用记录库装置 918、许可证库装置 916、客户信息库装置 917、数字证书库装置 919。系统的操作流程为:

- (1) 当用户申请许可证时, 由申请资料录入装置 912 将用户的申请许可证资料输入系统;
- (2) 申请资料输入后由许可证生成装置产生用户所需的许可证并交由服务维护装置处理;
- (3) 对于签章服务项目的维护管理工作, 完成定义、修改、删除等, 通过签章服务项目管理装置将维护申请提交给服务维护装置处理;
- (4) 许可证的维护管理, 包括登记、签发、变更、失效、停用、恢复等操作, 则通过许可证管理装置 920 将操作申请提交给服务维护装置处理;
- (5) 服务维护装置将各种处理后再将相关的数据信息与后台许可证库装置 916、客户信息库装置 917、签章使用记录库装置 918、数字证书库装置 919 等数据库交互更新。

其中, 签章服务项目是针对实际应用中集团性数字签章服务项目的使用; 而许可证的管理主要是针对签章许可证和打印许可证的管理维护工作; 签章使用记录库装置主要是用于记录用户使用数字印章的所有记录以便于计费系统进行统计核算。

图 10 是本发明提供的数字印章电子商务系统客户桌面端系统装置组成部分

之一的加盖签章控制插件装置示意图。该系统主要包括：许可证验证装置 1013、签章用户有效性验证装置 1015、签章控件生成装置 1018、许可证客户端管理装置 1019、签章图片客户端管理装置 1020。操作流程为：

- (1) 输入欲加盖数字印章的原始文档 1011；
- (2) 启动签章控制插件装置后提示选择签章使用许可证 1012，从许可证客户端管理装置 1019 中获取许可证；
- (3) 通过签章许可证验证装置 1013 验证许可证的有效性，如果验证 1014 通过则进行下一步，否则跳出签章过程；
- (4) 如果许可证验证通过后，基于用户数字证书通过签章用户有效性验证装置 1015 验证，如果验证 1016 通过则进行下一步，否则跳出签章过程；
- (5) 用户身份验证能过后，从签章图片客户端管理装置 1020 中获取签章图片 1017 并提交给签章控件生成装置 1018；
- (6) 签章控件生成装置 1018 就会在原始文档 1011 中选定的位置上插入数字印章控件；

上述所说的各种验证装置由于要实时验证其有效性均需在线验证。这里许可证客户端管理装置和签章图片客户端管理装置都可通过网上从许可证管理装置和签章服务项目管理装置中获得并下载。安装到本地机后就可直接使用。

图 11 是本发明中客户桌面端服务系统的组成部分之一打印签章控制插件装置示意图。图中实现的是利用水印条码存储数字签名的打印签章控制插件装置，主要包括：打印许可证验证装置 1110、签章用户有效性验证装置 1112、签章识别信息获取装置 1104、条码的条码生成装置 1105、文档提取装置 1117、数字签名生成装置 1118、水印条码生成装置 1106、条码嵌入装置 1107、文档打印装置 1119、数字证书获取装置 1120、数字证书客户端管理装置 1121。工作过程如下：

- (1) 点击打印签章控制插件装置后，系统提示选择印签使用许可证；
- (2) 系统自动作签章图片/许可证客户端管理装置中获取所有许可证，用户选择好许可证后交由打印许可证验证装置 1110 验证如果验证 1111 通过则进行下一步，否则跳出打印过程提示验证许可证不通过；
- (3) 如果打印许可证验证装置 1110 验证通过则进行签章用户有效性验证，交由签章用户有效性验证装置 1112 验证，如果验证 1113 通过则进行下一步，否则跳出打印过程并提示验证签章用户身份不通过；
- (4) 签章用户身份验证通过后，调用签章识别码获取装置 1104 获取签章识别编码；
- (5) 将获取的识别编码通过条码生成装置 1105 生成条码提交给条码生成装置 1106；
- (6) 文档提取装置 1117 对含签章文档进行处理，对原始文档关键内容进行提取；
- (7) 调用数字证书获取装置 1120 从数字证书客户端管理装置 1121 中获取数字证书并提交给数字签名生成装置 1118
- (8) 上述文档提取装置 1117 提取的文档关键内容输入到数字签名生成装置 1118 中与数字证书一起，采用公开密钥算法对文档内容做数字签名。这种算法是现有技术已公开的技术。
- (9) 将数字签名生成装置生成的文档的数字签名信息作为水印信息提交给水印条码生成装置 1106，最终生成条码；

(10) 调用条码嵌入装置将 1106 生成的条码嵌入到欲打印的文档中，并调用打印输出装置打印此文档；

此方法是将水印条码与数字印章相结合，以达到更高的安全性。但在通用的数字印章系统中打印插件可简化成只有打印许可证验证 1110 和签章用户有效性验证 1112 二个验证过程通过后直接调用打印输出装置，而数字签名则在生成签章控件时作为水印信息加入到印章中，与此插件无关。二种方法都能实现打出的含签章的纸质文档可验证文档有无篡改以及印章的真实性、有效性和合法性。

图 12 是本发明提供的客户桌面端服务系统装置的签章控件装置示意图，主要签章控件装置的功能主要为生成数字印章和验证数字印章二部分

其中图 12A，是本发明提供的签章控件生成数字印章操作的示意图，此图实现的方法采用的是将文档的数字签名信息作为水印信息加入到印章图像中，使得印章图像达到无论是电子的还是纸质的文档都可实现的防伪造、防篡改的效力。其主要包括：数字证书获取装置 1202、数字证书客户端管理装置 1225、签章图片获取装置 1203、签章图片客户端管理装置 1210、文档提取装置 1204、数字签名生成装置 1205、水印信息嵌入装置 1206、签章信息保存装置 1207、签章图片显示装置 1208、电子文档锁定装置 1209。操作的工作过程如下：

- (1) 在图 10 中由加盖签章控制插件装置在文档中插入数字印章控件后，系统从数字证书客户端管理装置 1225 中利用数字证书获取装置 1202 将数字证书提取出来；
- (2) 由签章图片获取装置 1203 从签章图片客户端管理装置 1210 中获取签章图片；
- (3) 再利用文档提取装置 1204 从原始文档中将文档内容提取出来提交给数字签名生成装置 1205 生成数字签名；
- (4) 将数字签名生成装置 1205 生成的数字签名提交给水印信息嵌入装置 1206 生成含水印的数字印章图片，并同时由签章信息保存装置 1207 将数字证书、含水印的数字印章图片、签章时间、签章用户等信息保存入签章控件中；
- (5) 最后由签章图片显示装置 1208 将水印信息嵌入装置 1206 生成的含水印的数字印章图片显示出来。为保护文档调用电子文档锁定装置 1209 将文档锁定，限制用户修改。

其中图 12B，是本发明提供的签章控件验证数字印章操作示意图，此图是相对于图 12A 的印章生成方法而采用的数字印章验证方法。其主要包括：信息提取装置 1212、水印信息提取装置 1214、签章图片获取装置 1213、文档提取装置 1215、数字签名验证装置 1216、数字证书获取装置 1217、数字签名验证警告显示装置 1220、签章有效性验证装置 1219、签章用户有效性验证装置 1221、存在疑问的验证报告显示装置 1223、验证报告显示装置 1224。操作的工作过程如下：

- (1) 输入待验证含印章文档 1211；
- (2) 选取控件后，由签章控件信息提取装置 1212 从控件中提取所有信息；
- (3) 控件信息获取后，一方面调用签章图片获取装置 1213 将含水印的数字印章图片提取出来，并交由水印信息提取装置 1214 提取水印，交由数字签名验证装置 1216 处理；另一方面通过文档提取装置 1215 从待验证含印章文档 1211 中提取文档的主要信息交由数字签名验证装置 1216 处理。

(4) 由图 12A 所示，数字印章中含有的水印信息是原电子文档的数字签名信息，利用水印信息提取装置提取的信息也就是原文档的数字签名信息，将此

信息与签章文档中提取的文档信息交由数字签名验证装置 1216 验证, 如果验证通过则进行下一步, 否则调用数字签名验证警告显示装置 1220 显示警告;

(5) 如果数字签名验证 1218 通过则调用签章有效性验证装置 1219 验证数字印章的有效性, 如果验证通过则进行下一步, 否则提示签章有效性验证失败;

(6) 如果签章有效性验证通过则调用签章用户有效性验证装置 1221 验证签章用户的身份是否合法, 如果验证通过则生成验证结果报, 并交由验证报告显示装置 1224 显示, 否则交由存在疑问的验证报告显示装置 1223 显示, 根据该结果可以确定数字水印的真伪。

通过上面的描述, 可以发现, 本发明提供的数字印章电子商务系统的技术要点及其效果如下:

1、为保障签章图片的真实性, 采用了商务系统签章图片统一管理技术

该系统的目的是保证数字印章的有效性和安全性, 构架该系统的装置包括: 签章图片录入装置、识别编码生成装置、签章图片生成装置、识别编号加密装置、水印嵌入装置、签章有效状态维护装置、电子签章档案库装置。装置需要的输入参数: 客户提交的签章图片申请资料 (需有印章图像的基准模板), 签章图片的形成流程为:

- (1) 通过签章图片录入装置录入用户提交的签章图片申请资料;
- (2) 对于录入的数据, 首先为签章生成一个识别编号, 调用识别编号加密装置生成识别编号加密并提交给水印嵌入装置和签章有效状态维护装置;
- (3) 基于申请资料经签章图片生成装置产生原始签章图片并交由签章图片水印嵌入装置, 签章图片嵌入装置将提交来的编码信息作为水印信息加入到印章中以达到签章图片的伪作用, 并提交给签章有效状态维护装置进行存贮和维护;
- (4) 签章有效状态维护装置唯一识别编码和最后生成的印章图像存入电子签章档案库装置, 并将申请资料存档。签章档案库装置也需实时与许可证库装置、数字证书库装置、客户信息库装置进行交互、更新;

2、利用网站服务装置实现与客户端的交流

网站服务装置客户查询资料、了解讯息、交互操作的主要方法, 也是调用服务器端所有服务的唯一对外接口, 客户桌面端的签章调用所需服务器端的服务都是通过网站服务装置进行通讯的。该系统的主要装置包括: 客户服务装置、签章状态查询装置、许可证状态查询装置、数字证书状态查询装置、网站服务装置、电子签章档案库装置、许可证库装置、数字证书库装置、客户信息库装置。其服务内容及方法为:

(1) 网站服务装置提供客户服务、签章状态查询服务、许可证状态查询服务、数字证书状态查询服务, 用户通过浏览器了解各项服务介绍、进行服务申请、以及资料提交, 且可通过许可证状态查询装置、数字证书状态查询装置验证许可证的有效状态和数字证书的当前状态;

(2) 网页中收集到的所有请求和资料都提交给网站服务装置, 并由网站服务装置与后台电子签章档案库装置、许可证库装置、数字证书库装置、客户信息库装置等进行交互。

3、服务管理装置管理的内容及方法

服务管理装置主要是面向数字印章电子商务系统中所有应用到的服务内容的管理和维护, 主要的维护内容为: 签章许可证、打印许可证的登记、签发、变

更、失效、停用、恢复等操作，以及用户使用数字印章的操作记录，如签章时间、签章用户验证时间及结果和许可证验证时间和结果等。构造该系统所需的装置包括：申请资料录入装置、许可证生成装置、签章服务项目管理装置、许可证管理装置、服务维护装置、签章使用记录库装置、许可证库装置、客户信息库装置、数字证书库装置。其服务内容及处理流程为：

- (1) 由申请资料录入装置将用户的申请许可证资料输入系统；
- (2) 申请资料输入后由许可证生成装置产生用户所需的许可证并交由服务维护装置处理；
- (3) 完成定义、修改、删除等维护管理工作，通过签章服务项目管理装置将维护申请数据提交给服务维护装置处理；
- (4) 许可证的维护管理则通过许可证管理装置将申请调用的操作提交给服务维护装置处理；
- (5) 服务维护装置将各种调用处理后再将相关的数据信息与后台数据库交互、更新。

4、客户端添加数字印章的方法与装置

添加数字印章这本发明里分为两个操作：一个是用于添加数字印章的加盖签章控制插件装置；另一个是签章控件的生成装置。

操作所需装置包括：许可证验证装置、签章用户有效性验证装置、签章控件生成装置、许可证客户端管理装置、签章图片客户端管理装置、数字证书获取装置、数字证书客户端管理装置、签章图片获取装置、签章图片客户端管理装置、文档提取装置、数字签名生成装置、水印信息嵌入装置、签章信息保存装置、签章图片显示装置、电子文档锁定装置。所需参数为：欲加盖数字印章的原始文档、签章许可证、数字证书（可存储于具有 USB 接口的电子钥匙 EKEY，或者其它安全存储装置中）。其操作流程为：

- (1) 从许可证客户端管理装置中获取许可证；
- (2) 通过签章许可证验证装置验证许可证的有效性
- (3) 如果许可证验证通过后，基于数字证书通过签章用户有效性验证装置验证；
- (4) 用户身份验证通过后，从签章图片客户端管理装置中获取签章图片并提交给签章控件生成装置；
- (5) 签章控件生成装置再调用签章图片获取装置从签章图片客户端管理装置中获取签章图片；
- (6) 再利用文档提取装置从原始文档中将文档内容提取出来提交给数字签名生成装置生成数字签名；
- (7) 将生成的数字签名提交给水印信息嵌入装置，生成含水印的数字印章图片，并同时由签章信息保存装置将数字证书、含水印的数字印章图片、签章时间、签章用户等信息保存入签章控件中；
- (8) 由签章图片显示装置将含水印的数字印章图片显示出来，并在原始文档中选定的位置上插入，最后为限制用户修改调用电子文档锁定装置 1209 将文档锁定，

3、数字印章验证方法与装置

数字印章的验证特指对电子文档的真实性、完整性、对签署者身份有效性(反抵赖)以及对数字印章有效性的验证。对数字印章的验证可以离线进行，不过这样验证都可能不能获得有关签署者目前身份的有效性、签章目前有效性的及时结

果。其所需装置包括：签章控件装置、数字签名验证设备、结果输出设备。装置需要的输入参数包括：原始的输入文档、由 CA 签发的盖章人或单位的数字证书，那么鉴别方法的基本步骤是：

- (1) 打开带有数字印章（签章控件）的原始输入文档，验证端可以不在线；
- (2) 如果文档完整（未被不法修改），则签章控件将显示完好的签章图片（不包含签章加密标识信息），否则显示警告；
- (3) 选择文档中签章控件装置，选择“验证”，利用数字签名验证设备和存入在签章控件中的数字证书解密并比较，产生一份签章验证报告，显示签署者、签署时间、签署者当前有效性（需在线）、签章编号、签章当前有效性（需在线）以及文档完好的报告信息；并把该结果报告输出给结果输出设备；

4、签章打印方法与装置

数字印章打印为满足需要将电子文档及其签章物理输出成纸质文件的需要，其装置包括：网站服务装置、签章控件装置、打印签章控件插件装置、数字证书客户端管理装置。装置需要的输入参数包括：原始的输入文档、签章打印许可证。打印的基本步骤是：

- (1) 打开原始输入文档；
- (2) 通过集成在应用软件（如 MS-OFFICE）菜单项中的打印签章控制插件启动打印；
- (3) 选择签章打印许可证，插入数字证书存储介质通过网站服务装置利用数字证书客户端管理装置验证许可证和使用者身份。
- (4) 通过验证的，将数字印章随原文输出到纸介质上，此时输出的数字印章图片可用于提取水印信息，用于核对图片真实性；



图 1A



图 1B

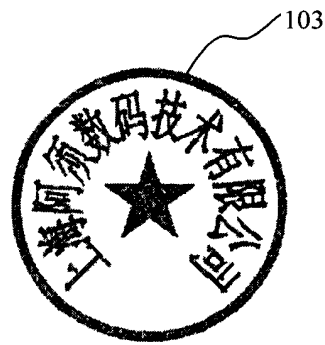


图 1C

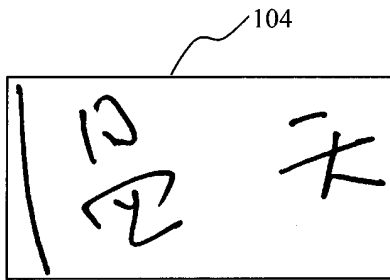


图 1D

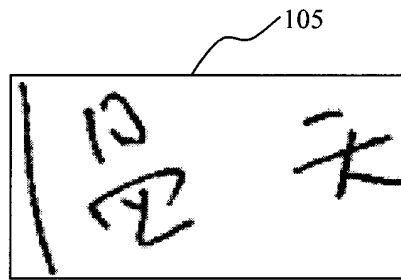


图 1E

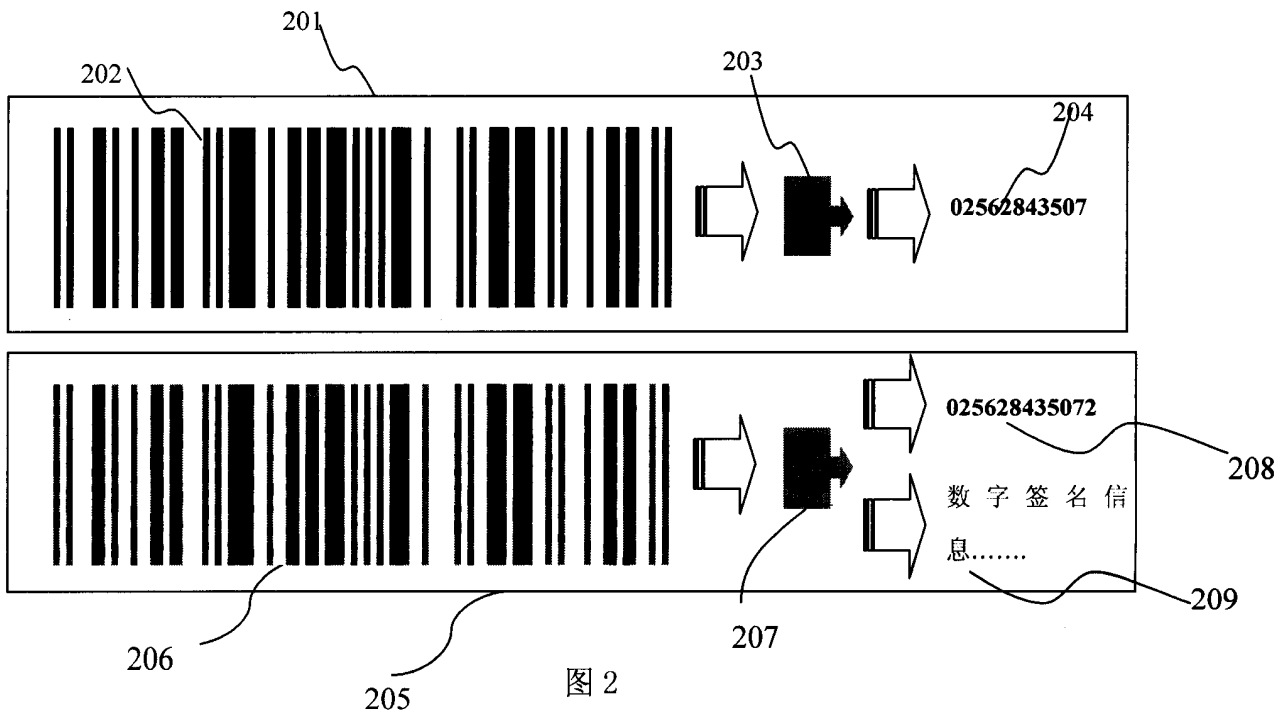


图 2

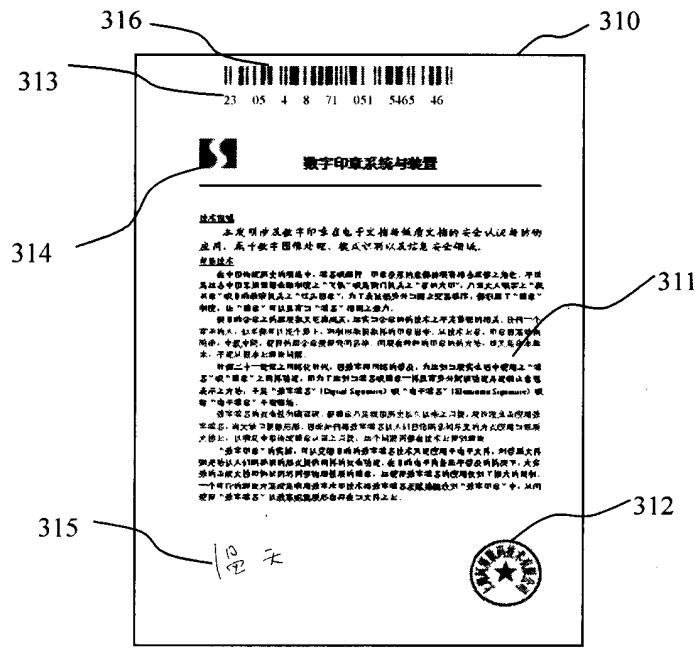


图 3

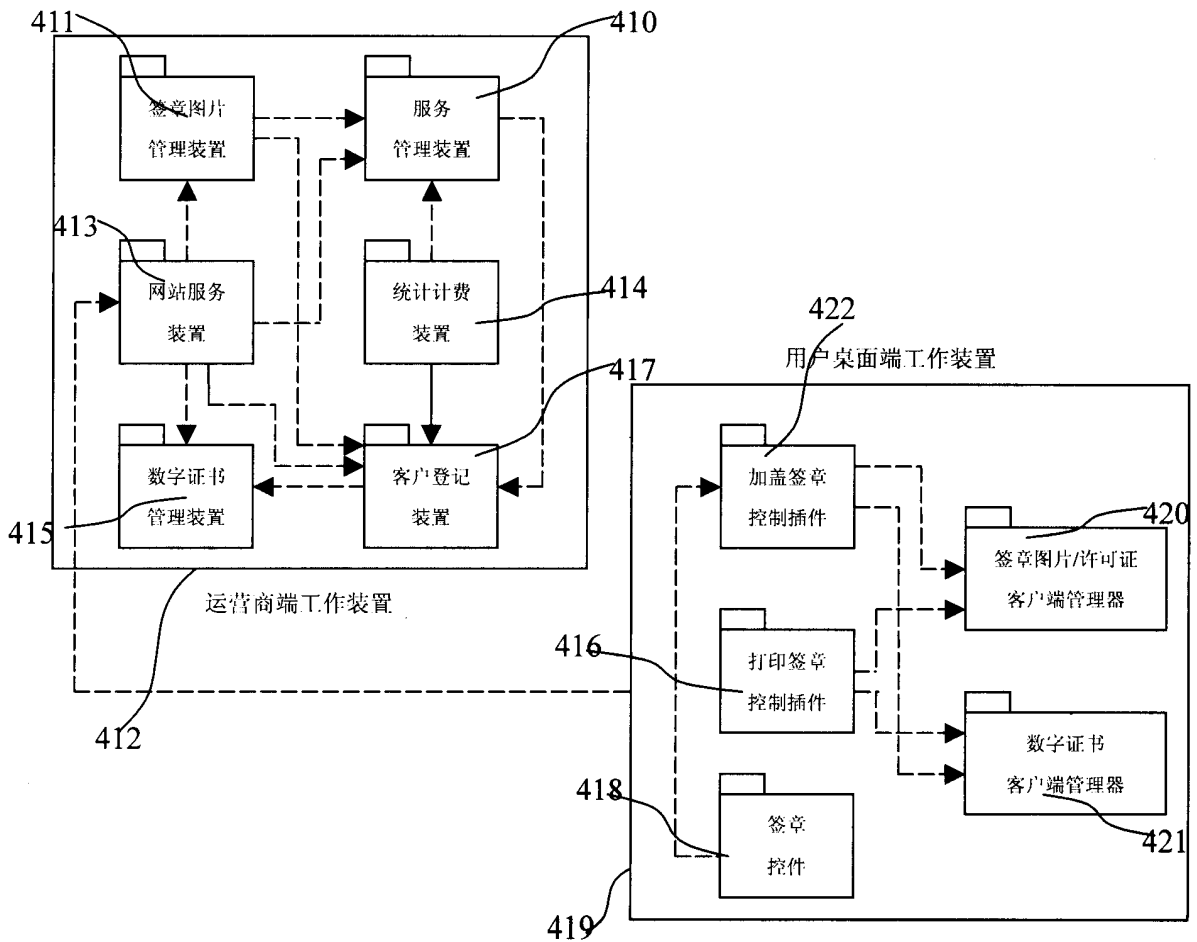


图 4

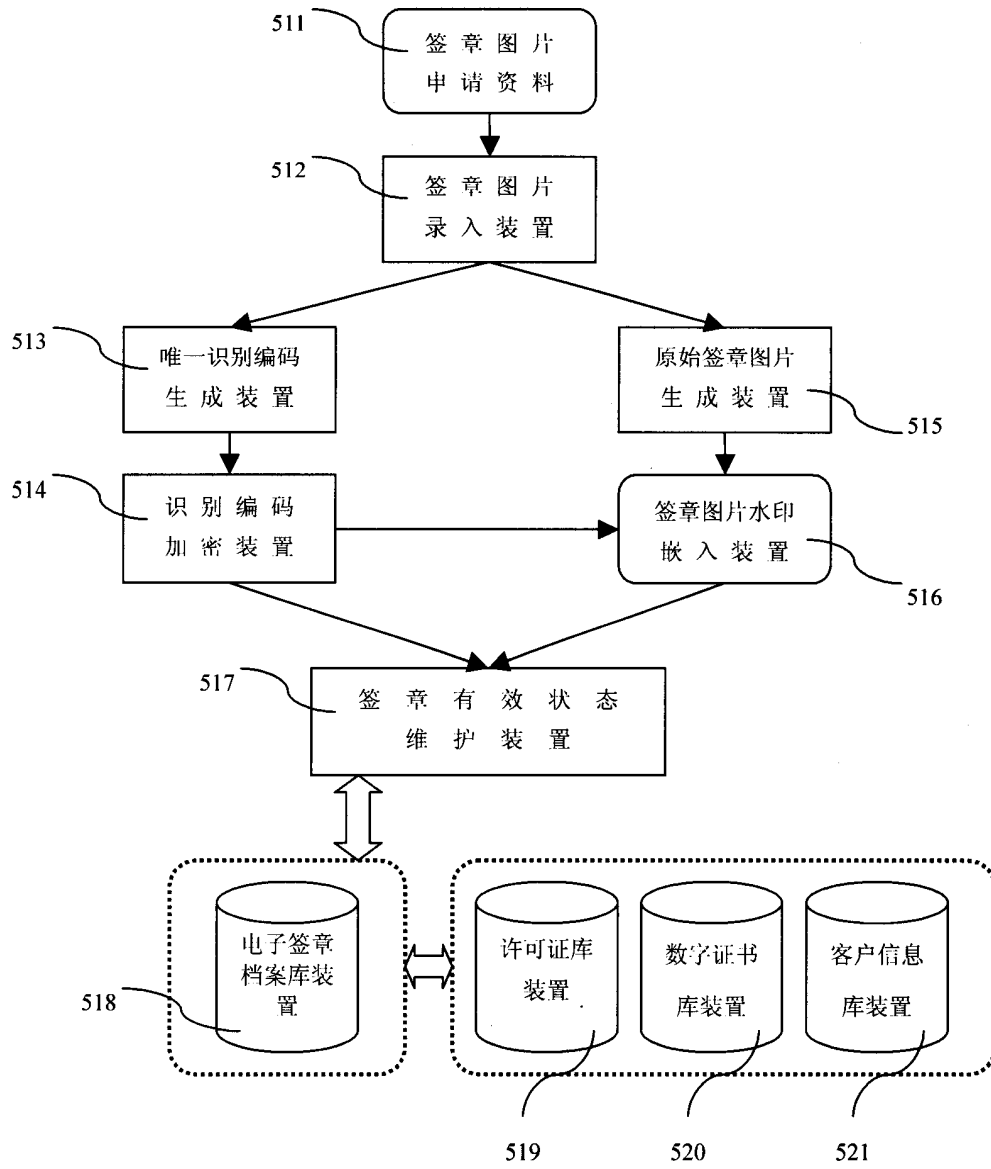


图 5

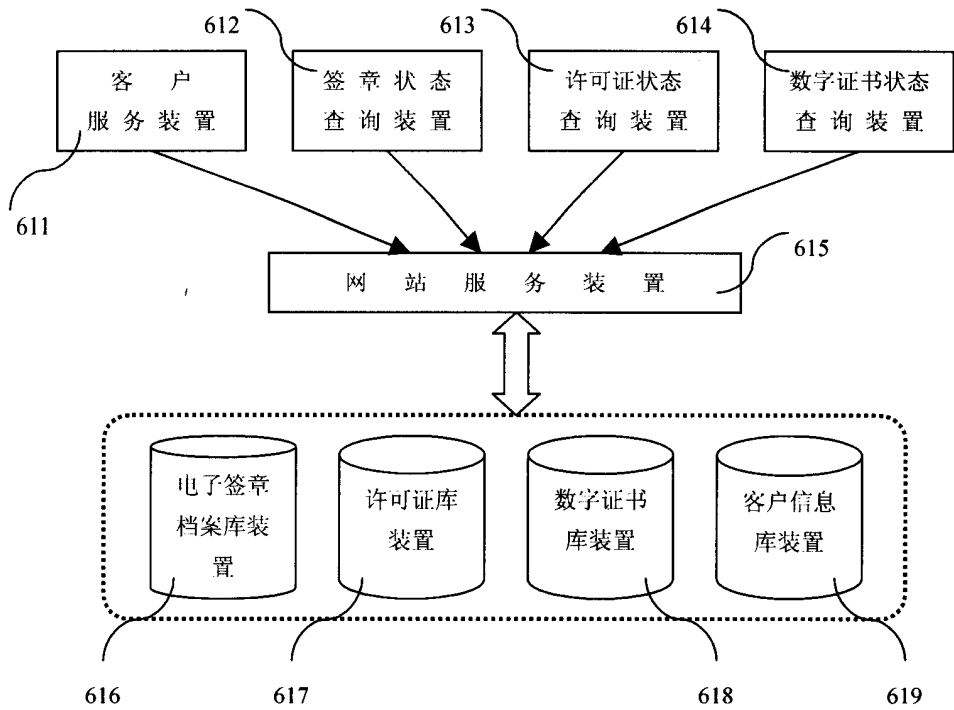


图 6

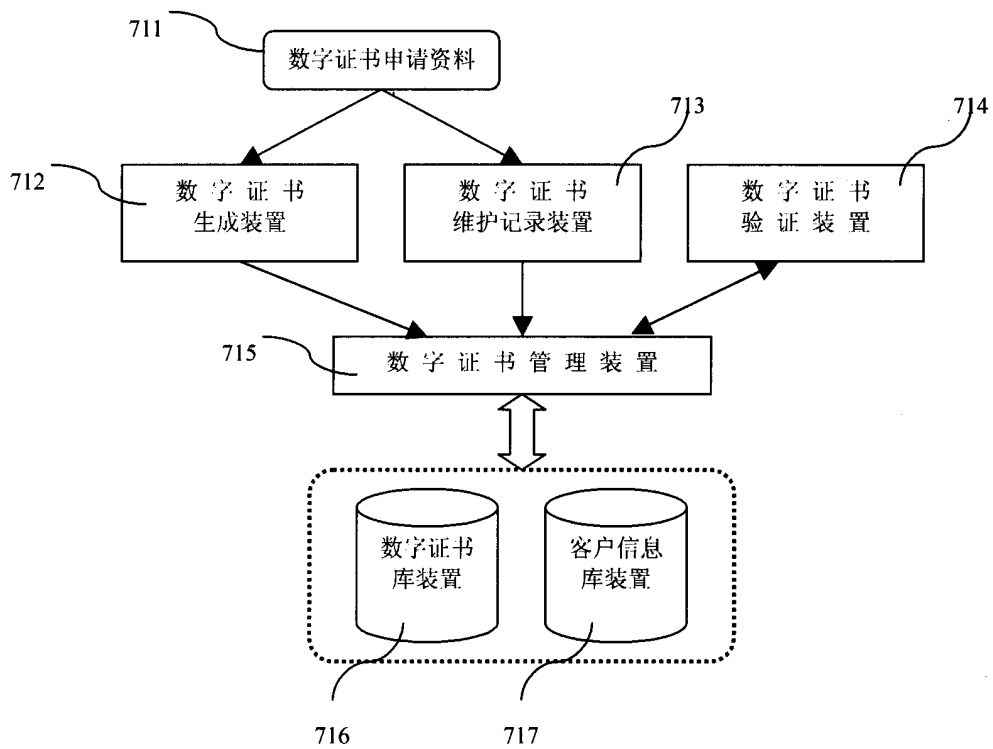


图 7

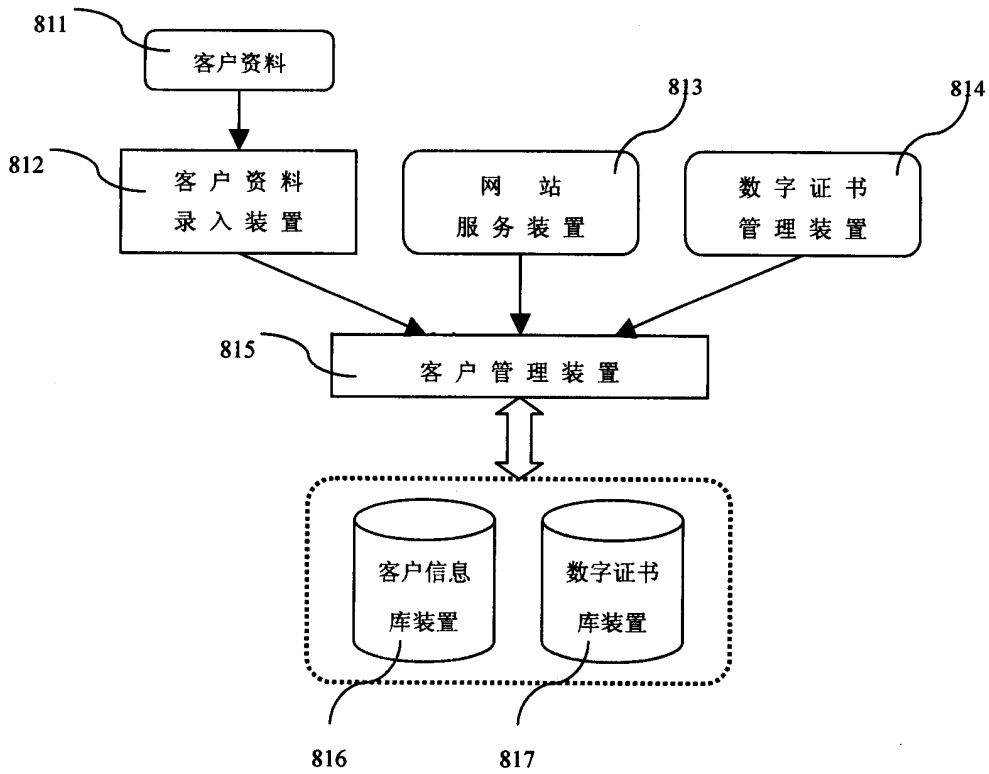


图8

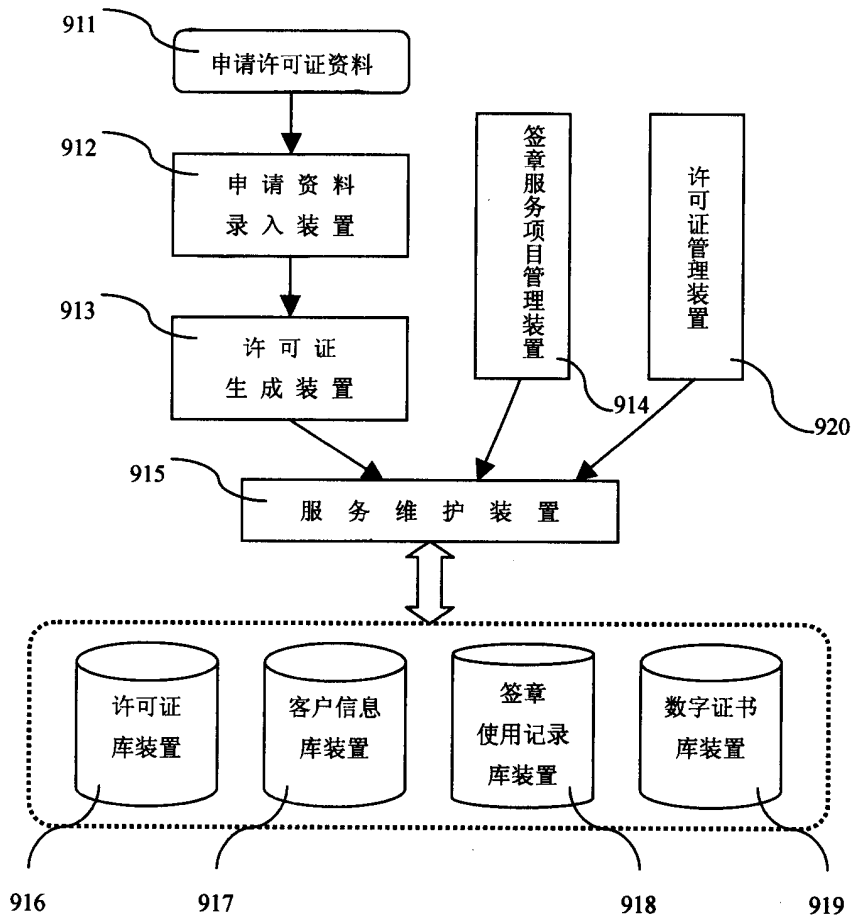


图9

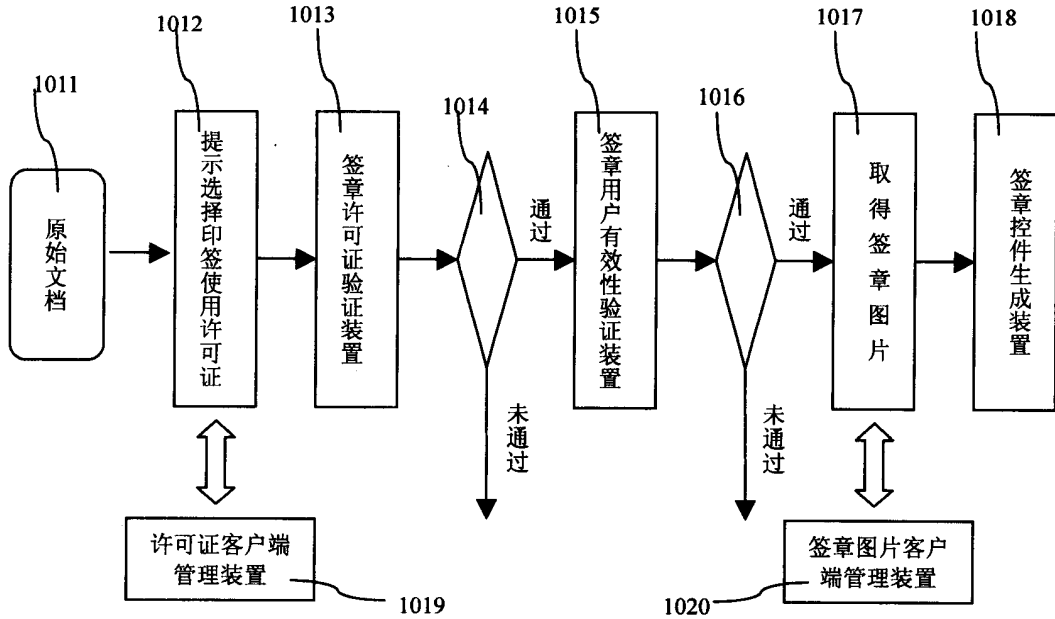


图 10

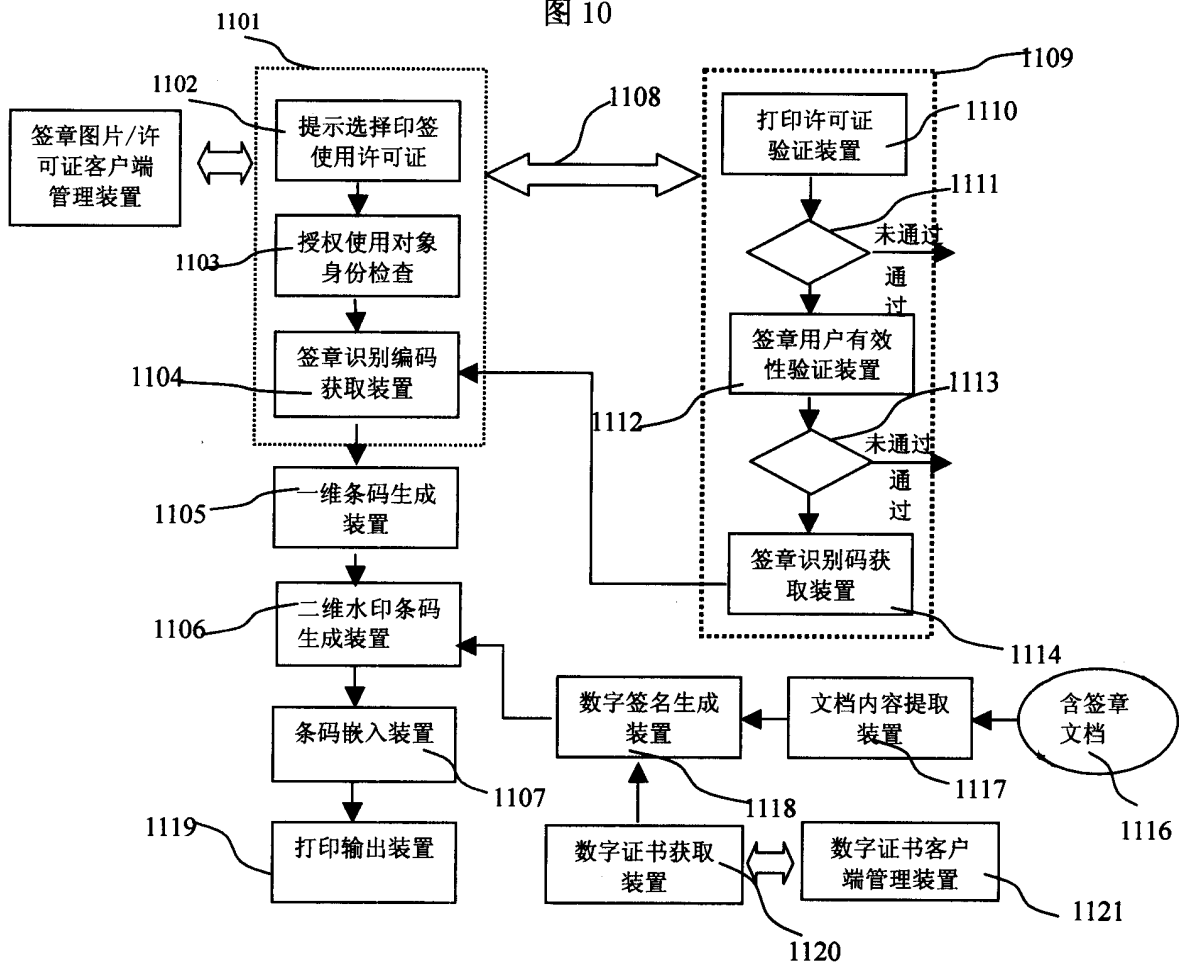


图 11

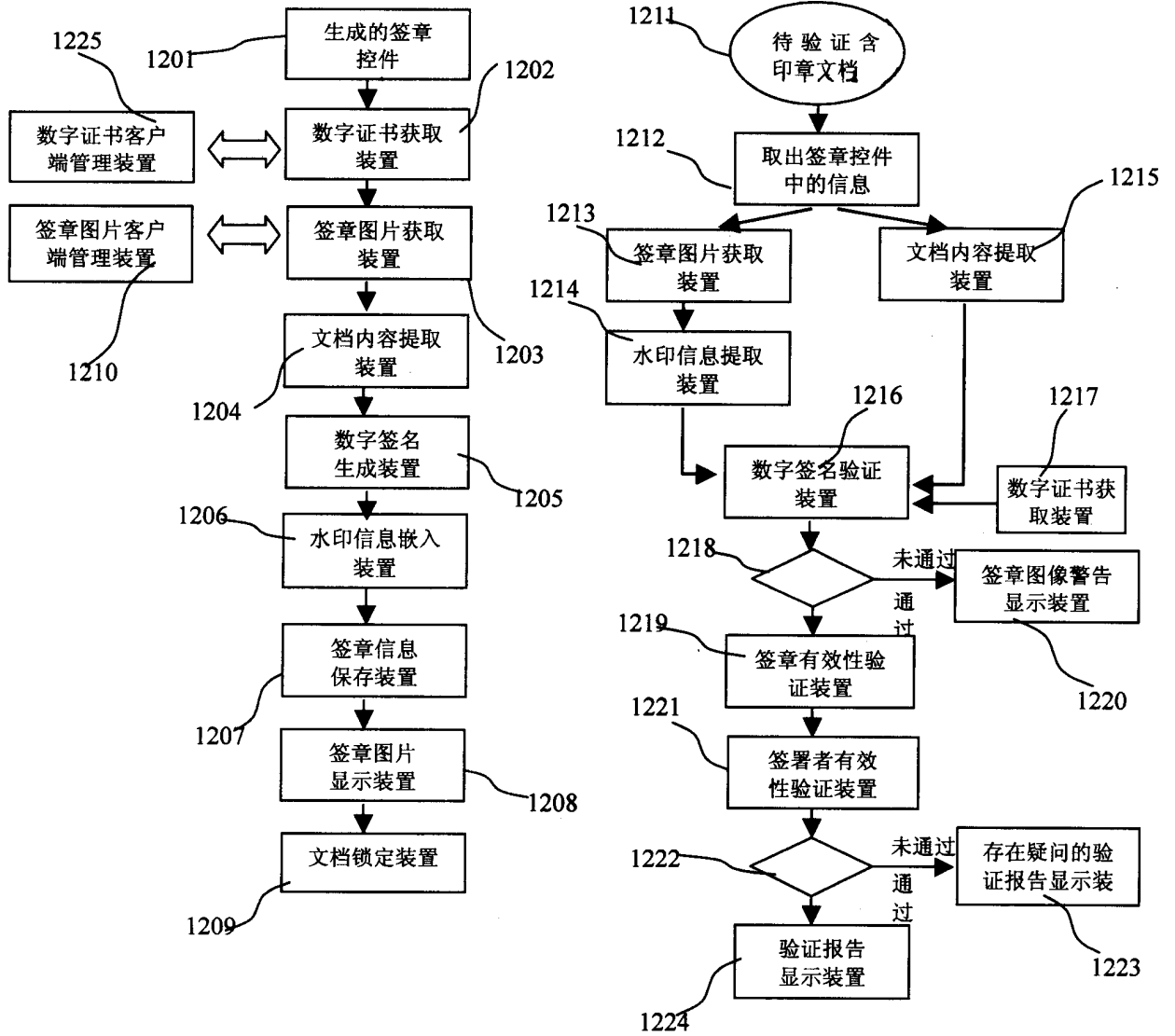


图 12A

图 12B