[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)
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710030493.3

[43] 公开日 2009 年 4 月 1 日

[11] 公开号 CN 101398915A

[22] 申请日 2007.9.24
[21] 申请号 200710030493.3
[71] 申请人 广州市百成科技有限公司
地址 510275 广东省广州市黄埔区云埔工业区埔南路 2 号
[72] 发明人 许兆然 张大年
权利要求书 2 页 说明书 6 页 附图 2 页

[54] 发明名称

一种基于互联网的电子印章平台系统

[57] 摘要

本发明涉及一种基于互联网的电子印章平台，涉及信息安全领域。 它是基于互联网面向公众应用的开放平台，将物理印章体系及应用电子化和网络化，采用了标准的多层结构。 具有电子印章的制作、发放、管理，查询，验证等功能，为用户提供电子印章，电子签名、身份确认、数据安全等服务。

1. 一种基于互联网的电子印章平台系统。平台集中储存和管理应用中电子印章。并通过互联网络为用户提供了电子印章的制作、发放、管理、备案、查询和验证等服务。

2. 如权利要求 1 所述的一种基于互联网的电子印章平台系统，其特征在于：电子印章制作与发放的主要步骤为：

   1）使用电子印章的用户首先去平台注册帐户，并在注册时提交数字证书做为标识信息与帐户绑定；

   2）电子印章平台系统管理员审核用户的注册帐户信息，同时可以修改帐户所绑定的证书，即重新绑定证书；

   3）电子印章平台系统印章管理员根据用户的要求制作印章外观。可以通过平台系统预定义模板制作，也可以由用户直接提交印章外观图片制作；

   4）电子印章平台系统印章管理员选择合适的水印图片嵌入到印章外观图像中，以保护印章图像的完整性；

   5）印章管理员输入各项信息，合成印章数据；同时使用印章管理员自己的证书对印章各项关键数据进行数字签名，实现印章数据来源可追溯性和完整性保护；

   6）印章数据制作完毕后，压缩储存在数据库中；

   7）印章管理员可以根据实际情况启用，暂停，销毁已制作电子印章；

   8）印章管理员可以将印章分配给使用用户，并将印章颁发给该用户；

   9）颁发印章时，印章管理员在操作计算机上插上装有步骤 1）中数字证书的安全设备（包括但不限于各种 USBKEY 和指纹签名器），然后选择印章要导入的设备类型，设置好使用次数等导入参数；

   10）系统检测插入的安全设备中是否有步骤 1）中绑定的用户证书；如果有，使用此证书签名，保证此证书的有效性；

   11）如果步骤 9）中签名通过，系统将印章数据写入安全设备中，数据在写入过程中是加密的；

   12）将写入印章数据的设备发放给相关用户，同时平台系统记录相关日志。

3. 如权利要求 1 所述的一种基于互联网的电子印章平台系统，其特征在于：包括中心服务器，Web 服务平台，系统管理控制台和印章管理控制台。中心服务器提供电子印章储存和管理的核心功能；Web 服务平台对外提供发布各种电子印章相关服务；系统管理控制台和印章管理控制台为后台管理控制程序，便于管理人员对印章平台进行操作管理。

4. 如权利要求 1 所述的一种基于互联网的电子印章平台系统，其特征在于：除了按 2 中所述步骤发放电子印章外，也支持印章在线使用。即印章集中储存在服务器上，分配给用户后就不再颁发导出。用户使用印章时需要登录电子印章平台系统，通过网络在线得到印章数据，进行签盖；

5. 如权利要求 2 所述的一种基于互联网的电子印章平台系统，其特征在于：在权利要求 2 的步骤 5）中被用于签名的印章各项关键数据包括：印章序列号，印章标题，印章所属单位，印章制作公文编号，

印章所嵌入水印编号，印章描述，印章制作者 ID；

6. 如权利要求 2 所述的一种基于互联网的电子印章平台系统，其特征在于：颁发到安全设备中的电子印章数据可以通过设置授权使用次数进行控制。每签盖一次印章设备中的授权使用次数减 1，当次数为 0 时，设备中的印章不能再被使用，只能通过重新授权或在线更新方式取得新授权；

7. 如权利要求 5 所述的一种基于互联网的电子印章平台系统，其特征在于：存放在安全设备中的电子印章可以通过在线更新的方式更新印章的最新状态和数据；

8. 如权利要求 2 所述的一种基于互联网的电子印章平台系统，其特征在于：用户也可以通过互联网络自己注册帐户，并提交证书进行绑定；

9. 如权利要求 7 所述的一种基于互联网的电子印章平台系统，其特征在于：用户可以通过互联网络申请提交印章制作请求，用户提交印章外观和其他印章信息。印章管理员在后台审批用户的印章请求；

10. 如权利要求 8 所述的一种基于互联网的电子印章平台系统，其特征在于：用户可以通过互联网络下载印章数据到安全设备中。用户在下载印章时，需要首先插上设备；然后使用设备中的证书签名，以保证用户的身份正确；最后再将印章数据下载到设备中；

11. 如权利要求 2 所述的一种基于互联网的电子印章平台系统，其特征在于：用户可以通过互联网络在线验证平台所发放印章的真实有效性；

12. 如权利要求 2 所述的一种基于互联网的电子印章平台系统，其特征在于：系统支持 DCOM 和 HTTP 两种数据通信模式；

13. 如权利要求 8，9，10 所述的一种基于互联网的电子印章平台系统，其特征在于：在进行印章数据的在线提交，在线更新和在线下载时，用户使用自己的数字证书对提交的数据签名，在平台服务器端对签名进行验证，以保证数据的完整性和来源可追溯性。

一种基于互联网的电子印章平台系统

技术领域

本发明涉及电子信息安全领域。它是基于互联网面向公众应用的开放平台，具有电子印章的制作、发放、管理，查询，验证等功能，为用户提供电子印章，电子签名、身份确认、数据安全等服务。

背景技术

PKI 技术

PKI(Pubic Key Infrastructure)是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。用户可利用 PKI 平台提供的服务进行安全通信。使用基于公钥技术系统的用户建立安全通信信任机制的基础是：网上进行的任何需要安全服务的通信都是建立在公钥的基础之上的，而与公钥成对的私钥只掌握在他们与之通信的另一方。这个信任的基础是通过公钥证书的使用来实现的。

对称加密

传统使用私密密钥(也称为对称密钥)对信息进行加密，加密和解密信息时使用同一个密钥。在通信双方进行数据加密之前，必须先将密钥进行安全交换。

非对称加密

与对称加密不同，公开密钥加密法的基本特点是加密与解密的密钥是不同的，它基于公钥密码体制。在这种加密系统中，使用一把公开密钥将明文转为密文，使用另外一把密钥(与公开密钥有关系，但不同)对信息进行解密，将密文转为明文。因此，在公开密钥算法中包含着一对公钥及私钥。公钥可公开存放，被其他用户访问，用来为密钥持有者发送加密信息。用户使用自己的私钥进行解密，由于私钥只被用户自己持有，因此可以保证加密信息的机密性。类似的，使用私钥对信息加密可以向对方确保信息来源于私钥拥有者，数字签名正基于此原理，

数字签名及验证

数字签名就是信息发送者用其私钥对从所传报文中提取出的数字摘要进行 RSA 算法加密操作，当信息接收者收到报文后，就可以用发送者的公钥对数字签名进行验证。因为只有用发送方的公钥才能正确解密，所以保证了信息发送者的身份认证和不可抵赖性；而接收方将得到的明文用与发送方相同的 HASH 算法运算，将得到的散列值与解密后的数字摘要对比，就可判断信息传输过程中是否被更改，从而保证了信息的完整性。

CA 与数字证书

单纯的 PKI 技术如数字加密，数字签名等并不能解决在电子环境下的信任和认证问题，必须有一种机制可以标明计算机电子网络环境下用户的身份，其他用户也可以通过这种机制对其身份进行验证。CA 是认证中心的英文 Certification Authority 的缩写。它为电子环境中各个实体颁发数字证书，以证明各实体

身份的真实性，并负责在交易中检验和管理证书；它是电子商务和网上银行交易的权威性、可信赖性及公正性的第三方机构。同时CA使得复杂的PKI技术以一种更简单，更符合人们使用习惯的应用形式出现。

数字证书是各实体在网上信息交流及商务交易活动中的身份证明。该数字证书具有唯一性。它将实体的公开密钥同实体本身联系在一起，为实现这一目的，必须使数字证书符合X.509国际标准，同时数字证书的来源必须是可靠的。CA认证机构专门负责数字证书的发放和管理，确保网上信息的安全。

数字水印

数字水印是一种信息隐藏技术，它将数字信号，如图像、文字、符号、数字等一切可以作为标记、标识的信息与原始数据(如图像、音频、视频数据)紧密结合并隐藏其中，并可以经历一些不破坏源数据价值的操作而能保存下来。

电子印章系统采用易碎水印来保护印章图像，当印章图象被更改后，哪怕是一个像素，都会破坏水印本身，从而达到验证保护的目的。

USB KEY技术

USB KEY以智能卡技术为基础。它是将一个带有微处理器、存储器等微型集成电路芯片的，具有标准规格的智能卡片和USB控制器及连接器结合在一起，包装在一个外壳中。具有快速运算、存储量大、安全性高以及难以破译和伪造等特点。

USB KEY可以和PKI技术紧密结合。一般设备都内置了高强度的加解密算法，而且可以在USB Key内极为安全的智能芯片上存储私有密钥和数字证书。从而保证了最核心的加解密运算可在设备内部完成。

此外，USB KEY便于携带，通过USB标准接口通讯，无需读卡设备。因此其用途十分广泛，网络银行、电子政务和电子商务等领域均已开始应用这种设备。

指纹验证

电子印章系统中的指纹验证和识别是通过专门的指纹仪来实现。指纹仪的作用有两点：1.存储用户数据：将一些重要数据如用户名、密码等存储到指纹仪中，用户使用这些数据时通过指纹验证，读出这些数据。2.存储用户私钥，并使用专门的CSP算法进行数字签名：在安装CA证书的时候，将证书的私钥存储到指纹仪中。等到需要进行数字签名的时候，通过指纹验证将私钥取出，进行数字签名。指纹验证识别有以下技术特点：智能图像处理、智能特征抽取、旋转不变性及平移不变性、模式特征点线结合，匹配准确度高、模糊快速搜索功能、智能神经网络、定点运算和嵌入式操作系统等。

发明背景

电子印章是物理印章体系的电子化和网络化，是电子网络中的身份确认与授权“手段”，它将现代科学技术和人们的传统习惯结合在一起。是传统印章发展到信息社会后的一个新的阶段。

电子印章通过使用硬软件技术，以电子化的方式模拟物理印章的使用，使用户在电子政务，电子商务等活动中拥有一种符合传统用章习惯的应用体验；同时电子印章又采用了先进的加密，签名，信息隐藏等

安全技术，从而是其具有物理印章不可比拟的安全性和可追溯性。

现阶段电子印章是数字签名技术的一项应用，但它把晦涩的电子签名技术变成了人们习以为常的签名盖章方式，更合符人们传统信用习惯与公信、诚信体系，大大消除了电子签名的应用障碍，对电子签名的应用推广具有非常巨大的价值。

在很多国家，电子签名已具有法律效力。《中华人民共和国电子签名法》第十三条规定同时满足下列四个条件的电子签名就视为可靠的电子签名，同时规定了可靠的电子签名与手写签名或者盖章具有同等的法律效力。

（一）电子签名制作数据用于电子签名时，属于电子签名人专有；

（二）签署时电子签名制作数据仅由电子签名人控制；

（三）签署后对电子签名的任何改动能够被发现；

（四）签署后对数据电文内容和形式的任何改动能够被发现。

电子印章平台本质上是一个电子印章中心服务机构，它基于计算机网络的，面向社会、面向公众的开放平台。它是物理印章管理体系的电子化与网络化的体现，它为各级用户提供了电子印章的制作、发放、管理、备案、查询和验证等服务。

电子印章平台是由电子印章管理系统发展而来，但它同时也是电子印章发展的必然趋势。只有平台的建立，电子印章的标准化，规范化和完全具有法律协力才有了技术基础。

发明内容

本发明中的电子印章系统在应用是将物理印章体系的电子化和网络化。电子印章在技术上是以数字签名技术为基础，但又不等同于数字签名，而是以更合符人们传统信用习惯与公信、诚信体系、让数字签名技术更快为人们所接受。在法律上电子印章系统满足《电子签名法》所规定的合法有效电子签名的四个条件。

此外电子印章系统还具有以下特点：

1.印章由中心系统集中制作、管理，其流程根据我国行政体制及其运作方法设计，同时和有关行业具体定义保持一致。印章管理中心本身就是一个印章权威管理部门的电子化体现。因此从源头保证了印章的权威性和唯一性。印章的制作、发放、管理直到销毁都严格依据国家有关政策和规定执行；

2．中心紧密结合用户权限来分发印章，通过使用安全硬件外设存储印章，保证了印章使用的安全和可控； 印章的制作、发放、使用和销毁都有严格的日志记录，有助于安全审计。用户可以在印章中心来鉴别验证印章本身的真实性和有效性；

3.具有较强的开放性。印章中心对外功能接口全面且清晰，可以和不同功能和特点的客户端结合，比如在线盖章客户端、离线盖章客户端，基于 Word/Excel 盖章客户端或基于 XML 的盖章客户端等，同样可以和未来新开发的客户端结合；

因为具有独立和开放的印章中心，使印章的使用安全性和权威性都大大增强，并且利于日后系统功能的扩展。

系统结构设计

本发明系统采用标准的多层体系结构，见附图 1：

系统为标准的多层结构，由数据库存储、中间应用层、Web 服务层和客户端表现层构成。

1．数据库层

数据库层负责系统的数据存储和逻辑功能。本系统采用大型关系数据库，具有较高的可伸缩性、可靠性和安全性。同时从降低到开发难度和提高性能的角度考虑，系统会将一些最基本的业务逻辑封装成存储过程，以方便中间应用层调用。本系统数据库的一个特点是绝大部分数据库逻辑功能使用存储过程完成，这样做的好处一是可以提高数据库操作速度；二是数据库逻辑变化时只需修改存储过程即可，不用修改并重新编译应用程序。目前数据库层支持的数据库产品是 MS SQL Server 2000 和 Oracle(9i 以上)

2．中间应用层

中间应用层是系统的核心，它提供了大部分的功能和服务。电子印章系统的中间应用层由 COM+组件构成，按照功能可以划分成四个逻辑功能部分：系统管理、印章管理、印章使用监督及验证和事件（业务数据）日志记录。系统管理组件完成系统基础数据，如单位、用户等数据的管理。印章制作组件提供印章制作、发放和管理功能，印章使用监督及验证组件提供印章使用日志的查询和印章合法性的验证功能；事件日志记录向业务系统提供重要业务数据的管理功能。上述 COM+组件主要是用来完成业务逻辑功能，被客户端调用。而数据访问组件提供的是统一的数据库操作服务，被其他 COM+组件调用。这样的设计里各组件功能清晰，业务逻辑和数据库存储分离，有利于系统的重用和扩展。通过 Windows 提供的“组件服务”控制台，可以很方便得部署和设置这些组件。

3．Web 层

Web 层由 Web 应用和 Web 服务构成，从结构图上可以看出它们调用和封装了中间业务层的功能接口，并已自己的形式发布出来。Web 应用层主要提供用户交互使用的功能界面，包括用户注册，印章在线申请，印章在线下载，印章在线查询以及平台后台管理等功能。而 Web 服务层提供不带有人机交互界面的服务功能，主要包括印章的在线更新，在线验证，印章申请在线提交，印章数据在线传递等功能。Web 服务层使用 XML 技术封装数据，使用 HTTP 协议传递数据。这样就保证了在复杂网络环境和多类型平台系统的 Internet 环境下应用电子印章服务。

4．管理控制台和客户端程序

系统管理控制台和印章管理控制台为普通的可执行程序，它们直接和中间应用层的 COM+组件服务器相连接，使用 DCOM 协议进行通信，因为 DCOM 协议对通信网络的要求较为严格，需要开放特定的端口，所以

系统管理控制台和印章管理控制台适用于安装在与印章服务器同一内网环境中或者同一台计算机上。

客户端由安全设备（硬件），二次控件包（软件）和完整的盖章软件组成。客户端系统基于专用的硬件设备，提供 PKI 功能，电子印章功能和重要数据安全存储功能，适用于复杂广域网环境下的各种应用模式。

现阶段完整的盖章软件包括基于 MS Word，MS Excel，金山 WPS 和 Acrobat PDF 的盖章软件。盖章软件由于基于的公文编辑软件不同而有不同的技术实现方式，但大体上都是通过公文编辑软件提供的特定 API 而实现插件或类似插件的功能，将盖章操作界面集成在公文编辑环境中，使用户像编辑公文那样使用电子印章的各项功能。已盖章文档中的印章也是以对象形式嵌入在文档中的，里面包含很多印章及文档的属性信息，而不是简单的图片加数字签名，这也就保证了印章的唯一性和不可复制性。

除了上述盖章客户端软件外，电子印章系统还提供二次开发包，其他应用系统通过开发包可以实现在窗体和 Web 页面上的电子印章应用。

此发明的应用实施步骤为：

1．构建标准电子印章平台，统一储存和管理整个平台应用中的电子印章。平台支持印章集中和分散使用两种模式。

2．标准电子印章平台包括中心服务器，Web 服务平台，系统管理控制台和印章管理控制台。中心服务器提供电子印章储存和管理的核心功能；Web 服务平台对外提供发布各种电子印章相关服务；系统管理控制台和印章管理控制台为后台管理控制程序，便于管理人员对印章平台进行操作管理。

3．使用电子印章的用户首先去平台注册帐户，并在注册时提交数字证书做为标识信息与帐户绑定；

4．电子印章平台系统管理员审核用户的注册帐户信息，同时可以修改帐户所绑定的证书，即重新绑定证书；

5．电子印章平台系统印章管理员根据用户的要求制作印章外观。可以通过平台系统预定义模板制作，也可以由用户直接提交印章外观图片制作；

6．电子印章平台系统印章管理员选择合适的水印图片嵌入到印章外观图像中，以保护印章图像的完整性；

7．印章管理员输入各项信息，合成印章数据；同时使用印章管理员自己的证书对印章各项关键数据进行数字签名，实现印章数据来源可追溯性和完整性保护；

8．印章数据制作完毕后，压缩储存在数据库中；

9．印章管理员可以根据实际情况启用，暂停，销毁已制作电子印章；

10．印章管理员可以将印章分配给使用用户，并将印章颁发给该用户；

11．颁发印章时，印章管理员在操作计算机上插上装有步骤 1）中数字证书的安全设备（包括但不限于各种 USBKEY 和指纹签名器），然后选择印章要导入的设备类型，设置好使用次数等导入参数；

12．系统检测插入的安全设备中是否有步骤 1）中绑定的用户证书；如果有，使用此证书签名，保证此证书的有效性；

13．如果步骤 11 中签名通过，系统将印章数据写入安全设备中，数据在写入过程中是加密的；

14．将写入印章数据的设备发放给相关用户，同时平台系统记录相关日志。

此发明有以下有益成果,可见附图 2：

1．可以在 G2B 业务系统和部分 G2G 应用中，采用印章分散管理和使用的模式。

2．通过与电子印章二次开发接口相结合，用户使用安全设备就可以在业务系统中使用其中的证书和电子印章。通过授权使用次数的技术手段，可以保证印章分散使用的受控和使用记录信息的收集。

3．在 G2G 应用中 ，用户必须登录进电子印章系统在线使用印章。因此用户需要安装应用电子印章机要客户端系统，配备专有的安全设备，比如指纹签名器。即可在业务系统，如内部 OA 中完成电子公文签章发文应用、收文验章应用。由于上述过程都是实时在线的，因此印章的使用都是有严格控制并有及时而充分的记录。

4．G2G 系统中其他不需要使用印章的用户，可选择安装电子印章验证端客户端系统，用于对电子公文真伪性验证应用。

5．用户可以通过印章申请及发放终端，在广域网上申请、下载、更新，查询及验证印章

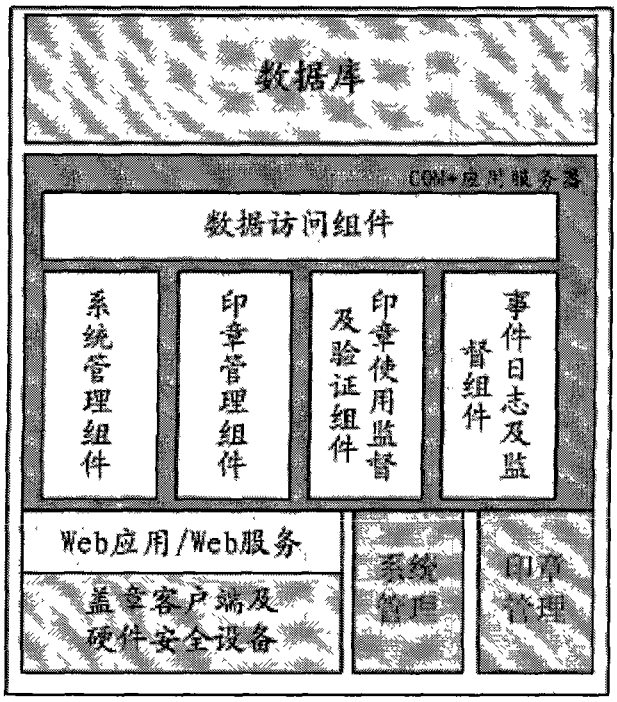
数据库
COM+应用服务器
数据访问组件
系统管理组件
印章管理组件
印章使用监督及验证组件
事件日志及监督组件
Web应用/Web服务
盖章客户端及硬件安全设备
系统管理
印章管理

图 1

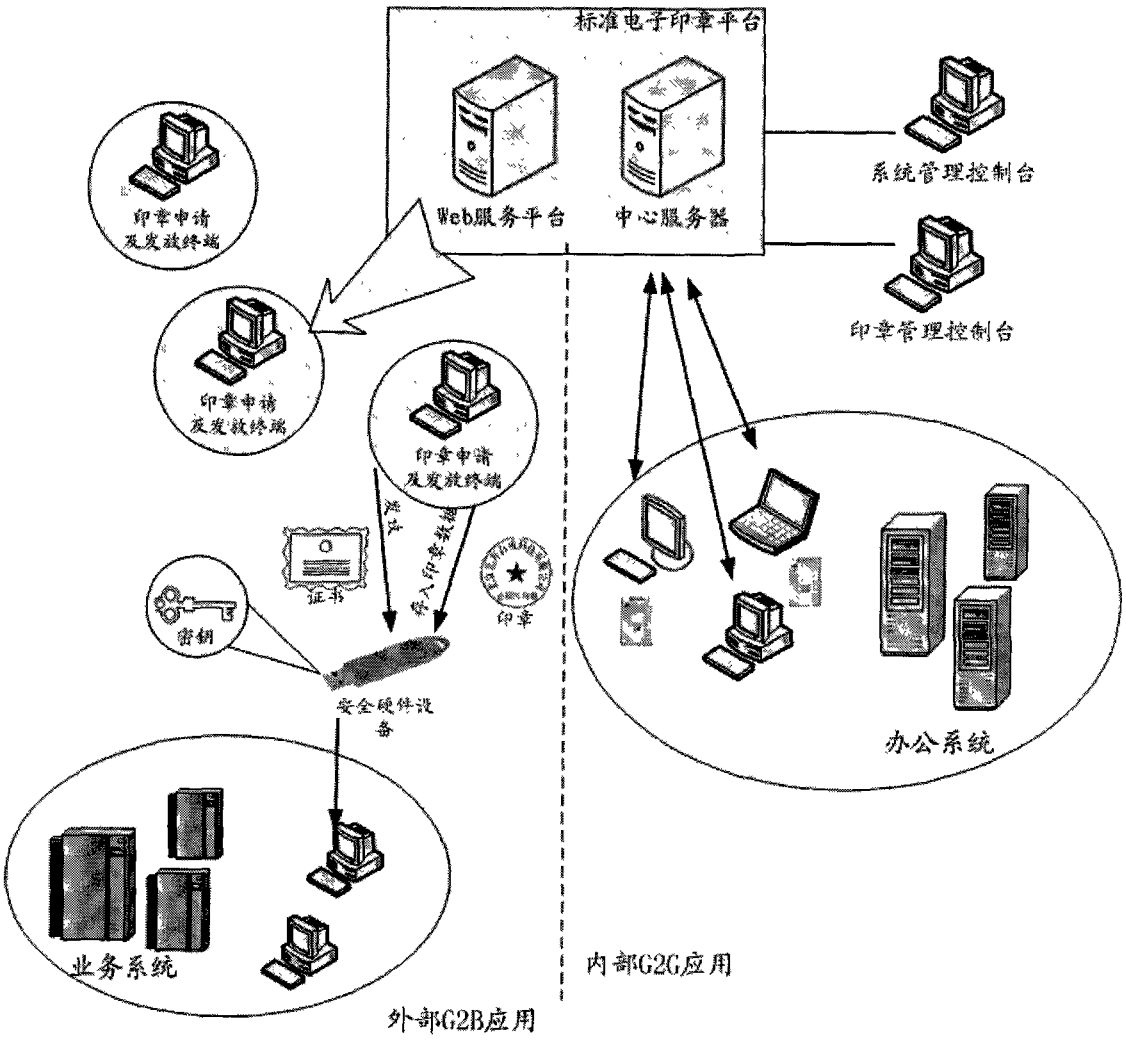
标准电子印章平台
Web服务平台
中心服务器
系统管理控制台
印章管理控制台
印章申请及发放终端
印章申请及发放终端
印章申请及发放终端
证书
密钥
印章
安全硬件设备
办公系统
业务系统
内部G2G应用
外部G2B应用

图 2