

## (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  
2017 年 2 月 16 日 (16.02.2017)



(10) 国际公布号  
**WO 2017/024934 A1**

- (51) 国际专利分类号:  
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2016/091524
- (22) 国际申请日: 2016 年 7 月 25 日 (25.07.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:  
201510484844.2 2015 年 8 月 7 日 (07.08.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 高翔 (GAO, Xiang) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。胡远平 (HU, Yuanping) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法

务部, Zhejiang 311121 (CN)。刘凯 (LIU, Kai) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。贡鹏 (GONG, Peng) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。汪卫国 (WANG, Weiguo) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA,

[见续页]

(54) Title: ELECTRONIC SIGNING METHOD, DEVICE AND SIGNING SERVER

(54) 发明名称: 实现电子签章的方法、装置及签章服务器

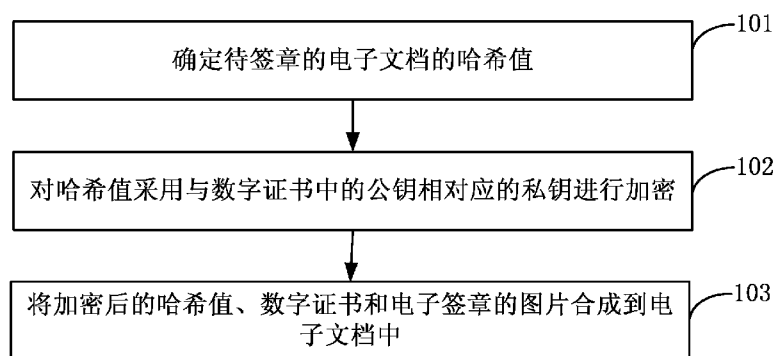


图 1A

101 DETERMINE A HASH VALUE OF AN ELECTRONIC DOCUMENT TO BE SIGNED  
102 PERFORM ENCRYPTION ON THE HASH VALUE BY USING A PRIVATE KEY  
CORRESPONDING TO A PUBLIC KEY OF A DIGITAL CERTIFICATE  
103 SYNTHESIZE THE ENCRYPTED HASH VALUE, THE DIGITAL CERTIFICATE AND  
AN IMAGE OF AN ELECTRONIC SIGNATURE IN THE ELECTRONIC DOCUMENT

(57) Abstract: The present application provides an electronic signing method and device. The method comprises: determining a hash value of an electronic document to be signed; performing encryption on the hash value by using a private key corresponding to a public key of a digital certificate; and synthesizing the encrypted hash value, the digital certificate and an image of an electronic signature in the electronic document. The technical solution of the present invention addresses the problem of a high implementation cost of a USBKey signing solution in the prior art, thus providing an Internet signing mode and reducing costs for users.

(57) 摘要: 本申请提供一种实现电子签章的方法及装置, 该方法包括: 确定待签章的电子文档的哈希值; 对所

述哈希值采用与数字证书中的公钥相对应的私钥进行加密; 将所述加密后的哈希值、所述数字证书和所述电子签章的图片合成到所述电子文档中。在本发明的技术方案可以解决现有技术中的 U 盾签章方案实施成本高的问题, 实现互联网签章的模式, 降低用户成本。



WO 2017/024934 A1



RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

- (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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR,

**本国际公布:**

— 包括国际检索报告(条约第 21 条(3))。

## 实现电子签章的方法、装置及签章服务器

### 技术领域

本申请涉及互联网技术领域，尤其涉及一种实现电子签章的方法、装置及签章服务器。

### 5 背景技术

当需要对大型互联网金融企业为用户提供的电子文件进行电子签章时，现有技术通过电子签章所用的私钥是放置在U盾中，当用户使用电子签章时，将U盾插入电脑，电子签章系统通过获取U盾内的与数字证书中的公钥相对应的私钥对电子文档进行签章，由于使用该方案的前提是必须使用户购买U盾，因此当大量用户需要电子签章时，实施成本高，推广难度大。

### 发明内容

有鉴于此，本申请提供一种新的技术方案，可以解决在用户量大时以互联网方式实时申请电子文档的电子签章，降低电子签章过程的硬件成本的技术问题。

15 为实现上述目的，本申请提供技术方案如下：

根据本申请的第一方面，提出了一种实现电子签章的方法，包括：

确定待签章的电子文档的哈希值；

对所述哈希值采用与数字证书中的公钥相对应的私钥进行加密；

20 将所述加密后的哈希值、所述数字证书和所述电子签章的图片合成到所述电子文档中。

根据本申请的第二方面，提出了一种实现电子签章的方法，包括：

确定待签章的电子文档的哈希值；

将所述电子文档的所述哈希值、第二秘钥通过第二专用网络发送给所述

第三方业务平台，所述第二秘钥由所述签章服务器和所述第三方业务平台之间预设的秘钥；

在所述第三方业务平台采用所述第二秘钥对所述哈希值进行加密后，通过所述第二专用网络接收所述加密后的所述哈希值；

5 将所述加密后的哈希值、数字证书和电子签章的图片合成到所述电子文档中。

根据本申请的第三方面，提出了一种实现电子签章的装置，包括：

确定模块，用于确定待签章的电子文档的哈希值；

第一加密模块，用于对所述确定模块确定的所述哈希值采用与数字证书  
10 中的公钥相对应的私钥进行加密；

签章合成模块，用于将所述第一加密模块加密后的所述哈希值、所述数字证书和所述电子签章的图片合成到所述电子文档中。

根据本申请的第四方面，提出了一种签章服务器，包括：

处理器；用于存储所述处理器可执行指令的存储器；

15 其中，所述处理器被配置为：

确定待签章的电子文档的哈希值；

对所述哈希值采用与数字证书中的公钥相对应的私钥进行加密；

将所述加密后的哈希值、所述数字证书和所述电子签章的图片合成到所述电子文档中。

20 根据本申请的第五方面，提出了一种签章服务器，包括：

处理器；用于存储所述处理器可执行指令的存储器；

其中，所述处理器被配置为：

确定待签章的电子文档的哈希值；

将所述电子文档的所述哈希值、第二秘钥通过第二专用网络发送给所述  
25 第三方业务平台，所述第二秘钥由所述签章服务器和所述第三方业务平台之间预设的秘钥；

在所述第三方业务平台采用所述第二秘钥对所述哈希值进行加密后，通

过所述第二专用网络接收所述加密后的所述哈希值；

将所述加密后的哈希值、数字证书和电子签章的图片合成到所述电子文档中。

由以上技术方案可见，本申请通过对哈希值采用与数字证书中的公钥相对应的私钥进行加密，将加密后的哈希值、数字证书和电子签章的图片合成到电子文档中，从而解决了现有技术中的U盾签章方案实施成本高的问题，实现了互联网签章的模式，降低了用户成本，通过对哈希值加密以及将加密后的哈希值和数字证书合成到电子文档上，提升了电子签章的安全性和公信力。

## 10 附图说明

图1A示出了根据本发明的一示例性实施例的实现电子签章的方法的流程示意图；

图1B示出了根据本发明的一示例性实施例的电子签章的图片的示意图；

图1C示出了根据本发明的一示例性实施例的数字证书的示意图；

15 图2A示出了根据本发明的另一示例性实施例的实现电子签章的方法的流程示意图；

图2B示出了根据本发明的另一示例性实施例的场景图；

图3A示出了根据本发明的又一示例性实施例的实现电子签章的方法的流程示意图；

20 图3B示出了根据本发明的又一示例性实施例的场景图；

图4A示出了根据本发明的又一示例性实施例的实现电子签章的方法的流程示意图；

图4B示出了根据本发明的又一示例性实施例的场景图；

图5示出了根据本发明的一示例性实施例的签章服务器的结构示意图；

25 图6示出了根据本发明的一示例性实施例的实现电子签章装置的结构示意图；

图 7 示出了根据本发明的另一示例性实施例的实现电子签章装置的结构示意图。

## 具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本发明相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本发明的一些方面相一致的装置和方法的例子。

在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在...时”或“当...时”或“响应于确定”。

为对本申请进行进一步说明，提供下列实施例：

根据本申请一个实施例，通过对哈希值采用与数字证书中的公钥相对应的私钥进行加密，将加密后的哈希值、数字证书和电子签章的图片合成到电子文档中，从而解决了现有技术中的 U 盾签章方案实施成本高的问题，实现了互联网签章的模式，降低了用户成本，通过对哈希值加密以及将加密后的哈希值和数字证书合成到电子文档上，提升了电子签章的安全性和公信力。

图 1A 示出了根据本发明的一示例性实施例的实现电子签章的方法的流

程示意图，图 1B 示出了根据本发明的一示例性实施例的电子签章的示意图，图 1C 示出了根据本发明的一示例性实施例的数字证书的示意图；可以应用在签章服务器上。如图 1A 所示，实现电子签章的方法包括如下步骤：

步骤 101，确定待签章的电子文档的哈希值；

5 步骤 102，对哈希值采用与数字证书中的公钥相对应的私钥进行加密；

步骤 103，将加密后的哈希值、数字证书和电子签章的图片合成到电子文档中。

在步骤 101 中，在一实施例中，电子文档可以是本地文件（例如，证明文件、电子回单等）；在另一实施例中，电子文档可以来自第一业务平台，10 第一业务平台可以为支付类金融业务平台（例如，支付宝），相应的，电子文档可以为资产证明、账单、电子回单；在另一实施例中，电子文档可以来自第二业务平台，第二业务平台可以为存款类金融业务平台（例如，招财宝），相应的，电子文档可以为借款和利息证明；在再一实施例中，电子文档可以来自第三业务平台，第三业务平台可以为互联网金融业务平台（例如，网商15 银行），相应的，电子文档可以为终端用户申请的电子凭证等等，由此可知，本申请对电子文档的来源不做限制。

在一实施例中，电子签章可以为第一业务平台对应的企业的电子签章、第二业务平台对应的企业的电子签章、第三业务平台对应的企业的电子签章。在一实施例中，可以通过哈希（Hash）算法提取电子文档的哈希值。

20 在步骤 102 中，在一实施例中，可以根据电子文档的来源确定对哈希值的加密方式，例如，如果电子文档来自第一业务平台，可以在签章服务器中设置加密机，通过加密机的第一秘钥（也可称为主秘钥，MainKey）来加密数字证书中的私钥；再例如，如果电子文档来自第二业务平台，可以通过第一专用网络将哈希值发送给第三方认证中心（例如，CA 中心），由第三方25 认证中心通过使用与数字证书中的公钥相对应的私钥对哈希值进行加密，之后通过第一专用网络将加密后的哈希值返还给签章服务器；再例如，如果电子文档来自第三业务平台，可以将哈希值、签章服务器和第三方金融平台之

间设定的第二秘钥通过第二专用网络发送给第三业务平台的加密机，由第三业务平台通过加密机采用双方设定的第二秘钥对哈希值进行加密，之后，第三业务平台再将加密后的哈希值返回给签章服务器。通过对不同来源的电子文档采用不同的加密方式对哈希值进行加密，还可以满足个性化的业务需求。

5       在步骤 103 中，在一实施例中，可以从相应的业务平台（第一业务平台、第二业务平台、第三业务平台）获取相应的电子签章的图片，将加密后的哈希值、数字证书和电子签章的图片合成到电子文档中的合成方式可以参见现有技术的相关描述，在此不再详述。

      如图 1B 所示，合成在电子文档上的电子签章为“AB 公司”，当监听到  
10       “AB 公司”的电子签章上的点击事件时，显示图 1C 所示的数字证书的相关信息，由于数字证书是通过第三方认证中心获取到的，因此可以使用户通过数字证书验证电子签章的真伪性。

      由上述描述可知，本发明实施例通过步骤 S101-S103 实现了互联网签章的模式，解决了现有技术中的 U 盾签章方案实施成本高的问题，降低了用户  
15       成本，通过对哈希值加密以及将加密后的哈希值和数字证书合成到电子文档上，提升了电子签章的安全性和公信力。

      图 2A 示出了根据本发明的另一示例性实施例的实现电子签章的方法的流程示意图，图 2B 示出了根据本发明的另一示例性实施例的实现电子签章的方法的场景图；本实施例以电子文档来自第一业务平台提供为例进行示例  
20       性说明。如图 2A 所，实现电子签章的方法包括如下步骤：

      步骤 201，确定待签章的电子文档的哈希值；

      步骤 202，获取数字证书以及数字证书中的公钥相对应的私钥，该私钥经过加密的；

      步骤 203，对经过加密的私钥进行解密；

25       步骤 204，采用解密后的私钥对哈希值进行加密；

      步骤 205，将加密后的哈希值、数字证书和电子签章的图片合成到电子文档中。

上述步骤 201 的描述可以参见上述步骤 101 的相关描述,在此不再详述。

在步骤 202 至步骤 204 中,在一实施例中,可以从云端数据库获取数字证书和经过加密的私钥,其中,可以通过签章服务器上的加密机的第一秘钥(也可称为主秘钥)对与数字证书中的公钥相对应的私钥进行加密,之后存储  
5 存储在云端数据库中,在需要时在对存储在云端数据库的经过加密的私钥进行解密。在另一实施例中,云端数据库可以存储有海量的数字证书和与数字证书中的公钥相对应的私钥,从而实现对大量数字证书和与数字证书中的公钥相对应的私钥的安全存储。

上述步骤 205 的描述可以参见上述步骤 103 的相关描述,在此不再详述。

10 作为一个示例性场景,如图 2B 所示,签章服务器 22 从第三方认证中心 21 申请了数字证书,通过签章服务器 22 本地的加密机(图中未示)的第一秘钥来加密与数字证书中的公钥相对应的私钥,将加密后的私钥和数字证书存储至云端数据库 23 中。签章服务器 22 从第一业务平台 24 获取到需要进行电子签章的电子文档,采用哈希算法提取电子文档的哈希值,从云端数据库  
15 23 获取数字证书和经过加密的私钥,连同哈希值一起传送到签章服务器 22 本地的加密机中,在签章服务器 22 本地的加密机中对与数字证书中的公钥相对应的私钥进行解密,得到与数字证书中的公钥相对应的私钥,加密机再对哈希值采用该私钥进行加密,最后,签章服务器 22 将加密后的哈希值、数字证书和电子签章合成到电子文档上,进而可以将电子文档提供给用户。由于  
20 通过第一秘钥对与数字证书中的公钥相对应的私钥进行解密,以及通过与数字证书公钥相对应的私钥对哈希值加密的过程都在签章服务器的加密机的内部处理,因此确保了与数字证书中的公钥相对应的私钥在使用过程的安全。

本实施例中,由于在云端数据库存储了数字证书和加密后的私钥,在对电子文档进行电子签章时,从云端数据库获取数字证书和数字证书的加密后的私钥,可以避免现有技术中在第三方认证中心的加密机只能保存有限  
25 数量的与数字证书中的公钥相对应的私钥,从而可以支持互联网签章的大数据量和高并发的特性,并确保了与数字证书中的公钥相对应的私钥的安全性。

图 3A 示出了根据本发明的又一示例性实施例的实现电子签章的方法的流程示意图, 图 3B 示出了根据本发明的又一示例性实施例的实现电子签章的方法的场景图; 本实施例以电子文档由第二业务平台提供进行示例性说明。如图 3A 所示, 实现电子签章的方法包括如下步骤:

5        步骤 301, 确定待签章的电子文档的哈希值;

      步骤 302, 将电子文档的哈希值通过第一专用网络发送给第三方认证中心, 其中, 第三方认证中心用于生成数字证书并采用与数字证书中的公钥相对应的私钥对哈希值加密;

      步骤 303, 通过第一专用网络接收来自第三方认证中心加密后的哈希值;

10       步骤 304, 将加密后的哈希值、数字证书和电子签章的图片合成到电子文档中。

      上述步骤 301 的描述可以参见上述步骤 101 的相关描述, 在此不再详述。

      在步骤 302 和步骤 303 中, 在一实施例中, 第一专用网络可以为连接在签章服务器和认证中心的专用通信网络, 在该专用通信网络中未接入其他设备, 通过第一专用网络传输哈希值和加密后的哈希值, 可以确保哈希值的安全性。

      上述步骤 304 的描述可以参见上述步骤 103 的相关描述, 在此不再详。

      作为一个示例性场景, 如图 3B 所示, 签章服务器 31 与第三方认证中心 32 联合签章。在联合签章过程中, 签章服务器 31 通过哈希算法提取电子文档的哈希值, 签章服务器 31 通过第一专用网络将哈希值发送给第三方认证中心 32, 由第三方认证中心 32 使用与数字证书中的公钥相对应的私钥对哈希值进行加密, 之后, 通过第一专用网络将加密后的哈希值返回给签章服务器 31, 签章服务器 31 将加密后的哈希值、数字证书、电子签章合成到电子文档中, 进而可以将电子文档提供给用户。

25       本实施例中, 将电子文档的哈希值通过第一专用网络发送给第三方认证中心, 在第三方认证中心通过与数字证书中的公钥相对应的私钥对哈希值进行加密后, 通过第一专用网络接收加密后的哈希值, 将加密后的哈希值、数

字证书和电子签章的图片合成到电子文档中，解决了现有技术中的 U 盾签章方案实施成本高的问题，降低了用户成本，通过利用存储在第三方认证中心的与数字证书中的公钥相对应的私钥对哈希值加密，再将数字证书、加密后的哈希值合成到电子文档上，提升了电子签章的公信力，同时，可以使电子文档不出被泄漏至其它无关的企业，确保电子文档的商业安全。

图 4A 示出了根据本发明的又一示例性实施例的实现电子签章的方法的流程示意图，图 4B 示出了根据本发明的又一示例性实施例的实现电子签章的方法的场景图；本实施例以电子文档来自第三业务平台提供为例进行示例性说明。如图 4A 所示，实现电子签章的方法包括如下步骤：

10 步骤 401，确定待签章的电子文档的哈希值；

步骤 402，将电子文档的哈希值、第二秘钥通过第二专用网络发送给第三方业务平台，其中，第二秘钥为签章服务器和第三方业务平台之间预设的秘钥或者共同协商的密钥；

步骤 403，通过第二专用网络接收加密后的哈希值；

15 步骤 404，将加密后的哈希值、数字证书和电子签章的图片合成到电子文档中。

上述步骤 401 的描述可以参见上述步骤 101 的相关描述，在此不再详述。

在步骤 402 和步骤 403 中，在一实施例中，第二专用网络可以为连接在签章服务器和第三方业务平台的专用通信网络，在该专用通信网络中未接入  
20 其他设备，通过第二专用网络传输哈希值和加密后的哈希值，可以确保哈希值的安全性。在一实施例中，第三方业务平台可以为上述实施例中的第一业务平台、第二业务平台、第三业务平台等能够提供电子文档的平台。

上述步骤 404 的描述可以参见上述步骤 103 的相关描述，在此不再详。

作为一个示例性场景，如图 4B 所示，签章服务器 41 从第三方业务平台  
25 42 获取电子文档，采用哈希算法提取电子文档的哈希值，将哈希值传输给第三方业务平台 42 的加密机，由第三方业务平台 42 的加密机通过第二秘钥对哈希值进行加密，然后第三业务平台 42 将加密后的哈希值返还给的签章服务

器 41, 签章服务器 41 将加密后的哈希值、数字证书、电子签章合成到电子文档中, 进而可以将电子文档提供给用户。

本实施例可以满足第三方业务平台 42 要求保管与数字证书中的公钥相对应的私钥的需求, 提高了电子签章方式的灵活性。

5 通过上述实施例, 可以在不同的业务场景中有着不同的电子签章的适用方案, 因此在发挥各种电子签章的使用方案的优势时, 满足了个性化的业务需求。

对应于上述的实现电子签章的方法, 本申请还提出了图 5 所示的根据本申请的一示例性实施例的签章服务器的示意结构图。请参考图 5, 在硬件层  
10 面, 该网络服务器包括处理器、内部总线、网络接口、内存以及非易失性存储器, 当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行, 在逻辑层面上形成实现电子签章的装置。当然, 除了软件实现方式之外, 本申请并不排除其他实现方式, 比如逻辑器件抑或软硬件结合的方式等等, 也就是说以下处理流程的执行主体  
15 并不限于各个逻辑单元, 也可以是硬件或逻辑器件。

图 6 为根据本发明的一示例性实施例的实现电子签章的装置的结构示意图; 如图 6 所示, 该实现电子签章的装置可以包括: 确定模块 61、第一加密模块 62、签章合成模块 63。其中:

确定模块 61, 用于确定待签章的电子文档的哈希值;

20 第一加密模块 62, 用于对确定模块 61 确定的哈希值采用与数字证书中的公钥相对应的私钥进行加密;

签章合成模块 63, 用于将第一加密模块 62 加密后的哈希值、数字证书和电子签章的图片合成到电子文档中。

图 7 为根据本发明的一示例性实施例的实现电子签章的装置的结构示意图; 如图 7 所示, 在上述图 6 所示实施例的基础上, 第一加密模块 62 可包括:  
25

获取单元 621, 用于获取数字证书以及与数字证书中的公钥相对应的私钥, 该私钥是经过加密的;

解密单元 622, 用于对获取单元 621 取到的经过加密的私钥进行解密;

加密单元 623, 用于采用解密单元 622 解密后的私钥对哈希值进行加密。

在一实施例中, 装置还可包括:

第二加密模块 64, 用于通过第一秘钥对与数字证书中的公钥相对应的私  
5 钥进行加密;

存储模块 65, 用于存储第二加密模块 64 加密后的私钥和数字证书。

在一实施例中, 数字证书和加密后的私钥从云端数据库获取。

在一实施例中, 第一加密模块 62 可包括:

第一发送单元 624, 用于将电子文档的哈希值通过第一专用网络发送给  
10 第三方认证中心, 其中, 第三方认证中心用于生成数字证书并采用与数字证  
书中的公钥相对应的私钥对哈希值加密;

第一接收单元 625, 用于通过第一专用网络接收来自第三方认证中心加  
密后的哈希值。

在一实施例中, 第一专用网络为连接在签章服务器和第三方认证中心的  
15 专用通信网络。

在一实施例中, 装置还可包括:

发送模块 66, 用于将电子文档的哈希值、第二秘钥通过第二专用网络发  
送给第三方业务平台, 其中, 第二秘钥为签章服务器和第三方业务平台之间  
预设的秘钥;

20 接收模块 67, 用于通过第二专用网络接收来自第三方认证中心加密后的  
哈希值。

上述实施例可见, 可以在不同的业务场景中有着不同的电子签章的适用  
方案, 因此在发挥各种电子签章的使用方案的优势时, 满足了个性化业务需  
求。

25 本领域技术人员在考虑说明书及实践这里公开的发明后, 将容易想到本  
申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性  
变化, 这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申

请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

## 权 利 要 求 书

1、一种实现电子签章的方法，其特征在于，应用于签章服务器上，所述方法包括：

确定待签章的电子文档的哈希值；

5 对所述哈希值采用与数字证书中的公钥相对应的私钥进行加密；

将所述加密后的哈希值、数字证书和电子签章的图片合成到所述电子文档中。

2、根据权利要求 1 所述的方法，其特征在于，所述对所述哈希值采用与数字证书中的公钥相对应的私钥进行加密，包括：

10 获取数字证书以及与所述数字证书中的公钥相对应的私钥，该私钥是经过加密的；

对所述经过加密的私钥进行解密；

采用所述解密后的私钥对所述哈希值进行加密。

3、根据权利要求 2 所述的方法，其特征在于，所述方法还包括：

15 通过第一秘钥对所述私钥进行加密；

存储所述数字证书和加密后的私钥。

4、根据权利要求 2 所述的方法，其特征在于，所述数字证书和所述经过加密的私钥从云端数据库获取。

5、根据权利要求 1 所述的方法，其特征在于，所述对所述哈希值采用与数字证书中的公钥相对应的私钥进行加密，包括：

将所述电子文档的所述哈希值通过第一专用网络发送给第三方认证中心，其中，所述第三方认证中心用于生成所述数字证书并采用与所述数字证书中的公钥相对应的私钥对所述哈希值加密；

25 通过所述第一专用网络接收来自所述第三方认证中心加密后的所述哈希值。

6、根据权利要求 5 所述的方法，其特征在于，所述第一专用网络为连接

在所述签章服务器和所述第三方认证中心的专用通信网络。

7、一种实现电子签章的方法，其特征在于，应用于签章服务器上，所述方法包括：

确定待签章的电子文档的哈希值；

5 将所述电子文档的所述哈希值、第二秘钥通过第二专用网络发送给所述第三方业务平台，所述第二秘钥为所述签章服务器和所述第三方业务平台之间预设的秘钥；

在所述第三方业务平台采用所述第二秘钥对所述哈希值进行加密后，通过所述第二专用网络接收加密后的哈希值；

10 将所述加密后的哈希值、数字证书和电子签章的图片合成到所述电子文档中。

8、根据权利要求 7 所述的方法，其特征在于，所述第二专用网络为连接在签章服务器和所述第三业务平台的专用通信网络。

9、一种实现电子签章的装置，其特征在于，所述装置包括：

15 确定模块，用于确定待签章的电子文档的哈希值；

第一加密模块，用于对所述确定模块确定的所述哈希值采用与数字证书中的公钥相对应的私钥进行加密；

签章合成模块，用于将所述第一加密模块加密后的所述哈希值、所述数字证书和所述电子签章的图片合成到所述电子文档中。

20 10、根据权利要求 9 所述的装置，其特征在于，所述第一加密模块包括：

获取单元，用于获取数字证书以及与所述数字证书中的公钥相对应的私钥，该私钥是经过加密的；

解密单元，用于对所述获取单元获取到的所述经过加密的私钥进行解密；

25 加密单元，用于采用所述解密单元解密后的所述私钥对所述哈希值进行加密。

11、根据权利要求 10 所述的装置，其特征在于，所述装置还包括：

第二加密模块，用于通过第一秘钥对与所述数字证书中的公钥相对应的

私钥进行加密；

存储模块，用于存储所述数字证书和与所述数字证书中的公钥相对应的私钥。

12、根据权利要求 10 所述的装置，其特征在于，所述数字证书和所述加密后的私钥从云端数据库获取。

13、根据权利要求 9 所述的装置，其特征在于，所述第一加密模块包括：

第一发送单元，用于将所述电子文档的所述哈希值通过第一专用网络发送给所述第三方认证中心，其中，所述第三方认证中心用于生成所述数字证书并采用与所述数字证书中的公钥相对应的私钥对所述哈希值加密；

10 第一接收单元，用于通过所述第一专用网络接收来自所述第三方认证中心加密后的所述哈希值。

14、根据权利要求 13 所述的装置，其特征在于，所述第一专用网络为连接在所述签章服务器和所述第三方认证中心的专用通信网络。

15、根据权利要求 9 所述的装置，其特征在于，所述装置还包括：

15 发送模块，用于将所述电子文档的所述哈希值、第二秘钥通过第二专用网络发送给所述第三业务平台，所述第二秘钥为所述签章服务器和所述第三方业务平台之间预设的秘钥；

接收模块，用于通过所述第二专用网络接收来自所述第三方认证中心加密后的所述哈希值。

20 16、根据权利要求 15 所述的装置，其特征在于，所述第二专用网络为连接在签章服务器和所述第三业务平台的专用通信网络。

17、一种签章服务器，其特征在于，所述签章服务器包括：

处理器；

用于存储处理器可执行指令的存储器；

25 其中，所述处理器被配置为：

确定待签章的电子文档的哈希值；

对所述哈希值采用与数字证书中的公钥相对应的私钥进行加密；

将加密后的所述哈希值、所述数字证书和电子签章的图片合成到所述电子文档中。

18、一种签章服务器，其特征在于，所述签章服务器包括：

处理器；

5 用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为：

确定待签章的电子文档的哈希值；

10 将所述电子文档的所述哈希值、第二密钥通过第二专用网络发送给所述第三方业务平台，所述第二密钥由所述签章服务器和所述第三方业务平台之间预设的密钥；

在所述第三方业务平台采用所述第二密钥对所述哈希值进行加密后，通过所述第二专用网络接收所述加密后的所述哈希值；

将所述加密后的哈希值、数字证书和电子签章的图片合成到所述电子文档中。

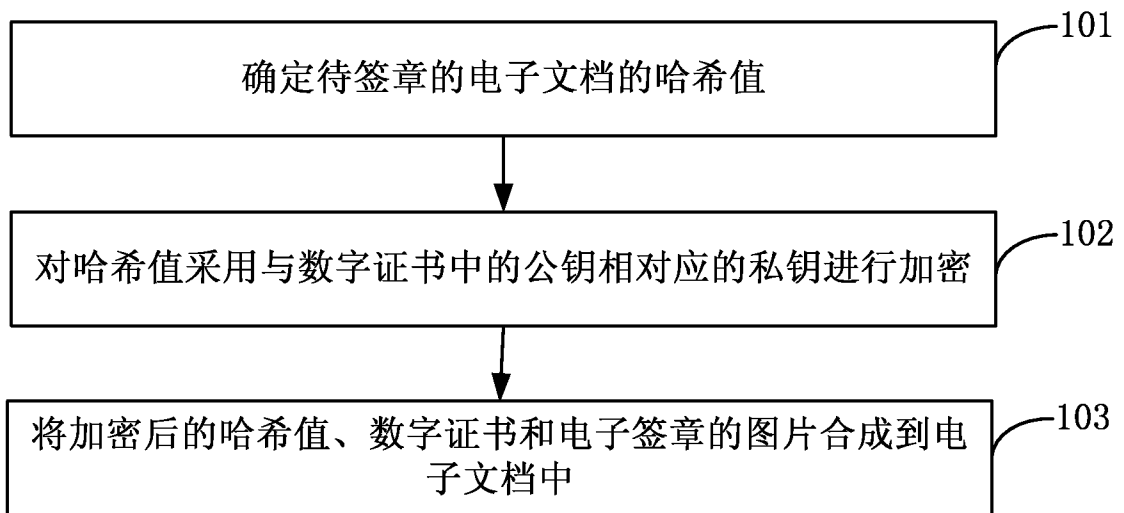


图 1A

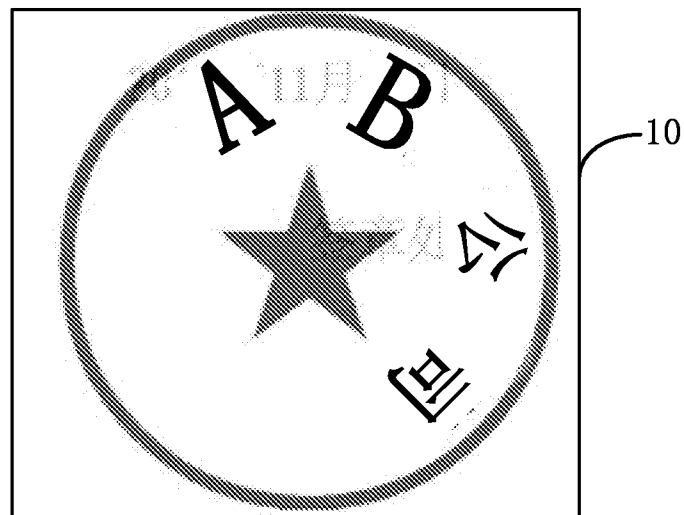


图 1B

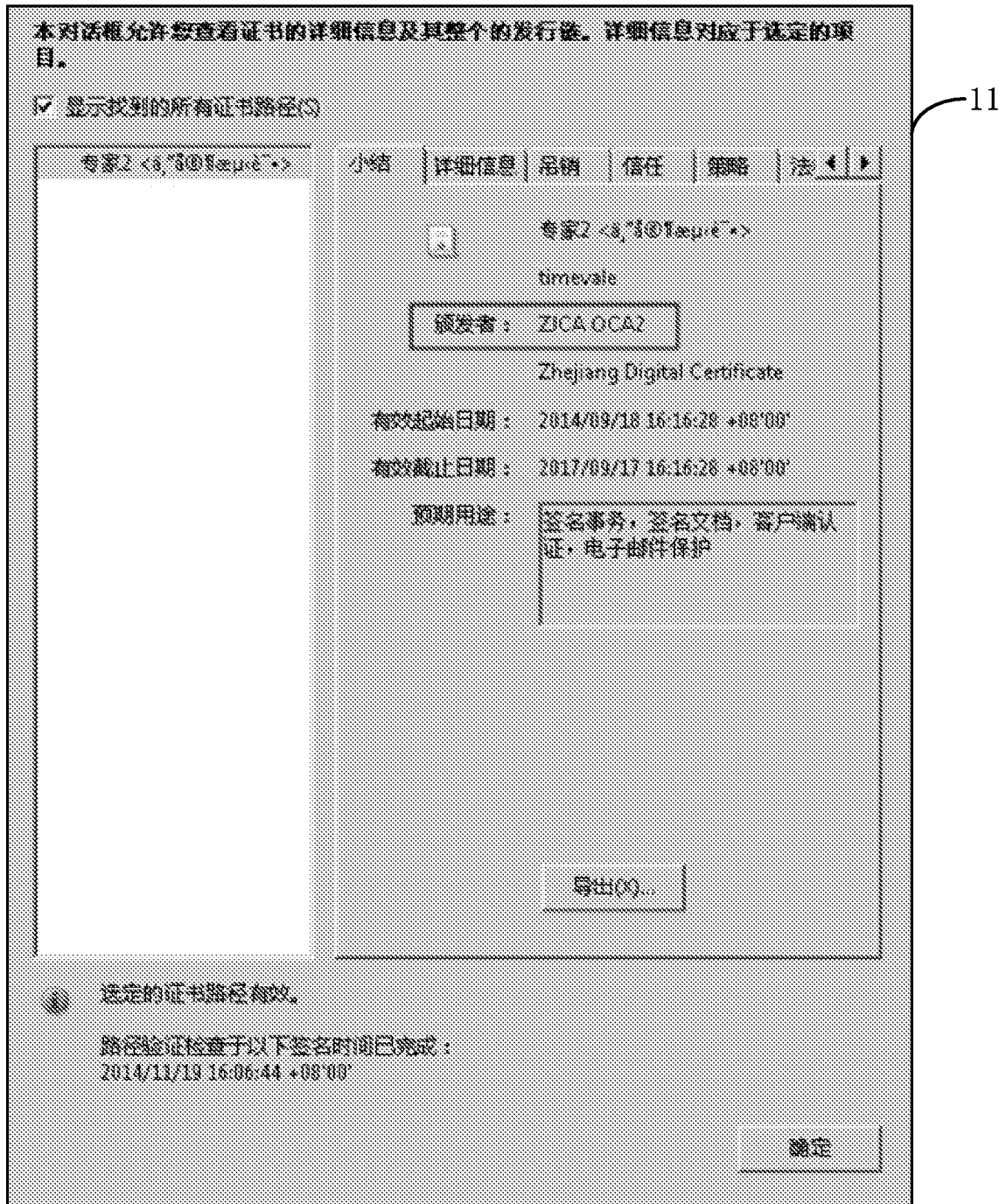


图 1C

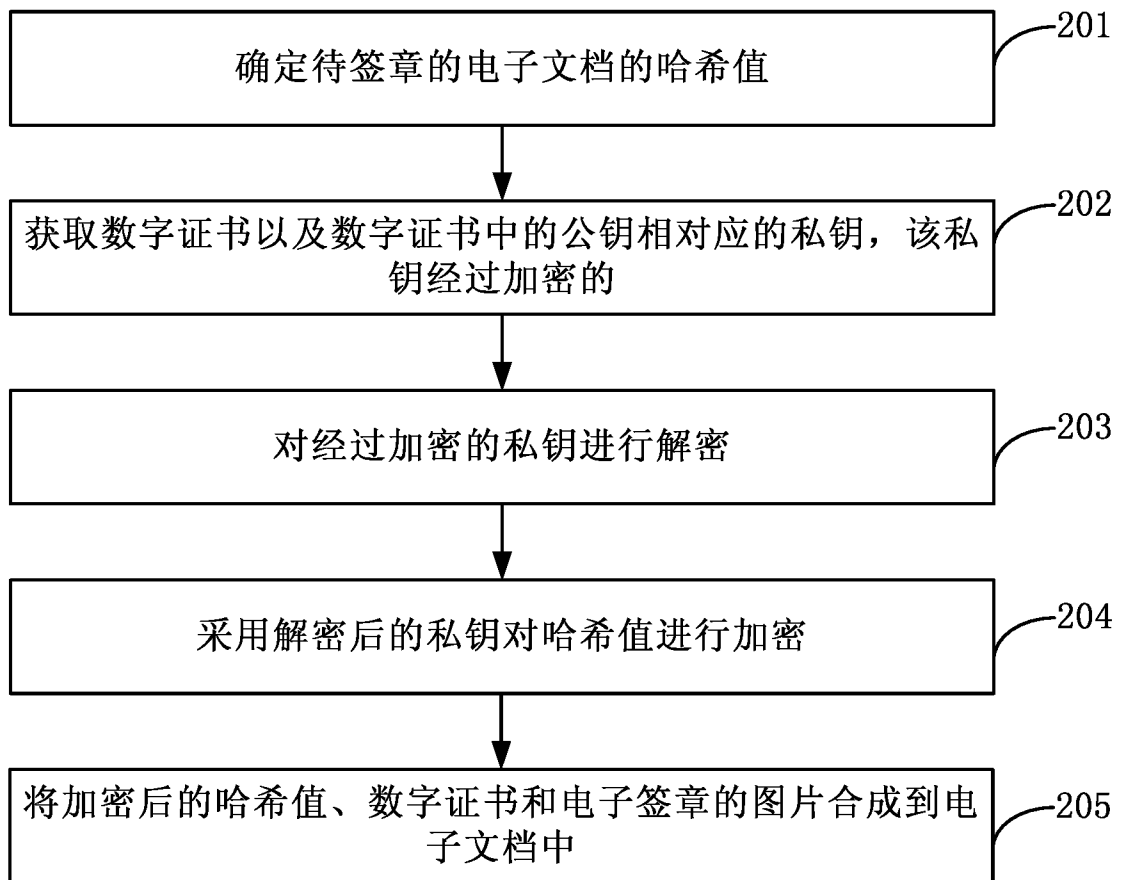


图 2A

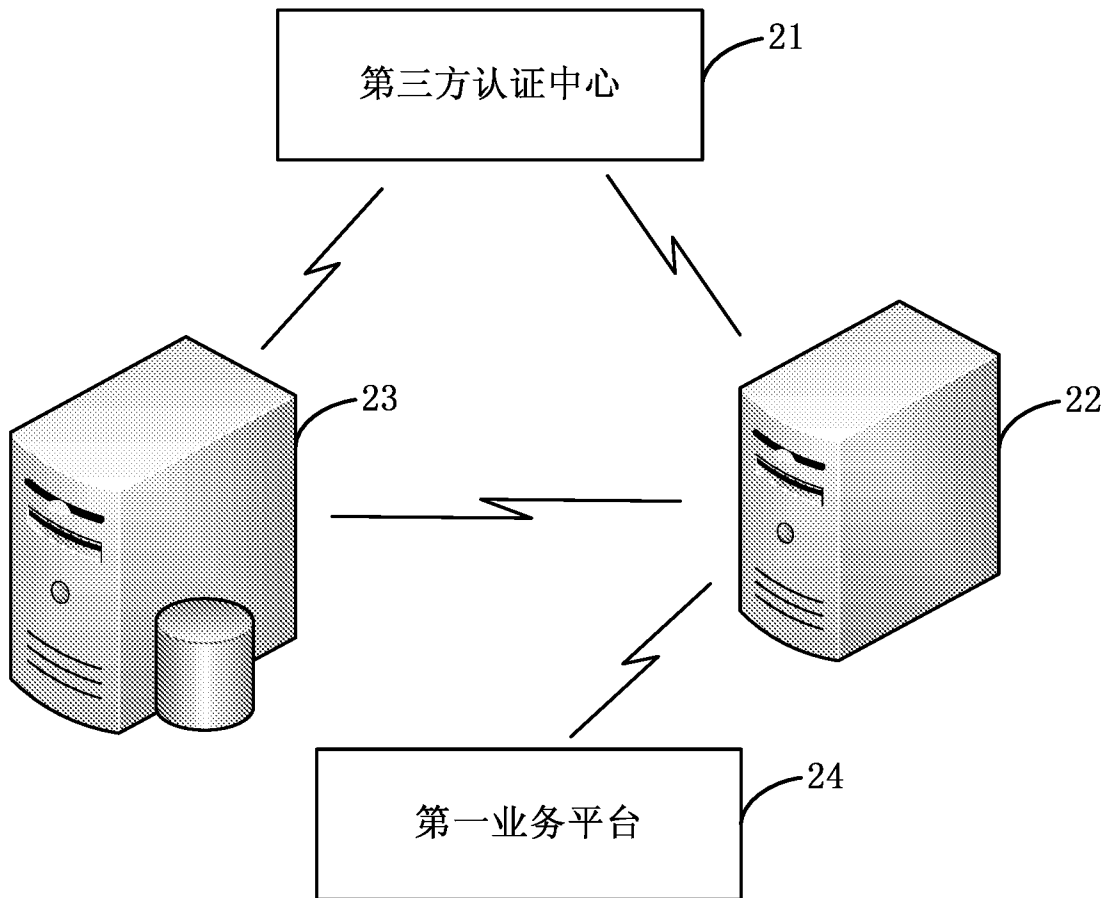


图 2B

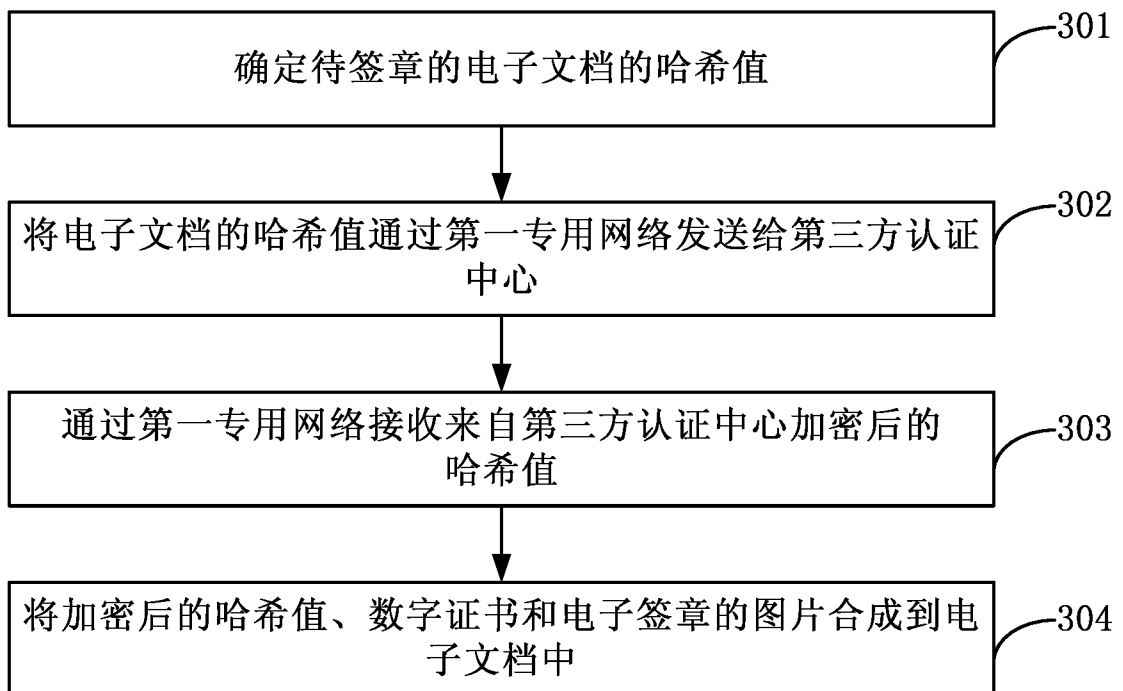


图 3A

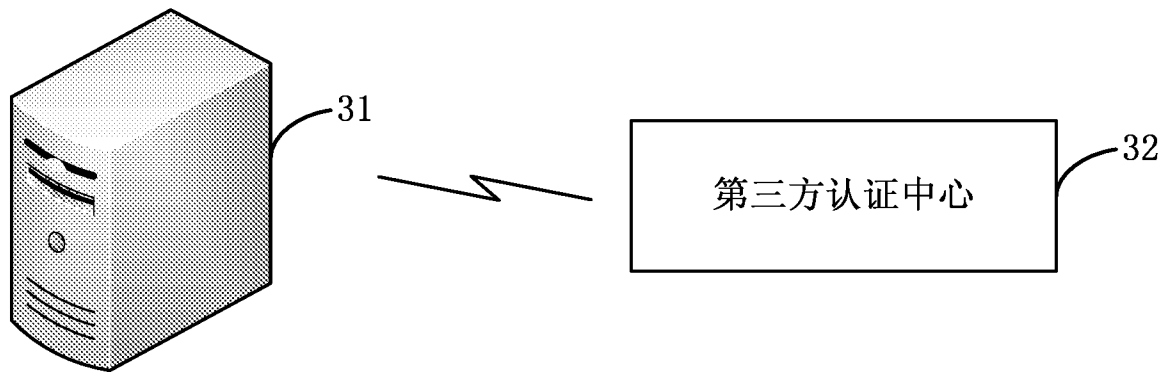


图 3B

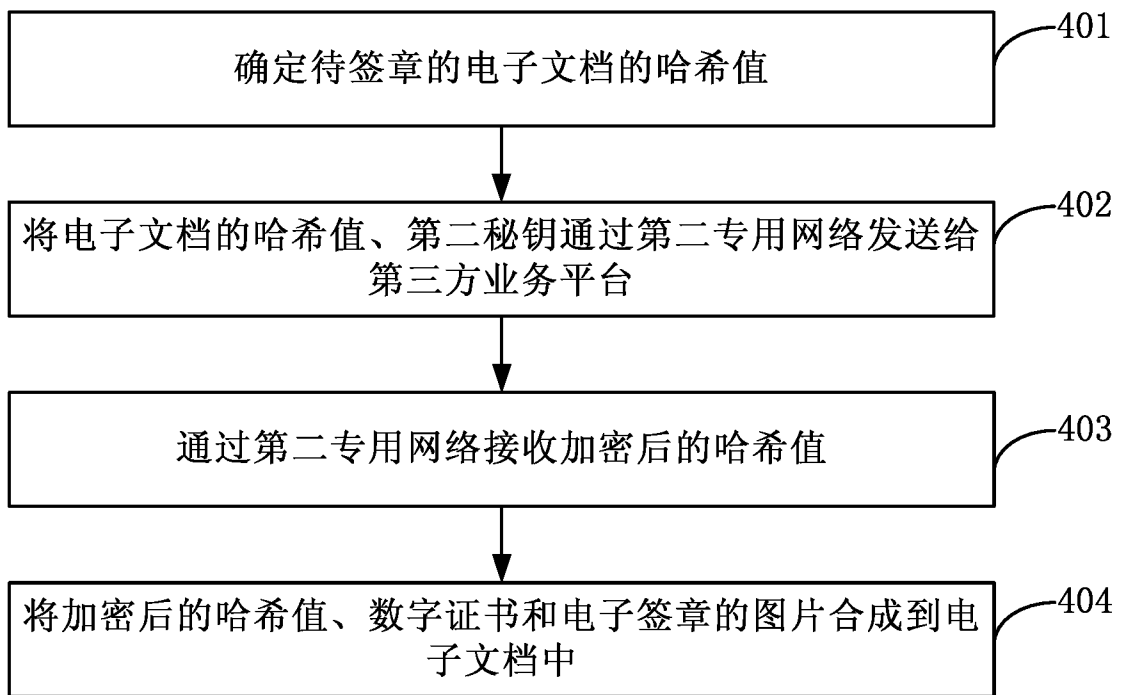


图 4A

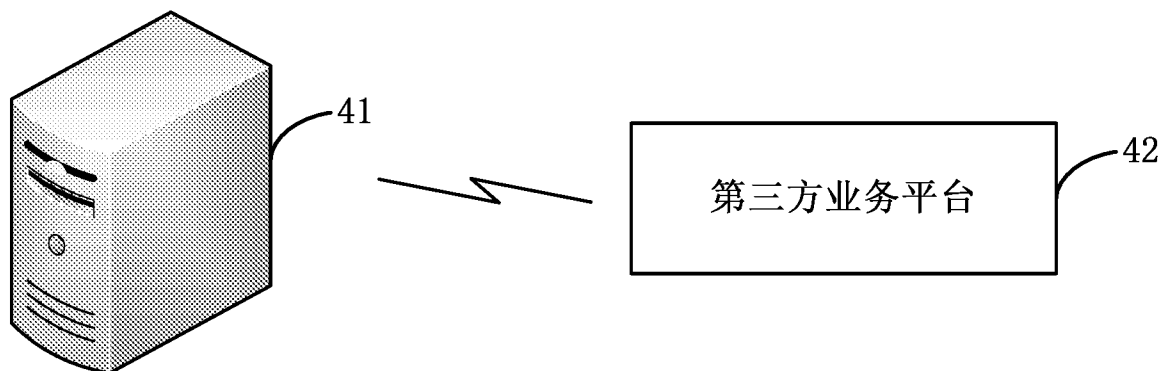


图 4B

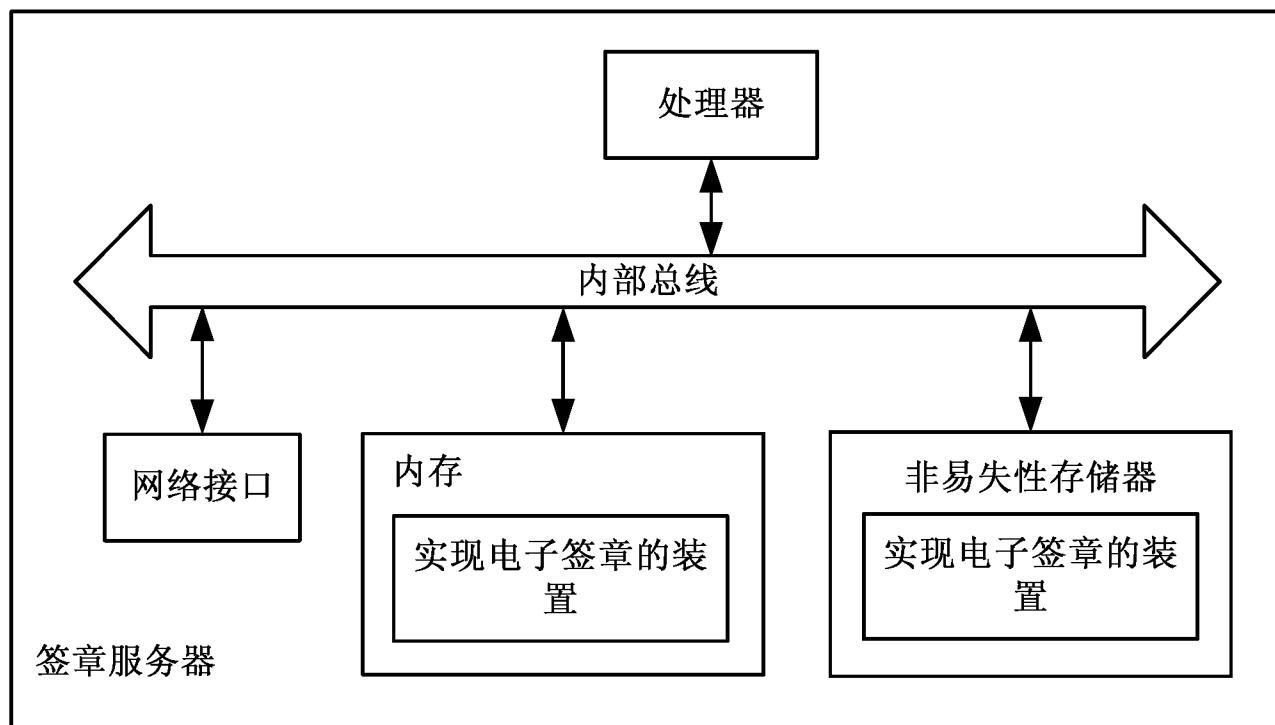


图 5

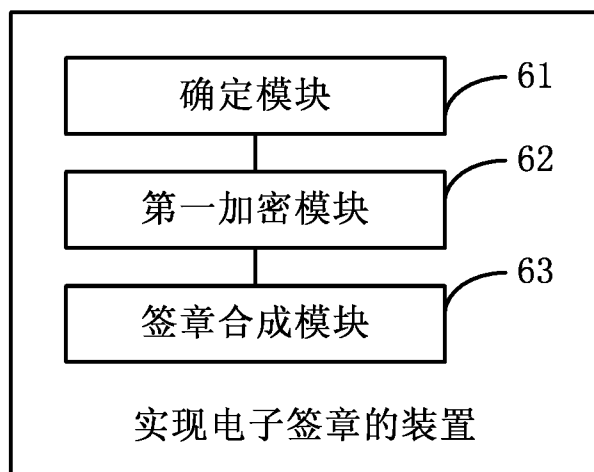


图 6

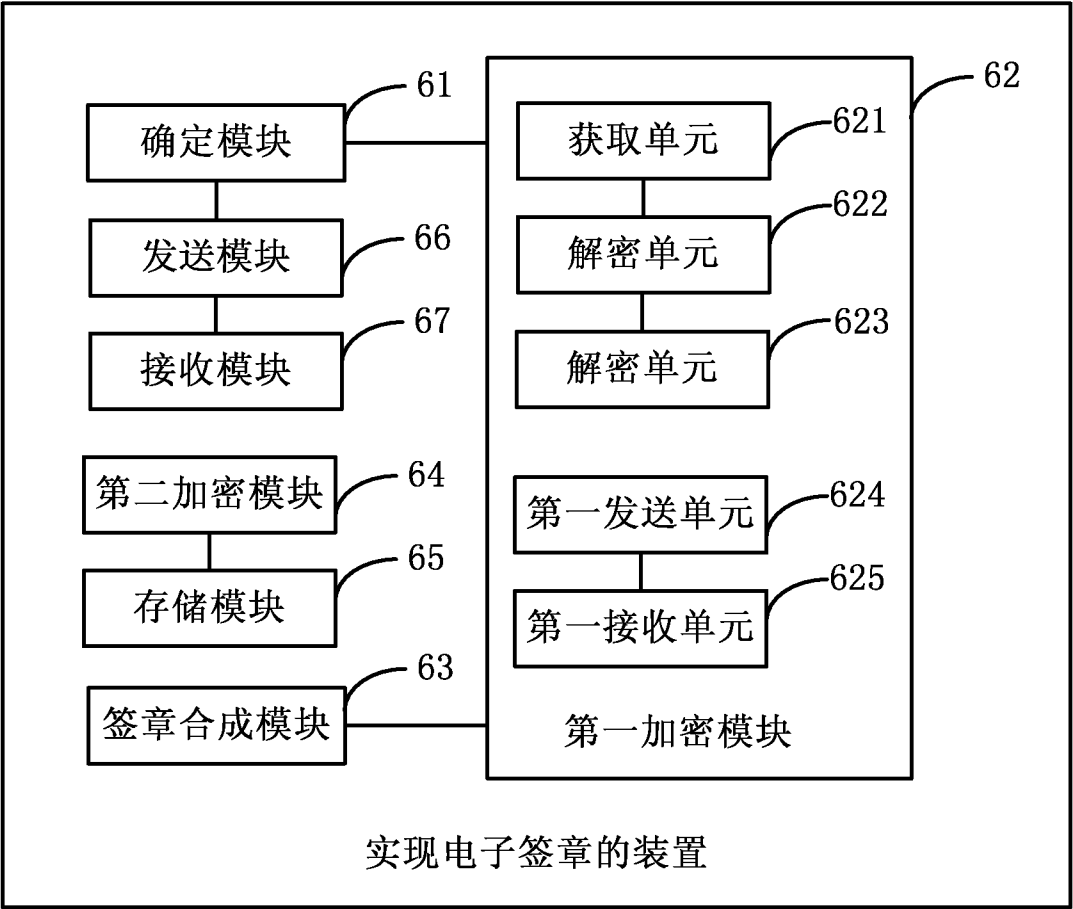


图 7

# INTERNATIONAL SEARCH REPORT

International application No.

**PCT/CN2016/091524**

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT; CNKI; WPI; EPODOC; IEEE: electronic signature, certify, digital certificate, public key, private key, secret key, ELECTRONIC, SIGNATURE, DOCUMENT, CONTRACT, HASH, ABSTRACT, PRIVATE, PUBLIC, ENCRYPT+, WATERMARK, PICTURE

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                               | Relevant to claim No. |
|-----------|------------------------------------------------------------------------------------------------------------------|-----------------------|
| X         | CN 103873255 A (HANGZHOU DIANZI UNIVERSITY), 18 June 2014 (18.06.2014), description, paragraphs [0038]-[0044]    | 1-18                  |
| X         | US 2005132195 A1 (DIETL, J.), 16 June 2005 (16.06.2005), description, paragraphs [0059]-[0061]                   | 1-18                  |
| A         | CN 103259665 A (FUJIAN ETIM INFORMATION & TECHNOLOGY CO., LTD.), 21 August 2013 (21.08.2013), the whole document | 1-18                  |
| A         | CN 101714222 A (LIU, Xueming et al.), 26 May 2010 (26.05.2010), the whole document                               | 1-18                  |

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

|                                                                                                                                                                         |                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| * Special categories of cited documents:                                                                                                                                | “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention                                              |
| “A” document defining the general state of the art which is not considered to be of particular relevance                                                                | “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone                                                                     |
| “E” earlier application or patent but published on or after the international filing date                                                                               | “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art |
| “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) | “&” document member of the same patent family                                                                                                                                                                                                    |
| “O” document referring to an oral disclosure, use, exhibition or other means                                                                                            |                                                                                                                                                                                                                                                  |
| “P” document published prior to the international filing date but later than the priority date claimed                                                                  |                                                                                                                                                                                                                                                  |

|                                                                                                                                                                                                                    |                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Date of the actual completion of the international search<br>26 September 2016 (26.09.2016)                                                                                                                        | Date of mailing of the international search report<br><b>24 October 2016 (24.10.2016)</b> |
| Name and mailing address of the ISA/CN:<br>State Intellectual Property Office of the P. R. China<br>No. 6, Xitucheng Road, Jimenqiao<br>Haidian District, Beijing 100088, China<br>Facsimile No.: (86-10) 62019451 | Authorized officer<br><b>XIN, Haiming</b><br>Telephone No.: (86-10) <b>82246953</b>       |

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.

**PCT/CN2016/091524**

| Patent Documents referred<br>in the Report | Publication Date | Patent Family    | Publication Date  |
|--------------------------------------------|------------------|------------------|-------------------|
| CN 103873255 A                             | 18 June 2014     | None             |                   |
| US 2005132195 A1                           | 16 June 2005     | US 2007277042 A1 | 29 November 2007  |
|                                            |                  | WO 2005060152 A1 | 30 June 2005      |
|                                            |                  | EP 1704667 A1    | 27 September 2006 |
|                                            |                  | AT 458325 T      | 15 March 2010     |
| CN 103259665 A                             | 21 August 2013   | None             |                   |
| CN 101714222 A                             | 26 May 2010      | None             |                   |

## 国际检索报告

国际申请号

PCT/CN2016/091524

## A. 主题的分类

H04L 9/32 (2006.01) i

按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类

## B. 检索领域

检索的最低限度文献 (标明分类系统和分类号)

H04L; G06Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))

CNPAT; CNKI; WPI; EPODOC; IEEE: 电子签章, 文档, 合同, 证明, 哈希, 散列, 摘要, 数字证书, 公钥, 私钥, 密钥, 加密, 图片, ELECTRONIC, SIGNATURE, DOCUMENT, CONTRACT, HASH, ABSTRACT, PRIVATE, PUBLIC, ENCRYPT+, WATERMARK, PICTURE

## C. 相关文件

| 类 型* | 引用文件, 必要时, 指明相关段落                                                               | 相关的权利要求 |
|------|---------------------------------------------------------------------------------|---------|
| X    | CN 103873255 A (杭州电子科技大学) 2014年 6月 18日 (2014 - 06 - 18)<br>说明书第0038-0044段       | 1-18    |
| X    | US 2005132195 A1 (DIETL, JOSEF) 2005年 6月 16日 (2005 - 06 - 16)<br>说明书第0059-0061段 | 1-18    |
| A    | CN 103259665 A (福建伊时代信息科技股份有限公司) 2013年 8月 21日 (2013 - 08 - 21)<br>全文            | 1-18    |
| A    | CN 101714222 A (刘学明 等) 2010年 5月 26日 (2010 - 05 - 26)<br>全文                      | 1-18    |

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

\* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&amp;” 同族专利的文件

国际检索实际完成的日期

2016年 9月 26日

国际检索报告邮寄日期

2016年 10月 24日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)  
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10) 62019451

受权官员

辛海明

电话号码 (86-10) 82246953

国际检索报告  
关于同族专利的信息

国际申请号

PCT/CN2016/091524

| 检索报告引用的专利文件 |            |    | 公布日<br>(年/月/日) | 同族专利 |            |    | 公布日<br>(年/月/日) |
|-------------|------------|----|----------------|------|------------|----|----------------|
| CN          | 103873255  | A  | 2014年 6月 18日   | 无    |            |    |                |
| US          | 2005132195 | A1 | 2005年 6月 16日   | US   | 2007277042 | A1 | 2007年 11月 29日  |
|             |            |    |                | WO   | 2005060152 | A1 | 2005年 6月 30日   |
|             |            |    |                | EP   | 1704667    | A1 | 2006年 9月 27日   |
|             |            |    |                | AT   | 458325     | T  | 2010年 3月 15日   |
| CN          | 103259665  | A  | 2013年 8月 21日   | 无    |            |    |                |
| CN          | 101714222  | A  | 2010年 5月 26日   | 无    |            |    |                |

表 PCT/ISA/210 (同族专利附件) (2009年7月)