(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106170006 A
(43)申请公布日 2016.11.30

(21)申请号 201610867436.X

(22)申请日 2016.09.29

(71)申请人 广州鹤一互联网科技有限公司
地址 510000 广东省广州市天河区黄埔大道西78号3601房自编之四

(72)发明人 曹海

(74)专利代理机构 北京超凡志成知识产权代理事务所(普通合伙) 11371
代理人 邓超

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

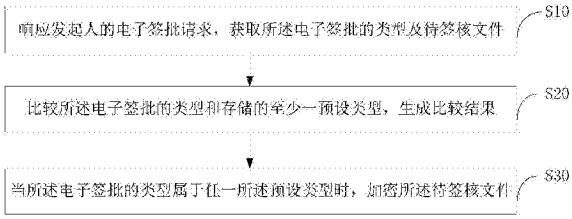
权利要求书2页 说明书7页 附图2页

(54)发明名称

一种电子签批安全管理方法及系统

(57)摘要

本发明提出了一种电子签批安全管理方法，包括：响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件；比较所述电子签批的类型和存储的至少一预设类型；当所述电子签批的类型属于所述预设类型时，加密所述待签核文件。本发明还提供了一种电子签批安全管理系统。该电子签批安全管理方法及系统自动识别发起人发起的电子签批的类型，并根据存储的至少一预设类型判断该电子签批的重要性，对属于预设类型的电子签批加密传输，从而避免非法分子对重要信息的窃取，对用户造成不必要的损失。



CN 106170006 A

1.一种电子签批安全管理方法，其特征在于，包括：

响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件；

比较所述电子签批的类型和存储的至少一预设类型；

当所述电子签批的类型属于任一所述预设类型时，加密所述待签核文件。

2.根据权利要求1所述的电子签批安全管理方法，其特征在于，还包括：

响应发起人的电子签批请求，获取发起人设置的至少一签核人的签核顺序；

根据所述签核顺序，生成文件传输路径。

3.根据权利要求2所述的电子签批安全管理方法，其特征在于，还包括：

当所述电子签批的类型不属于任一所述预设类型时，根据所述文件传输路径建立一常规通道；

在所述常规通道传输所述待签核文件至签核人端；

当接收到来自签核人端的已签核文件时，关闭所述常规通道。

4.根据权利要求2所述的电子签批安全管理方法，其特征在于，所述“加密所述待签核文件”包括：

根据所述文件传输路径建立一常规通道；

对所述常规通道进行加密，建立一加密通道；

在所述加密通道传输所述待签核文件至签核人端；

当接收到来自签核人端的已签核文件时，关闭所述加密通道。

5.根据权利要求2所述的电子签批安全管理方法，其特征在于，所述“加密所述待签核文件”包括：

根据所述文件传输路径建立一常规通道；

对所述待签核文件加密；

在所述常规通道传输所述加密的待签核文件至签核人端；

接收来自签核人端的加密的已签核文件，根据存储的发起人和签核人之间关联的解密密钥，对所述加密的已签核文件解密；

关闭所述常规通道。

6.一种电子签批安全管理系统，其特征在于，包括获取单元、存储器、比较单元和处理器，

所述获取单元，用于响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件；

所述比较单元，用于比较所述电子签批的类型和所述存储器存储的至少一预设类型，生成比较结果；

所述处理器，用于当所述电子签批的类型属于任一所述预设类型时，加密所述待签核文件。

7.根据权利要求6所述的电子签批安全管理系统，其特征在于，所述获取单元还用于响应发起人的电子签批请求获取发起人设置的至少一签核人的签核顺序，及根据所述签核顺序生成文件传输路径。

8.根据权利要求7所述的电子签批安全管理系统，其特征在于，还包括传输单元，所述传输单元包括：

通道建立模块，用于根据所述文件传输路径建立一常规通道；

文件传输模块，用于在所述常规通道发送所述待签核文件至签核人端，及接收来自签核人端的已签核文件；

通道关闭模块，用于关闭所述常规通道。

9.根据权利要求7所述的电子签批安全管理系统，其特征在于，还包括传输单元，所述传输单元包括：

通道建立模块，用于根据所述文件传输路径建立一常规通道；

加密模块，用于对所述常规通道进行加密，建立一加密通道；

文件传输模块，用于在所述加密通道发送所述待签核文件至签核人端，及接收来自签核人端的已签核文件；

通道关闭模块，用于关闭所述加密通道。

10.根据权利要求7所述的电子签批安全管理系统，其特征在于，还包括传输单元，所述传输单元包括

通道建立模块，用于根据所述文件传输路径建立一常规通道；

加密模块，用于对所述待签核文件加密；

文件传输模块，用于在所述常规通道发送所述加密的待签核文件至签核人端，及接收来自签核人端的加密的已签核文件；

解密模块，用于所述存储器存储的发起人和签核人之间关联的解密密钥，对所述加密的已签核文件解密；

通道关闭模块，用于关闭所述常规通道。

一种电子签批安全管理方法及系统

技术领域

[0001] 本发明涉及电子签批技术领域，具体而言，涉及一种电子签批安全管理方法及系统。

背景技术

[0002] 对于公司内部签批流程，通常需要将待签批文件打印出来，然后给到各个签批人处进行签批签字盖章。这样的签批流程较为繁琐，工作效率低下。由此，电子签批应运而生。近年来，电子签批在企业流程、行业应用、移动支付和个人信息安全等各种场景中得到越来越多的应用。

[0003] 但现有的电子签批大多通过公共网络传输签批文件，缺乏对传输的签批文件的保护机制。对于企业来说，企业的财政开支状况、项目申请及研发文档等都是非常机密的材料，一些不法的竞争者经常通过技术手段窃取机密，使受害者遭受巨大的经济损失。

发明内容

[0004] 本发明正是基于上述问题，提出了一种对签批文件具有保护机制的电子签批方法及系统。

[0005] 有鉴于此，本发明一方面提出了一种电子签批安全管理方法，包括：

[0006] 响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件；

[0007] 比较所述电子签批的类型和存储的至少一预设类型；

[0008] 当所述电子签批的类型属于任一所述预设类型时，加密所述待签核文件。

[0009] 进一步地，还包括：

[0010] 响应发起人的电子签批请求，获取发起人设置的至少一签核人的签核顺序；

[0011] 根据所述签核顺序，生成文件传输路径。

[0012] 进一步地，还包括：

[0013] 当所述电子签批的类型不属于任一所述预设类型时，根据所述文件传输路径建立一常规通道；

[0014] 在所述常规通道传输所述待签核文件至签核人端；

[0015] 当接收到来自签核人端的已签核文件时，关闭所述常规通道。

[0016] 进一步地，所述“加密所述待签核文件”包括：

[0017] 根据所述文件传输路径建立一常规通道；

[0018] 对所述常规通道进行加密，建立一加密通道；

[0019] 在所述加密通道传输所述待签核文件至签核人端；

[0020] 当接收到来自签核人端的已签核文件时，关闭所述加密通道。

[0021] 进一步地，所述“加密所述待签核文件”包括：

[0022] 根据所述文件传输路径建立一常规通道；

[0023] 对所述待签核文件加密；

[0024] 在所述常规通道传输所述加密的待签核文件至签核人端；

[0025] 接收来自签核人端的加密的已签核文件，根据存储的发起人和签核人之间关联的解密密钥，对所述加密的已签核文件解密；

[0026] 关闭所述常规通道。

[0027] 本发明另一方面还提供了一种电子签批安全管理系统，包括获取单元、存储器、比较单元和处理器。

[0028] 所述获取单元，用于响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件。

[0029] 所述比较单元，用于比较所述电子签批的类型和所述存储器存储的至少一预设类型，生成比较结果。

[0030] 所述处理器，用于当所述电子签批的类型属于任一所述预设类型时，加密所述待签核文件。

[0031] 进一步地，所述获取单元还用于响应发起人的电子签批请求获取发起人设置的至少一签核人的签核顺序，及根据所述签核顺序生成文件传输路径。

[0032] 进一步地，还包括传输单元，所述传输单元包括通道建立模块、文件传输模块和通道关闭模块。通道建立模块，用于根据所述文件传输路径建立一常规通道。文件传输模块，用于在所述常规通道发送所述待签核文件至签核人端，及接收来自签核人端的已签核文件。通道关闭模块，用于关闭所述常规通道。

[0033] 进一步地，还包括传输单元，所述传输单元包括通道建立模块、加密模块、文件传输模块和通道关闭模块。通道建立模块，用于根据所述文件传输路径建立一常规通道。加密模块，用于对所述常规通道进行加密，建立一加密通道。文件传输模块，用于在所述加密通道发送所述待签核文件至签核人端，及接收来自签核人端的已签核文件。通道关闭模块，用于关闭所述加密通道。

[0034] 进一步地，还包括传输单元，所述传输单元包括通道建立模块，加密模块、文件传输模块、解密模块和通道关闭模块。通道建立模块，用于根据所述文件传输路径建立一常规通道。加密模块，用于对所述待签核文件加密。文件传输模块，用于在所述常规通道发送所述加密的待签核文件至签核人端，及接收来自签核人端的加密的已签核文件。解密模块，用于所述存储器存储的发起人和签核人之间关联的解密密钥，对所述加密的已签核文件解密。通道关闭模块，用于关闭所述常规通道。

[0035] 本发明实施例提供的电子签批安全管理方法及系统，自动识别发起人发起的电子签批的类型，并根据存储的至少一预设类型判断该电子签批的重要性，对属于预设类型的电子签批加密传输，从而避免非法分子对重要信息的窃取，对用户造成不必要的损失。

[0036] 为使本发明的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附附图，作详细说明如下。

附图说明

[0037] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本发明的某些实施例，因此不应被看作是对范围的限定，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这

些附图获得其他相关的附图。

[0038] 图1示出了本发明实施例提供的一种电子签批安全管理方法的第一流程示意图；

[0039] 图2示出了本发明实施例提供的一种电子签批安全管理方法的第二流程示意图；

[0040] 图3示出了本发明实施例提供的一种电子签批安全管理系统的结构示意图。

[0041] 主要元件符号说明：

[0042] 100-电子签批安全管理系统；10-获取单元；20-存储器；30-比较单元；40-传输单元；41-通道建立模块；42-文件传输模块；43-通道关闭模块；44-通道加密模块；45-文件加密模块；46-文件解密模块；50-处理器。

具体实施方式

[0043] 为了便于理解本发明，下面将参照相关附图对电子签批安全管理方法及系统进行更清楚、完整地描述。附图中给出了电子签批安全管理方法及系统的优选实施例。电子签批安全管理方法及系统可以通过许多不同的形式来实现，并不限于本文所描述的实施例。因此，以下对在附图中提供的本发明的实施例的详细描述并非旨在限制要求保护的本发明的范围，而是仅仅表示本发明的选定实施例。基于本发明的实施例，本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0044] 实施例1

[0045] 图1示出了本发明实施例提供的一种电子签批安全管理方法的流程示意图。如图1所示，本发明实施例提供的电子签批安全管理方法，包括：

[0046] 步骤S10，响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件。

[0047] 具体地，响应发起人在用户终端的电子签批请求，获取发起人发起的电子签批的类型，以及发起人设置的至少一签核人。所述用户终端可以是手机、电脑等。在注册账户后，用户可以通过安装在用户终端的电子签批软件或用户终端浏览器中的电子签批网页完成电子签批流程。根据待签核事项的重要性或签核人的职位等，发起人可以通过用户终端上的电子签批软件设置所述电子签批为不同类型，如发起人选定的职位最高的签核人为董事长，则设置该电子签批为类型A；发起人发起的电子签批涉及商业秘密，则设置该电子签批为类型B等。

[0048] 进一步地，响应发起人在用户终端的电子签批请求，获取发起人通过移动网络或无线网络上传的待签核文件。所述待签核文件是指合同、请假条、样品申请单等需要至少一签核人签字的文件。

[0049] 进一步地，响应发起人的电子签批请求，获取发起人设置的至少一签核人的签核顺序，及根据所述签核顺序生成文件传输路径。在某些情况下，发起人发起的一电子签批同时需要多个签核人签字，则发起人需根据公司的签核流程，或签核人的职位、部门等设置签核人的签核顺序。根据获取的签核顺序，生成对应的文件传输路径。所述文件传输路径是指待签核文件在不同传输节点间的流转路径。例如，一电子签批的签核顺序为物料部经理、财务部经理、研发部经理，则对应的文件传输路径为发起人端、物料部经理端、品质部经理端、研发部经理端、发起人端。

[0050] 步骤S20，比较所述电子签批的类型和存储的至少一预设类型，生成比较结果。

[0051] 具体地，获取服务器端存储的至少一预设类型。所述预设类型为区分待签核文件

重要性的标准。比较发起人发起的电子签批的类型和所述预设类型，生成比较结果。当所述电子签批的类型不属于任一所述预设类型时，表示待签核文件重要性弱，对保密工作不做要求等；但当所述电子签批的类型属于一所述预设类型时，表示待签核文件重要性强，需要保密签核等。

[0052] 步骤S30，当所述电子签批的类型属于任一所述预设类型时，加密所述待签核文件。

[0053] 具体地，当所述比较结果为发起人发起的电子签批的类型不属于任一所述预设类型时，常规传输所述待签核文件。根据所述文件传输路径建立一常规通道。所述常规通道为不做加密、加扰等预处理的信号传输通道。根据发起人设置的签核顺序在常规通道传输待签核文件至每一签核人端。优选地，当接收到来自最后一签核人完成签批的已签核文件时，关闭所述常规通道，从而节约网络资源。

[0054] 进一步地，当所述比较结果为发起人发起的电子签批的类型属于一所述预设类型时，加密传输所述待签核文件。具体地，根据所述文件传输路径建立一常规通道。根据HTTPS协议(Hyper Text Transfer Protocol over Secure Socket Layer，基于SSL的超文本传输协议)、SSL协议(Secure Sockets Layer，安全套接层)、CA认证(Certificate Authority，认证授权)、VPN(Virtual Private Network，虚拟专用网)或RAR压缩加密等加密方式对所述常规通道加密，从而建立一加密通道，确保信息的安全性。根据发起人设置的签核顺序在加密通道传输待签核文件至每一签核人端。优选地，当接收到来自最后一签核人完成签批的已签核文件时，关闭所述加密通道，从而节约网络资源。

[0055] 实施例2

[0056] 图2示出了本发明实施例提供的一种电子签批安全管理方法的流程示意图。如图2所示，本发明实施例提供的电子签批安全管理方法，包括：

[0057] 步骤S1，响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件。

[0058] 具体地，响应发起人在用户终端的电子签批请求，获取发起人发起的电子签批的类型，发起人设置的至少一签核人以及发起人通过移动网络或无线网络上传的待签核文件。所述用户终端可以是手机、电脑等。在注册账户后，用户可以通过安装在用户终端的电子签批软件或用户终端浏览器中的电子签批网页完成电子签批流程。

[0059] 步骤S2，响应发起人的电子签批请求，获取发起人设置的至少一签核人的签核顺序，及根据所述签核顺序生成文件传输路径。

[0060] 需要说明的是，步骤S1和步骤S2的执行不分先后顺序。

[0061] 具体地，响应发起人的电子签批请求，获取发起人设置的至少一签核人的签核顺序，及根据所述签核顺序生成文件传输路径。在某些情况下，发起人发起的一电子签批同时需要多个签核人签字，则发起人需根据公司的签核流程，或签核人的职位、部门等设置签核人的签核顺序。根据获取的签核顺序，生成对应的文件传输路径。

[0062] 步骤S3，比较所述电子签批的类型和存储的至少一预设类型，当所述电子签批的类型不属于任一所述预设类型时，执行步骤S4；当所述电子签批的类型属于所述预设类型时，执行步骤S5。

[0063] 具体地，获取服务器端存储的至少一预设类型。所述预设类型为区分待签核文件重要性的标准。比较发起人发起的电子签批的类型和所述预设类型。当所述电子签批的类

型不属于任一所述预设类型时，表示待签核文件重要性弱，对保密工作不做要求等，执行步骤S4；当所述电子签批的类型属于所述预设类型时，表示待签核文件重要性强，需要保密签核等，执行步骤S5。

[0064] 步骤S4，常规传输所述待签核文件。

[0065] 具体地，当发起人发起的电子签批的类型不属于任一所述预设类型时，常规传输所述待签核文件。根据所述文件传输路径建立一常规通道。根据发起人设置的签核顺序在常规通道传输待签核文件至每一签核人端。优选地，当接收到来自最后一签核人完成签批的已签核文件时，关闭所述常规通道，从而节约网络资源。

[0066] 步骤S5，加密传输所述待签核文件。

[0067] 具体地，当发起人发起的电子签批的类型属于所述预设类型时，加密传输所述待签核文件。本实施例中，加密传输所述待签核文件包括两种实施方式。一种实施方式为建立一加密通道，及在该加密通道传输所述待签核文件。具体地，根据所述文件传输路径建立一常规通道。根据HTTPS协议、SSL协议、CA认证、VPN或RAR压缩加密等加密方式对所述常规通道加密，从而建立一加密通道。根据发起人设置的签核顺序在加密通道传输待签核文件至每一签核人端。优选地，当接收到来自最后一签核人完成签批的已签核文件时，关闭所述加密通道，从而节约网络资源。

[0068] 另一种实施方式为建立一常规通道，对所述待签核文件加密，及在所述常规通道传输所述加密的待签核文件。具体地，根据所述文件传输路径建立一常规通道。根据SSH协议(SecureShell，安全外壳协议)、PGP协议(Pretty Good Privacy，安全加密)、RSA(非对称加密算法)或用户口令加密等加密方式对所述待签核文件加密。根据发起人设置的签核顺序在常规通道传输待签核文件至每一签核人端。当接收到来自最后一签核人完成签批的加密的已签核文件时，根据存储的解密密钥，对所述加密的已签核文件解密。所述解密密钥可以是发起人和签核人之间预先约定的口令、密码等。优选地，当接收到来自最后一签核人完成签批的加密的已签核文件时，关闭所述常规通道，从而节约网络资源。这种方式对传输通道要求比较低，且文件加密技术相比通道加密技术更容易实现。

[0069] 实施例3

[0070] 图3示出了本发明实施例提供的一种电子签批安全管理系统的结构示意图。如图3所示，本发明实施例提供的一种电子签批安全管理系统100，包括获取单元10、存储器20、比较单元30、传输单元40和处理器50。获取单元10、存储器20、比较单元30和传输单元40均与处理器50通信连接。

[0071] 获取单元10用于响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件，获取发起人设置的至少一签核人的签核顺序，及根据所述签核顺序生成文件传输路径。

[0072] 具体地，根据待签核事项的重要性或签核人的职位等，发起人可以通过用户终端上的电子签批软件设置所述电子签批为不同类型。处理器50控制获取单元10响应发起人的电子签批请求，获取发起人发起的电子签批的类型。同时，处理器50控制获取单元10获取发起人通过移动网络或无线网络上传的待签核文件。所述待签核文件是指合同、请假条、样品申请单等需要至少一签核人签字的文件。进一步地，在某些情况下，发起人发起的一电子签批同时需要多个签核人签字，则发起人需根据公司的签核流程，或签核人的职位、部门等设

置签核人的签核顺序。处理器50控制获取单元10获取发起人设置的至少一签核人的签核顺序，及根据所述签核顺序生成文件传输路径。所述文件传输路径是指待签核文件在不同传输节点间的流转路径。

[0073] 存储器20用于存储至少一预设类型。所述预设类型为区分待签核文件重要性的标准，如涉及商业秘密等的待签核文件的类型为一预设类型。

[0074] 比较单元30用于比较发起人发起的电子签批的类型和所述预设类型，生成比较结果。

[0075] 传输单元40用于传输所述待签核文件。

[0076] 本实施例中，传输单元40包括通道建立模块41、文件传输模块42和通道关闭模块43。通道建立模块41用于根据所述文件传输路径建立一常规通道。文件传输模块42用于在所述常规通道发送所述待签核文件至签核人端，及接收来自签核人端的已签核文件。通道关闭模块43用于关闭所述常规通道。

[0077] 进一步地，传输单元40还包括通道加密模块44。通道加密模块44用于对所述常规通道进行加密及安全认证，建立一加密通道。文件传输模块42还用于在所述加密通道发送所述待签核文件至签核人端，及接收来自签核人端的已签核文件。通道关闭模块43还用于关闭所述加密通道。

[0078] 处理器50用于根据所述比较结果控制传输单元40加密传输或常规传输所述待签核文件。

[0079] 当比较单元30生成的比较结果为发起人发起的电子签批的类型不属于存储器20存储的任一预设类型时，处理器50控制传输单元40常规传输所述待签核文件。具体地，处理器50控制通道建立模块41根据所述文件传输路径建立一常规通道，及控制文件传输模块42根据发起人设置的签核顺序在常规通道传输待签核文件至每一签核人端。优选地，当文件传输模块42接收到来自最后一签核人完成签批的已签核文件时，处理器50控制通道关闭模块43关闭所述常规通道，从而节约网络资源。

[0080] 当比较单元30生成的比较结果为发起人发起的电子签批的类型属于存储器20存储的一预设类型时，处理器50控制传输单元40加密传输所述待签核文件。具体地，处理器50控制通道建立模块41根据所述文件传输路径建立一常规通道，及控制通道加密模块44根据HTTPS协议、SSL协议、CA认证、VPN或RAR压缩加密等加密方式对所述常规通道加密，从而建立一加密通道。处理器50控制文件传输模块42根据发起人设置的签核顺序在加密通道传输待签核文件至每一签核人端。优选地，当文件传输模块42接收到来自最后一签核人完成签批的已签核文件时，处理器50控制通道关闭模块43关闭所述加密通道，从而节约网络资源。

[0081] 另一实施例中，传输单元40还包括文件加密模块45和文件解密模块46。文件加密模块45用于对所述待签核文件加密。文件传输模块42还用于在所述常规通道发送所述加密的待签核文件至签核人端，及接收来自签核人端的加密的已签核文件。文件解密模块46用于所述存储器存储的发起人和签核人之间关联的解密密钥，对所述加密的已签核文件解密。

[0082] 相应地，当比较单元30生成的比较结果为发起人发起的电子签批的类型属于存储器20存储的一预设类型时，处理器50控制传输单元40加密传输所述待签核文件。具体地，处理器50控制通道建立模块41根据所述文件传输路径建立一常规通道，及控制文件加密模块

45根据SSH协议、PGP机制、RSA算法或用户口令加密等加密方式对所述待签核文件加密。处理器50控制文件传输模块42根据发起人设置的签核顺序在常规通道传输待签核文件至每一签核人端。当文件传输模块42接收到来自最后一签核人完成签批的加密的已签核文件时，处理器50控制文件解密模块46根据存储器20存储的解密密钥，对所述加密的已签核文件解密。所述解密密钥可以是发起人和签核人之间预约定的口令、密码等。优选地，当文件传输模块42接收到来自最后一签核人完成签批的加密的已签核文件时，处理器50控制通道关闭模块43关闭所述常规通道，从而节约网络资源。

[0083] 本发明实施例提供的电子签批安全管理方法及系统，自动识别发起人发起的电子签批的类型，并根据存储的至少一预设类型判断该电子签批的重要性，对属于预设类型的电子签批加密传输，从而避免非法分子对重要信息的窃取，对用户造成不必要的损失。

[0084] 本发明实施例所提供的系统，其实现原理及产生的技术效果和前述方法实施例相同，为简要描述，系统实施例部分未提及之处，可参考前述方法实施例中相应内容。

[0085] 在这里示出和描述的所有示例中，任何具体值应被解释为仅仅是示例性的，而不是为限制，因此，示例性实施例的其他示例可以具有不同的值。应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。

[0086] 在本申请所提供的几个实施例中，应该理解到，所揭露的装置可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，又例如，多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些通信接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0087] 所述为分离部件说明的单元可以是或者也可以不是物理上分开的，为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0088] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

[0089] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

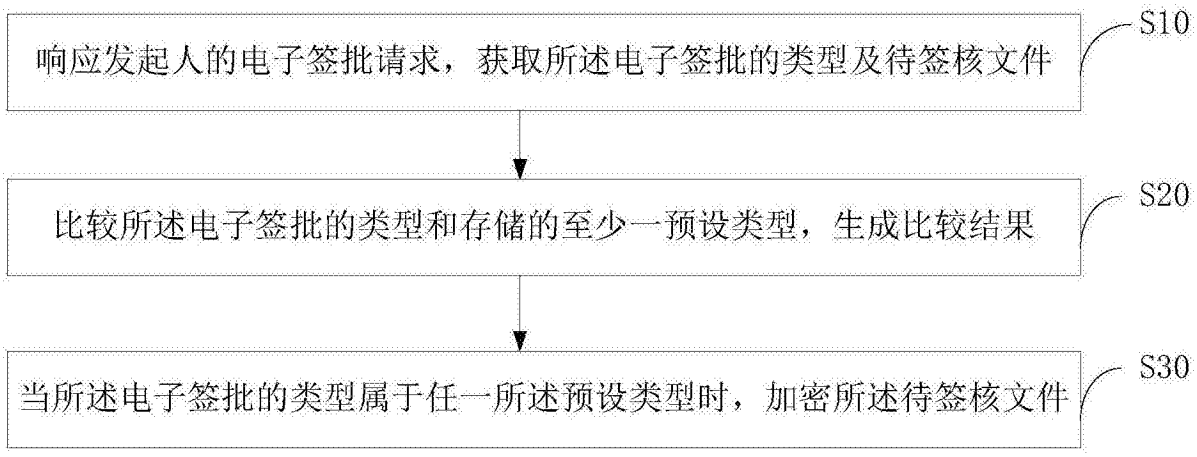

响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件
S10
比较所述电子签批的类型和存储的至少一预设类型，生成比较结果
S20
当所述电子签批的类型属于任一所述预设类型时，加密所述待签核文件
S30

图1

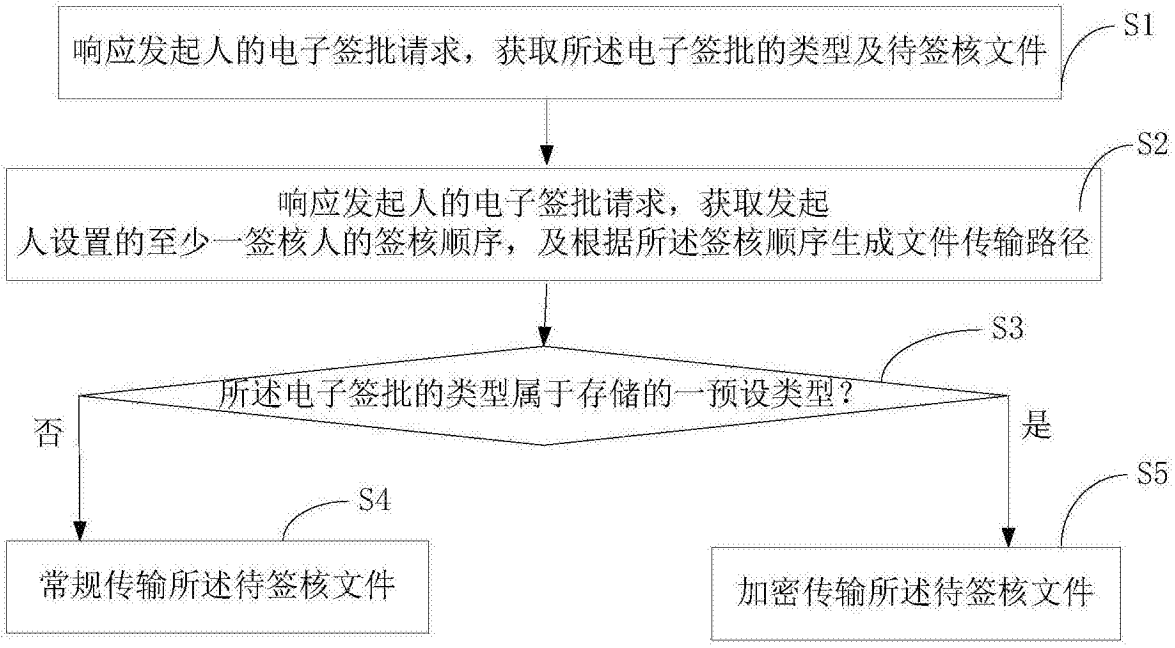

响应发起人的电子签批请求，获取所述电子签批的类型及待签核文件
S1
响应发起人的电子签批请求，获取发起
人设置的至少一签核人的签核顺序，及根据所述签核顺序生成文件传输路径
S2
所述电子签批的类型属于存储的一预设类型？
S3
否
是
S4
常规传输所述待签核文件
S5
加密传输所述待签核文件

图2

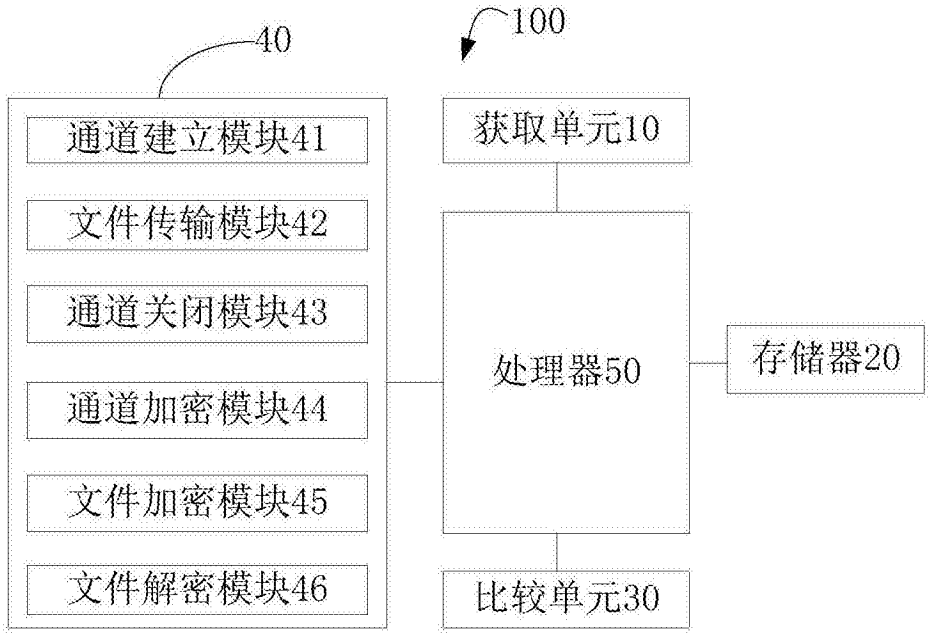

40
100
通道建立模块41
文件传输模块42
通道关闭模块43
通道加密模块44
文件加密模块45
文件解密模块46
获取单元10
处理器50
存储器20
比较单元30

图3