(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
2020 年 3 月 5 日 (05.03.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/042217 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) *H04L 29/08* (2006.01)

(21) 国际申请号: PCT/CN2018/104856

(22) 国际申请日: 2018 年 9 月 10 日 (10.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811016964.X 2018年8月31日 (31.08.2018) CN

(71) 申请人: 密信技术（深圳）有限公司 (MESINCE TECHNOLOGY LIMITED) [CN/CN]; 中国广东省深圳市南山区南海大道1057号科技大厦二期A座502#, Guangdong 518067 (CN)。

(72) 发明人: 王高华 (WANG, Gaohua); 中国广东省深圳市南山区南海大道1057号科技大厦二期A座502#, Guangdong 5180067 (CN)。 苏志辉 (SU, Zhihui); 中国广东省深圳市南山区南海大道1057号科技大厦二期A座502#, Guangdong 5180067 (CN)。 唐占国 (TANG, Zhanguo); 中国广东省深圳市南山区南海大道1057号科技大厦二期A座502#, Guangdong 5180067 (CN)。 余鹏 (YU, Peng); 中国广东省深圳市南山区南海大道1057号科技大厦二期A座502#, Guangdong 5180067 (CN)。

(74) 代理人: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市南山区粤海街道高新技术产业园北区松坪山路3号奥特讯电力大厦201, Guangdong 518057 (CN)。

(54) **Title:** METHOD AND APPARATUS FOR SIGNING AND/OR ENCRYPTING BROWSER FILE, BROWSER, AND MEDIUM

(54) **发明名称**: 浏览器文件的签名及/或加密方法、装置、浏览器及介质

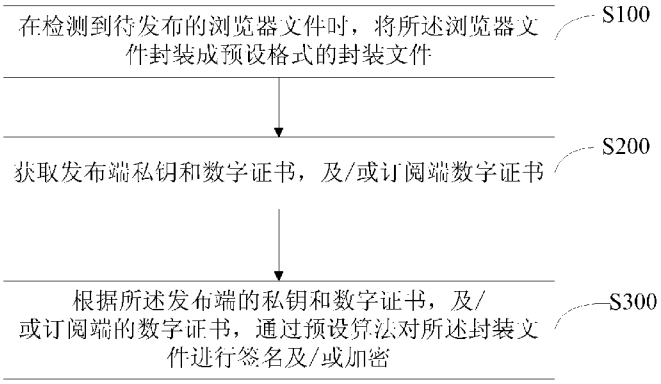

图 2

(57) **Abstract:** A method for uniformly signing and/or encrypting a browser file, a browser, an apparatus for uniformly signing and encrypting a browser file, and a computer readable storage medium. The method comprises the following steps: when a browser file to be published is detected, packaging the browser file to be a package file in a preset format (S100); obtaining the private key and the digital certificate of a publishing end, and/or the digital certificate of a subscribing end (S200); and according to the private key and the digital certificate of the publishing end, and/or the digital certificate of the subscribing end, signing and/or encrypting the package file by means of a preset algorithm (S300). The browser comprises a signing and encrypting interface, and by means of the signing and encrypting interface, the browser packages different types of files to be MIME, and then signs and/or encrypts the MIME by using PKCS7.

(57) **摘要**: 一种浏览器文件的统一签名及/或加密方法、一种浏览器、一种浏览器文件的统一签名和加密装置和一种计算机可读存储介质。所述方法包括以下步骤：在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件（S100）；获取发布端私钥和数字证书，及/或订阅端数字证书（S200）；根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密（S300）。所述浏览器包括签名加密界面，浏览器通过签名加密界面将不同类型的文件封装为MIME，然后再使用PKCS7对其进行签名及/或加密。

WO 2020/042217 A1

[见续页]

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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, 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。

(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, 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)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

浏览器文件的签名及/或加密方法、装置、浏览器及介质

[1] 技术领域

[2] 本申请涉及信息安全领域，尤其涉及一种浏览器文件的统一签名及/或加密方法、装置及计算机可读存储介质。

[3] 背景技术

[4] 签名（又称公钥数字签名、电子签章）是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，是一种用于鉴别信息所有者的方法。加密是一种对信息进行加密，使得只有拥有读取权限的人才可以读取信息的数字技术。

[5] 随着互联网技术的发展，人们的生活与网络技术越来越密不可分。浏览器是互联网传输各种文件、照片、音频和视频等信息的主要工具。在现有技术中，由于互联网具备开放性，未经签名和加密的浏览器文件容易被第三方用户篡改或截取，导致浏览器文件的安全性和可靠性较低。

[6] 上述内容仅用于辅助理解本申请的技术方案，并不代表承认上述内容是现有技术。

[7] 发明内容

[8] 本申请的主要目的在于提供一种浏览器文件的统一签名及/或加密方法、装置及计算机可读存储介质，旨在对浏览器文件进行统一签名及/或加密，提升信息的安全性和可靠性。

[9] 为实现上述目的，本申请提供一种浏览器文件的统一签名及/或加密方法，所述浏览器文件的统一签名及/或加密方法包括如下步骤：

[10] 在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件；

[11] 获取发布端私钥和数字证书，及/或订阅端数字证书；以及

[12] 根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密。

[13] 此外，为实现上述目的，本申请还提供一种浏览器，其中，所述浏览器包括签名和加密程序，所述签名和加密程序在所述浏览器上执行实现如上所述的浏览器文件的统一签名及/或加密方法的步骤。

[14] 此外，为实现上述目的，本申请还提供一种浏览器文件的统一签名和加密模块，其中，所述装置包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的签名和加密程序，所述签名和加密程序被所述处理器执行时实现如上所述的浏览器文件的统一签名及/或加密方法的步骤。

[15] 此外，为实现上述目的，本申请还提供一种计算机可读存储介质，其中，所述计算机可读存储介质上存储有签名和加密程序，所述签名和加密程序被处理器执行时实现如上所述的浏览器文件的统一签名及/或加密方法的步骤。

[16] 本申请实施例提出的一种浏览器文件的统一签名及/或加密方法、装置、浏览器和计算机可读存储介质，在检测到待发布的浏览器文件时，将所述浏览器文件封装成多用途因特网邮件扩展格式的封装文件，然后通过发布端的证书管理模块获取发布端私钥和数字证书，及/或订阅端数字证书，最后根据所述发布端的私钥和数字证书及/或订阅端数字证书，通过公钥加密标准对所述封装文件进行签名及/或加密。这样，实现了通过统一种签名及/或加密方法对待发布的的浏览器文件进行签名及/或加密，从而实现了对浏览器文件进行统一签名和加密，提升信息的安全性和可靠性的目的。

[17] 附图说明

[18] 图1是本申请实施例方案涉及的硬件运行环境的终端结构示意图；

[19] 图2为本申请浏览器文件的统一签名及/或加密方法第一实施例的流程示意图；

[20] 图3为本申请中发布端对浏览器文件进行签名的细化流程示意图的流程示意图；

[21] 图4为本申请中订阅端处理签名文件的流程示意图；

[22] 图5为本申请中发布端对已签名的浏览器文件进行加密的流程示意图；

[23] 图6为本申请中发布端对未签名的浏览器文件进行加密的流程示意图；

[24] 图7为本申请中订阅端处理加密文件的流程示意图。

[25] 本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

[26] 具体实施方式

[27] 应当理解，此处所描述的具体实施例仅用以解释本申请，并不用于限定本申请。

[28] 本申请实施例的主要解决方案是：

[29] 在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件；

[30] 获取发布端的私钥和数字证书，及/或订阅端数字证书；

[31] 根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密。

[32] 本申请实施例提出的一种浏览器文件的统一签名及/或加密方法，通过MIME和PKCS实现浏览器文件的统一签名和加密，从而解决了浏览器发布信息时信息安全性和可靠性低的技术问题。

[33] 如图1所示，图1是本申请实施例方案涉及的硬件运行环境的终端结构示意图。

[34] 本申请实施例终端可以为PC机及/或智能移动终端等。

[35] 如图1所示，该终端可以包括：处理器1001，例如CPU，通信总线1002，显示器1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信。存储器1005可以是高速RAM存储器，也可以是稳定的存储器（non-volatile memory），例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[36] 如图1所示的终端可以运行所述浏览器，所述浏览器在所述终端上运行时，可以实现如上所述的浏览器文件的统一签名及/或加密方法。所述浏览器既可以作为订阅端，也可以作为发布端。

[37] 本领域技术人员可以理解，图1中示出的终端结构并不构成对终端的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[38] 如图1所示，作为一种计算机可读存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及签名和加密程序。

[39] 在图1所示的终端中，网络接口1004主要用于连接后台服务器，与后台服务器进行数据通信；用户接口1003主要用于连接客户端（用户端），与客户端进行

数据通信，进而实现通过客户端输出数据的目的；而处理器1001可以用于调用存储器1005中存储的签名和加密程序，并执行以下操作：

[40] 在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件；

[41] 获取发布端私钥和数字证书，及/或订阅端数字证书；

[42] 根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密。

[43] 参照图2，本申请浏览器文件的统一签名及/或加密方法第一实施例，所述浏览器文件的统一签名及/或加密方法包括：

[44] 步骤100、在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件；

[45] 在本实施例中，在浏览器接收到发布文件的指令时，根据所述指令确定待发布的文件，即待发布的的浏览器文件。然后将所述浏览器文件封装为MIME（Multipurpose Internet Mail Extensions，多用途因特网邮件扩展）格式。

[46] 具体地，MIME的最初目的是为了在发送电子邮件时能附加非文本文件的多媒体数据，让邮件客户端软件能根据其类型进行处理。MIME支持的常用文件类型包括：.gif、.pdf、.ppt、.doc、.js、.zip、.mp3及.wav等，因此可以通过使用MIME封装各种类型的文件。其中 MIME TYPE（类型）定义了丰富的Content-Type（内容类型）用于指定文件的类型，并且可以不断地扩展补充类型。结合Content-Disposition（容量配置）指定文件处理机制，Content-Disposition固定使用attachment（附件），并使用filename参数指定封装的原始文件（即待处理文件）文件名（如：sample.txt），Content-Transfer-Encoding（内容传输编码）指定文件传输的编码方式，（例如：base64），封装后的MIME格式文件可以为各种应用场景提供文件类型和文件解析的方法，从而可以获得原始的文件。

[47] 例如，MIME文件的文件结构如下：

[48] MIME:

[49] Content-Type: application/text

[50] Content-Disposition: attachment; filename=sample.txt

[51] Content-Transfer-Encoding: base64

[52] MIAGCSqGSIb3DQEHAqCAMIACA.....

[53] 步骤S200、获取发布端私钥和数字证书，及/或订阅端数字证书；

[54] 在本实施例中，所述浏览器包括证书库管理程序，所述浏览器在执行所述证书管理程序时，可以同实现通过用户人工导入本地证书，或者通过互联网获取网络存储的数字证书的目的。所述人工导入的本地证书和所述通过互联获取的数字证书组成了所述浏览器的证书库。发布端私钥和数字证书可以从所述证书库中获取。

[55] 所述订阅者的数字证书可以通过证书库获取，其中所述证书库中的数据可以包括存储在云端服务器中的网络证书库（或云证书库）的数据，也可以包括浏览器已经下载、并缓存的本地证书库中的数据，即浏览器在执行所述证书管理程序时，可以同时支持通过浏览器所在操作系统的内置证书库，或外部存储设备中的证书库获取数字证书及/或密钥。其中，所述订阅者的数字证书用于加密。

[56] 步骤S300、根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密。

[57] 在本实施例中，先将已封装的MIME格式文件，通过DER（Distinguished Encoding Rules，可辨别编码规则）编码为PKCS(Public-Key Cryptography Standards,公钥加密标准协议)7.ContentInfo结构的已编码文件。其中，所述编码文件封装的是所述待发布的浏览器文件的数据内容（即待发布的浏览器文件的文件内容信息）。

[58] 例如，ContentInfo的结构可以是：

[59] ContentInfo ::= SEQUENCE {

[60] contentType ContentType,

[61] content [0] EXPLICIT ANY DEFINED BY contentType OPTIONAL }

[62] 然后，通过浏览器获取发布端的数字证书及私钥，订阅端的数字证书。然后可以根据所述发布端的数字证书及私钥对所述已编码文件进行签名操作，生成签名文件；也可以根据所述订阅端的数字证书对所述已编码文件进行加密操作，生成加密文件；还可以根据所述订阅端的数字证书，对所述签名文件进行加密

操作，生成签名加密文件。

[63] 具体地，对所述已编码文件进行签名操作的具体步骤可以是：

[64] 将所述已编码文件、发布端的数字证书及证书私钥作为数字签名的输入量，生成公钥加密标准签名数据类型的签名文件；

[65] 通过第三方时间戳服务获取时间戳；

[66] 将所述时间戳添加进所述签名文件，生成已签名文件。

[67] 另外，对所述已编码文件进行加密操作的具体步骤可以是：

[68] 生成随机密钥，并通过随机密钥封装所述编码文件；

[69] 通过所述订阅端的数字证书封装所述随机密钥；

[70] 将通过所述随机密钥封装的编码文件，及通过所述订阅端的数字证书封装的随机密钥编码成加密文件。

[71] 另外，对所述签名文件进行加密操作的步骤可是：

[72] 生成随机密钥，并通过随机密钥封装所述已签名文件；

[73] 通过所述订阅端的数字证书封装所述随机密钥；

[74] 将通过所述随机密钥封装的已签名文件，及通过所述订阅端的数字证书封装的随机密钥编码成加密文件。

[75] 在本实施例中，基于MIME和PKCS7技术提供一种在浏览器上实现对各种文件进行统一添加数字签名和进行加密的方法，来解决互联网上发布文件时无法做到版权保护和防止信息泄露的问题。通过浏览器调用户密钥和数字证书对待发布的明文文件签名，使用数字证书签名过的文件发布到浏览器上可以防止内容被非法篡改而侵权，通过浏览器用数字证书对文件进行加密发布，只有合法用户才能通过浏览器调用用户密钥解密已经加密的内容文件。

[76] 进一步地，参照图3，本申请浏览器文件的统一签名及/或加密方法第二实施例，基于上述第一实施例，所述步骤S300包括：

[77] 步骤S301、将所述封装文件编码为预设结构的已编码文件；

[78] 步骤S302、将所述已编码文件、发布端的私钥和数字证书作为所述预设算法的签名输入，生成签名数据；

[79] 步骤S303、通过第三方时间戳服务获取时间戳；

[80] 步骤S304、将所述时间戳添加进所述签名数据，生成已签名文件。

[81] 具体地，先将已封装的MIME格式文件，通过DER（Distinguished Encoding Rules，可辨别编码规则）编码为PKCS(Public-Key Cryptography Standards,公钥加密标准协议)7.ContentInfo结构的已编码文件。其中，所述编码文件封装的是所述待发布的浏览器文件的数据内容（即待发布的浏览器文件的文件内容信息）。

[82] 例如，ContentInfo的结构可以是：

[83] ContentInfo ::= SEQUENCE {

[84] contentType ContentType,

[85] content [0] EXPLICIT ANY DEFINED BY contentType OPTIONAL }

[86] 然后，将所述已编码文件和所述发布端的数字证书作为PKCS数字签名程序的输入量，生成PKCS7.SignedData类型数据。其中，签名过程基于ContentInfo.content和SignedData.authenticated attributes按照签名规则计算摘要messageDigest，而后使用PrivateKey（即通过CA获取的所述发布端的私钥）计算EncryptedDigest。并把ContentInfo和证书Certificate，以及计算得来的EncryptedDigest和摘要算法DigestAlgorithmIdentifiers以及其他SignedData成员结构共同组装为SignedData签名数据。

[87] 进一步地，对所述EncryptedDigest计算摘要hash，并按照RFC3161时间戳标准，从第三方可信时间戳服务获取一个时间戳。其中所述时间戳能够证明签名的存在时间。然后把时间戳数据附加到所述SignedData中，构造一个有时间戳的签名数据。

[88] 进一步地，将所述带时间戳SignedData（即带时间戳的签名数据）按照PKCS7标准，用DER编码为一个签名的PKCS7.ContentInfo。其中SignedData为ContentInfo.content，而ContentInfo.contentType使用signedData类型（oid为1.2.840.113549.1.7.2）。

[89] 最后把这个签名ContentInfo用DER编码保存为磁盘文件，使用.p7m为后缀名保存。所述后缀为.p7m文件就是一个签名文件。

[90] 在本实施例中，通过PKCS7技术实现了对待发布的浏览器文件进行签名的目的，这样使得文件发布到浏览器上时，可以防止内容被非法篡改。

[91] 进一步地，参照图4，本申请浏览器文件的统一签名及/或加密方法第三实施例，基于上述第二实施例，所述步骤S300之后，还包括：

[92] 步骤S400、在接收到所述已签名文件时，获取所述已签名文件的签名信息；

[93] 步骤S500、在所述签名信息未被篡改时，通过所述预设算法解析所述已签名文件；

[94] 步骤S600、根据解析结果获取并输出所述已签名文件的签名信息，及所述待发布的浏览器文件的原文，其中，所述签名信息包括身份验证级别、签名时间和签名证书中的至少一个。

[95] 在本实施例中，当用户通过浏览器点击文件链接，或添加本地文件至浏览器时，浏览器先判断所述文件链接或本地文件是否为P7M文件，当用户点击WEB上发布的P7M文件链接，或用户在本地拖入或输入一个P7M文件到浏览器中时。先判定其是否为签名文件。在所述文件为签名文件时，先获取其加密值EncryptedDigest、基于PM7文件原文（即所述待发布的浏览器文件）的编码文件ContentInfo、发布端数字证书及时间戳等签名信息，并根据所述签名信息验证所述签名文件是否被篡改。在所述签名文件未被篡改时，通过PKCS解析出所述封装文件，并通过MIME解析出所述待发布的浏览器文件。

[96] 具体地，把p7m用DER编码解析，其结构为PKCS7.ContentInfo。解析出的ContentInfo.contentType如果为signedData类型，则判定当前文件为签名文件。

[97] 在判定所述文件为签名文件时，解析出SignedData.contentInfo，签名证书Certificate，签名属性authenticated attributes以及签名的摘要加密值encryptedDigest，并定义为解析所得encryptedDigest。

[98] 进一步地，根据签名方法计算encryptedDigest，定义为计算所得encryptedDigest，并比较所述解析所得encryptedDigest与所述计算所得encryptedDigest是否一致，如果一致，则验证签名时间戳的有效性和验证数字证书是否被吊销，否则，判定所述签名文件已被篡改。其中验证时间戳有效性时，可以判断解析所得时间戳与计算所得时间戳是否一致，当一致时，所述时间戳有效，否则无效。在所述时间戳有效且所述数字证书为被吊销时，判定签名文件为被篡改。

[99] 在所述签名文件未被篡改时，解析出发布端的证书信息和所述已签名文件的明

文信息，并输出所述证书信息和所述已签名文件。证书信息的解析可以通过X509.Certificate格式解析。

[100] 另外，所述已签名文件的明文信息的解析具体步骤如下：

[101] 第一步：把验证签名中已经解析SignedData.contentInfo中的content用OCTECT STRING解码为MIME文件；

[102] 第二步：解析出MIME中的标识文件类型的Content-Type，结合Content-Disposition标识的附件attachment和filename参数，以及Content-Transfer-Encoding指定文件传输的编码，解析出原始的文件（即所述已签名文件的明文信息），使用filename进行命名保存（所述filename即所述待发布的浏览器文件）。在本实施例中，在浏览器检测到文件时，先判断所述文件是否为签名文件，在所述文件为签名文件时，判断所述文件是否被篡改，在所述签名文件未被篡改时，解析出所述待发布的浏览器文件，这样可以通过文件签名确定所述文件的归属者。

[103] 最后，在浏览器解析出所述已签名文件的明文信息时，浏览器渲染所述已签名文件的明文信息和签名信息，然后通过终端的显示装置输出所述已签名文件的明文信息和所述签名信息，这样，使得用户可以直观的了解当前文件的版权所有者的信息。

[104] 需要说明的是，所述签名信息包括身份验证级别、签名时间、时间戳和签名证书中的至少一个。在所述签名文件的显示界面可以包括所述签名信息对应的图标，所述签名信息对应的图标可以包括签章图标，用以表示当前文件是否带有签名数据，身份级别图标，用以表示当前文件的不同身份认证级别，身份描述图标，用以展示签名者的名字及证书签发者名称，时间戳图标，用于展示所述签名时间的时间来源等。其中，所述时间戳图标用于判断所述签名时间是否可靠，其中，所述时间戳为第三方证据，例如可以根据RF3161标准确定。

[105] 在本实施例中，在接收到签名文件时，先对所述签名文件进行验证，然后在所述签名文件为被篡改时，解析并输出所述已签名文件的签名证书和原文明文，这样使得订阅者可以通过输出数据获悉当前显示内容的签名信息，提高了当前输出内容的可靠性。

[106] 进一步地，参照图5，本申请浏览器文件的统一签名及/或加密方法第四实施例

，基于上述第一至第三实施例，所述步骤S304之后，还包括：

[107] 步骤S305、生成随机密钥，并通过所述随机密钥封装所述已签名文件；

[108] 步骤S306、通过所述订阅端的数字证书封装所述随机密钥；

[109] 步骤S307、将通过所述随机密钥封装的已签名文件，及通过所述订阅端的数字证书封装的所述随机密钥编码成加密文件。

[110] 在本实施例中，根据订阅端的数字证书，对已签名文件进行加密。订阅端的数字证书包含公钥和私钥。其中公钥可以公开，用于给指定的加密人来加密文件，但私钥仅订阅者自己唯一拥有，用于对加密的文件进行解密。

[111] 具体地，由于所述签名文件为PKCS7.ContentInfo数据结构，所以在对已签名文件进行加密时，先由系统产生一个随机密钥key，然后使用订阅端的公钥证书（当存在多个订阅端时，使用多个不同的公钥证书），对随机秘钥key加密封装为RecipientInfos。

[112] 进一步地，使用随机密钥key对签名文件中包含的待处理文件ContentInfo.content封装为PKCS7.EncryptedContentInfo数据类型的数据，这个EncryptedContentInfo.contentType使用待处理文件的ContentInfo.contentType，最后，再将所述RecipientInfos和EncryptedContentInfo编码为PKCS7.EnvelopedData数据结构，生成加密文件。

[113] 在本实施例中，使用订阅端公钥封装随机密钥，再使用随机密钥封装文件内容信息，最后生成加密文件，这样使得文件传输的安全性提高。

[114] 进一步地，参照图6，本申请浏览器文件的统一签名及/或加密方法第五实施例，基于上述第一至第四实施例，所述步骤S300包括：

[115] 步骤308、将所述封装文件编码为所述预设结构的已编码文件；

[116] 步骤309、生成随机密钥，并通过随机密钥封装所述已编码文件；

[117] 步骤310、通过所述订阅端的数字证书封装所述随机密钥；

[118] 步骤311、将通过所述随机密钥封装的编码文件，及通过所述订阅端的数字证书封装的所述随机密钥编码成加密文件。

[119] 在本实施例中，先将所述封装文件编码为PKCS内容信息结构的已编码文件，然后通过订阅端的数字字证书，对已签名文件进行加密。订阅端的数字证书包

含公钥和私钥。其中公钥可以公开给指定的加密人来加密文件，但私钥仅接收者自己唯一拥有，用于对加密的文件进行解密。

[120] 具体地，先由系统产生一个随机密钥key，然后使用订阅端的公钥证书（当存在多个订阅端时，使用多个不同的公钥证书），对随机秘钥key加密封装为RecipientInfos。

[121] 进一步地，使用随机密钥key对已编码文件中包含的待处理文件ContentInfo.content封装为PKCS7.EncryptedContentInfo数据类型的数据，所述EncryptedContentInfo.contentType使用待处理文件的ContentInfo.contentType，最后，再将所述RecipientInfos和EncryptedContentInfo编码为PKCS7.EnvelopedData数据结构，生成加密文件。

[122] 在本实施例中，使用订阅端公钥封装随机密钥，在使用随机密钥封装文件内容信息，最后生成加密文件，这样使得文件传输的安全性提高。

[123] 进一步地，参照图7，本申请浏览器文件的统一签名及/或加密方法第六实施例，基于上述第一至第五实施例，所述步骤S300之后，还包括：

[124] 步骤700、在接收到所述加密文件时，获取所述订阅端的数字证书，其中所述订阅端数字证书包括订阅端的私钥；

[125] 步骤800、根据所述订阅端私的钥解析所述加密文件，获取所述随机密钥；

[126] 步骤900、根据所述随机密钥解析出所述待发布的浏览器文件。

[127] 在本实施例中，在接收到文件时，先判断所述文件是否为加密文件，在文件为加密文件时，通过所述证书管理模块获取订阅端的私钥，并通过所述私钥解析出加密文件中的随机密钥。进一步地，再根据所述随机密钥解析出原始文件（即待发布的浏览器文件）。

[128] 具体地，在接收到后缀为.p7m的文件时，通过DER编码解析所述文件，当解析出的ContentInfo.contentType为envelopedData类型（oid为1.2.840.113549.1.7.2）时，判定所述文件为加密文件。

[129] 获取订阅端的私钥，并通过所述订阅端的私钥从RecipientInfos中解密出所述随机秘钥key。进一步地，通过所述随机秘钥key解密EnvelopedContentInfo.encryptContent，解密出的结果就是被加密的ContentInfo.content。

[130] 根据解密结果判断解密出的EnvelopedContentInfo.contentType是否为SignedData（oid为1.2.840.113549.1.7.2），如果是，则解密得到的是一个签名数据，如果EnvelopedContentInfo.contentType为data类型（oid为1.2.840.113549.1.7.1），则解析出所述待处理文件。

[131] 另外，在所述文件为加密文件时，在所述文件的显示界面显示加密图标，表示所述文件为加密文件。

[132] 在本实施例中，在接收到文件时，先判断所述文件是否为加密文件，在文件为加密文件时，获取订阅端的私钥，并通过所述私钥解析出加密文件中的随机密钥。进一步地，再根据所述随机密钥解析出原始文件，这样，实现了解析加密文件的目的，从而提高了信息传输的安全性。

[133] 此外，本申请实施例还提出一种浏览器，其中，所述浏览器包括：签名和加密程序，所述签名和加密程序被所述处理器执行时实现如上所述的浏览器文件的统一签名及/或加密方法的步骤。

[134] 此外，本申请实施例还提出一种浏览器文件的统一签名及/或加密装置，其中，所述浏览器文件的统一签名及/或加密装置包括：浏览器、存储器、处理器及存储在所述存储器上并可在所述处理器上运行的签名和加密程序，所述签名和加密程序被所述处理器执行时实现如上所述的浏览器文件的统一签名及/或加密方法的步骤。

[135] 此外，本申请实施例还提出一种计算机可读存储介质，其中，所述计算机可读存储介质上存储有签名和加密程序，所述签名和加密程序被处理器执行时实现如以上实施例所述的浏览器文件的统一签名及/或加密方法的步骤。

[136] 需要说明的是，在本文中，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、物品或者系统不仅包括那些要素，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、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[137] 上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

[138] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个计算机可读存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本申请各个实施例所述的方法。

[139] 以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

权利要求书

[权利要求 1] 一种浏览器文件的统一签名及/或加密方法，其中，所述浏览器文件的统一签名及/或加密方法包括以下步骤：

在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件；

获取发布端的私钥和数字证书，及/或订阅端数字证书；以及

根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密。

[权利要求 2] 如权利要求1所述的浏览器文件的统一签名及/或加密方法，其中，所述根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密的步骤包括：

将所述封装文件编码为预设结构的已编码文件；

将所述已编码文件、发布端的私钥和数字证书作为所述预设算法的签名输入，生成签名数据；

通过第三方时间戳服务获取时间戳；以及

将所述时间戳添加进所述签名数据，生成已签名文件。

[权利要求 3] 如权利要求2所述的浏览器文件的统一签名及/或加密方法，其中，所述预设格式包括多用途因特网扩展MIME格式；所述预设结构包括公钥加密标准内容信息结构；所述预设算法包括公钥加密标准PKCS。

[权利要求 4] 如权利要求2所述的浏览器文件的统一签名及/或加密方法，其中，所述根据所述发布端的私钥和数字证书，及/或订阅端数字证书，对所述封装文件进行签名及/或加密的步骤之后，还包括：

在接收到所述已签名文件时，获取所述已签名文件的签名信息；

在所述签名信息未被篡改时，通过所述预设算法解析所述已签名文件；以及

根据解析结果获取并输出所述已签名文件的签名信息，及所述待发布的浏览器文件的原文，其中，所述签名信息包括身份验证级别、签名时间和签名证书中的至少一个。

[权利要求 5] 如权利要求4所述的浏览器文件的统一签名及/或加密方法，其中，所述签名信息通过显示界面中对应的图标输出。

[权利要求 6] 如权利要求5所述的浏览器文件的统一签名及/或加密方法，其中，所述对应的图标包括签章图标、身份级别图标、身份描述图标和时间戳图标中的至少一个。

[权利要求 7] 如权利要求6所述的浏览器文件的统一签名及/或加密方法，其中，所述签章图标，用以表示当前文件是否带有签名数据。

[权利要求 8] 如权利要求6所述的浏览器文件的统一签名及/或加密方法，其中，所述身份级别图标，用以表示当前文件的不同身份认证级别。

[权利要求 9] 如权利要求6所述的浏览器文件的统一签名及/或加密方法，其中，所述身份描述图标，用以展示签名者的名字及证书签发者名称。

[权利要求 10] 如权利要求6所述的浏览器文件的统一签名及/或加密方法，其中，所述时间戳图标，用于展示所述签名时间的时间来源。

[权利要求 11] 如权利要求6所述的浏览器文件的统一签名及/或加密方法，其中，所述时间戳图标，用于根据所述时间戳图标判断所述签名时间是否可靠。

[权利要求 12] 如权利要求2所述的浏览器文件的统一签名及/或加密方法，其中，所述将所述时间戳添加进所述签名数据，生成已签名文件的步骤之后，还包括：

生成随机密钥，并通过所述随机密钥封装所述已签名文件；

通过所述订阅端的数字证书封装所述随机密钥；以及

将通过所述随机密钥封装的已签名文件，及通过所述订阅端的数字证书封装的所述随机密钥编码成加密文件。

[权利要求 13] 如权利要求1所述的浏览器文件的统一签名及/或加密方法，其中，所述根据所述发布端的私钥和数字证书及/或订阅端数字证书，通过公钥加密标准对所述封装文件进行签名及/或加密的步骤包括：

将所述封装文件编码为所述预设结构的已编码文件；

生成随机密钥，并通过随机密钥封装所述已编码文件；

通过所述订阅端的数字证书封装所述随机密钥；以及

将通过所述随机密钥封装的编码文件，及通过所述订阅端的数字证书封装的所述随机密钥编码成加密文件。

[权利要求 14] 如权利要求12或13所述的浏览器文件的统一签名及/或加密方法，其中，所述根据所述发布端的私钥和数字证书及/或订阅端数字证书，通过公钥加密标准对所述封装文件进行签名及/或加密的步骤之后，还包括：

在接收到所述加密文件时，获取所述订阅端的数字证书，其中所述订阅端数字证书包括订阅端的私钥；

根据所述订阅端私的钥解析所述加密文件，获取所述随机密钥；以及

根据所述随机密钥解析出所述待发布的浏览器文件。

[权利要求 15] 一种浏览器，其中，所述浏览器包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的的签名和加密程序，所述签名和加密程序被所述处理器执行时实现以下步骤：

在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件；

获取发布端的私钥和数字证书，及/或订阅端数字证书；以及

根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密。

[权利要求 16] 一种浏览器文件的统一签名及/或加密装置，其中，所述浏览器文件的统一签名及/或加密装置包括如权利要求15所述的浏览器。

[权利要求 17] 一种计算机可读存储介质，其中，所述计算机可读存储介质上存储有签名和加密程序，所述签名和加密程序被处理器执行时实现以下步骤：

在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件；

获取发布端的私钥和数字证书，及/或订阅端数字证书；以及

根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过

预设算法对所述封装文件进行签名及/或加密。

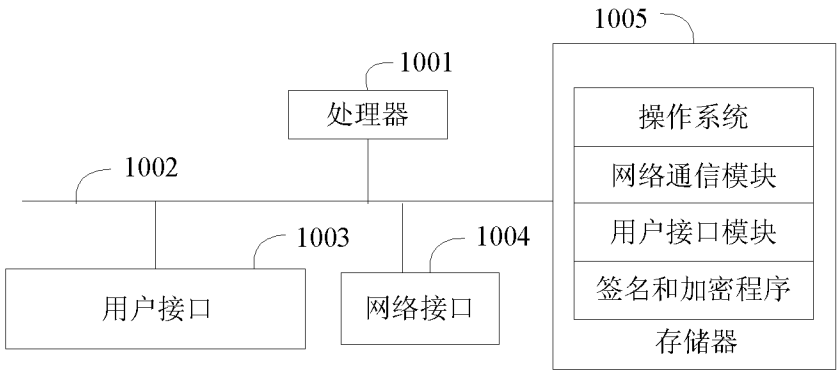
1005
1001
处理器
操作系统
网络通信模块
1002
用户接口模块
1003
1004
签名和加密程序
用户接口
网络接口
存储器

图 1

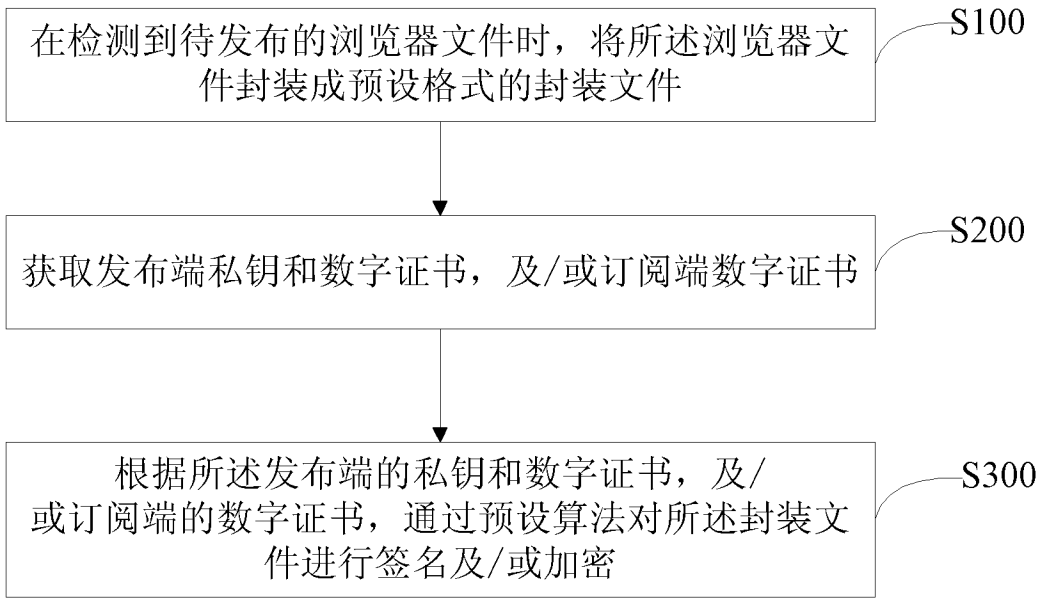
在检测到待发布的浏览器文件时，将所述浏览器文件封装成预设格式的封装文件
S100
获取发布端私钥和数字证书，及/或订阅端数字证书
S200
根据所述发布端的私钥和数字证书，及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密
S300

图 2

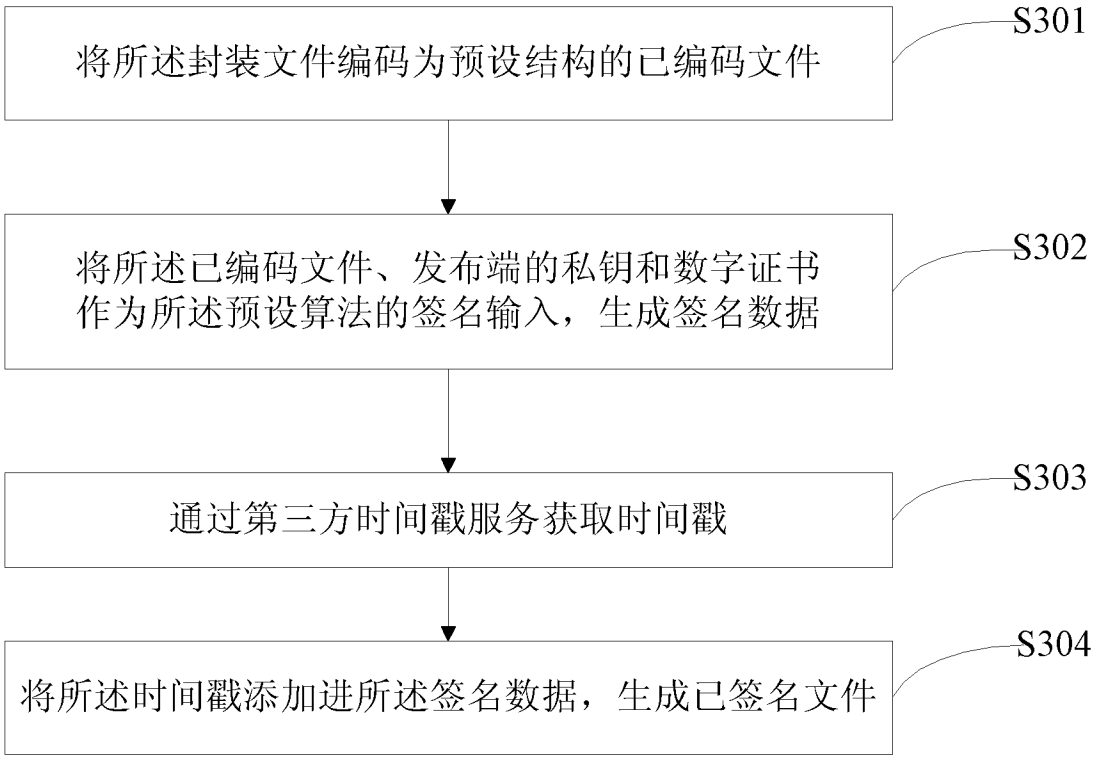
将所述封装文件编码为预设结构的已编码文件
S301
将所述已编码文件、发布端的私钥和数字证书作为所述预设算法的签名输入，生成签名数据
S302
通过第三方时间戳服务获取时间戳
S303
将所述时间戳添加进所述签名数据，生成已签名文件
S304

图 3

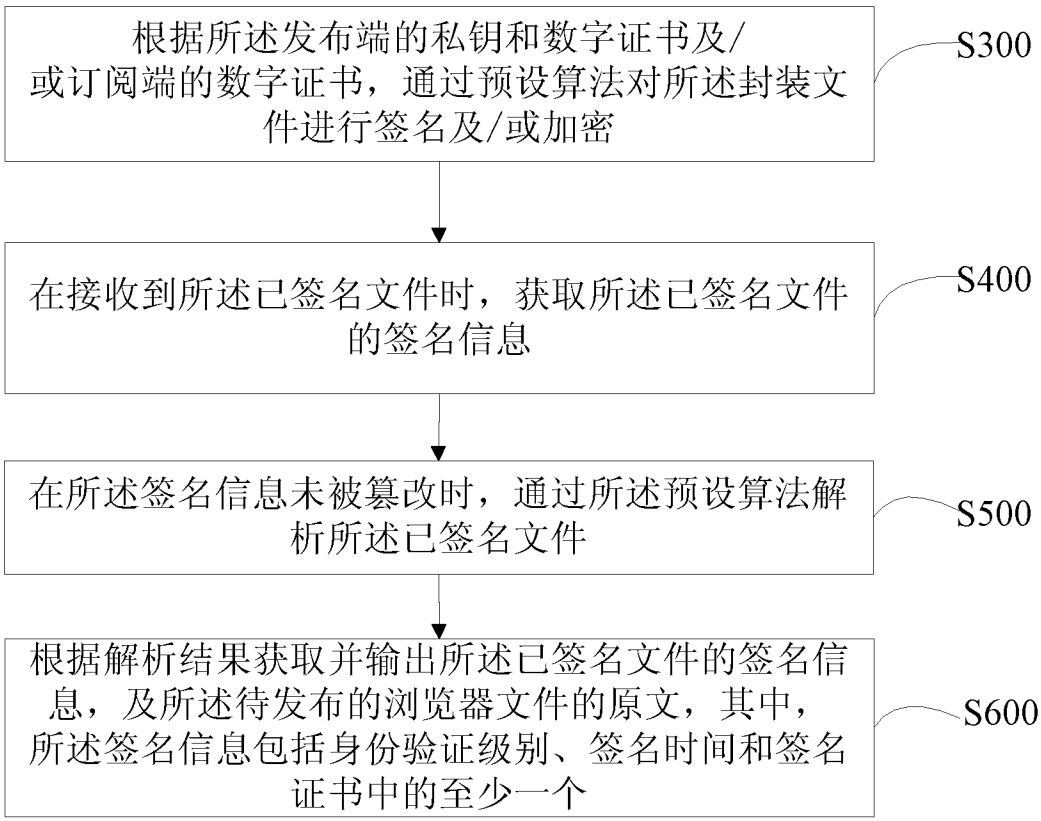
根据所述发布端的私钥和数字证书及/或订阅端的数字证书，通过预设算法对所述封装文件进行签名及/或加密
S300
在接收到所述已签名文件时，获取所述已签名文件的签名信息
S400
在所述签名信息未被篡改时，通过所述预设算法解析所述已签名文件
S500
根据解析结果获取并输出所述已签名文件的签名信息，及所述待发布的浏览器文件的原文，其中，所述签名信息包括身份验证级别、签名时间和签名证书中的至少一个
S600

图 4

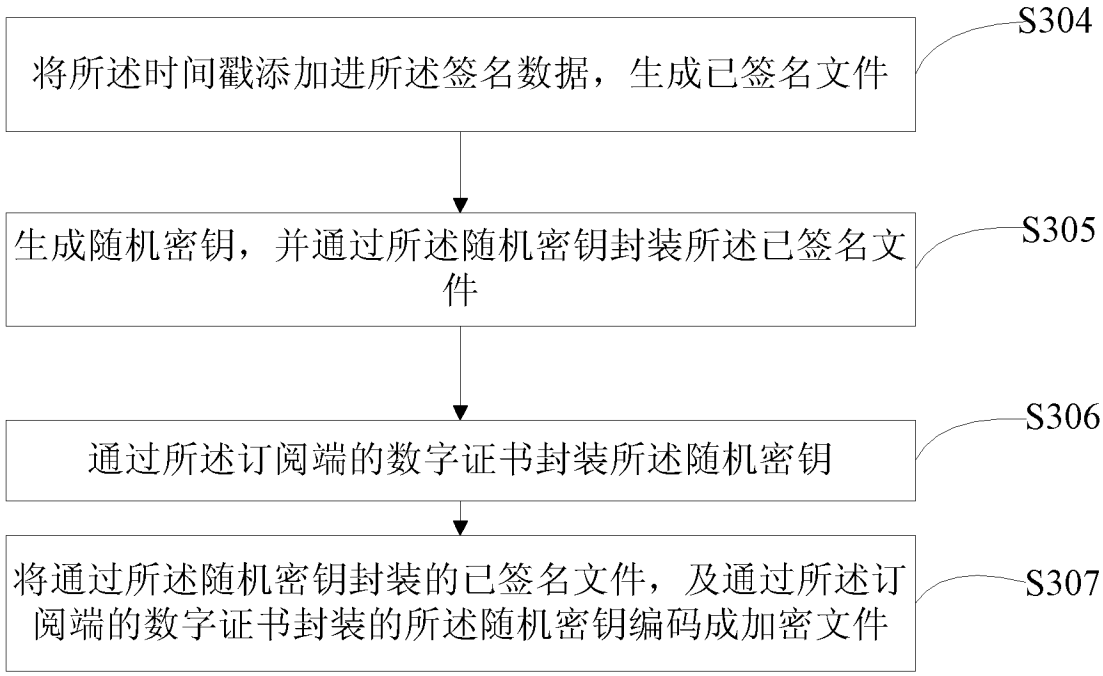
将所述时间戳添加进所述签名数据，生成已签名文件
S304
生成随机密钥，并通过所述随机密钥封装所述已签名文件
S305
通过所述订阅端的数字证书封装所述随机密钥
S306
将通过所述随机密钥封装的已签名文件，及通过所述订阅端的数字证书封装的所述随机密钥编码成加密文件
S307

图 5

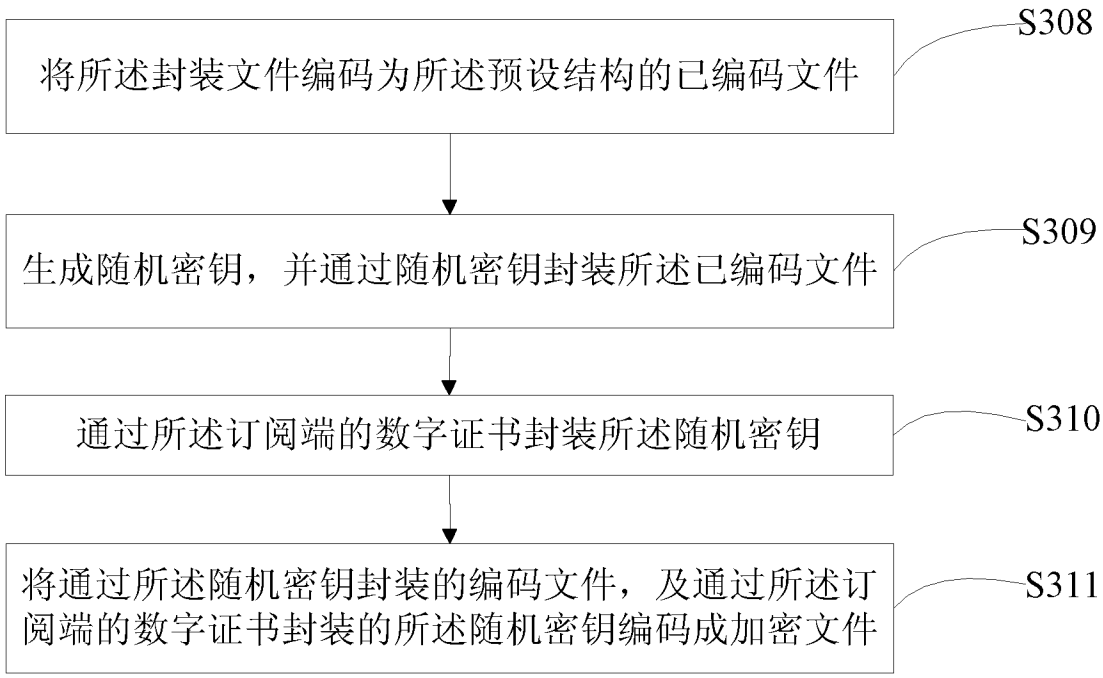
将所述封装文件编码为所述预设结构的已编码文件
S308
生成随机密钥，并通过随机密钥封装所述已编码文件
S309
通过所述订阅端的数字证书封装所述随机密钥
S310
将通过所述随机密钥封装的编码文件，及通过所述订阅端的数字证书封装的所述随机密钥编码成加密文件
S311

图 6

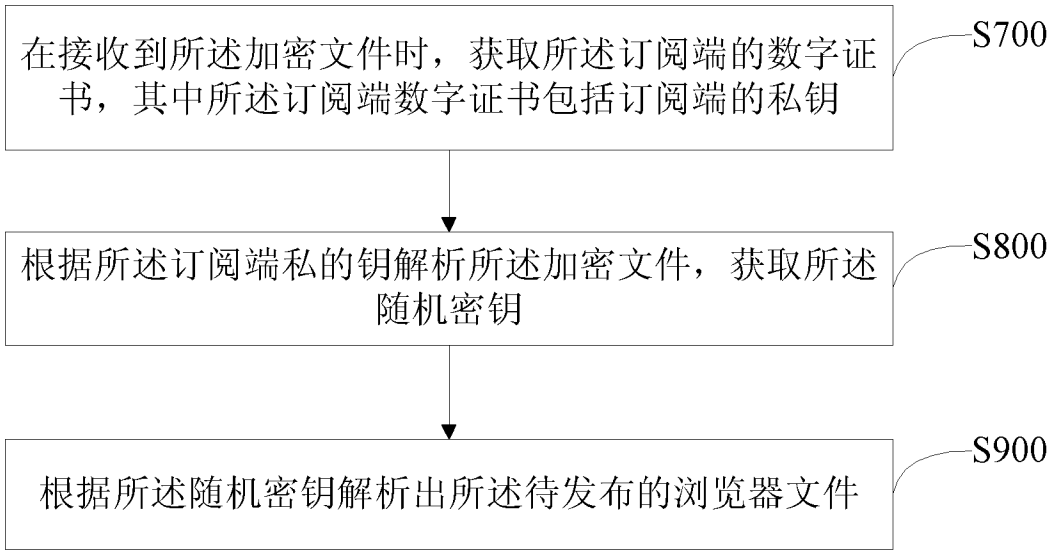
在接收到所述加密文件时，获取所述订阅端的数字证书，其中所述订阅端数字证书包括订阅端的私钥
S700
根据所述订阅端私的钥解析所述加密文件，获取所述随机密钥
S800
根据所述随机密钥解析出所述待发布的浏览器文件
S900

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/104856

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; H04L 29/08(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

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, WPI, EPODOC, CNKI, IEEE: 浏览器, 文件, 签名, 加密, 封装, 发布, 订阅, 私钥, 密钥, 证书, 编码, 多用途因特网扩展, 公钥加密标准, browser, file, document, sign+, encrypt+, encapsulat+, releas+, subscrib+, private, key, certificat+, cod+, MIME, PKCS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 105282143 A (TECHNICAL CENTER OF AIR TRAFFIC MANAGEMENT BUREAUOF CAAC) 27 January 2016 (2016-01-27) description, paragraphs [0005]-[0011]	1-17
Y	CN 101026674 A (CANON K. K.) 29 August 2007 (2007-08-29) description, page 2, lines 3-10, page 7, lines 9-11 and page 10, lines 5-7, and figures 10 and 11	1-17
A	CN 108173860 A (SHENZHEN FANHAI SANJIANG TECHNOLOGY DEVELOPMENT CO., LTD.) 15 June 2018 (2018-06-15) entire document	1-17
A	CN 106789963 A (BEIJING YANGPUWEIYE TECHNOLOGY DEVELOPMENT CO., LTD.) 31 May 2017 (2017-05-31) entire document	1-17
A	CN 106330462 A (GUANGDONG ELECTRONIC CERTIFICATION AUTHORITY CO., LTD.) 11 January 2017 (2017-01-11) entire document	1-17

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 April 2019	**04 June 2019**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/104856

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 105282143 A	27 January 2016	None	
CN 101026674 A	29 August 2007	JP 2007221373 A	30 August 2007
		KR 20070082566 A	21 August 2007
		US 2007188797 A1	16 August 2007
		EP 1821499 A1	22 August 2007
CN 108173860 A	15 June 2018	None	
CN 106789963 A	31 May 2017	None	
CN 106330462 A	11 January 2017	None	

国际检索报告

国际申请号 PCT/CN2018/104856

A. 主题的分类

H04L 9/08(2006.01)i; H04L 29/08(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

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, WPI, EPODOC, CNKI, IEEE: 浏览器，文件，签名，加密，封装，发布，订阅，私钥，密钥，证书，编码，多用途因特网扩展，公钥加密标准，browser, file, document, sign+, encrypt+, encapsulat+, releas+, subscrib+, private, key, certificat+, cod+, MIME, PKCS

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
Y	CN 105282143 A (民航局空管局技术中心) 2016年 1月 27日 (2016-01-27) 说明书第[0005]-[0011]段	1-17
Y	CN 101026674 A (佳能株式会社) 2007年 8月 29日 (2007-08-29) 说明书第2页第3-10行，第7页第9-11行，第10页第5-7行，说明书附图图10-11	1-17
A	CN 108173860 A (深圳市泛海三江科技发展有限公司) 2018年 6月 15日 (2018-06-15) 全文	1-17
A	CN 106789963 A (北京洋浦伟业科技发展有限公司) 2017年 5月 31日 (2017-05-31) 全文	1-17
A	CN 106330462 A (广东省电子商务认证有限公司) 2017年 1月 11日 (2017-01-11) 全文	1-17

☐ 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

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 4月 4日	2019年 6月 4日
ISA/CN的名称和邮寄地址 中国国家知识产权局(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 李玉坤 电话号码 86-(10)-53961358

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/104856

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	105282143	A	2016年 1月 27日		无		
CN	101026674	A	2007年 8月 29日	JP	2007221373	A	2007年 8月 30日
				KR	20070082566	A	2007年 8月 21日
				US	2007188797	A1	2007年 8月 16日
				EP	1821499	A1	2007年 8月 22日
CN	108173860	A	2018年 6月 15日		无		
CN	106789963	A	2017年 5月 31日		无		
CN	106330462	A	2017年 1月 11日		无		