(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 106982190 A
(43)申请公布日 2017.07.25

(21)申请号 201610029844.8

(22)申请日 2016.01.18

(71)申请人 卓望数码技术(深圳)有限公司
地址 518057 广东省深圳市南山区高新技术产业园南区深港产学研基地大楼西座六楼南翼

(72)发明人 彭涛 王巍 刘志诚 霍要峰

(74)专利代理机构 深圳市顺天达专利商标代理有限公司 44217
代理人 李琴

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

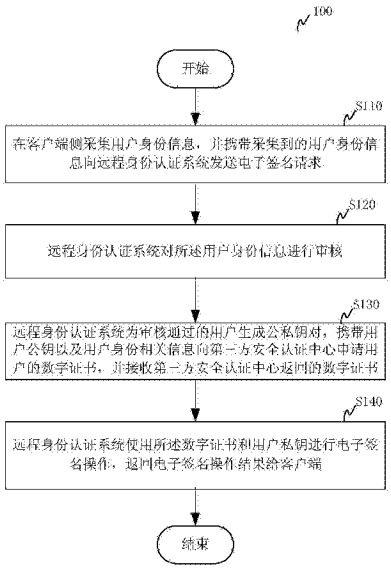
权利要求书2页 说明书5页 附图4页

(54)发明名称

一种电子签名方法和系统

(57)摘要

本发明涉及一种电子签名方法和系统。所述方法包括如下步骤:S1、在客户端侧采集用户身份信息,并携带采集到的用户身份信息向远程身份认证系统发送电子签名请求;S2、远程身份认证系统对所述用户身份信息进行审核;S3、远程身份认证系统为审核通过的用户生成公私钥对,携带用户公钥以及用户身份相关信息向第三方安全认证中心申请用户的数字证书,并接收第三方安全认证中心返回的数字证书;S4、远程身份认证系统使用所述数字证书和用户私钥进行电子签名操作,返回电子签名操作结果给客户端。本发明的电子签名方案实现安全便利的远程用户身份认证,确保了电子签名具备法律效力,尤其方便用户在进行银行、证券等行业开户时的远程操作。



CN 106982190 A

1.一种电子签名方法,其特征在于,包括如下步骤:

S1、在客户端侧采集用户身份信息,并携带采集到的用户身份信息向远程身份认证系统发送电子签名请求;

S2、远程身份认证系统对所述用户身份信息进行审核;

S3、远程身份认证系统为审核通过的用户生成公私钥对,携带用户公钥以及用户身份相关信息向第三方安全认证中心申请用户的数字证书,并接收第三方安全认证中心返回的数字证书;

S4、远程身份认证系统使用所述数字证书和用户私钥进行电子签名操作,返回电子签名操作结果给客户端。

2.根据权利要求1所述的电子签名方法,其特征在于,所述步骤S1进一步包括:

S11、通过摄像头采集用户的视频照片;

S12、通过摄像头采集用户的身份证信息;

S13、通过录音设备采集用户的音频信息;

S14、通过手写板采集用户的笔迹;

所述步骤S2进一步包括:

S21、核对视频照片与身份证照片确认用户身份的一致性;

S22、将身份证姓名和身份证号码发送到公安部系统远程核查确认用户身份。

3.根据权利要求2所述的电子签名方法,其特征在于,所述步骤S3进一步包括:

对所述视频照片、身份证信息、音频信息和笔迹分别进行哈希运算,将得到的哈希值作为用户身份标识与所述用户公钥一起发送至所述第三方安全认证中心申请用户的数字证书,并接收第三方安全认证中心返回的将所述哈希值作为扩展项签发的数字证书。

4.根据权利要求1所述的电子签名方法,其特征在于,所述步骤S4进一步包括:远程身份认证系统在完成电子签名操作后,销毁用户私钥。

5.根据权利要求1所述的电子签名方法,其特征在于,所述方法还包括:由远程身份认证系统保存采集到的所有用户身份信息。

6.一种电子签名系统,其特征在于,包括通信连接的客户端和远程身份认证系统,其中:

所述客户端采集用户身份信息,并携带采集到的用户身份信息向远程身份认证系统发送电子签名请求;

所述远程身份认证系统对所述用户身份信息进行审核,为审核通过的用户生成公私钥对,携带用户公钥以及用户身份相关信息向第三方安全认证中心申请用户的数字证书,并接收第三方安全认证中心返回的数字证书;

所述远程身份认证系统还使用所述数字证书和用户私钥进行电子签名操作,返回电子签名操作结果给所述客户端。

7.根据权利要求6所述的电子签名系统,其特征在于,所述客户端进一步包括信息采集模块,用于通过摄像头采集用户的视频照片和身份证信息,通过录音设备采集用户的音频信息,通过手写板采集用户的笔迹;

所述远程身份认证系统进一步包括信息审核模块,用于核对视频照片与身份证照片确认用户身份的一致性,并将身份证姓名和身份证号码发送到公安部系统远程核查确认用户

身份。

8.根据权利要求7所述的电子签名系统，其特征在于，所述远程身份认证系统进一步包括：

数字证书申请模块，用于对所述视频照片、身份证信息、音频信息和笔迹分别进行哈希运算，将得到的哈希值作为用户身份标识与所述用户公钥一起发送至所述第三方安全认证中心申请用户的数字证书，并接收第三方安全认证中心返回的将所述哈希值作为扩展项签发的数字证书。

9.根据权利要求6所述的电子签名系统，其特征在于，所述远程身份认证系统进一步包括密钥销毁模块，用于在完成电子签名操作后，销毁用户私钥。

10.根据权利要求6所述的电子签名系统，其特征在于，所述远程身份认证系统进一步包括证据保全模块，用于保存采集到的所有用户身份信息。

一种电子签名方法和系统

技术领域

[0001] 本发明涉及互联网安全认证领域，更具体地说，涉及一种电子签名方法和系统。

背景技术

[0002] 目前，银行、证券等行业开户时，都必须以实名制为基础，账户实行实名制，必须与身份证的姓名和绑定业务账户的姓名完全一致。用户个人携其本人身份证件亲自办理，当面与业务企业确立权利与义务关系。

[0003] 随着各行各业信息化的迅猛发展，传统的商业模式逐渐转变，互联网化已经是大势所趋。银行、证券等行业开户，仍然需要用户携带证件，到营业厅柜台进行当面身份核查，效率低下，且营业厅网点成本过高。特别是营业厅网点少的企业，传统的开户面签就像客户与企业之间的一道门槛，对业务的开展和推广形成了一定的阻碍。

发明内容

[0004] 本发明要解决的技术问题在于，针对现有技术的上述缺陷，提供一种电子签名方法和系统以实现安全便利的远程用户身份认证。

[0005] 本发明为解决其技术问题在第一方面提出一种电子签名方法，包括如下步骤：

[0006] S1、在客户端侧采集用户身份信息，并携带采集到的用户身份信息向远程身份认证系统发送电子签名请求；

[0007] S2、远程身份认证系统对所述用户身份信息进行审核；

[0008] S3、远程身份认证系统为审核通过的用户生成公私钥对，携带用户公钥以及用户身份相关信息向第三方安全认证中心申请用户的数字证书，并接收第三方安全认证中心(certificate authority,CA)返回的数字证书；

[0009] S4、远程身份认证系统使用所述数字证书和用户私钥进行电子签名操作，返回电子签名操作结果给客户端。

[0010] 根据本发明的一个实施例中，所述步骤S1进一步包括：

[0011] S11、通过摄像头采集用户的视频照片；

[0012] S12、通过摄像头采集用户的身份证信息；

[0013] S13、通过录音设备采集用户的音频信息；

[0014] S14、通过手写板采集用户的笔迹；

[0015] 所述步骤S2进一步包括：

[0016] S21、核对视频照片与身份证照片确认用户身份的一致性；

[0017] S22、将身份证姓名和身份证号码发送到公安部系统远程核查确认用户身份。

[0018] 根据本发明的一个实施例中，所述步骤S3进一步包括：

[0019] 对所述视频照片、身份证信息、音频信息和笔迹分别进行哈希运算，将得到的哈希值作为用户身份标识与所述用户公钥一起发送至所述第三方安全认证中心申请用户的数字证书，并接收第三方安全认证中心返回的将所述哈希值作为扩展项签发的数字证书。

[0020] 根据本发明的一个实施例中，所述步骤S4进一步包括：远程身份认证系统在完成电子签名操作后，销毁用户私钥。

[0021] 根据本发明的一个实施例中，所述方法还包括：由远程身份认证系统保存采集到的所有用户身份信息。

[0022] 本发明为解决其技术问题在第二方面提出一种电子签名系统，包括通信连接的客户端和远程身份认证系统，其中：

[0023] 所述客户端采集用户身份信息，并携带采集到的用户身份信息向远程身份认证系统发送电子签名请求；

[0024] 所述远程身份认证系统对所述用户身份信息进行审核，为审核通过的用户生成公私钥对，携带用户公钥以及用户身份相关信息向第三方安全认证中心申请用户的数字证书，并接收第三方安全认证中心返回的数字证书；

[0025] 所述远程身份认证系统还使用所述数字证书和用户私钥进行电子签名操作，返回电子签名操作结果给所述客户端。

[0026] 根据本发明的一个实施例中，所述客户端进一步包括信息采集模块，用于通过摄像头采集用户的视频照片和身份证信息，通过录音设备采集用户的音频信息，通过手写板采集用户的笔迹；

[0027] 所述远程身份认证系统进一步包括信息审核模块，用于核对视频照片与身份证照片确认用户身份的一致性，并将身份证姓名和身份证号码发送到公安部系统远程核查确认用户身份。

[0028] 根据本发明的一个实施例中，所述远程身份认证系统进一步包括：

[0029] 数字证书申请模块，用于对所述视频照片、身份证信息、音频信息和笔迹分别进行哈希运算，将得到的哈希值作为用户身份标识与所述用户公钥一起发送至所述第三方安全认证中心申请用户的数字证书，并接收第三方安全认证中心返回的将所述哈希值作为扩展项签发的数字证书。

[0030] 根据本发明的一个实施例中，所述远程身份认证系统进一步包括密钥销毁模块，用于在完成电子签名操作后，销毁用户私钥。

[0031] 根据本发明的一个实施例中，所述远程身份认证系统进一步包括证据保全模块，用于保存采集到的所有用户身份信息。

[0032] 本发明的电子签名方法和系统通过采集用户身份信息确认用户身份，通过将用户身份信息的哈希值作为扩展项签发到具备法律效力的第三方CA签发的用户数字证书里面，作为用户身份标识，使用该数字证书进行电子签名操作，可以防篡改，签名可追溯，因而解决了远程用户身份认证中的安全性及便利性问题，尤其方便用户在进行银行、证券等行业开户时的远程操作。

附图说明

[0033] 下面将结合附图及实施例对本发明作进一步说明，附图中：

[0034] 图1是本发明一个实施例的电子签名方法的流程图；

[0035] 图2是本发明一个实施例的电子签名方法应用于远程开户的交互过程示意图；

[0036] 图3是图2中远程身份认证系统向第三方CA申请数字证书的详细交互过程示意图；

[0037] 图4是本发明一个实施例的电子签名系统的逻辑结构图。

具体实施方式

[0038] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0039] 图1示出了根据本发明一个实施例的电子签名方法100的流程图。如图1所示，该电子签名方法100包括如下步骤：

[0040] 步骤S110中，在客户端侧采集用户身份信息，并携带采集到的用户身份信息向远程身份认证系统发送电子签名请求。具体来说，所述用户身份信息包括视频信息、音频信息、身份证信息、签名笔迹等，用于确认用户身份。

[0041] 随后步骤S120中，远程身份认证系统对所述用户身份信息进行审核以确认用户身份，具体可包括：通过对视频照片与身份证照片进行比对以确认用户身份的一致性，通过将身份证姓名及身份证号码发送到公安部系统远程核查确认用户身份的正确性和合法性等。

[0042] 随后步骤S130中，远程身份认证系统为审核通过的用户生成公私钥对，携带用户公钥以及用户身份相关信息向第三方安全认证中心申请用户的数字证书，并接收第三方安全认证中心返回的数字证书。

[0043] 随后步骤S140中，远程身份认证系统使用所述数字证书和用户私钥进行电子签名操作，返回电子签名操作结果给客户端。

[0044] 本发明以上提出的电子签名方案，充分利用了具备法律效力的第三方CA的合法性和电子签名的合法性，解决了远程用户身份认证中的安全性及便利性问题，方便用户在进行银行、证券等行业开户时远程操作。

[0045] 图2示出了本发明一个实施例的电子签名方法应用于远程开户的交互过程。具体如图2所示，该远程开户过程包括如下步骤：

[0046] 步骤S201，客户端通过摄像头采集用户的视频照片；

[0047] 步骤S202，客户端通过摄像头采集用户的身份证信息；

[0048] 步骤S203，客户端通过录音设备采集用户的音频信息；

[0049] 步骤S204，客户端向用户展示开户协议，接收用户的电子签名请求；

[0050] 步骤S205，客户端通过手写板采集用户的签名笔迹；

[0051] 步骤S206，客户端携带采集到的上述用户身份信息向远程身份认证系统申请开户；

[0052] 步骤S207，远程身份认证系统核对采集到的视频照片与身份证照片以确认用户身份的一致性；

[0053] 步骤S208，远程身份认证系统将身份证姓名和身份证号码发送到公安局系统远程核查以确认用户身份的正确性和合法性；

[0054] 步骤S209，前述用户身份信息审核通过后，远程身份认证系统向第三方CA申请用户的数字证书；

[0055] 步骤S210，远程身份认证系统使用第三方CA签发的数字证书和用户私钥为开户协议进行电子签名，从而确保了电子签名后的电子协议具备法律效力；

[0056] 步骤S211，远程身份认证系统销毁用户私钥，以防止私钥泄露，提升电子签名的安全性；

[0057] 步骤S212，远程身份认证系统将采集到的所有用户身份信息进行保存，实现证据保全；

[0058] 步骤S213，远程身份认证系统返回开户完成的操作结果给客户端。

[0059] 具体一个实施例中，远程身份认证系统向第三方CA申请数字证书的详细交互过程如图3所示，包括如下步骤：

[0060] 步骤S301，远程身份认证系统对视频照片进行哈希(hash)运算；

[0061] 步骤S302，远程身份认证系统对身份证信息进行哈希运算；

[0062] 步骤S303，远程身份认证系统对音频信息进行哈希运算；

[0063] 步骤S304，远程身份认证系统对签名笔迹进行哈希运算；

[0064] 步骤S305，远程身份认证系统生成用户的公私钥对；

[0065] 步骤S306，远程身份认证系统携带用户公钥、用户身份以及前述计算的各哈希值向第三方CA申请用户的数字证书；

[0066] 步骤S307，CA签发用户数字证书，并将前述的各哈希值签入数字证书的扩展项中，作为用户身份标识。

[0067] 步骤S308，CA返回数字证书给远程身份认证系统。远程身份认证系统使用该数字证书对开户协议进行电子签名，可以防篡改，且签名可追溯。

[0068] 基于本发明以上所介绍的电子签名方法，本发明还提出一种电子签名系统。图4示出了根据本发明一个实施例的电子签名系统100的逻辑结构图。如图4所示，该电子签名系统包括通信连接的客户端410和远程身份认证系统420。客户端410用于采集用户身份信息，并携带采集到的用户身份信息向远程身份认证系统420发送电子签名请求。远程身份认证系统420用于对用户身份信息进行审核，为审核通过的用户生成公私钥对，携带用户公钥以及用户身份相关信息向第三方安全认证中心40申请用户的数字证书，并接收第三方安全认证中心40返回的数字证书。远程身份认证系统420还用于使用所述数字证书和用户私钥进行电子签名操作，返回电子签名操作结果给客户端410。

[0069] 具体如图4所示，客户端410进一步包括信息采集模块411，其与摄像头10、录音设备20和手写板30通信连接，用于通过摄像头10采集用户的视频照片和身份证信息，通过录音设备20采集用户的音频信息，通过手写板30采集用户的笔迹。远程身份认证系统420进一步包括信息审核模块421、密钥生成模块422、数字证书申请模块423、签名模块424、密钥销毁模块425和证据保全模块426。信息审核模块421用于对采集到的用户身份信息进行审核，具体包括：核对视频照片与身份证照片确认用户身份的一致性，并将身份证姓名和身份证号码发送到公安部系统远程核查确认用户身份等。密钥生成模块422用于为审核通过的用户生成公私钥对。数字证书申请模块423用于携带用户公钥以及用户身份相关信息向第三方安全认证中心40申请用户的数字证书，并接收第三方安全认证中心40返回的数字证书。具体实施例中，数字证书申请模块423可对所述视频照片、身份证信息、音频信息和笔迹分别进行哈希运算，将得到的哈希值作为用户身份标识与所述用户公钥一起发送至第三方安全认证中心40申请用户的数字证书，并接收第三方安全认证中心40返回的将所述哈希值作为扩展项签发的数字证书。签名模块424用于使用第三方安全认证中心40签发的数字证书

和用户私钥进行电子签名操作，返回电子签名操作结果给客户端410。使用该数字证书进行电子签名，可以防篡改，且签名可追溯。密钥销毁模块425用于在签名模块424完成电子签名操作后，销毁用户私钥，以防止私钥泄露，提升电子签名的安全性。证据保全模块426用于将采集到的所有用户身份信息进行保存，实现证据保全。

[0070] 本申请以上介绍的电子签名方案通过采集用户身份信息确认用户身份，通过将用户身份信息的哈希值作为扩展项签发到具备法律效力的第三方CA签发的用户数字证书里面作为用户身份标识，使用该数字证书进行电子签名操作，可以防篡改，签名可追溯，因而解决了远程用户身份认证中的安全性及便利性问题，确保了电子签名具备法律效力，尤其方便用户在进行银行、证券等行业开户时的远程操作。

[0071] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

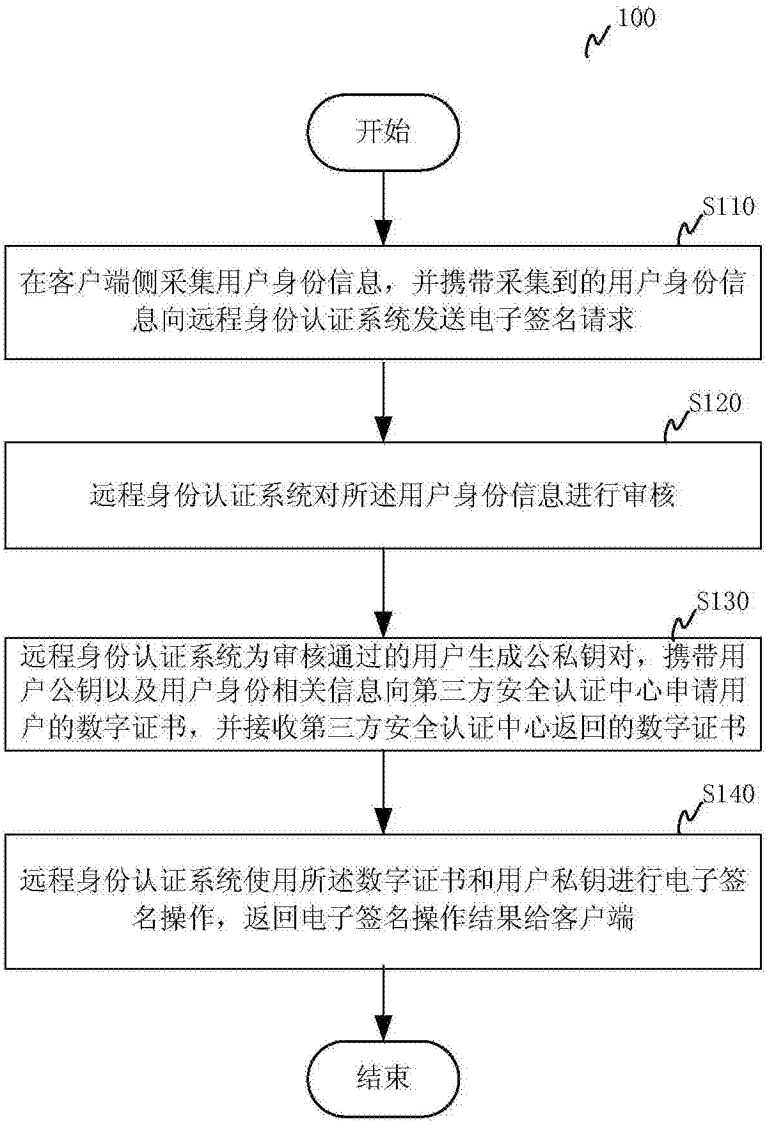

100
开始
S110
在客户端侧采集用户身份信息，并携带采集到的用户身份信息向远程身份认证系统发送电子签名请求
S120
远程身份认证系统对所述用户身份信息进行审核
S130
远程身份认证系统为审核通过的用户生成公私钥对，携带用户公钥以及用户身份相关信息向第三方安全认证中心申请用户的数字证书，并接收第三方安全认证中心返回的数字证书
S140
远程身份认证系统使用所述数字证书和用户私钥进行电子签名操作，返回电子签名操作结果给客户端
结束

图1

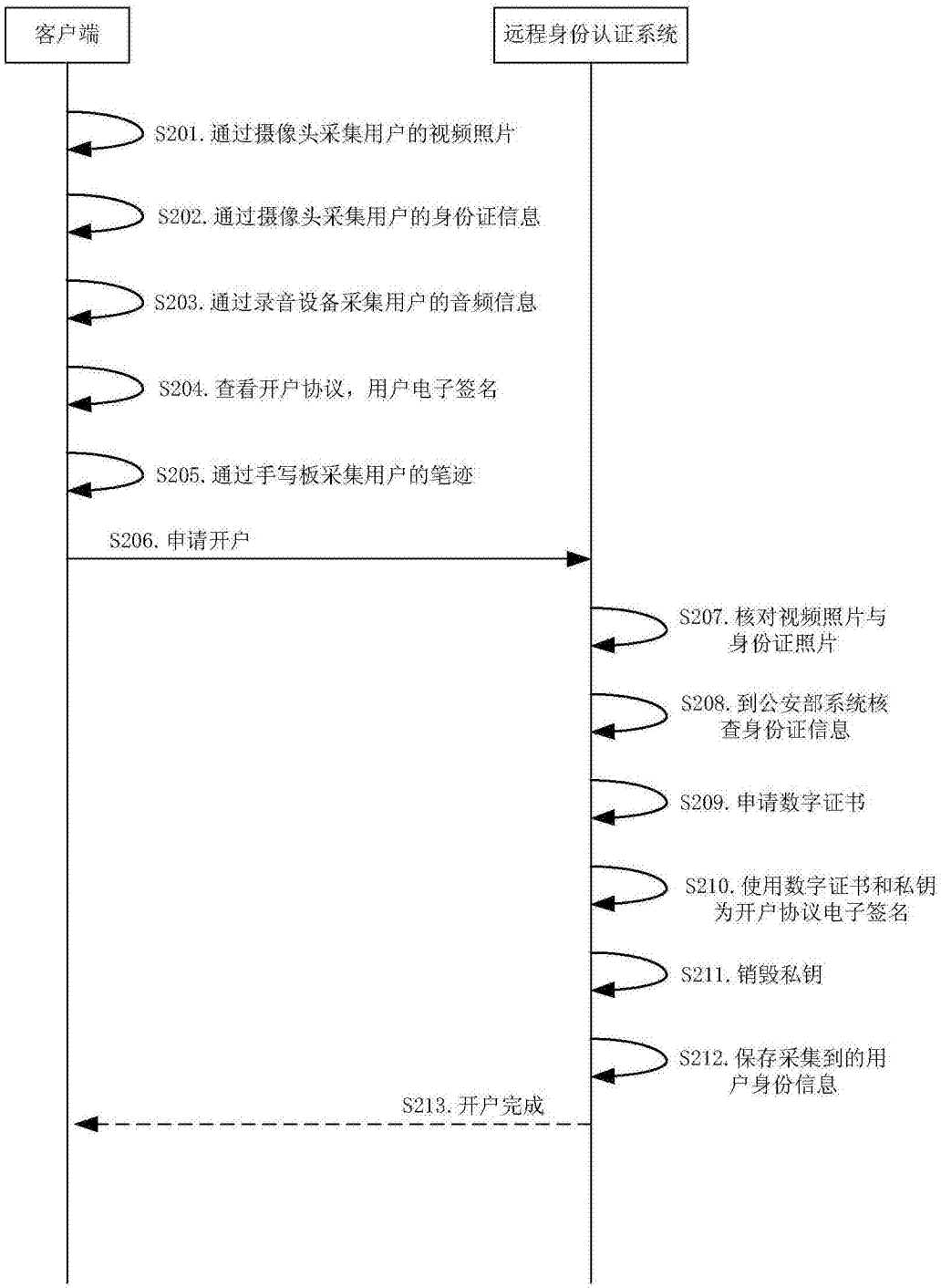

客户端
远程身份认证系统
S201. 通过摄像头采集用户的视频照片
S202. 通过摄像头采集用户的身份证信息
S203. 通过录音设备采集用户的音频信息
S204. 查看开户协议，用户电子签名
S205. 通过手写板采集用户的笔迹
S206. 申请开户
S207. 核对视频照片与身份证照片
S208. 到公安部系统核查身份证信息
S209. 申请数字证书
S210. 使用数字证书和私钥为开户协议电子签名
S211. 销毁私钥
S212. 保存采集到的用户身份信息
S213. 开户完成

图2

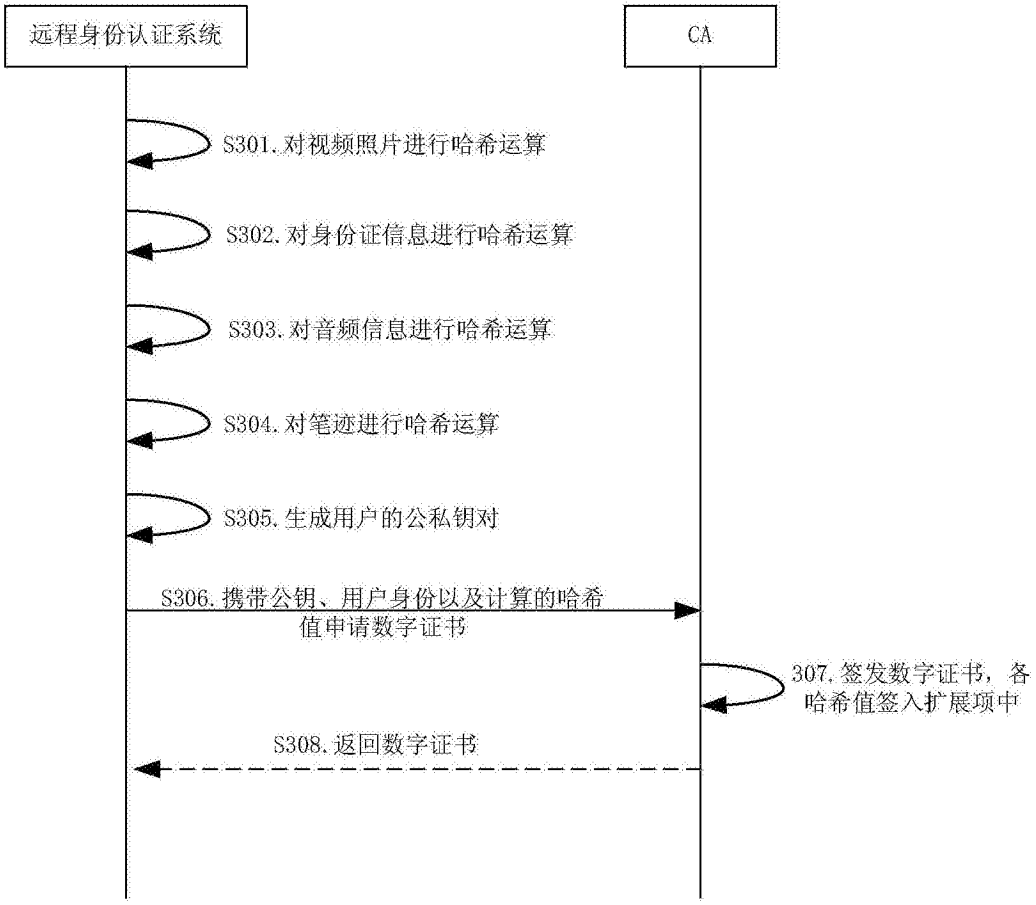

远程身份认证系统
CA
S301.对视频照片进行哈希运算
S302.对身份证信息进行哈希运算
S303.对音频信息进行哈希运算
S304.对笔迹进行哈希运算
S305.生成用户的公私钥对
S306.携带公钥、用户身份以及计算的哈希值申请数字证书
307.签发数字证书，各哈希值签入扩展项中
S308.返回数字证书

图3

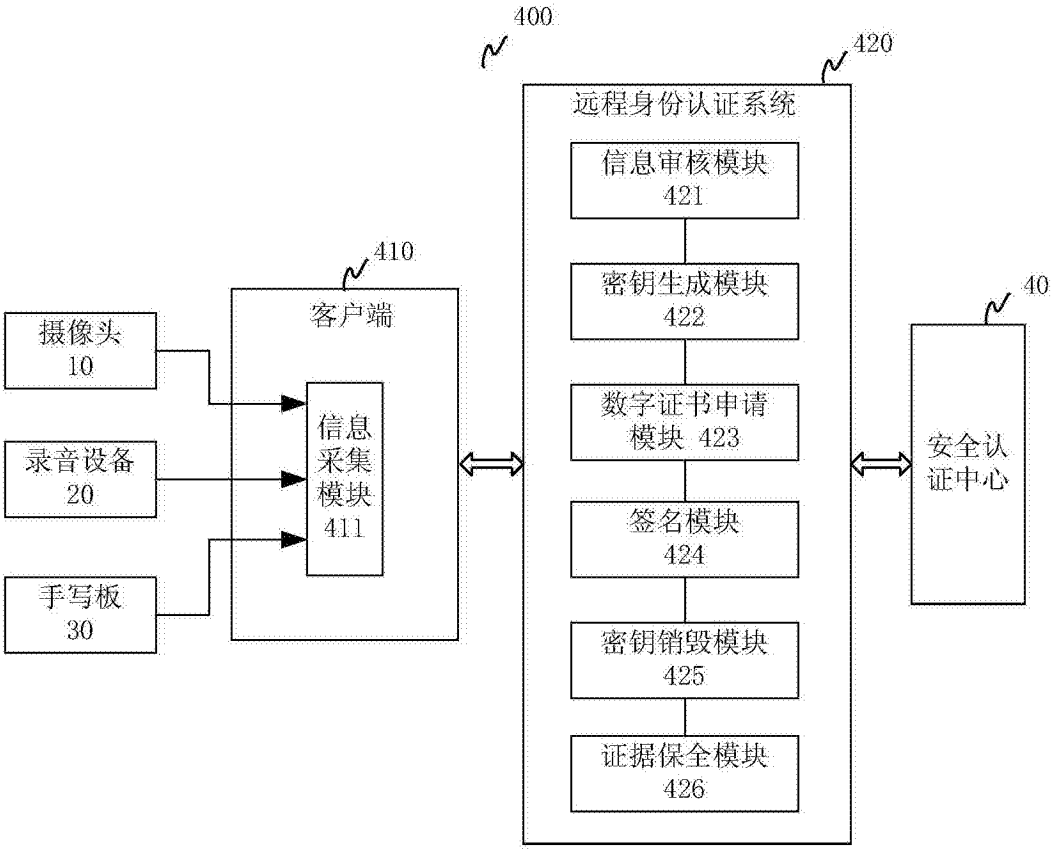

400
420
远程身份认证系统
信息审核模块
421
密钥生成模块
422
数字证书申请
模块 423
签名模块
424
密钥销毁模块
425
证据保全模块
426
410
客户端
信息
采集
模块
411
摄像头
10
录音设备
20
手写板
30
40
安全认
证中心

图4