(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109684801 B
(45)授权公告日 2023.06.16

(21)申请号 201811372204.2
(22)申请日 2018.11.16
(65)同一申请的已公布的文献号
申请公布号 CN 109684801 A
(43)申请公布日 2019.04.26
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心
(72)发明人 谷晨 落红卫
(74)专利代理机构 北京亿腾知识产权代理事务所(普通合伙) 11309
专利代理师 陈霁 周良玉
(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/32(2013.01)
G06V 40/50(2022.01)
G06Q 10/10(2023.01)
G06Q 50/26(2012.01)
(56)对比文件
CN 108809659 A,2018.11.13
CN 105591744 A,2016.05.18
审查员 杨怡睿

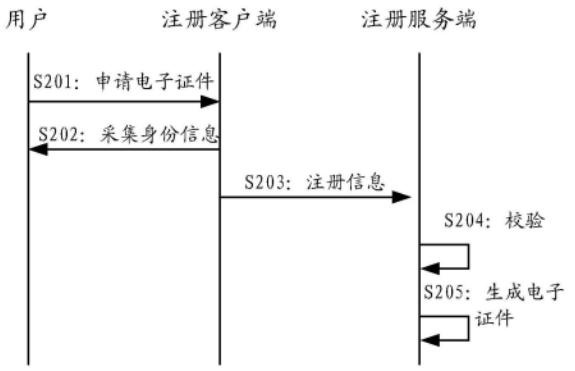
权利要求书4页 说明书15页 附图6页

(54)发明名称

电子证件的生成、签发和验证方法及装置

(57)摘要

本说明书实施例提供一种电子证件的生成、签发方法，以及基于该电子证件的身份认证方法，以及对应装置。根据以上方法，基于对用户的实体证件的校验生成电子证件，从而确保电子证件的权威性和可靠性。在该电子证件的签发过程中，提供多种签发模式选择，在保证安全性的同时提供一定灵活性。在签发获得电子证件的基础上，可以基于该电子证件实现身份认证。



CN 109684801 B

1.一种电子证件的签发方法,通过签发服务端执行,用于签发电子证件,所述电子证件与用户注册信息关联存储,所述用户注册信息包括用户实体证件本身的物理标识信息;所述签发方法包括:

接收用户通过签发客户端发起的第一请求,所述第一请求至少包括,签发模式信息;

向签发客户端返回第一消息,所述第一消息至少包括业务流水号;

接收来自签发客户端的第二请求,所述第二请求基于所述业务流水号而生成,并包括与所述签发模式信息指示的签发模式所对应的所述用户的身份信息,以及口令信息;

将所述身份信息和口令信息与预先存储的注册信息中对应信息进行比对,在比对一致的情况下,将与所述注册信息关联存储的电子证件返回给所述签发客户端。

2.根据权利要求1所述的方法,其中所述第一请求还包括,所述用户的用户终端上与身份信息获取相关的控件的控件版本信息。

3.根据权利要求2所述的方法,还包括,根据所述签发模式信息以及所述控件版本信息,确定对所述第一请求的审批结果;

在所述审批结果为审批不通过的情况下,向签发客户端返回拒绝通知;和/或,将所述业务流水号设定为空号。

4.根据权利要求1所述的方法,其中所述签发模式信息指示采用实体证件的第一模式,所述第一消息还包括挑战值;

所述用户的身份信息包括,所述用户的用户终端利用所述挑战值读取的实体证件的物理标识信息。

5.根据权利要求1所述的方法,其中所述签发模式信息指示不采用实体证件的第二模式,

所述用户的身份信息包括以下中的一项或多项:用户实名信息,生物特征信息。

6.一种电子证件的申领方法,通过签发客户端执行,用于申领电子证件,所述电子证件与用户注册信息关联存储,所述用户注册信息包括用户实体证件本身的物理标识信息;所述申领方法包括:

响应于用户的申领操作指令,向签发服务端发出第一请求,所述第一请求至少包括签发模式信息;

接收返回的第一消息,所述第一消息至少包括业务流水号;

获取与所述签发模式信息指示的签发模式所对应的所述用户的身份信息,以及口令信息;

至少基于所述业务流水号,所述用户的身份信息,以及口令信息生成第二请求,将该第二请求发送到所述签发服务端;

从签发服务端接收电子证件。

7.根据权利要求6所述的方法,其中所述申领操作指令包括,对签发模式的选择指令,

所述向签发服务端发出第一请求包括,根据所述选择指令确定签发模式信息,将所述签发模式信息包含在所述第一请求中。

8.根据权利要求6所述的方法,其中所述第一请求还包括,所述用户的用户终端上与身份信息获取相关的控件的控件版本信息。

9.根据权利要求6所述的方法,还包括,响应于所述申领操作指令,向所述用户发出所

述签发客户端的应用鉴权请求；

接收用户输入的鉴权信息；

基于所述鉴权信息进行应用鉴权。

10.根据权利要求6所述的方法，其中所述签发模式信息指示采用实体证件的第一模式，所述第一消息还包括挑战值；

所述获取与所述签发模式信息指示的签发模式所对应的所述用户的身份信息包括：

获取用户终端利用所述挑战值读取的实体证件的物理标识信息。

11.根据权利要求6所述的方法，其中所述签发模式信息指示不采用实体证件的第二模式，

所述获取与所述签发模式信息指示的签发模式所对应的所述用户的身份信息包括以下中的一项或多项：

接收用户输入的用户实名信息；

通过用户终端采集所述用户的生物特征信息。

12.一种基于电子证件的用户身份认证方法，通过认证服务端执行，所述电子证件与用户注册信息关联存储，所述用户注册信息包括用户实体证件本身的物理标识信息；所述认证方法包括：

接收用户通过认证客户端发起的认证请求，所述认证请求至少包括认证模式信息；

向所述认证客户端返回请求结果消息，所述请求结果消息包括，业务流水号；

接收来自所述认证客户端的核验数据，所述核验数据基于所述业务流水号而生成，并包括与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

对所述核验数据进行校验，并向所述认证客户端返回认证结果。

13.根据权利要求12所述的方法，其中所述认证请求还包括，所述用户的用户终端上与身份信息获取相关的控件的控件版本信息。

14.根据权利要求13所述的方法，还包括，根据所述认证模式信息以及所述控件版本信息，确定对所述认证请求的审批结果；

在所述审批结果为审批不通过的情况下，向所述认证客户端返回拒绝通知；和/或，将所述业务流水号设定为空号。

15.根据权利要求12所述的方法，其中所述认证模式信息指示采用实体证件的第一模式，所述请求结果消息还包括挑战值；

所述用户的身份信息还包括，所述用户的用户终端利用所述挑战值读取的实体证件的物理标识信息。

16.根据权利要求12所述的方法，其中所述认证模式信息指示不采用实体证件的第二模式，

所述用户的身份信息还包括以下中的一项或多项：用户实名信息，生物特征信息。

17.一种基于电子证件的用户身份认证方法，通过认证客户端执行，所述电子证件与用户注册信息关联存储，所述用户注册信息包括用户实体证件本身的物理标识信息；所述认证方法包括：

响应于用户针对业务的认证指令，向认证服务端发出认证请求，所述认证请求至少包

括，认证模式信息；

接收返回的请求结果消息，所述请求结果消息至少包括业务流水号；

获取与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

基于所述业务流水号，所述用户的身份信息生成核验数据，将该核验数据发送到所述认证服务端；

从认证服务端接收认证结果。

18.根据权利要求17所述的方法，还包括，

根据所述电子证件的注册信息项和签发模式，确定所述电子证件支持的第一核验参数集合；

获取所述业务要求核验的第二核验参数集合；

向认证服务端发出认证请求包括，在所述第一核验参数集合包含所述第二核验参数集合的情况下，向认证服务端发出所述认证请求。

19.根据权利要求17所述的方法，其中所述认证模式信息指示采用实体证件的第一模式，所述请求结果消息还包括挑战值；

所述获取与所述认证模式信息指示的认证模式所对应的所述用户的身份信息包括：

读取所述电子证件；以及

获取用户终端利用所述挑战值读取的实体证件的物理标识信息。

20.根据权利要求17所述的方法，其中所述获取与所述认证模式信息指示的认证模式所对应的所述用户的身份信息还包括以下中的一项或多项：

接收用户输入的用户实名信息；

通过用户终端采集所述用户的生物特征信息。

21.一种电子证件的签发装置，部署在签发服务端，用于签发电子证件，所述电子证件与用户注册信息关联存储，所述用户注册信息包括用户实体证件本身的物理标识信息；所述签发装置包括：

第一请求接收单元，配置为接收用户通过签发客户端发起的第一请求，所述第一请求至少包括，签发模式信息；

第一消息发送单元，配置为向签发客户端返回第一消息，所述第一消息至少包括业务流水号；

第二请求接收单元，配置为接收来自签发客户端的第二请求，所述第二请求基于所述业务流水号而生成，并包括与所述签发模式信息指示的签发模式所对应的所述用户的身份信息，以及口令信息；

电子证件发送单元，配置为将所述身份信息和口令信息与预先存储的注册信息中对应信息进行比对，在比对一致的情况下，将与所述注册信息关联存储的电子证件返回给所述签发客户端。

22.一种电子证件的申领装置，部署在签发客户端，用于申领电子证件，所述电子证件与用户注册信息关联存储，所述用户注册信息包括用户实体证件本身的物理标识信息；所述申领装置包括：

第一请求发送单元，配置为响应于用户的申领操作指令，向签发服务端发出第一请求，

所述第一请求至少包括签发模式信息；

第一消息接收单元，配置为接收返回的第一消息，所述第一消息至少包括业务流水号；

身份信息获取单元，配置为获取与所述签发模式信息指示的签发模式所对应的所述用户的身份信息，以及口令信息；

第二请求发送单元，配置为至少基于所述业务流水号，所述用户的身份信息，以及口令信息生成第二请求，将该第二请求发送到所述签发服务端；

电子证件接收单元，配置为从签发服务端接收电子证件。

23.一种基于电子证件的用户身份认证装置，部署在认证服务端，所述电子证件与用户注册信息关联存储，所述用户注册信息包括用户实体证件本身的物理标识信息；所述认证装置包括：

认证请求接收单元，配置为接收用户通过认证客户端发起的认证请求，所述认证请求至少包括认证模式信息；

结果消息发送单元，配置为向所述认证客户端返回请求结果消息，所述请求结果消息包括，业务流水号；

核验数据接收单元，配置为接收来自所述认证客户端的核验数据，所述核验数据基于所述业务流水号而生成，并包括与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

认证结果发送单元，配置为对所述核验数据进行校验，并向所述认证客户端返回认证结果。

24.一种基于电子证件的用户身份认证装置，部署在认证客户端，所述电子证件与用户注册信息关联存储，所述用户注册信息包括用户实体证件本身的物理标识信息；所述认证装置包括：

认证请求发送单元，配置为响应于用户针对业务的认证指令，向认证服务端发出认证请求，所述认证请求至少包括，认证模式信息；

结果消息接收单元，配置为接收返回的请求结果消息，所述请求结果消息至少包括业务流水号；

身份信息获取单元，配置为获取与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

核验数据发送单元，配置为基于所述业务流水号，所述用户的身份信息生成核验数据，将该核验数据发送到所述认证服务端；

认证结果接收单元，配置为从认证服务端接收认证结果。

25.一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求1-20中任一项所述的方法。

电子证件的生成、签发和验证方法及装置

技术领域

[0001] 本说明书一个或多个实施例涉及身份安全认证领域，尤其涉及电子证件的生成、签发和验证方法及装置。

背景技术

[0002] 在线下的各种应用场景中，传统对用户的身份核验通常是基于证件实现的，即遵循“由证件实现证实人的身份真实性”逻辑。具体实现中，自然人提供证件(如身份证、护照等)，由代表场景商户的自然人(如酒店的前台人员，行政办理大厅的窗口办事人员)通过视检的方式确认用户与证件的对应关系，并且通过视检或是读卡设备的协助确认证件的真实性，在此基础上从证件上获取所需要的验证信息，即可认为该验证信息是可信身份信息，之后根据场景商户的业务逻辑提供服务。以上逻辑的核心是实体证件。

[0003] 随着互联网技术的发展，人们对于便捷性和安全性的需求越来越强。一方面对于线上业务，也存在着与线下应用场景类似的身份核验要求。例如远程开户，需要验证用户使用的身份信息是正确的，且用户使用的是自己的身份信息，甚至于更严格的要求，需要用户证明拥有有效的合法身份证。另一方面，在线下场景中，如何在没有实体证件时进行可靠的真实身份核验，都成为了需要解决的问题。

[0004] 因此，希望能有改进的方案，可以更加安全有效地实现身份信息的核验。

发明内容

[0005] 本说明书一个或多个实施例描述了一种电子证件的注册、签发方法，以及基于该电子证件的身份认证方法。通过以上方法，可以安全有效便利地实现身份信息的核验。

[0006] 根据第一方面，提供了一种生成电子证件的方法，通过注册服务端执行，包括：

[0007] 接收用户的注册信息，所述注册信息包括所述用户的身份信息和口令信息，所述用户的身份信息至少包括，实体证件的物理标识信息；

[0008] 根据维护的可信信息库，对所述用户的身份信息进行校验；

[0009] 在校验通过的情况下，为所述用户生成电子证件，并将所述电子证件与所述用户的注册信息关联存储。

[0010] 根据第二方面，提供了一种电子证件的签发方法，通过签发服务端执行，用于签发根据第一方面生成的电子证件，所述签发方法包括：

[0011] 接收用户通过签发客户端发起的第一请求，所述第一请求至少包括，签发模式信息；

[0012] 向签发客户端返回第一消息，所述第一消息至少包括业务流水号；

[0013] 接收来自签发客户端的第二请求，所述第二请求基于所述业务流水号而生成，并包括与所述签发模式信息指示的签发模式所对应的所述用户的身份信息，以及口令信息；

[0014] 将所述身份信息和口令信息与预先存储的注册信息中对应信息进行比对，在比对一致的情况下，将与所述注册信息关联存储的电子证件返回给所述签发客户端。

[0015] 根据第三方面，提供一种电子证件的申领方法，通过签发客户端执行，用于申领根据第一方面生成的电子证件，所述申领方法包括：

[0016] 响应于用户的申领操作指令，向签发服务端发出第一请求，所述第一请求至少包括签发模式信息；

[0017] 接收返回的第一消息，所述第一消息至少包括业务流水号；

[0018] 获取与所述签发模式信息指示的签发模式所对应的所述用户的身份信息，以及口令信息；

[0019] 至少基于所述业务流水号，所述用户的身份信息，以及口令信息生成第二请求，将该第二请求发送到所述签发服务端；

[0020] 从签发服务端接收电子证件。

[0021] 根据第四方面，提供了一种基于电子证件的用户身份认证方法，通过认证服务端执行，所述电子证件通过第一方面的方法而生成，所述认证方法包括：

[0022] 接收用户通过认证客户端发起的认证请求，所述认证请求至少包括认证模式信息；

[0023] 向所述认证客户端返回请求结果消息，所述请求结果消息包括，业务流水号；

[0024] 接收来自所述认证客户端的核验数据，所述核验数据基于所述业务流水号而生成，并包括与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

[0025] 对所述核验数据进行校验，并向所述认证客户端返回认证结果。

[0026] 根据第五方面，提供了一种基于电子证件的用户身份认证方法，通过认证客户端执行，所述电子证件通过第一方面的方法而生成，所述认证方法包括：

[0027] 响应于用户针对业务的认证指令，向认证服务端发出认证请求，所述认证请求至少包括，认证模式信息；

[0028] 接收返回的请求结果消息，所述请求结果消息至少包括业务流水号；

[0029] 获取与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

[0030] 基于所述业务流水号，所述用户的身份信息生成核验数据，将该核验数据发送到所述认证服务端；

[0031] 从认证服务端接收认证结果。

[0032] 根据第六方面，提供了一种生成电子证件的装置，部署在注册服务端，包括：

[0033] 注册信息接收单元，配置为接收用户的注册信息，所述注册信息包括所述用户的身份信息和口令信息，所述用户的身份信息至少包括，实体证件的物理标识信息；

[0034] 校验单元，配置为根据维护的可信信息库，对所述用户的身份信息进行校验；

[0035] 证件生成单元，配置为在校验通过的情况下，为所述用户生成电子证件，并将所述电子证件与所述用户的注册信息关联存储。

[0036] 根据第七方面，提供了一种电子证件的签发装置，部署在签发服务端，用于签发根据第六方面的装置所生成的电子证件，所述签发装置包括：

[0037] 第一请求接收单元，配置为接收用户通过签发客户端发起的第一请求，所述第一请求至少包括，签发模式信息；

[0038] 第一消息发送单元，配置为向签发客户端返回第一消息，所述第一消息至少包括业务流水号；

[0039] 第二请求接收单元，配置为接收来自签发客户端的第二请求，所述第二请求基于所述业务流水号而生成，并包括与所述签发模式信息指示的签发模式所对应的所述用户的身份信息，以及口令信息；

[0040] 电子证件发送单元，配置为将所述身份信息和口令信息与预先存储的注册信息中对应信息进行比对，在比对一致的情况下，将与所述注册信息关联存储的电子证件返回给所述签发客户端。

[0041] 根据第八方面，提供了一种电子证件的申领装置，部署在签发客户端，用于申领根据第六方面的装置生成的电子证件，所述申领装置包括：

[0042] 第一请求发送单元，配置为响应于用户的申领操作指令，向签发服务端发出第一请求，所述第一请求至少包括签发模式信息；

[0043] 第一消息接收单元，配置为接收返回的第一消息，所述第一消息至少包括业务流水号；

[0044] 身份信息获取单元，配置为获取与所述签发模式信息指示的签发模式所对应的所述用户的身份信息，以及口令信息；

[0045] 第二请求发送单元，配置为至少基于所述业务流水号，所述用户的身份信息，以及口令信息生成第二请求，将该第二请求发送到所述签发服务端；

[0046] 电子证件接收单元，配置为从签发服务端接收电子证件。

[0047] 根据第九方面，提供了一种基于电子证件的用户身份认证装置，部署在认证服务端，所述电子证件通过第六方面的装置而生成，所述认证装置包括：

[0048] 认证请求接收单元，配置为接收用户通过认证客户端发起的认证请求，所述认证请求至少包括认证模式信息；

[0049] 结果消息发送单元，配置为向所述认证客户端返回请求结果消息，所述请求结果消息包括，业务流水号；

[0050] 核验数据接收单元，配置为接收来自所述认证客户端的核验数据，所述核验数据基于所述业务流水号而生成，并包括与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

[0051] 认证结果发送单元，配置为对所述核验数据进行校验，并向所述认证客户端返回认证结果。

[0052] 根据第十方面，提供了一种基于电子证件的用户身份认证装置，部署在认证客户端，所述电子证件通过第六方面的装置而生成，所述认证装置包括：

[0053] 认证请求发送单元，配置为响应于用户针对业务的认证指令，向认证服务端发出认证请求，所述认证请求至少包括，认证模式信息；

[0054] 结果消息接收单元，配置为接收返回的请求结果消息，所述请求结果消息至少包括业务流水号；

[0055] 身份信息获取单元，配置为获取与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

[0056] 核验数据发送单元，配置为基于所述业务流水号，所述用户的身份信息生成核验

数据，将该核验数据发送到所述认证服务端；

[0057] 认证结果接收单元，配置为从认证服务端接收认证结果。

[0058] 根据第十一方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第一方面到第五方面的方法。

[0059] 根据第十二方面，提供了一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面到第五方面的方法。

[0060] 通过本说明书实施例提供的方法和装置，基于对用户的实体证件的校验生成电子证件，从而确保电子证件的权威性和可靠性。在该电子证件的签发过程中，提供多种签发模式选择，在保证安全性的同时提供一定灵活性。在签发获得电子证件的基础上，可以基于该电子证件实现身份认证，从而使得用户身份核验更加安全而便捷。

附图说明

[0061] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，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它的附图。

[0062] 图1为本说明书披露的一个实施例的实施场景示意图；

[0063] 图2示出根据一个实施例的注册电子证件的过程；

[0064] 图3示出根据一个实施例的签发电子证件的过程示意图；

[0065] 图4示出根据一个实施例的基于电子证件的身份认证过程示意图；

[0066] 图5示出根据一个实施例的电子证件生成装置的示意性框图；

[0067] 图6示出根据一个实施例的签发装置的示意性框图；

[0068] 图7示出根据一个实施例的申领装置的示意性框图；

[0069] 图8示出根据一个实施例的认证装置的示意性框图；

[0070] 图9示出根据一个实施例的认证装置的示意性框图。

具体实施方式

[0071] 下面结合附图，对本说明书提供的方案进行描述。

[0072] 根据本说明书实施例提供的构思，依靠电子证件的注册、签发，为用户提供与实体证件具有对应权威性的电子证件。在此基础上，在线上或线下的各种场景中，可以基于该电子证件对用户进行身份认证和核验。

[0073] 图1为本说明书披露的一个实施例的实施场景示意图。图1的实施场景可以分为三个阶段：注册阶段，签发阶段，以及认证阶段。

[0074] 注册阶段涉及用户信息的注册和电子证件的生成。该阶段由注册客户端和注册服务端协同完成。注册客户端通常包含线下的机具，具有高度可信的安全策略，与注册服务端协同，可以对用户的身份信息进行全面准确的验证。为了保证电子证件的权威性，注册时要求用户提供全面的信息，包括实体证件的物理信息（例如身份证的卡信息），以及其他身份内容信息，例如证件内容信息作为实名信息，生物特征信息作为实人信息，等等。

[0075] 签发阶段涉及已经生成的电子证件的申领和签发。该阶段通过签发客户端和签发服务端来完成。签发客户端是线上的客户端，与签发服务端协同，实现电子证件的签发。签发后用户就拥有了注册的实体证件对应的电子证件，可用于后续的认证。

[0076] 在实际应用中，注册服务端和签发服务端通常为一个物理实体，只是在逻辑上进行区分。因此，如图1所示，将其合并地标注为注册签发服务端。但是需要理解，在两者之间同步有用户注册信息和电子证件数据的基础上，注册服务端和签发服务端也可以分开部署。

[0077] 在认证阶段，认证客户端与认证服务端协同，实现基于电子证件的身份认证过程。该过程可以为线上场景，也适用于线下场景。

[0078] 在实际应用中，签发客户端与认证客户端通常为一个实体，例如都通过某个可信应用实现，例如支付宝。注册签发服务端和认证服务端可以是一个实体，也可以是不同的实体，例如认证服务端可以是引入的第三方核验源。

[0079] 下面描述以上各个阶段的具体执行方式和执行过程。

[0080] 图2示出根据一个实施例的注册电子证件的过程。

[0081] 首先在步骤S201，用户通过注册客户端申请注册电子证件。

[0082] 上述注册客户端例如是移动终端上安装的App(例如支付宝App)，或者PC机上的应用软件客户端，但是都需要连接有用于读取实体证件的物理标识信息的硬件设备。例如，银行系统或酒店配备有专用PC客户端，且连接有专用机具。这样机具内置安全策略，并且配置有专用的可信读卡器，可以读取用户的实体证件的物理标识信息，比如二代身份证芯片中的DN号。如果注册客户端通过移动终端上安装的App实现，那么则要求该移动终端具有硬件通信功能，例如近场通信功能NFC，并具有对应的控件。

[0083] 然后，在步骤S202，注册客户端采集用户的身份信息。需要采集的身份信息根据注册服务端的核验要求而设置。为了确保电子证件的权威性，一般来说，颁发电子证件时的身份验证是高安全级别的验证，因此需要全面的身份信息，其中需要采集和验证用户实体证件的物理信息，作为实证信息。此外，还可以包含实名信息，和/或实名实人信息。

[0084] 实名信息是用户一系列有关联的身份信息的数字呈现，通常为文本形式。实名信息例如包括，姓名，性别，身份证号，民族，等等。实名信息是较为基础的身份信息。

[0085] 实人信息是用以证明用户本人的信息的数字呈现，通常包含生物特征信息，例如人脸信息，指纹信息，等等。

[0086] 实证信息是用户拥有的实体证件信息的数字呈现，通常包含用户的实体证件的物理标识信息，其中实体证件例如是实体身份证，护照等，实体证件的物理标识信息是证件物理实体本身的标识信息，用于标识和区分实体证件，例如身份证的卡信息，护照的实体信息，更具体的，比如二代身份证芯片中的DN号，新一代护照中的芯片序列号等。

[0087] 可以利用多种方式来采集用户的身份信息。

[0088] 在一个实施例中，在该步骤S202，通过专用机具，读取用户实体证件的物理标识信息，例如，身份证的卡信息(芯片DN号)。在一个例子中，在上述专用机具读取实体证件时，可以一并读取到用户的身份内容信息作为实名信息。身份内容信息是证件上可读可视的信息，例如身份证上显示的用户姓名，身份证号，有效期等等。或者，可以接受用户输入的身份内容信息。另外，还采集用户的生物特征信息作为实人信息，例如利用摄像头采集人脸信

息，或采集指纹信息。可以将这些信息共同作为上述的身份信息。

[0089] 在又一实施例中，通过移动终端的硬件通信功能(例如NFC功能)以及相应的控件，读取用户实体证件的物理标识信息，例如芯片DN号；通过用户手工输入方式采集身份证号、姓名、民族信息等身份内容信息；利用摄像头采集人脸信息。将这些信息共同作为上述的身份信息。

[0090] 在以上的身份信息之外，还获取用户输入的口令信息。

[0091] 然后，在步骤S203，注册客户端将注册信息发送给服务端，其中注册信息包含以上获取的身份信息和口令信息。

[0092] 接着，在步骤S204，注册服务端根据维护的可信信息库，对所述用户的身份信息进行校验。

[0093] 可以理解，注册服务端维护有可信信息库，其中记载有可信的用户身份信息。上述可信信息库例如是公安库中的公民资料等。相应地，注册服务端可以包括上述可信信息库的数据库，或者可以访问上述可信信息库的数据库，从而基于该可信信息库，对当前用户的身份信息进行校验。校验的过程一般包括，将接收到的注册信息中的各个身份信息项，与可信信息库中的对应信息项进行比对。

[0094] 在校验通过的情况下，在步骤S205，为用户生成电子证件，并将所述电子证件与所述用户的注册信息关联存储。

[0095] 在一个实施例中，校验通过之后，注册服务端可以对上述身份信息进行哈希，由此生成电子证件数据。在另一实施例中，每个向注册服务端申请电子证件的申请请求具有一个序列号，注册服务端将该序列号与身份信息进行组合，对组合的结果进行哈希，由此生成电子证件。在一种实施方式中，电子证件的生成还可以基于更多信息项，例如注册的时间信息，签名信息，黑名单信息，等等。

[0096] 在生成电子证件后，注册服务端将电子证件与用户的注册信息关联存储。例如，可以将该用户的用户信息存储为(身份信息，口令信息，电子证件)，其中身份信息包括身份证卡信息，以及其他身份信息，例如实名信息，实名实人信息等。

[0097] 可以理解，在不同实施例中，口令信息可以与身份信息一同作为注册信息，提交到注册服务端，也可以在不同步骤中，与身份信息分别提交到服务端。例如，在一个例子中，注册客户端可以首先将用户的身份信息提供给服务端进行校验，服务端校验通过之后，再要求用户提供口令信息。

[0098] 口令信息的关联存储可以与电子证件的关联同步进行，也可以单独进行。例如，在一个例子中，在服务端对用户的身份信息校验通过之后，可以首先将口令信息与该身份信息绑定，即关联存储，此时注册服务端维护的用户信息可以是(身份信息，口令信息)。然后，注册服务端根据用户的身份信息生成电子证件，并进一步地将该电子证件也绑定到上述用户信息。此时，注册服务端维护的用户信息更新为(身份信息，口令信息，电子证件)。在另一例子中，在注册服务端对用户的身份信息校验通过之后，为该用户生成电子证件，然后将电子证件，口令信息与上述身份信息一并关联存储，例如存储为(身份信息，口令信息，电子证件)。

[0099] 通过以上过程，注册服务端在对用户的身份信息校验之后，生成电子证件。由于该电子证件的生成需要读取用户的实体证件的物理标识信息，因此，确保了电子证件的权威

性和可靠性。

[0100] 接着，描述电子证件的签发过程。

[0101] 图3示出根据一个实施例的签发电子证件的过程示意图。

[0102] 首先，在步骤S301，用户通过签发客户端发出申领指令，请求签发电子证件。

[0103] 在一个实施例中，签发客户端通过可信应用实现，例如用户可以通过支付宝申领电子证件。

[0104] 签发客户端与图2的注册客户端可以是同样的实体，也可以是不同的实体。例如，在一个例子中，用户在银行开户时，通过银行专用客户端注册了电子证件，之后，通过支付宝应用请求签发电子证件。在另一例子中，用户通过第一应用注册了电子证件，之后，通过第二应用请求签发电子证件。

[0105] 接着，可选的，在步骤S302，签发客户端可以对用户进行应用层面的鉴权。例如，在用户使用支付宝请求申领电子证件的情况下，支付宝可以首先对用户进行应用鉴权，判断用户是否具有对应的操作权限。

[0106] 具体地，步骤302可以包括，响应于上述申领指令，向用户发出应用鉴权请求。例如向用户呈现要求用户输入鉴权信息的界面。鉴权信息例如可以是，账户密码，人脸，指纹等等。

[0107] 接着，接收用户输入的鉴权信息，例如用户手工输入账户密码，或者用摄像头拍摄人脸，或者录入指纹，等等。

[0108] 然后，基于用户录入的鉴权信息，对用户的本次操作进行应用鉴权。例如，对比用户本次录入的信息与之前在应用中记录的信息是否相同。如果应用鉴权没有通过，则拒绝用户接入。在一个实施例中，还向用户返回提示信息，例如“不具备访问权限”或者“登录失败”。

[0109] 在鉴权通过的情况下，继续执行后续步骤。

[0110] 接着，在步骤S303，客户端向签发服务端发出签发请求。

[0111] 在一个实施例中，签发请求中包含签发模式信息。签发模式例如包括，采用实体证件的模式(以下称为第一模式)和不采用实体证件的模式(以下称为第二模式)。在其他实施例中，还可以设置更多类型的签发模式，例如实体证件+人脸的模式，实体证件+指纹的模式，等等。下面结合第一模式和第二模式的例子进行描述。

[0112] 在一个实施例中，用户在步骤S301的申领指令中，可以包含对签发模式的选择。例如，在一个具体例子中，用户点击“利用实体身份证申领电子证件”，从而在发出申领指令的同时，选择采用第一模式进行签发；或者点击“输入实名信息申领电子证件”，从而选择采用第二模式进行签发。

[0113] 在另一实施例中，在用户发出申领指令后，签发客户端向用户提供进一步的选项，要求用户对签发模式进行选择。

[0114] 在另一实施例中，签发客户端根据用户终端的硬件配置状况，或者根据默认设置，确定签发模式。

[0115] 以上多种方式确定的签发模式可以包含在签发请求中。

[0116] 此外，签发请求中还可以包含以下多种信息。例如，在一个实施例中，签发请求包含签发客户端对应的应用的应用信息，例如应用信息为支付宝app。在一个实施例中，签发

请求还包括,用户在签发客户端中的用户标识。可选的,签发请求还可以包含时间戳。

[0117] 在一个实施例中,签发请求包含用户终端上与身份信息获取相关的控件的控件版本信息,例如读卡控件的版本,人脸采集控件的版本,文本输入控件的版本,等等。

[0118] 更具体的,在一个例子中,签发请求包含以下信息:

[0119] 应用标识(app=Alipay)、用户标识(userid=hello123)、时间戳(timestamp=20180101001122333)、控件版本(读卡控件版本=1234;人脸控件版本=abcd;文本输入控件版本=xx)、签发模式(mode=1(实体证件参与))。

[0120] 接收到这样的签发请求后,在步骤S304,签发服务端对签发请求进行审批。

[0121] 审批的内容可以包括,用户是否已经注册了电子证件,和/或,是否支持用户以前述的签发模式获取电子证件。

[0122] 例如,如果用户并未注册电子证件,那么审批结果为不通过,拒绝用户接入。

[0123] 在一个实施例中,签发请求中包含签发模式信息和控件版本信息。在这样的情况下,签发服务端可以根据该签发模式信息以及所述控件版本信息,确定签发审批结果。在签发模式信息与控件版本信息不匹配的情况下,审批不通过,拒绝用户接入。上述不匹配的情况包括,例如,签发模式信息指示采用实体证件的模式,但是控件版本信息显示,用户终端没有读卡控件,或者控件版本不足以支持读卡需要。

[0124] 在审批之后,在步骤S305,服务端向客户端返回通知消息。在一个实施例中,通知消息包含审批是否通过的通知。如果审批未通过,则该通知消息指示申请失败,拒绝接入。如果审批通过,则在通知消息中进一步包含为当前签发业务分配的业务流水号。例如,此时的通知消息可以为:申请结果=成功,流水号=123456789。

[0125] 或者,在另一实施例中,在审批未通过的情况下,通知消息中仍然可以包含业务流水号,但是该业务流水号被设置为空号。

[0126] 此外,在一个实施例中,通知消息可以根据签发模式,选择性的包含挑战值。例如,在签发模式为采用实体证件的第一模式的情况下,服务端向客户端返回一个挑战值,包含在上述通知消息中,该挑战值用于后续客户端读取实体证件时使用。在签发模式不涉及实体证件的读取时,通知消息中可以不包含挑战值。

[0127] 或者,在另一实施例中,不管签发模式如何,通知消息中总是包含挑战值,供客户端选择性的使用。

[0128] 在接收到上述通知消息之后,客户端就开始准备申领所需的身份信息。也就是,在步骤S306,获取与签发模式对应的用户身份信息,以及口令信息。

[0129] 下面仍以采用实体证件的第一模式和不采用实体证件的第二模式为例进行描述。

[0130] 如果步骤S303的签发请求中包含的签发模式信息指示第一模式,则意味着需要读取实体证件。如前所述,在该第一模式下,通知消息中包含挑战值。此时,客户端利用该挑战值和读卡控件,获取实体证件的物理标识。在实体证件为带有智能芯片的身份证的情况下,客户端将该挑战值传递给读卡控件,读卡控件进一步地将该挑战值赋予智能芯片。智能芯片利用该挑战值,对芯片DN号等信息进行加密运算,将加密过的物理标识信息返回给读卡控件。读卡控件再利用挑战值对其进行解密,从而获取到芯片DN号。如此,通过挑战值获取到实体证件的物理标识信息。

[0131] 此外,在第一模式下,也可以根据需要进一步获取其他身份信息,例如调用文本输

入控件，接收用户输入的实名信息，采集用户的生物特征信息作为实人信息，等等。

[0132] 如果步骤S303的签发请求中包含的签发模式信息指示第二模式，则不需要读取实体证件。如果通知消息中包含有挑战值，则可以忽略该挑战值。此时，按照第二模式具体设定的信息项，采集用户身份信息。在一个例子中，可以调用文本输入控件，接收用户输入的实名信息。或者，可以直接调用用户之前使用客户端应用时存储的实名信息。这些实名信息可以包括，姓名，性别，身份证号，有效期等等。此外，可以采集用户的生物特征信息作为实人信息，例如利用摄像头采集人脸信息等等。

[0133] 除了获取与签发模式对应的身份信息，还获取用户的口令信息。然后，在步骤S307，签发客户端基于以上身份信息，口令信息和之前的业务流水号，生成下载请求，发送到签发服务端。

[0134] 可以理解，通过业务流水号，签发客户端和签发服务端的多次交互构成一个连续会话。服务端在接收到上述下载请求后，通过其中的业务流水号就可以确定，该下载请求所针对的业务背景上下文。

[0135] 接着，在步骤S308，签发服务端对下载请求中的用户身份信息进行对比校验。

[0136] 如前所述，签发服务端与注册服务端通常为一个物理实体，只是在业务逻辑上进行区分，因此，签发服务端存储并维护有注册阶段的用户注册信息和电子证件。在一种实施方式中，两者也可以分开部署，此时签发服务端可以通过与注册服务端数据同步而存储有用户注册信息和电子证件的数据，或者通过对同一数据库的存取实现数据共享，例如注册服务端将用户注册信息和电子证件的数据存入一个数据库，签发服务端通过访问该数据库获取用户注册信息和电子证件数据。基于此，签发服务端可以将下载请求中的用户身份信息和口令信息，分别与上述预先存储的注册信息中的对应信息进行比对。

[0137] 在比对一致的情况下，在步骤S309，服务端将与注册信息关联存储的电子证件返回给签发客户端。

[0138] 签发客户端可以将获得的电子证件保存在用户终端的安全存储区中，或存储在客户端对应的可信应用中。通常，电子证件可以通过可视化的方式在可信应用中展示，例如公安一所的CTID网证等等。

[0139] 通过以上方式，用户可以通过不同签发模式申领获得注册的电子证件。在获得这样的电子证件的基础上，用户可以进行基于该电子证件的身份认证。

[0140] 接着，描述基于电子证件的认证过程。

[0141] 图4示出根据一个实施例的基于电子证件的身份认证过程示意图。

[0142] 首先，在步骤S401，用户通过认证客户端发出针对某项业务的认证指令，请求基于电子证件进行身份认证。

[0143] 在一个实施例中，认证客户端通过可信应用实现，例如用户可以通过支付宝申请进行身份认证。

[0144] 认证客户端与图3的签发客户端可以是同样的实体，也可以是不同的实体。例如，在一个例子中，用户通过某个应用申领了电子证件，之后，通过支付宝请求基于电子证件进行身份认证。

[0145] 此外，用户发出认证指令所针对的业务，可以是在线业务，也可以线下场景中的业务。在线上业务的情况下，该业务可以是认证客户端本身中的业务，也可以是来自某个业务

应用的业务。

[0146] 以认证客户端是支付宝为例，用户请求认证针对的业务可以支付宝中的业务，也可以是支付宝的子应用中的业务，或者支付宝所支撑的应用(如余额宝、花呗、网商银行等)中的业务，也可以是支付宝之外、但是被允许调用支付宝的认证服务的第三方应用(如滴滴、饿了吗等等)中的业务。

[0147] 接着，可选的，在步骤S402，认证客户端可以对用户进行应用层面的鉴权。例如，在用户使用支付宝请求进行身份认证的情况下，支付宝可以首先对用户进行应用鉴权，判断用户是否具有对应的操作权限。

[0148] 鉴权的过程与图3的步骤S302类似，不再赘述。

[0149] 在鉴权通过的情况下，继续执行后续步骤。

[0150] 接着，在步骤S403，对认证能力和业务要求进行判断。换而言之，判断认证能力是否满足业务要求。一般的，认证能力与电子证件的注册过程和签发过程相关。因此，可以根据电子证件的注册信息项和签发模式，确定电子证件支持的核验参数集合，或称为第一核验参数集合。更具体而言，注册信息项表明了电子证件注册时提供了哪些信息项，签发模式表明用户以何种方式申领获得了该电子证件。这些信息可以例如通过电子证件的属性信息等方式获取。例如，在一个具体例子中，电子证件的注册信息项包含，实体证件的卡信息，姓名，身份证号，以及人脸信息，签发模式为非实体证件参与模式。由于签发时未使用实体证件，第一核验参数集合包括：姓名，身份证号，以及人脸信息。

[0151] 另一方面，获取业务要求核验的第二核验参数集合。

[0152] 在一个实施例中，各种业务预先向认证客户端登记本业务需要验证的身份信息，于是，认证客户端可以通过预先登记的信息确定出发出请求的业务所需核验的信息，即第二核验参数集合。在另一实施例中，业务可以通过步骤301中的认证指令，指示出需要验证的身份信息，于是，认证客户端可以通过上述认证指令，确定出业务所需的第二核验参数集合。

[0153] 认证客户端比对上述第一核验参数集合和第二核验参数集合。如果第二核验参数集合未完全落入第一核验参数集合范围之内，则意味着，存在一些业务需要认证的参数没有落在认证范围之内，认证能力不满足业务要求，此时可以提示用户拒绝认证。例如，某线上业务要求必须进行认证实体证件的信息，即第二核验参数集合包含实体证件信息。然而，电子证件签发时采用的是实体证件不参与的签发模式，因此，第一核验参数集合不包含实体证件信息。在这样的情况下，则认为认证能力不满足业务要求。

[0154] 如果第一核验参数集合包含第二核验参数集合，则意味着，业务需要验证的参数完全落入可认证的参数范围之内，认证能力可以满足业务要求，则继续执行步骤S404，向认证服务端发出认证请求。

[0155] 在一个实施例中，在认证请求中包含认证模式信息。认证模式的设置规则与签发模式的设置规则可以相同，也可以不同。例如，在一个实施例中，将认证模式划分为采用实体证件，以及不采用实体证件的两大类共6种模式，分别是采用实体证件的实名认证/实人认证/实人实名认证，以及不采用实体证件的实名认证/实人认证/实人实名认证。在其他例子中，也可以对认证模式进行其他的划分和设置。

[0156] 在一个实施例中，上述认证模式由用户进行选择；在另一实施例中，上述认证模式

由业务进行设定。

[0157] 此外，认证请求中还可以包含以下多种信息。例如，在一个实施例中，认证请求包含认证客户端对应的应用的应用信息，例如应用信息为支付宝app。在一个实施例中，认证请求还包括，用户在认证客户端中的用户标识。可选的，认证请求还可以包含时间戳。

[0158] 在一个实施例中，认证请求包含用户终端上与身份信息获取相关的控件的控件版本信息，例如读卡控件的版本，人脸采集控件的版本，文本输入控件的版本，等等。

[0159] 接收到这样的认证请求后，在步骤S405，认证服务端对认证请求进行审批。

[0160] 审批的内容例如可以包括，用户是否注册有电子证件，是否支持用户以当前认证模式进行身份认证，等等。

[0161] 例如，如果用户并未注册电子证件，那么审批结果为不通过，拒绝用户接入。

[0162] 在一个实施例中，认证请求中包含认证模式信息和控件版本信息。在这样的情况下，认证服务端可以根据该认证模式信息以及所述控件版本信息，确定审批结果。在认证模式信息与控件版本信息不匹配的情况下，审批不通过，拒绝用户接入。上述不匹配的情况包括，例如，认证模式信息指示采用实体证件的模式，但是控件版本信息显示，用户终端没有读卡控件，或者控件版本不足以支持读卡需要。

[0163] 在审批之后，在步骤S406，认证服务端向认证客户端返回通知消息。在一个实施例中，通知消息包含审批是否通过的通知。如果审批未通过，则该通知消息指示申请失败，拒绝接入。如果审批通过，则在通知消息中进一步包含为当前认证业务分配的业务流水号。例如，此时的通知消息可以为：申请结果＝成功，流水号＝567823456。

[0164] 或者，在另一实施例中，在审批未通过的情况下，通知消息中仍然可以包含业务流水号字段，但是该业务流水号被设置为空号。

[0165] 此外，在一个实施例中，通知消息可以根据认证模式，选择性的包含挑战值。例如，在认证模式为采用实体证件的模式的情况下，服务端向客户端返回一个挑战值，包含在上述通知消息中，该挑战值用于后续客户端读取实体证件时使用。在认证模式不涉及实体证件的读取时，通知消息中可以不包含挑战值。

[0166] 或者，在另一实施例中，不管认证模式如何，通知消息中总是包含挑战值，供客户端选择性的使用。

[0167] 在接收到上述通知消息之后，客户端可以准备认证所需的身份信息。也就是，在步骤S407，获取与认证模式对应的用户身份信息，其中至少包含用户的电子证件。

[0168] 在一个实施例中，步骤S404的认证请求中包含的认证模式信息指示需要读取实体证件，在该模式下，通知消息中包含挑战值。此时，客户端利用该挑战值和读卡控件，获取实体证件的物理标识。该过程与结合图3的步骤S303的描述相同，不再赘述。

[0169] 此外，在该步骤中，需要获取用户申领的电子证件。在一个实施例中，电子证件存储在用户终端中特定的安全存储区。此时，通过访问该安全存储区读取电子证件。在另一实施例中，电子证件由作为认证客户端的当前可信应用(例如支付宝)存储。此时，可信应用可以对应地直接读取电子证件的数据。在又一实施例中，电子证件通过另一可信应用申领签发并存储，也就是，图3所示的签发客户端对应的可信应用，与执行图4的身份认证过程的认证客户端为不同的应用。在电子证件存储在其他应用中的情况下，可以利用API调用该其他应用读取该电子证件。

[0170] 在该步骤中，根据认证模式中认证内容的设定，还可以根据需要进一步获取其他身份信息，例如调用文本输入控件，接收用户输入的实名信息，采集用户的生物特征信息作为实人信息，等等。

[0171] 在一个实施例中，步骤S404的认证请求中包含的认证模式信息指示不采用实体证件。如果通知消息中包含有挑战值，则可以忽略该挑战值。此时，如上所述地获取用户申领的电子证件。此外，根据认证模式具体设定的信息项，采集用户身份信息，例如实名信息，实人信息，实名实人信息。

[0172] 接着，在步骤S408，认证客户端基于以上获取的身份信息，以及之前的业务流水号，生成核验请求数据，发送到认证服务端。

[0173] 在步骤S409，认证服务端对核验请求数据中的用户身份信息进行核验。

[0174] 如前所述，认证服务端与注册/签发服务端可以为一个物理实体，也可以是不同的实体。例如，在一个实施例中，认证服务端为引入的第三方核验源。不管部署为同一实体，或者分开部署，认证服务端存储有可信的用户身份信息，其中包含电子证件信息以及其他身份信息，或者认证服务端至少可以读取上述可信的用户身份信息。因此，认证服务端可以将核验请求中的用户身份信息，与可信的用户身份信息中的对应信息进行比对，从而进行核验。

[0175] 然后，在步骤S410，服务端将核验结果通知给认证客户端。

[0176] 在一个实施例中，需要身份认证的业务是认证客户端本身中的业务。在这样的情况下，认证客户端接收到核验结果后，就可以根据核验结果，推进业务逻辑。在另一实施例中，需要身份认证的业务是来自其他业务应用的业务。在这样的情况下，认证客户端接收到核验结果后，将该核验结果转发到该其他业务应用，使其根据核验结果推进业务逻辑。

[0177] 通过以上方式，基于图2注册、图3签发的电子证件，按照图4的方式进行身份核验。如此，在线上或线下的场景下，都可以基于与实体证件具有相应权威性的电子证件进行身份核验，在保证核验可靠性和权威性的同时，为用户提供极大便利。

[0178] 根据另一方面的实施例，提供一种生成电子证件的装置。图5示出根据一个实施例的电子证件生成装置的示意性框图。该装置部署在注册服务端。如图5所示，该生成装置500包括：

[0179] 注册信息接收单元51，配置为接收用户的注册信息，所述注册信息包括所述用户的身份信息和口令信息，所述用户的身份信息至少包括，实体证件的物理标识信息；

[0180] 校验单元52，配置为根据维护的可信信息库，对所述用户的身份信息进行校验；

[0181] 证件生成单元53，配置为在校验通过的情况下，为所述用户生成电子证件，并将所述电子证件与所述用户的注册信息关联存储。

[0182] 根据一种实施方式，上述实体证件的物理标识信息通过专用机具读取，所述专用机具配置有安全策略；或者，实体证件的物理标识信息通过移动终端的硬件通信功能和相应读卡控件读取。

[0183] 在一个实施例中，用户的身份信息还包括以下中的一项或多项：用户实名信息，生物特征信息。

[0184] 根据另一方面的实施例，还提供一种电子证件的签发装置。图6示出根据一个实施例的签发装置的示意性框图。该装置部署在签发服务端，用于签发前述装置500所生成的电

子证件。如图6所示，签发装置600包括：

[0185] 第一请求接收单元61，配置为接收用户通过签发客户端发起的第一请求，所述第一请求至少包括，签发模式信息；

[0186] 第一消息发送单元62，配置为向签发客户端返回第一消息，所述第一消息至少包括业务流水号；

[0187] 第二请求接收单元63，配置为接收来自签发客户端的第二请求，所述第二请求基于所述业务流水号而生成，并包括与所述签发模式信息指示的签发模式所对应的所述用户的身份信息，以及口令信息；

[0188] 电子证件发送单元64，配置为将所述身份信息和口令信息与预先存储的注册信息中对应信息进行比对，在比对一致的情况下，将与所述注册信息关联存储的电子证件返回给所述签发客户端。

[0189] 在一个实施例中，第一请求接收单元61所接收的第一请求还包括，用户的用户终端上与身份信息获取相关的控件的控件版本信息。

[0190] 根据一种实施方式，装置600还包括审批单元(未示出)，配置为根据所述签发模式信息以及所述控件版本信息，确定对第一请求的审批结果；在所述审批结果为审批不通过的情况下，向签发客户端返回拒绝通知；和/或，将所述业务流水号设定为空号。

[0191] 在一个实施例中，上述签发模式信息指示采用实体证件的第一模式，所述第一消息还包括挑战值；在这样的情况下，第二请求接收单元63所接收的用户的身份信息包括，所述用户的用户终端利用所述挑战值读取的实体证件的物理标识信息。

[0192] 在另一实施例中，上述签发模式信息指示不采用实体证件的第二模式，第二请求接收单元63所接收的用户的身份信息还包括以下中的一项或多项：用户实名信息，生物特征信息。

[0193] 根据另一方面的实施例，还提供一种电子证件的申领装置。图7示出根据一个实施例的申领装置的示意性框图。该申领装置部署在签发客户端，用于申领前述装置500生成的电子证件。如图7所示，申领装置700包括：

[0194] 第一请求发送单元71，配置为响应于用户的申领操作指令，向签发服务端发出第一请求，所述第一请求至少包括签发模式信息；

[0195] 第一消息接收单元72，配置为接收返回的第一消息，所述第一消息至少包括业务流水号；

[0196] 身份信息获取单元73，配置为获取与所述签发模式信息指示的签发模式所对应的所述用户的身份信息，以及口令信息；

[0197] 第二请求发送单元74，配置为至少基于所述业务流水号，所述用户的身份信息，以及口令信息生成第二请求，将该第二请求发送到所述签发服务端；

[0198] 电子证件接收单元75，配置为从签发服务端接收电子证件。

[0199] 在一个实施例中，上述申领操作指令包括对签发模式的选择指令；相应地，第一请求发送单元71根据所述选择指令确定签发模式信息，将所述签发模式信息包含在所述第一请求中。

[0200] 根据一种实施方式，第一请求发送单元71发送的第一请求还包括，所述用户的用户终端上与身份信息获取相关的控件的控件版本信息。

[0201] 在一个实施例中，装置700还包括鉴权单元(未示出)，配置为响应于所述申领操作指令，向所述用户发出所述签发客户端的应用鉴权请求；接收用户输入的鉴权信息；基于所述鉴权信息进行应用鉴权。

[0202] 在一个实施例中，所述签发模式信息指示采用实体证件的第一模式，所述第一消息还包括挑战值；在这样的情况下，身份信息获取单元73具体配置为，获取用户终端利用所述挑战值读取的实体证件的物理标识信息。

[0203] 在另一实施例中，所述签发模式信息指示不采用实体证件的第二模式，身份信息获取单元73具体配置为：接收用户输入的用户实名信息；和/或，通过用户终端采集所述用户的生物特征信息。

[0204] 根据又一方面的实施例，还提供一种基于电子证件的用户身份认证装置。图8示出根据一个实施例的认证装置的示意性框图。该装置部署在认证服务端，用于实现基于电子证件的用户身份认证，其中电子证件通过前述装置500而生成。如图8所示，认证装置800包括：

[0205] 认证请求接收单元81，配置为接收用户通过认证客户端发起的认证请求，所述认证请求至少包括认证模式信息；

[0206] 结果消息发送单元82，配置为向所述认证客户端返回请求结果消息，所述请求结果消息包括，业务流水号；

[0207] 核验数据接收单元83，配置为接收来自所述认证客户端的核验数据，所述核验数据基于所述业务流水号而生成，并包括与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

[0208] 认证结果发送单元84，配置为对所述核验数据进行校验，并向所述认证客户端返回认证结果。

[0209] 在一个实施例中，认证请求接收单元81所接收的认证请求还包括，用户的用户终端上与身份信息获取相关的控件的控件版本信息。

[0210] 根据一个实施例，装置800还包括审批单元(未示出)，配置为，根据所述认证模式信息以及所述控件版本信息，确定对所述认证请求的审批结果；在所述审批结果为审批不通过的情况下，向所述认证客户端返回拒绝通知；和/或，将所述业务流水号设定为空号。

[0211] 在一个实施例中，认证模式信息指示采用实体证件的第一模式，所述请求结果消息还包括挑战值；在这样的情况下，核验数据接收单元83接收到的用户的身份信息还包括，所述用户的用户终端利用所述挑战值读取的实体证件的物理标识信息。

[0212] 在一个实施例中，认证模式信息指示不采用实体证件的第二模式，核验数据接收单元83接收到的用户的身份信息还包括以下中的一项或多项：用户实名信息，生物特征信息。

[0213] 根据另一方面的实施例，还提供一种基于电子证件的用户身份认证装置，部署在认证客户端。图9示出根据一个实施例的认证装置的示意性框图。该装置用于实现基于电子证件的身份认证，其中所述电子证件通过前述装置500而生成。如图9所示，该认证装置900包括：

[0214] 认证请求发送单元91，配置为响应于用户针对业务的认证指令，向认证服务端发出认证请求，所述认证请求至少包括，认证模式信息；

[0215] 结果消息接收单元92，配置为接收返回的请求结果消息，所述请求结果消息至少包括业务流水号；

[0216] 身份信息获取单元93，配置为获取与所述认证模式信息指示的认证模式所对应的所述用户的身份信息，所述用户的身份信息至少包括所述电子证件的信息；

[0217] 核验数据发送单元94，配置为基于所述业务流水号，所述用户的身份信息生成核验数据，将该核验数据发送到所述认证服务端；

[0218] 认证结果接收单元95，配置为从认证服务端接收认证结果。

[0219] 根据一种实施方式，装置900还包括获取单元(未示出)，配置为根据所述电子证件的注册信息项和签发模式，确定所述电子证件支持的第一核验参数集合；以及获取所述业务要求核验的第二核验参数集合；相应地，认证请求发送单元91配置为，在所述第一核验参数集合包含所述第二核验参数集合的情况下，向认证服务端发出所述认证请求。

[0220] 在一个实施例中，认证模式信息指示采用实体证件的第一模式，所述请求结果消息还包括挑战值；在这样的情况下，身份信息获取单元93读取所述电子证件；以及获取用户终端利用所述挑战值读取的实体证件的物理标识信息。

[0221] 在一个实施例中，身份信息获取单元93配置为，接收用户输入的用户实名信息；和/或，通过用户终端采集所述用户的生物特征信息。

[0222] 根据另一方面的实施例，还提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行结合图2到图4所描述的方法。

[0223] 根据再一方面的实施例，还提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现结合图2到图4所述的方法。

[0224] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

[0225] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

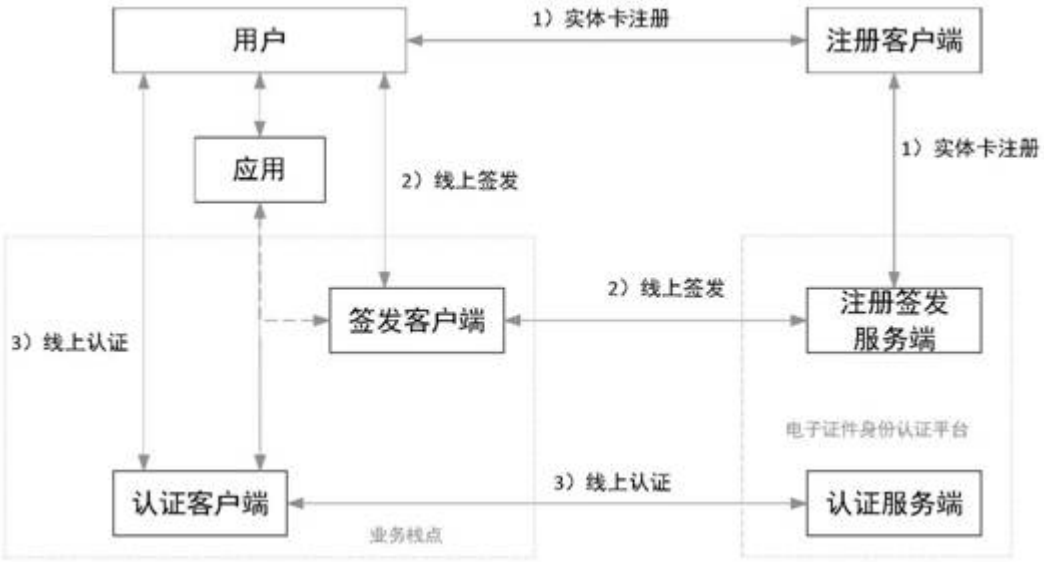

用户
1）实体卡注册
注册客户端
应用
2）线上签发
1）实体卡注册
2）线上签发
3）线上认证
签发客户端
注册签发
服务端
电子证件身份认证平台
3）线上认证
认证客户端
认证服务端
业务线点

图1

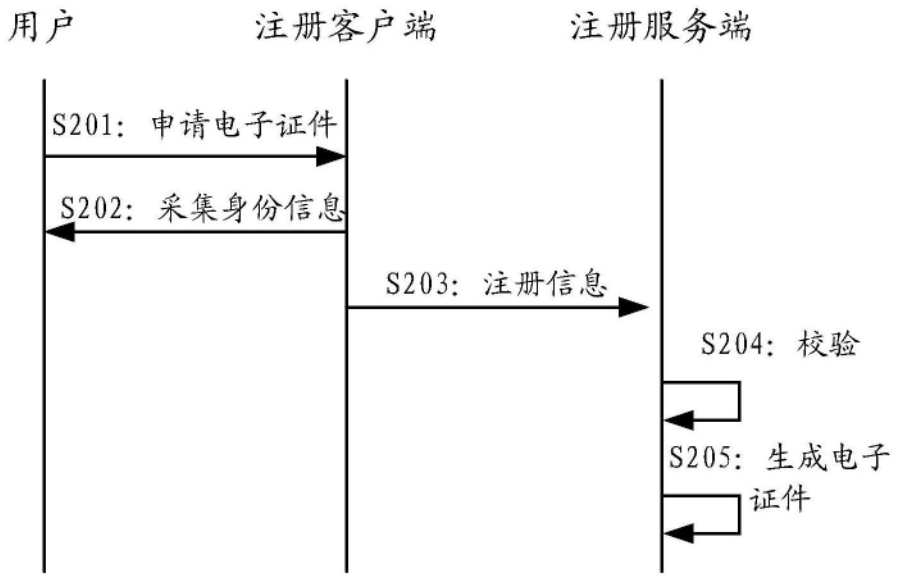

用户
注册客户端
注册服务端
S201：申请电子证件
S202：采集身份信息
S203：注册信息
S204：校验
S205：生成电子
证件

图2

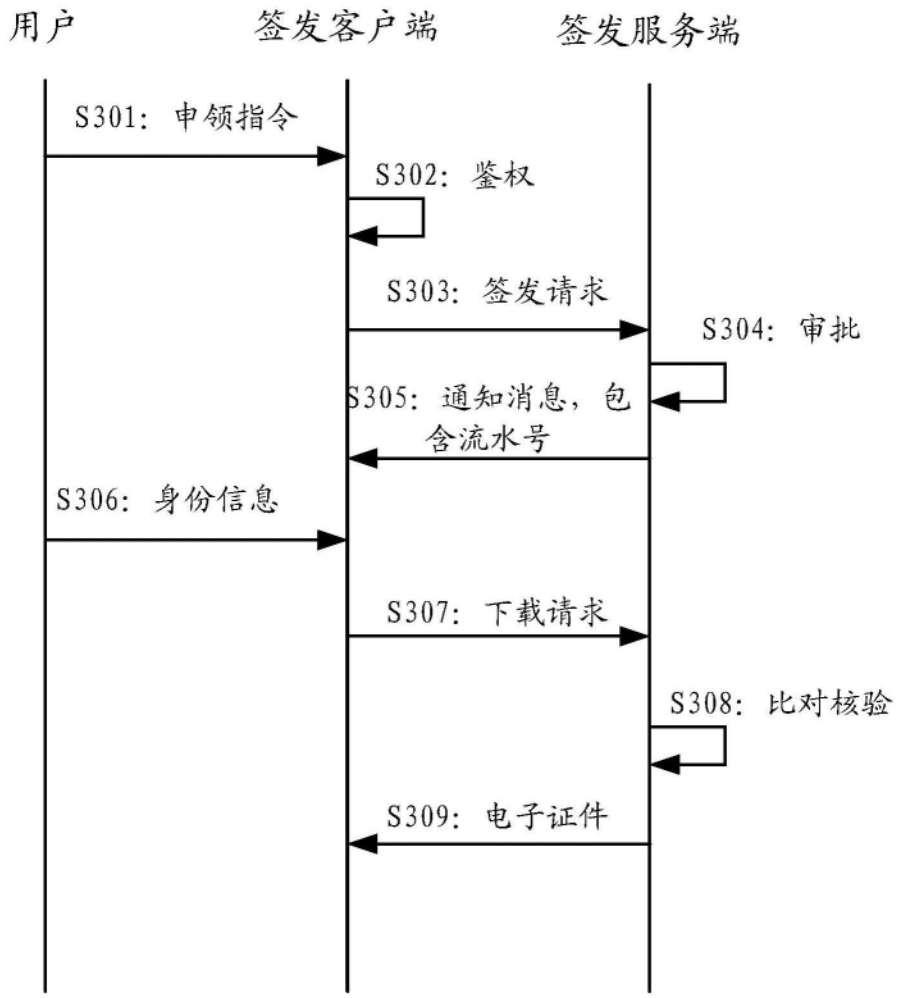

用户
签发客户端
签发服务端
S301：申领指令
S302：鉴权
S303：签发请求
S304：审批
S305：通知消息，包含流水号
S306：身份信息
S307：下载请求
S308：比对核验
S309：电子证件

图3

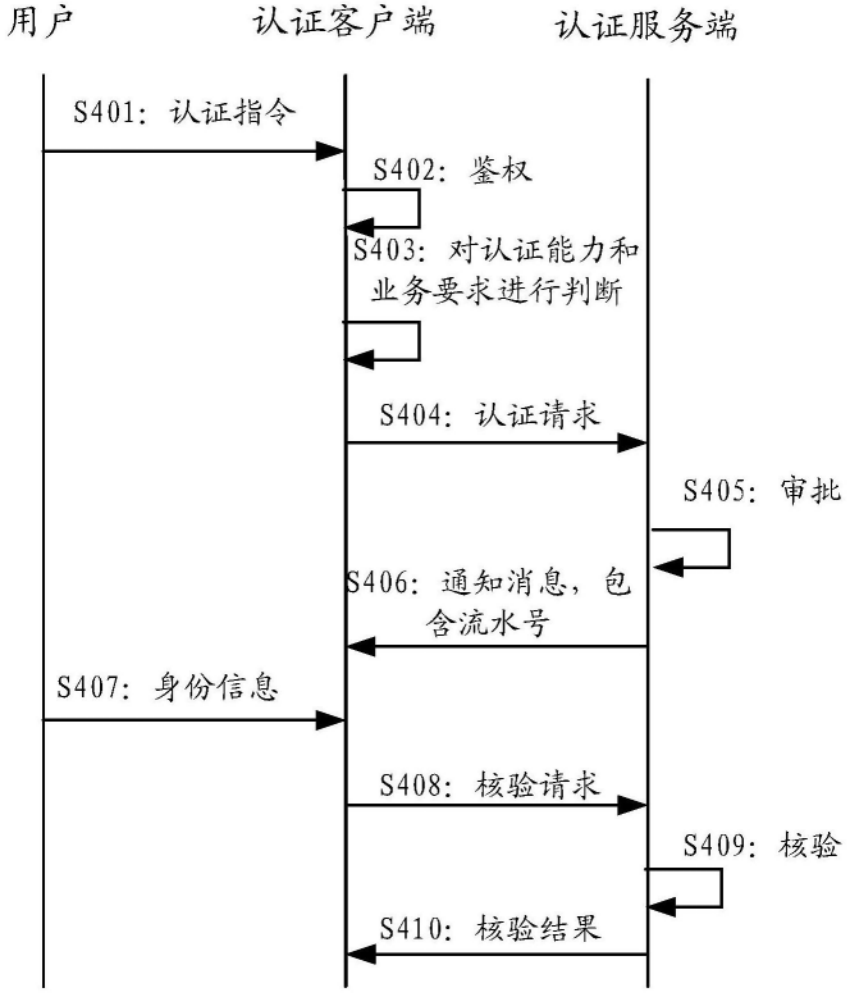

用户
认证客户端
认证服务端
S401：认证指令
S402：鉴权
S403：对认证能力和业务要求进行判断
S404：认证请求
S405：审批
S406：通知消息，包含流水号
S407：身份信息
S408：核验请求
S409：核验
S410：核验结果

图4

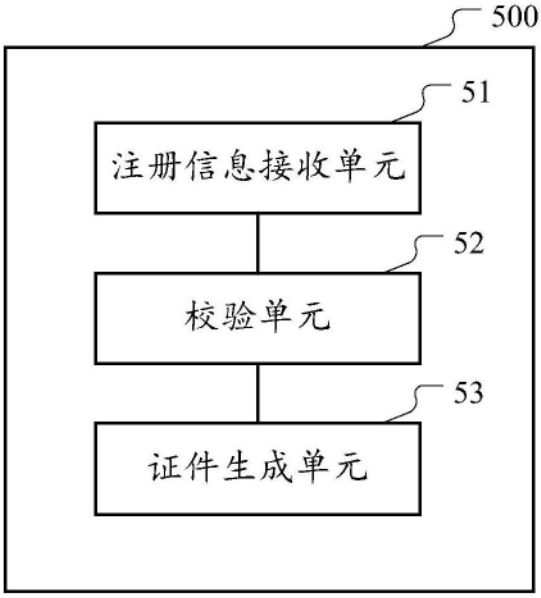

500
51
注册信息接收单元
52
校验单元
53
证件生成单元

图5

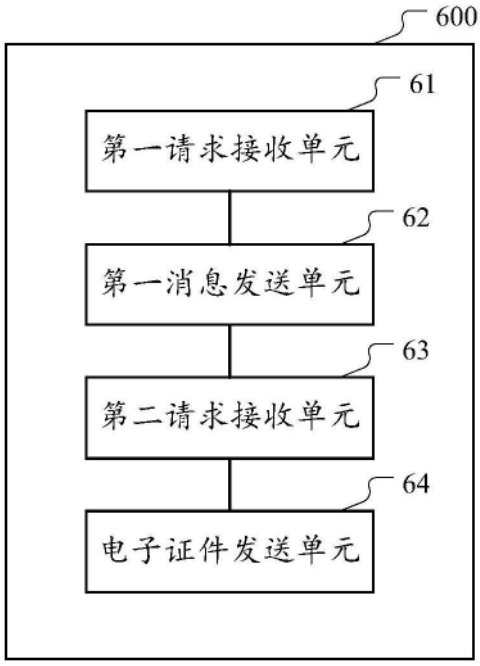

600
61
第一请求接收单元
62
第一消息发送单元
63
第二请求接收单元
64
电子证件发送单元

图6

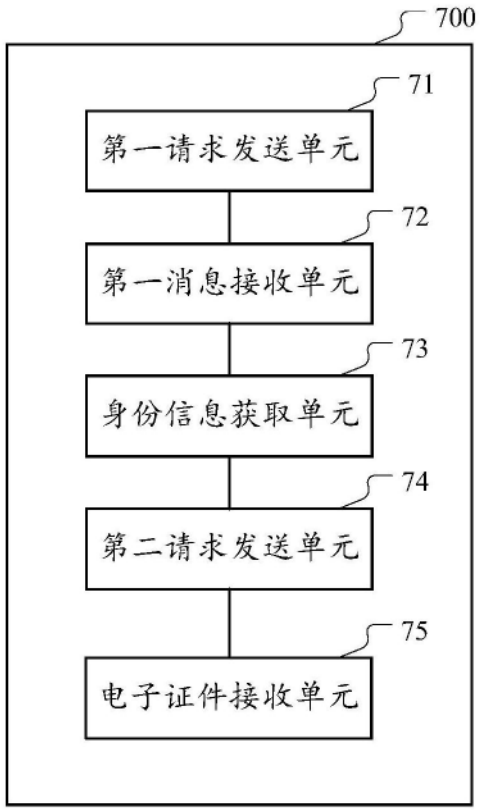

700
71
第一请求发送单元
72
第一消息接收单元
73
身份信息获取单元
74
第二请求发送单元
75
电子证件接收单元

图7

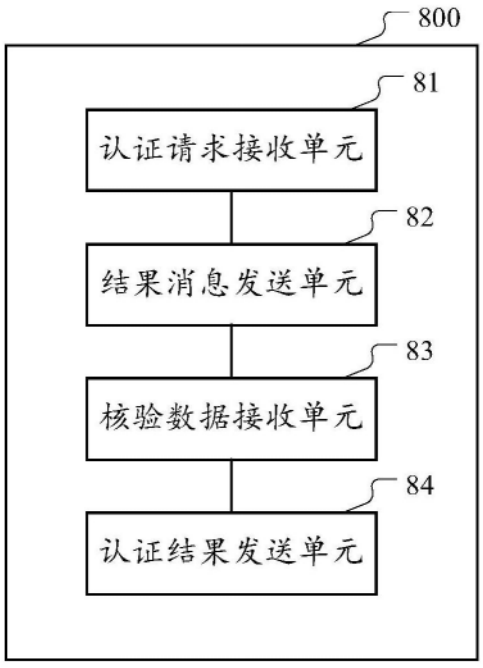

800
81
认证请求接收单元
82
结果消息发送单元
83
核验数据接收单元
84
认证结果发送单元

图8

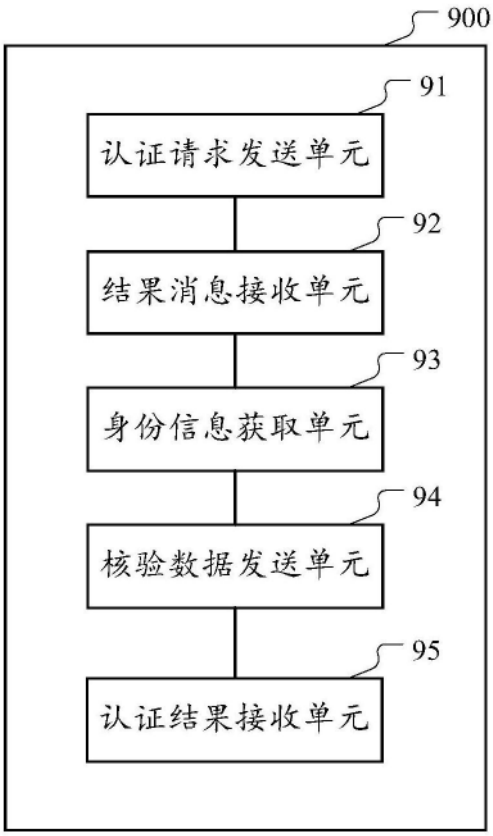

900
91
认证请求发送单元
92
结果消息接收单元
93
身份信息获取单元
94
核验数据发送单元
95
认证结果接收单元

图9