(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 110545274 A
(43)申请公布日 2019.12.06

(21)申请号 201910811610.2

(22)申请日 2019.08.30

(71)申请人 南瑞集团有限公司
地址 211100 江苏省南京市鼓楼南瑞路8号
申请人 南京南瑞信息通信科技有限公司
国网浙江省电力有限公司
国网浙江省电力有限公司温州供电公司
国家电网有限公司

(72)发明人 徐睿 杨华飞 郑立 刘坤 马锋 陈梦娴 蔡怡挺 朱犇 王佑 曹国强 游佳 张子谦

(74)专利代理机构 南京纵横知识产权代理有限公司 32224
代理人 丁朋华

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

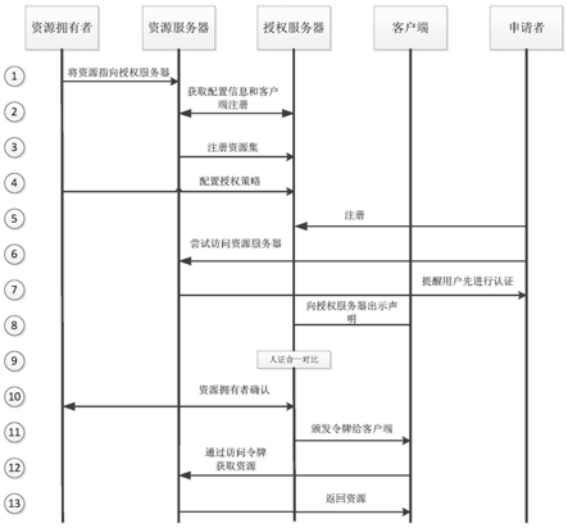
权利要求书2页 说明书9页 附图3页

(54)发明名称

一种基于人证合一的UMA服务的方法、装置和系统

(57)摘要

本发明公开了一种基于人证合一的UMA服务的方法、装置和系统，当资源申请者访问资源时，授权服务器根据资源申请者上传的头像照片，通过人证合一比对判断是否为注册用户本人，如果是，再根据资源授权策略获得申请者提供的访问证明，判断访问证明是否符合要求，如果符合要求，则表示已授权，如果不是注册用户本人或者访问证明不符合要求则未授权；授权服务器使用私钥签发包括授权结果的访问令牌给资源申请者的客户端；所述访问令牌用于提供给资源服务器通过公钥验签，如通过验签且已经授权，则资源被发送给资源申请者。本发明确保用户是合法用户并且一定是注册用户本人，不容易伪造和篡改，有效地保证了授权的安全性。



CN 110545274 A

1.一种基于人证合一的UMA服务的方法,其特征在于:包括步骤:

提供UMA服务的授权服务器接受资源服务器的注册,为资源服务器分配资源服务器ID号以及对应的公钥;

授权服务器接受资源服务器为其资源的注册,为资源分配唯一的资源标识符,所述资源被资源拥有者通过授权服务器配置授权策略;

当资源申请者访问资源时,授权服务器根据资源申请者上传的头像照片和预先存储的用户注册信息,通过人证合一比对判断是否为注册用户本人,如果是,再根据资源授权策略获得申请者提供的访问证明,判断访问证明是否符合要求,如果符合要求,则表示已授权,如果不是注册用户本人或者访问证明不符合要求则未授权;授权服务器使用私钥签发包括授权结果的访问令牌给资源申请者的客户端;所述访问令牌用于提供给资源服务器通过公钥验签,如通过验签且已经授权,并且资源访问次数正确,则资源被发送给资源申请者。

2.根据权利要求1所述的一种基于人证合一的UMA服务的方法,其特征是:所述用户注册信息包括传统注册信息和注册身份证件照;所述传统注册信息包括用户名、密码、性别,籍贯、联系方式;所述注册身份证件照为通过摄像头采集的身份证件照,核验身份证件照是否真实有效,如果身份证是真实有效的,则授权服务器加密保存传统用户信息、身份证件照,关联传统用户信息和身份证件照。

3.根据权利要求2所述的一种基于人证合一的UMA服务的方法,其特征是:所述核验身份证件照是否真实有效,具体步骤包括:

提供UMA服务的授权服务器接收用户使用摄像头拍摄的身份证件照;

授权服务器解析身份证件照,将姓名、身份证号码、头像数据发送给公安部数据库,查询身份证真伪,公安部数据库返回验证结果;

如果身份证验证成功则授权服务器将身份证件照保留到数据库中,如果身份证验证失败,则提示用户身份证验证失败并且删除身份证件照。

4.根据权利要求1所述的一种基于人证合一的UMA服务的方法,其特征是:所述通过人证合一比对判断是否为注册用户本人,具体为:

1)授权服务器接收用户头像照片;

2)提取用户头像特征值,获取数据库存放的身份证件上的头像特征值,对比两个特征值相似度,当相似度到达一定阈值即认为人和证为同一人。

5.根据权利要求1所述的一种基于人证合一的UMA服务的方法,其特征是:所述访问令牌包括用户信息和签名信息,用户信息包括用户ID、请求的资源标识符、资源操作权限、资源访问次数、以及用户是否已经授权,签名信息为对用户信息进行加密产生的数据。

6.一种基于人证合一的UMA服务的授权服务器,其特征在于:包括:

资源服务器注册模块,用于接受资源服务器的注册,为资源服务器分配资源服务器ID号以及对应的公钥;

资源注册模块,用于接受资源服务器为其资源的注册,为资源分配唯一的资源标识符,所述资源被资源拥有者通过授权服务器配置授权策略;

人证合一核验及获取资源模块,用于当资源申请者访问资源时,根据资源申请者上传的头像照片和预先存储的用户注册信息,通过人证合一比对判断是否为注册用户本人,如果是,再根据资源授权策略获得申请者提供的访问证明,判断访问证明是否符合要求,如果

符合要求，则表示已授权，如果不是注册用户本人或者访问证明不符合要求则未授权；授权服务器使用私钥签发包括授权结果的访问令牌给资源申请者的客户端；所述访问令牌用于提供给资源服务器通过公钥验签，如通过验签且已经授权，并且资源访问次数正确，则资源被发送给资源申请者。

7.根据权利要求6所述的一种基于人证合一的UMA服务的授权服务器，其特征在于：所述通过人证合一比对判断是否为注册用户本人，具体为：

1)授权服务器接收用户头像照片；

2)提取用户头像特征值，获取数据库存放的身份证件上的头像特征值，对比两个特征值相似度，当相似度到达一定阈值即认为人和证为同一人。

8.一种基于人证合一的 UMA服务的系统，其特征是：包括资源服务器、根据权利要求6或7 所述的授权服务器和终端设备；

所述资源服务器用于保存资源拥有者上传的资源；

所述授权服务器用于提供符合UMA协议要求的服务，用于用户注册、用户核验、资源服务器及其资源的注册、访问令牌的生成；

所述终端设备用于身份证件照和人脸头像的采集以及接收UMA服务推送信息。

9.根据权利要求8所述的一种基于人证合一的 UMA服务的系统，其特征是：所述资源包括文档等可见资源或者授权凭证。

10.根据权利要求8所述的一种基于人证合一的 UMA服务的系统，其特征是：所述终端与授权服务器通过HTTPS进行安全通信。

一种基于人证合一的UMA服务的方法、装置和系统

技术领域

[0001] 本发明涉及互联网和移动通信技术领域，具体涉及一种基于人证合一的UMA服务的方法、装置和系统。

背景技术

[0002] OAuth是一个安全协议，用于保护全球范围内大量且在不断增长的 Web API。OAuth 是一个委托协议，提供跨系统授权的方案，用可用性和安全性更高的委托协议取代了密码共享反模式。它用于连接不同的网站，还支持原生应用和移动应用与云服务之间的连接。它是各领域标准协议中的安全层，覆盖了从医疗到身份管理，从能源到社交网络的广阔应用领域。OAuth 已成为当今 Web 上占主导地位的安全手段。OAuth不是身份认证框架，但是可以加入身份认证使OAuth更加安全。

[0003] UMA(User Managed Access)是一个基于 OAuth 2.0 构建的协议，它让资源拥有者能够利用授权服务器对其资源的访问进行更丰富的控制。访问资源的客户端可能是受资源拥有者控制的，也可能是受其他用户控制的。UMA 协议基于 OAuth 2.0 构建的主要功能：用户对用户的授权。

[0004] 人脸识别是基于人的面部特征信息进行身份识别的一种生物识别技术，主要工作就是对人脸图像进行预处理然后提取特征值，然后通过特征值比对确认身份。该技术目前已经很成熟，应用广泛。

[0005] 身份证件OCR识别技术，OCR(Optical Character Recognition，光学字符识别)是指通过检测暗、亮的模式确定其形状，然后用字符识别方法将形状翻译成计算机文字的过程。可以利用该技术提取身份证件上的姓名，身份证号，头像图片等信息。

[0006] 专利申请号：201510493553.X，公开了一种基于生物识别的OAuth服务，包括步骤：用户在 OAuth 的系统服务平台注册；

系统服务平台向外部开放OAuth 服务；用户访问第三方应用，选择通过 OAuth 系统服务平台进行授权；OAuth 系统服务平台确定提供授权的目标智能终端；OAuth 系统服务平台将用户的授权请求路由到目标智能终端；用户在智能终端上选择是否同意授权，如同意，则在智能终端采集生物识别信息，如选择拒绝或不做任何操作则为拒绝授权；系统根据采集和识别的结果，判断是否为注册用户的生物识别信息，系统服务平台获取用户的识别结果或拒绝授权的操作后，指示第三方应用对应的平台授权结果。

[0007] 在上述专利中的授权业务流程中，存在以下几个缺点：

(1)无法对其他用户授权

只能通过系统服务平台对第三方应用授权，而且资源的拥有者只能是用户自己，当我们需要访问的资源需要其他用户授权时，该方案无法满足要求。

[0008] (2)对智能终端安全防护能力要求高

由于生物识别和对比都是在智能终端上进行，因此智能终端的对生物特征数据的存储和传输有安全需求，而目前市场上市场份额较高的是Android智能终端，大多数Android智

能终端安全防护能力并不高,而且很容易被root和安装恶意应用。

[0009] (3)无法确认用户的合法身份

只能保证注册和使用为同一用户,但是此用户是否为合法用户无法保证,在很多使用场景中,需要判断用户是否为合法用户,例如酒店,学校,银行,公司等。

发明内容

[0010] 为解决现有技术中的不足,本发明提供一种基于人证合一的UMA服务的方法、装置和系统,解决了现有的基于生物识别的OAuth 服务的方法不能核实注册者真实身份、无法对其他用户授权、对智能终端的安全防护能力要求高的问题,适用范围更广。

[0011] 为了实现上述目标,本发明采用如下技术方案:一种基于人证合一的UMA服务的方法,其特征在于:包括步骤:

提供UMA服务的授权服务器接受资源服务器的注册,为资源服务器分配资源服务器ID号以及对应的公钥;

授权服务器接受资源服务器为其资源的注册,为资源分配唯一的资源标识符,所述资源被资源拥有者通过授权服务器配置授权策略;

当资源申请者访问资源时,授权服务器根据资源申请者上传的头像照片和预先存储的用户注册信息,通过人证合一比对判断是否为注册用户本人,如果是,再根据资源授权策略获得申请者提供的访问证明,判断访问证明是否符合要求,如果符合要求,则表示已授权,如果不是注册用户本人或者访问证明不符合要求则未授权;授权服务器使用私钥签发包括授权结果的访问令牌给资源申请者的客户端;所述访问令牌用于提供给资源服务器通过公钥验签,如通过验签且已经授权,并且资源访问次数正确,则资源被发送给资源申请者。

[0012] 前述的一种基于人证合一的UMA服务的方法,其特征是:所述用户注册信息包括传统注册信息和注册身份证件照;所述传统注册信息包括用户名、密码、性别,籍贯、联系方式;所述注册身份证件照为通过摄像头采集的身份证件照,核验身份证件照是否真实有效,如果身份证是真实有效的,则授权服务器加密保存传统用户信息、身份证件照,关联传统用户信息和身份证件照。

[0013] 前述的一种基于人证合一的UMA服务的方法,其特征是:所述核验身份证件照是否真实有效,具体步骤包括:

1)提供UMA服务的授权服务器接收用户使用摄像头拍摄的身份证件照;

2)授权服务器解析身份证件照,将姓名、身份证号码、头像数据发送给公安部数据库,查询身份证真伪,公安部数据库返回验证结果;

3)如果身份证验证成功则授权服务器将身份证件照保留到数据库中,如果身份证验证失败,则提示用户身份证验证失败并且删除身份证件照。

[0014] 前述的一种基于人证合一的UMA服务的方法,其特征是:所述通过人证合一比对判断是否为注册用户本人,具体为:

1)授权服务器接收用户头像照片;

2)提取用户头像特征值,获取数据库存放的身份证件上的头像特征值,对比两个特征值相似度,当相似度到达一定阈值即认为人和证为同一人。

[0015] 前述的一种基于人证合一的UMA服务的方法,其特征是:所述访问令牌包括用户信

息和签名信息，用户信息包括用户ID、请求的资源标识符、资源操作权限、资源访问次数、以及用户是否已经授权，签名信息为对用户信息进行加密产生的数据。

[0016] 一种基于人证合一的UMA服务的授权服务器，其特征在于：包括：

资源服务器注册模块，用于接受资源服务器的注册，为资源服务器分配资源服务器ID号以及对应的公钥；

资源注册模块，用于接受资源服务器为其资源的注册，为资源分配唯一的资源标识符，所述资源被资源拥有者通过授权服务器配置授权策略；

人证合一核验及获取资源模块，用于当资源申请者访问资源时，根据资源申请者上传的头像照片和预先存储的用户注册信息，通过人证合一比对判断是否为注册用户本人，如果是，再根据资源授权策略获得申请者提供的访问证明，判断访问证明是否符合要求，如果符合要求，则表示已授权，如果不是注册用户本人或者访问证明不符合要求则未授权；授权服务器使用私钥签发包括授权结果的访问令牌给资源申请者的客户端；所述访问令牌用于提供给资源服务器通过公钥验签，如通过验签且已经授权，并且资源访问次数正确，则资源被发送给资源申请者。

[0017] 前述的一种基于人证合一的UMA服务的授权服务器，其特征在于：所述通过人证合一比对判断是否为注册用户本人，具体为：

1)授权服务器接收用户头像照片；

2)提取用户头像特征值，获取数据库存放的身份证件上的头像特征值，对比两个特征值相似度，当相似度到达一定阈值即认为人和证为同一人。

[0018] 一种基于人证合一的 UMA服务的系统，其特征是：包括资源服务器、根据前述的授权服务器和终端设备；

所述资源服务器用于保存资源拥有者上传的资源；

所述授权服务器用于提供符合UMA协议要求的服务，用于用户注册、用户核验、资源服务器及其资源的注册、访问令牌的生成；

所述终端设备用于身份证件照和人脸头像的采集以及接收UMA服务推送信息。

[0019] 前述的一种基于人证合一的 UMA服务的系统，其特征是：所述资源包括文档等可见资源或者授权凭证。

[0020] 前述的一种基于人证合一的 UMA服务的系统，其特征是：所述终端与授权服务器通过HTTPS进行安全通信。

[0021] 本发明所达到的有益效果：本发明利用身份证件核实注册人员的真实身份，然后利用人脸识别与OCR技术确认人和证件为同一人，并且利用COTS设备获取身份证件照和人脸头像照片，在不增加硬件成本的情况下提高授权服务的安全性和便捷性；本发明对COTS设备要求很低，唯一要求是具备前置摄像头，目前市场上智能终端的前置摄像头为标配，提高了授权设备的适用范围；本发明除了应用于用户对第三方应用授权，也应用于用户对其他用户授权，使用场景更加广泛。

[0022] 通过人证合一，确保用户是合法用户并且一定是注册用户本人，而授权凭证为通过人证比对确认后授权服务器生成的一种带签名信息的访问令牌，此访问令牌并不包含用户的身份信息，资源服务器通过在向授权服务器注册时获得的公钥验证签名信息保证访问令牌的合法性，进一步能证明用户已经获得授权。这种带签名信息的令牌不容易伪造和篡

改,有效地保证了授权的安全性。

附图说明

[0023] 图1是本发明实施例中的一种基于人证合一的 UMA服务的方法流程图;

图2是本发明实施例中的一种用户注册流程图;

图3是本发明实施例中的一种身份证件照核验流程图;

图4是本发明实施例中的一种人证合一比对流程图;。

具体实施方式

[0024] 下面结合附图对本发明作进一步描述。以下实施例仅用于更加清楚地说明本发明的技术方案,而不能以此来限制本发明的保护范围。

[0025] 实施例1:

一种基于人证合一的 UMA服务的系统,包括资源服务器、授权服务器和终端设备;

资源服务器用于保存资源拥有者上传的资源,所述资源包括文档等可见资源或者授权凭证;

授权服务器提供符合UMA协议要求的服务,用于用户注册、用户核验、资源服务器及其资源的注册、访问令牌的生成。

[0026] 终端设备为COTS设备(Commercial Off-The-Shelf,商用现成品或技术,指可以采购到的具有开放式标准定义的接口的软件或硬件产品,可以节省成本和时间,例如手机或者平板电脑就是一种COTS设备),终端设备上运行APP,用于身份证件照和人脸头像的采集以及接收UMA服务推送信息(当用户访问某个资源需要资源拥有者确认时,发送推送信息到APP提醒资源拥有者确认),终端与授权服务器通过HTTPS进行安全通信。

[0027] UMA服务服务的对象为资源服务器、资源拥有者、客户端、资源申请者。资源申请者和资源拥有者可以为同一人,若为不同人,相当于实现用户对其他用户的授权。资源拥有者通过设置一些授权策略允许其他用户和第三方客户端访问资源。资源申请者、客户端可以通过向授权服务器出示申请者信息或客户端信息,只要这些信息满足资源拥有者的授权策略要求就可以获取相关资源。

[0028] 实施例2:

一种基于人证合一的UMA服务的方法,包括如下步骤:

步骤1,在提供UMA服务的授权服务器上进行传统信息注册和身份证件照注册,授权服务器加密保存用户注册信息;

传统信息注册,传统信息注册包括用户名/密码,性别,籍贯,联系方式等,同时为用户自动生成唯一的用户ID(身份标识号)号,用户名和密码可以作为UMA服务的登陆凭证也可以作为低安全等级要求的用户认证信息;

身份证件照注册,通过COTS设备摄像头采集身份证件照,核验身份证件照是否真实有效,主要核查身份证姓名和号码是否一致以及身份证头像真伪;如果确认身份证是真实有效的,则授权服务器加密保存传统用户信息、身份证件照,关联传统用户信息和身份证件照;若身份证件照无效,则提示身份证验证失败,可以选择重新拍摄身份证件照。

[0029] 所述核验身份证件照是否真实有效,具体步骤包括:

4)提供UMA服务的授权服务器接收用户使用摄像头拍摄的身份证件照;用户需判断身份证件照是否清晰,如不清晰需要重新拍摄;

5)授权服务器(需获得公安部授权)解析身份证件照,将姓名、身份证号码、头像数据发送给公安部数据库,查询身份证真伪,公安部数据库返回验证结果;

6)如果身份证验证成功则授权服务器将身份证件照保留到数据库中,如果身份证验证失败,则提示用户身份证验证失败并且删除身份证件照,用户可以选择重新拍摄身份证件照。

[0030] 步骤2,授权服务器接受资源服务器的注册,为资源服务器分配资源服务器ID号以及对应的公钥(此公钥可以验签访问令牌)。

[0031] 步骤3,授权服务器接受资源服务器为其资源的注册,为资源分配唯一的资源标识符,所述资源被资源拥有者通过授权服务器配置授权策略;

不同的资源可以配置不同的授权策略。资源申请者和他们的客户端(浏览器/原生应用)需要提供能够满足授权策略要求的访问证明。例如,授权策略要求使用绑定的终端,那么终端的MAC地址即作为其中一个访问证明。如果资源未配置授权策略,该资源被视为不可访问。

[0032] 所述授权策略包括但不限于以下内容:

1)人证合一核验后,是否需要资源拥有者再次确认以及确认方式(账户密码或人脸识别等);

2)是否绑定授权终端,即采集人脸照片的终端是否绑定特定的终端还是任何终端皆可;

3)资源可访问的日期范围;

4)限定特定的用户访问;

5)资源可被访问的次数限制;

步骤4,当资源申请者需要访问资源时,授权服务器根据资源申请者上传的头像照片,通过人证合一比对判断是否为注册用户本人,如果是,则根据资源授权策略获得申请者提供的访问证明,判断访问证明是否符合要求,如果符合要求,则表示已授权,如果不是注册用户本人或者访问证明不符合要求则未授权;授权服务器使用私钥签发包括授权结果的访问令牌给资源申请者的客户端;所述访问令牌用于提供给资源服务器,资源服务器通过公钥验签访问令牌,判断访问令牌签名是否正确,如果访问令牌通过验签,则判断该用户是否已经授权以及资源访问次数是否正确,如已经授权并且资源访问次数正确则获取可访问资源标识符对应的资源并返回资源给资源申请者。

[0033] 访问证明例如:若需要资源拥有者再次确认,则授权服务器通过应用消息推送(终端APP接收)提醒资源拥有者进行授权确认;若需要提供绑定终端,则需提供作为人脸头像采集的终端的MAC地址;

访问令牌包括用户信息和签名信息,用户信息包括用户ID、请求的资源标识符、资源操作权限、资源访问次数(资源服务器和授权服务器有访问次数的记录,被授权的资源访问记录会加1,此信息为了防止重放攻击),以及是否已经授权等,签名信息为对用户信息进行HASH变换然后加密产生的数据;

资源申请者使用客户端(可以是浏览器或者原生应用)通过账号密码登陆资源服务器,

在没有授权的情况下尝试访问资源服务器的选定资源。授权服务器从这个初始请求中知道客户端尝试访问的是哪个资源，进而知道对应的资源拥有者以及授权服务器需要哪些访问证明(具体根据配置策略)；用户如同意授权则使用带有摄像头的COTS设备进行头像拍照并上传照片到授权服务器，如不同意则选取消或者不做任何操作；

授权服务器中的人证核验服务利用人脸识别技术和证件OCR技术对头像照片和身份证上的头像进行特征值提取和比对，简称人证合一比对，如图4所示，人证合一比对包括步骤：

1)授权服务器接收用户头像照片；用户需判断身份证件照是否清晰，如不清晰需要重新拍摄；

2)提取用户头像特征值，获取数据库存放的身份证件上的头像特征值，对比两个特征值相似度，当相似度到达一定阈值即认为人和证为同一人。

[0034] 授权服务器使用私钥签发访问令牌并且颁发访问令牌给用户客户端，而资源服务器可以通过在向授权服务器注册时获得的公钥验证签名信息保证访问令牌的合法性。

[0035] 实施例3：

如图1所示，一种基于人证合一的UMA服务的方法，包括如下步骤：

步骤1，用户在提供UMA服务的授权服务器上注册；如图2所示，注册包括：

传统信息注册，传统信息注册主要包括用户名/密码，性别，籍贯，联系方式等，同时为用户自动生成唯一的ID号，用户名和密码可以作为UMA服务的登陆凭证也可以作为低安全等级要求的用户认证；如图2所示，

身份证件照注册，通过COTS设备摄像头采集身份证件照，核验身份证件照是否真实有效，主要核查身份证姓名和号码是否一致以及身份证头像真伪；如果确认身份证是真实有效的，则授权服务器加密保存用户信息、身份证件照，关联注册的用户信息和身份证件照；若身份证件照无效，则提示身份证验证失败，可以选择重新拍摄身份证件照。

[0036] 如图3所示，核验身份证件照是否真实有效，具体步骤包括：

1)用户根据提供UMA服务的授权服务器要求请求注册服务，授权服务器等待接收用户身份证件照；

2)用户使用摄像头拍摄身份证件照；

3)用户需判断身份证件照是否清晰，如不清晰需要重新拍摄；

4)用户确认照片清晰后将照片提交给授权服务器；

6)授权服务器(获得公安部授权)解析身份证件照，将姓名，身份证号码，头像数据发送给公安部，查询身份证真伪；公安部返回验证结果；

7)如果身份证验证成功则授权服务器将身份证件照保留到数据库中，如果身份证验证失败，则提示用户身份证验证失败并且删除身份证件照，用户可以选择重新拍摄身份证件照。

[0037] 步骤2，资源服务器向提供UMA服务的授权服务器注册，获得授权服务器分配的资源服务器ID号以及对应的公钥(此公钥可以验签访问令牌)。

[0038] 步骤3，资源服务器向授权服务器注册其资源，获得资源标识符；资源拥有者通过授权服务器配置授权策略；

授权服务器为资源分配唯一标识符，并将资源的唯一标识符与一个 URL 一同返回给资源服务器。资源服务器将资源拥有者引导至该 URL，资源拥有者就可以交互式地管理与

该资源集关联的授权策略了；

不同的资源需要不同的授权策略。申请者和他们的客户端(浏览器/原生应用)需要提供能够满足授权策略要求的访问证明。如果没有为一个资源配置授权策略，则该资源被视为不可访问。例如授权策略要求要人证合一，那么申请者就需要拍摄人脸头像，这个人脸头像数据就是一个声明。如果授权策略要求使用绑定的终端，那么终端的MAC地址必须与绑定终端的MAC地址一致。

[0039] 下面列出来可能的一些授权策略选项：

1)是否需要资源拥有者再次确认以及确认方式(账户密码或人脸识别等)；

2)是否绑定授权终端，即拍摄人脸照片的终端是否绑定还是任何终端皆可；

3)资源可访问的日期范围；

4)限定特定的用户访问；

5)资源可被访问的次数限制；

步骤4，资源申请者使用客户端访问资源，授权服务器获得用户通过终端拍摄的头像照片，通过人证合一比对，若是用户本人，则根据资源授权策略进一步获得用户的访问证明，若符合要求，则表示已授权；授权服务器使用私钥签发包括授权结果的访问令牌给客户端，客户端将访问令牌发送给资源服务器，资源服务器通过公钥验签访问令牌，判断访问令牌签名是否正确，如果访问令牌通过验签，则判断该用户是否已经授权以及访问次数是否正确，如已经授权并且访问次数正确则获取可访问资源标识符对应的资源并返回资源给资源申请者。

[0040] 资源申请者使用客户端(可以是浏览器或者原生应用)通过账号密码登陆资源服务器，在没有授权的情况下尝试访问资源服务器的选定资源。资源服务器从这个初始请求中知道客户端尝试访问的是哪个资源，进而知道对应的资源拥有者以及授权服务器需要哪些访问证明(具体根据配置策略)；用户如同意授权则使用带有摄像头的COTS设备进行头像拍照并上传照片到授权服务器，如不同意则选取消或者不做任何操作；

授权服务器中的人证核验服务利用人脸识别技术和证件OCR技术对头像照片和身份证上的头像进行特征值提取和比对，简称人证合一比对，如图4所示；人证合一比对，包括步骤：

1)用户根据UMA服务的授权服务器要求请求人脸识别服务，授权服务器等待接收用户头像照片；

2)电脑端浏览器/移动端APP申请摄像头权限，用户需点击同意；

3)用户使用摄像头拍摄头像；

4)用户需判断身份证件照是否清晰，如不清晰需要重新拍摄；

5)用户确认照片清晰后将照片提交给授权服务器；

6)授权服务器中人证核验服务提取用户头像特征值，然后获取数据库存放的身份证件上的头像特征值，对比两个特征值相似度，当相似度到达一定阈值即认为人和证为同一人。

[0041] 授权服务器根据人证合一比对结果，判断是否为注册用户本人，如果是则根据配置策略是否还需资源拥有者进行授权确认，如果需要资源拥有者确认，则系统通过应用消息推送(终端APP接收)提醒资源拥有者进行授权确认，确认方式根据配置策略；

资源服务器通过步骤2获取的公钥验签访问令牌，判断访问令牌签名是否正确，如果访

问令牌通过验签，则判断该用户是否已经授权，如已经授权则获取可访问资源标识符及对应的资源并返回资源给客户端。

[0042] 实施例4：

一种基于人证合一的UMA服务的装置，包括：

用户注册模块，用于在提供UMA服务的授权服务器上进行传统信息注册和身份证件照注册，授权服务器加密保存用户注册信息；

资源服务器注册模块，用于授权服务器接受资源服务器的注册，为资源服务器分配资源服务器ID号以及对应的公钥；

资源注册模块，用于授权服务器接受资源服务器为其资源的注册，为资源分配唯一的资源标识符，所述资源被资源拥有者通过授权服务器配置授权策略；

人证合一核验及获取资源模块，用于当资源申请者访问资源时，授权服务器根据资源申请者上传的头像照片，通过人证合一比对判断是否为注册用户本人，如果是，再根据资源授权策略获得申请者提供的访问证明，判断访问证明是否符合要求，如果符合要求，则表示已授权，如果不是注册用户本人或者访问证明不符合要求则未授权；授权服务器使用私钥签发包括授权结果的访问令牌给资源申请者的客户端；所述访问令牌用于提供给资源服务器通过公钥验签，如通过验签且已经授权，则资源被发送给资源申请者。

[0043] 所述通过人证合一比对判断是否为注册用户本人，具体为：

1)授权服务器接收用户头像照片；

2)提取用户头像特征值，获取数据库存放的身份证件上的头像特征值，对比两个特征值相似度，当相似度到达一定阈值即认为人和证为同一人。

[0044] 在整个过程中，资源拥有者的个人信息和申请者的个人信息都没有被透露给资源服务器或客户端。另外，这两方也没有相互透露敏感的个人信息。申请者只需要最小限度地提供证明信息，满足资源拥有者设置的授权策略即可。

[0045] 授权服务器用于用户身份注册和验证、资源服务器的注册，申请者不需要同现实中出示身份证件给第三方，申请者只需拍摄头像照片发送给授权服务器，由授权服务器证明身份。避免了现实生活中个人信息泄露给第三方带来的身份冒用、滥用等问题。

[0046] 基于UMA框架和人证合一技术确保授权的安全以及提高授权的便利性，授权设备的多样化也更能适应多场景。

[0047] 通过实人实证确保授权的安全性，但实人实证不限于人脸识别。随着指纹等生物特征集成到身份证，所有能证明和身份证件属于同一个人的生物特征信息都属于实人实证的范畴。

[0048] 身份证核验成功后，可以直接保留身份证件照或者只保留头像特征值信息，因为有些使用场景如银行可能还存在需要人工比对身份证件头像与真人头像；

用户可以选择绑定终端或者不绑定终端，这取决于使用场景的安全级别要求，当安全级别较高时，建议绑定终端。

[0049] 访问令牌包括用户信息和签名信息，用户信息包括用户ID、请求的资源标识符、资源操作权限、资源访问次数、以及是否已经授权等，签名信息为对用户信息进行HASH计算然后加密产生的数据，而资源服务器可以通过在向授权服务器注册时获得的公钥验证签名信息保证访问令牌的合法性。但本发明不限于使用此方法生成和校验令牌，所有可以安全保

证令牌传输安全并能验证令牌的方法都在本文所指的访问令牌生成于校验范围内。

[0050] 本发明所指授权不局限于用户对其他用户的授权以及用户对第三方应用的授权，所有不能通过直接发送登陆凭证的授权都在本文所指授权范围内。

[0051] 系统提醒资源拥有者进行授权确认的方式不限于应用消息推送，所有能及时通知资源拥有者的方法都在本文所指的系统提醒范围内。

[0052] 本发明具有以下有益效果：

(1)更加安全便捷

移动终端如智能手机和平板电脑的普及以及摄像头作为移动终端的标配，为人脸识别服务提供了广泛的终端设备，而且现在几乎每人都随身携带至少一部移动终端设备。虽然不少终端设备存在安全性问题，但是本发明无需在终端上存放生物特征信息，对终端设备的安全性要求不高，所以可以在不增加硬件成本的条件下增加授权安全性和便利性。

[0053] (2)适用性强

人证合一验证比传统单一的账号密码或者生物识别更加安全，不仅适用于必须核实用户身份的使用场景，也适用于一般的授权登陆，具有更强的适用性。

[0054] (3)可扩展性强

不仅可以做到资源拥有者对其他用户授权，也可以做到资源拥有者对第三方应用授权(当申请者为第三方应用时)，系统的可扩展性更强。

[0055] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0056] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0057] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0058] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0059] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明技术原理的前提下，还可以做出若干改进和变形，这些改进和变形也应视为本发明的保护范围。

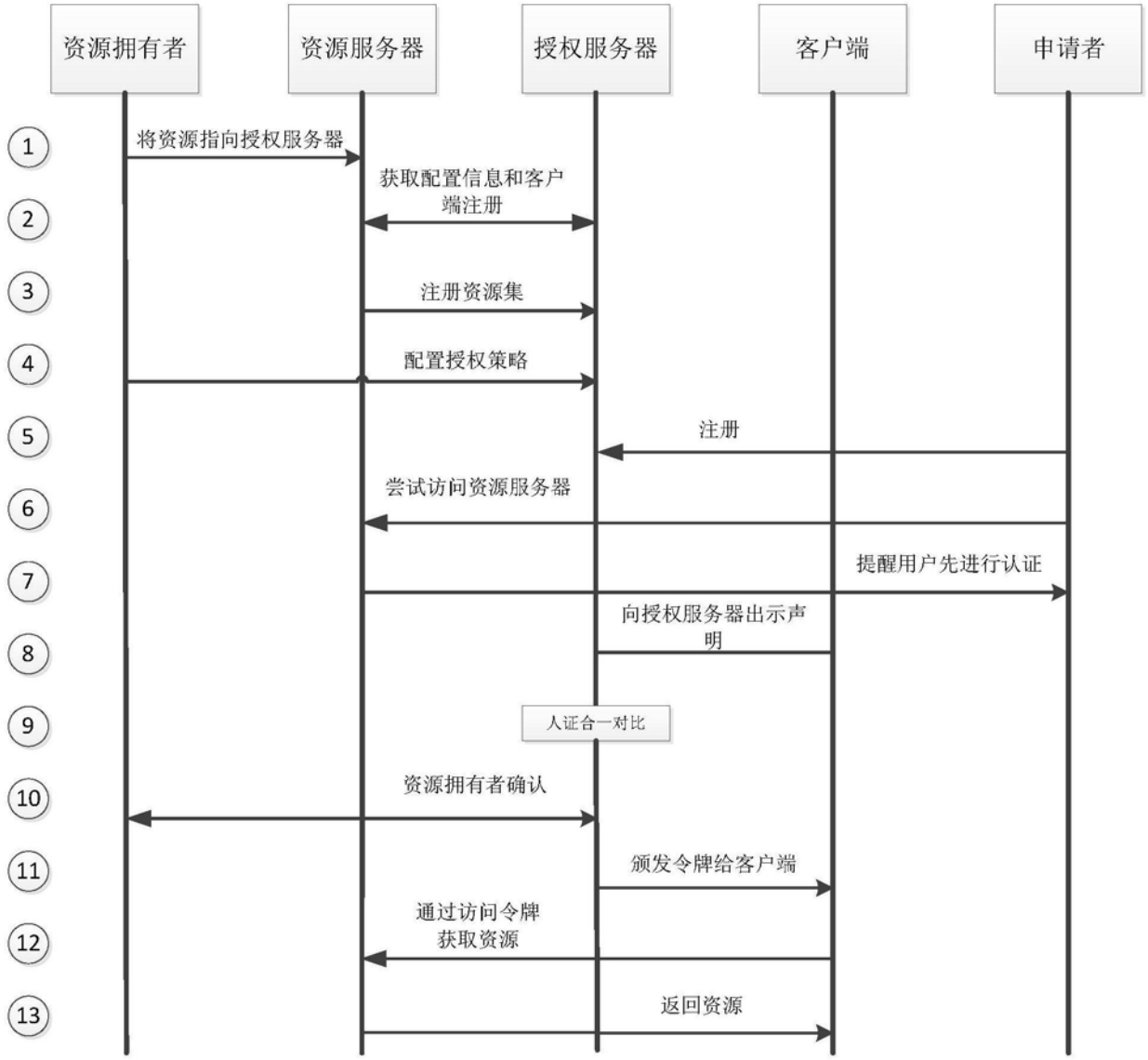

资源拥有者
资源服务器
授权服务器
客户端
申请者
1
将资源指向授权服务器
2
获取配置信息和客户端注册
3
注册资源集
4
配置授权策略
5
注册
6
尝试访问资源服务器
7
提醒用户先进行认证
8
向授权服务器出示声明
9
人证合一对比
10
资源拥有者确认
11
颁发令牌给客户端
12
通过访问令牌获取资源
13
返回资源

图1

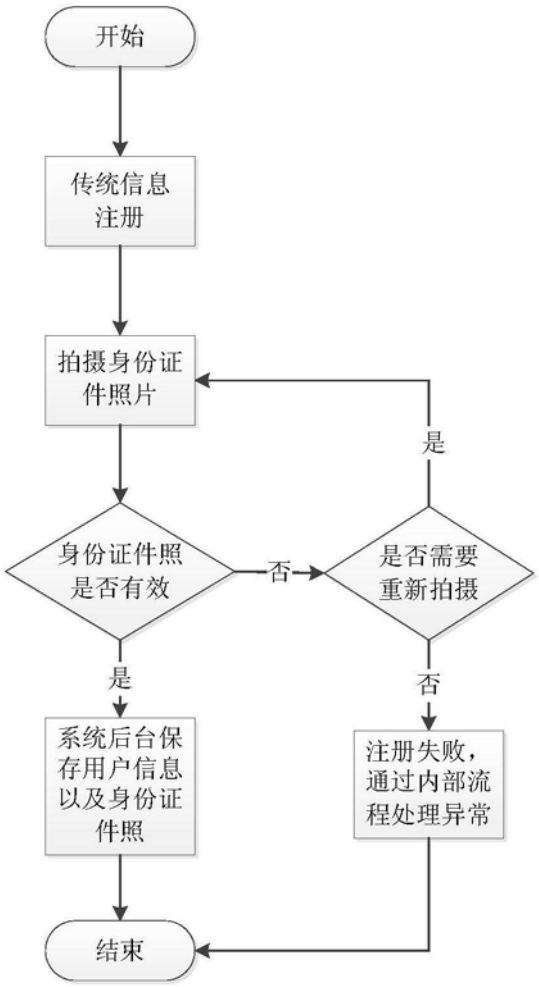

开始
传统信息注册
拍摄身份证件照片
身份证件照是否有效
否
是否需要重新拍摄
是
是
否
系统后台保存用户信息以及身份证件照
注册失败，通过内部流程处理异常
结束

图2

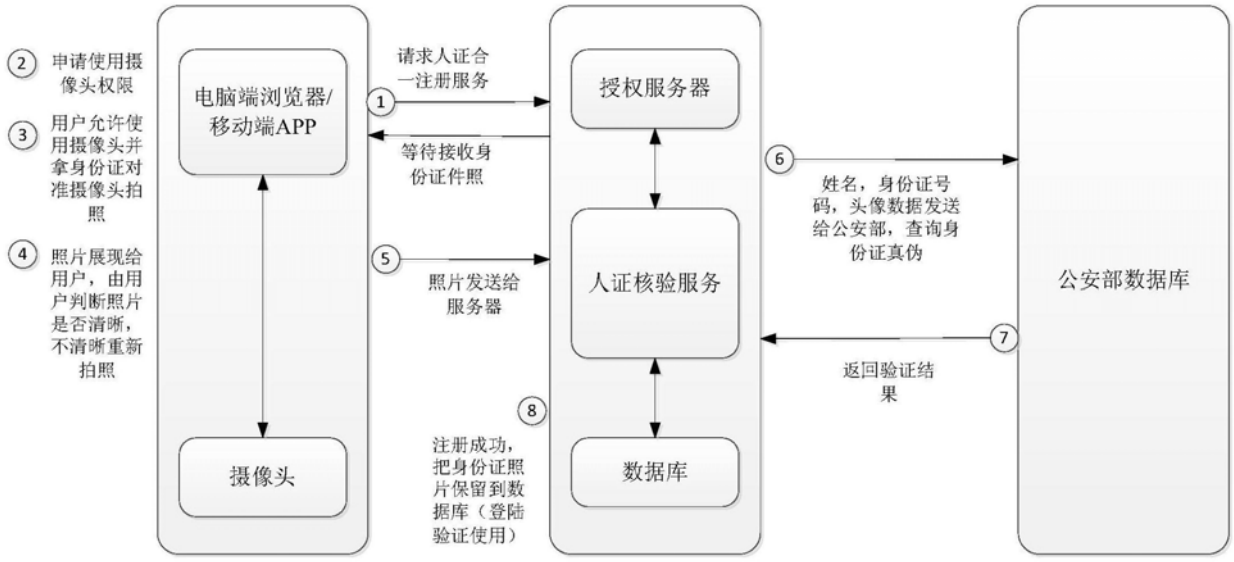

2 申请使用摄像头权限
3 用户允许使用摄像头并拿身份证对准摄像头拍照
4 照片展现给用户，由用户判断照片是否清晰，不清晰重新拍照
电脑端浏览器/移动端APP
摄像头
请求人证合一注册服务
1
等待接收身份证件照
5
照片发送给服务器
8
注册成功，把身份证照片保留到数据库（登陆验证使用）
授权服务器
人证核验服务
数据库
6
姓名，身份证号码，头像数据发送给公安部，查询身份证真伪
7
返回验证结果
公安部数据库

图3

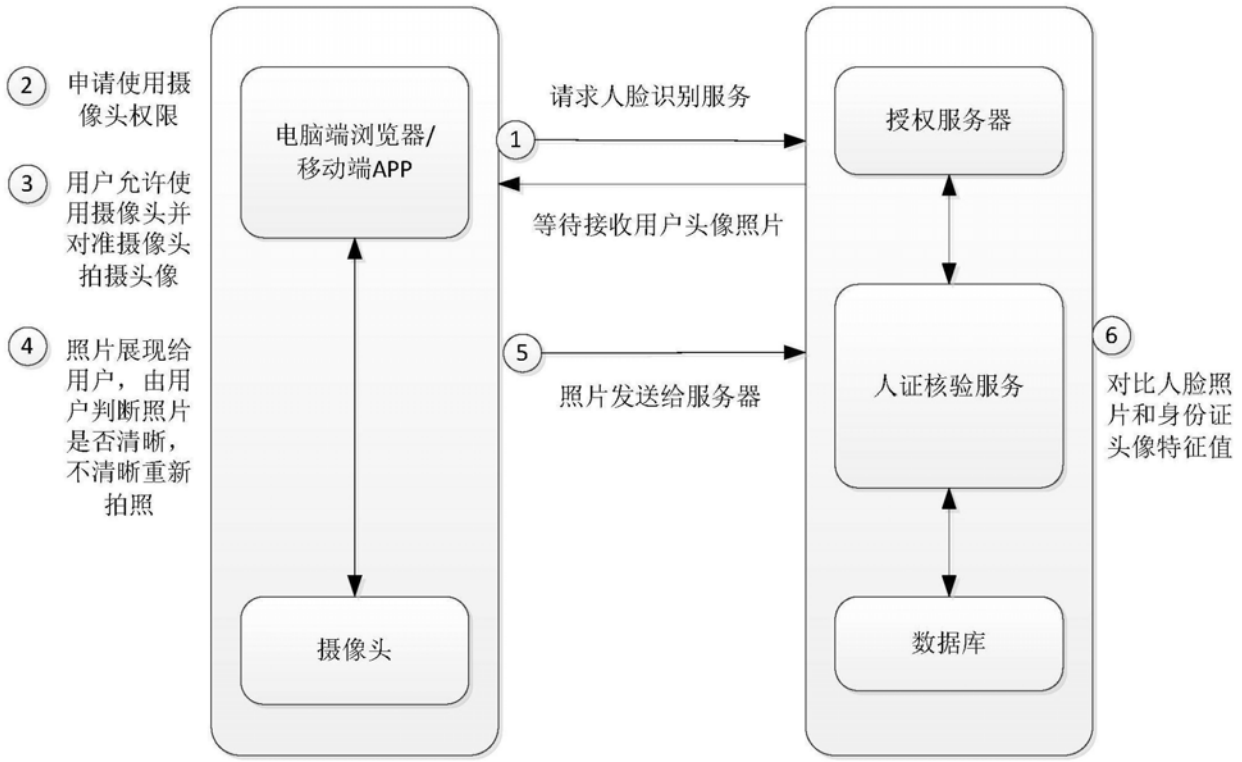

2
申请使用摄像头权限
3
用户允许使用摄像头并对准摄像头拍摄头像
4
照片展现给用户，由用户判断照片是否清晰，不清晰重新拍照
电脑端浏览器/移动端APP
摄像头
1
请求人脸识别服务
等待接收用户头像照片
5
照片发送给服务器
授权服务器
人证核验服务
数据库
6
对比人脸照片和身份证头像特征值

图4