(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104519066 B
(45)授权公告日 2017.11.28

(21)申请号 201410811778.0

(22)申请日 2014.12.23

(65)同一申请的已公布的文献号
申请公布号 CN 104519066 A

(43)申请公布日 2015.04.15

(73)专利权人 飞天诚信科技股份有限公司
地址 100085 北京市海淀区学清路9号汇智大厦B楼17层

(72)发明人 陆舟 于华章

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 103684782 A,2014.03.26,
CN 102307095 A,2012.01.04,
CN 103220148 A,2013.07.24,
CN 103501228 A,2014.01.08,
CN 103746801 A,2014.04.23,
US 2006174104 A1,2006.08.03,
US 2014344160 A1,2014.11.20,
CN 102882684 A,2013.01.16,

审查员 刘莉

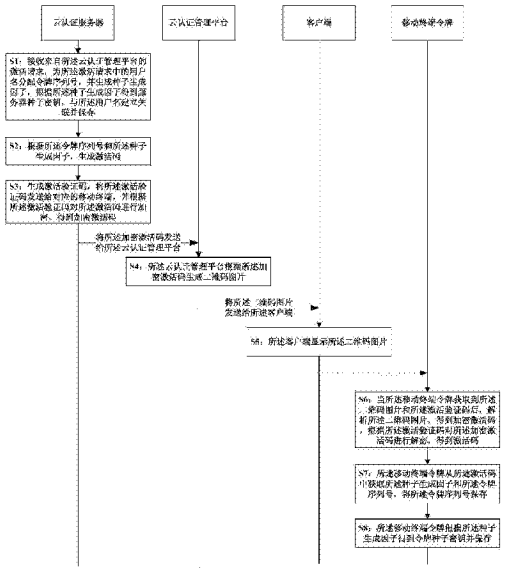
权利要求书5页 说明书13页 附图4页

(54)发明名称

一种激活移动终端令牌的方法

(57)摘要

本发明公开一种激活移动终端令牌的方法，属于信息安全领域，所述方法包括：云认证服务器根据激活请求，生成种子生成因子，根据种子生成因子得到服务器种子密钥并保存，根据种子生成因子生成激活码，并生成激活验证码发送至移动终端，用激活验证码对激活码加密得到加密激活码，云认证管理平台根据接收到的加密激活码生成二维码图片发送至客户端进行显示，移动终端令牌根据获取到的二维码图片得到加密激活码，用获取到的激活验证码对加密激活码解密得到激活码，并从中获取到种子生成因子，根据种子生成因子得到令牌种子密钥并保存。采用本发明的技术方案，实现在移动终端无网络时对令牌进行激活，保证种子的正确性，提高令牌安全性。



CN 104519066 B

1.一种激活移动终端令牌的方法，应用于包括云认证管理平台、云认证服务器、客户端和移动终端令牌组成的系统中，其特征在于，所述方法包括：

步骤S1：所述云认证服务器接收来自所述云认证管理平台的激活请求，为所述激活请求中的用户名分配令牌序列号，并生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存；

步骤S2：所述云认证服务器根据所述令牌序列号和所述种子生成因子，生成激活码并保存；

步骤S3：所述云认证服务器生成激活验证码，将所述激活验证码发送给对应的移动终端，并根据所述激活验证码对所述激活码进行加密，得到加密激活码，将所述加密激活码发送给所述云认证管理平台；

步骤S4：所述云认证管理平台根据所述加密激活码生成二维码图片，将所述二维码图片发送给所述客户端；

步骤S5：所述客户端显示所述二维码图片；

步骤S6：当所述移动终端令牌获取到所述二维码图片和所述激活验证码后，解析所述二维码图片，得到加密激活码，根据所述激活验证码对所述加密激活码进行解密，得到激活码；

步骤S7：所述移动终端令牌从所述激活码中获取所述种子生成因子和所述令牌序列号，将所述令牌序列号保存；

步骤S8：所述移动终端令牌根据所述种子生成因子得到令牌种子密钥并保存；

步骤T1：所述移动终端令牌根据所述令牌种子密钥生成动态口令，显示所述动态口令；

步骤T2：所述客户端接收用户输入的用户名和所述动态口令，将所述用户名和所述动态口令发送给所述云认证服务器；

步骤T3：所述云认证服务器根据所述用户名获取对应的服务器种子密钥，根据所述服务器种子密钥生成动态口令，判断生成的动态口令与接收到的动态口令是否匹配，如果是，则向所述客户端返回激活成功响应，结束；否则向所述客户端返回激活失败响应，结束。

2.根据权利要求1所述的方法，其特征在于，所述步骤S8具体包括：

步骤S8-1：所述移动终端令牌应用预设推导算法对所述种子生成因子进行推导，得到令牌种子密钥；

步骤S8-2：所述移动终端令牌应用所述令牌序列号对所述令牌种子密钥进行加密，得到加密令牌种子密钥并保存。

3.根据权利要求2所述的方法，其特征在于，所述步骤T1，具体包括：

步骤T1-1：所述移动终端令牌获取内部保存的所述令牌序列号和所述加密令牌种子密钥，应用所述令牌序列号对所述加密令牌种子密钥进行解密，得到令牌种子密钥；

步骤T1-2：所述移动终端令牌根据令牌种子密钥，应用口令生成算法，生成动态口令，显示动态口令。

4.根据权利要求1所述的方法，其特征在于，所述步骤S1中，所述云认证服务器接收到所述激活请求后，还包括：根据所述激活请求中的用户名获取对应的激活标识，判断所述激活标识，如果是已激活，则向所述云认证管理平台返回已激活响应，结束，如果是激活未确认，则获取保存的激活码，执行步骤S3，如果是未激活，则为所述激活请求中的用户名分配

令牌序列号，并生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存，执行步骤S2；

所述步骤S2还包括：将所述激活标识置为激活未确认；

所述步骤T3中，所述向客户端返回激活成功响应，还包括：将所述激活标识置为已激活。

5.根据权利要求1所述的方法，其特征在于，所述步骤T2具体包括：

步骤T2-1：所述客户端接收用户输入的用户名、密码和所述动态口令；

步骤T2-2：所述客户端判断接收到的用户名和密码是否正确，如果是，则执行步骤T2-3，否则报错，结束；

步骤T2-3：所述客户端将所述用户名和所述动态口令发送给所述云认证服务器。

6.根据权利要求1所述的方法，其特征在于，所述云认证服务器根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存，具体包括：

步骤c1：所述云认证服务器应用预设推导算法，对所述种子生成因子进行推导，得到服务器种子密钥；

步骤c2：所述云认证服务器根据所述用户名获取对应的企业密钥，应用所述企业密钥对所述服务器种子密钥进行加密，得到加密服务器种子密钥，将所述加密服务器种子密钥与所述用户名建立关联并保存。

7.根据权利要求6所述的方法，其特征在于，所述步骤c2之前，还包括：

步骤d1：密钥运维平台接收密钥持有者的管理员密钥；

步骤d2：所述密钥运维平台对所述管理员密钥进行预设运算，得到主密钥，将所述主密钥保存；

步骤d3：所述云认证服务器定时向所述密钥运维平台获取主密钥，判断获取到的主密钥与保存的主密钥是否相同，如果是，则执行步骤d4，否则用所述获取到的主密钥更新所述保存的主密钥，执行步骤d4；

步骤d4：所述云认证服务器根据用户名获取对应的企业ID，对所述主密钥和所述企业ID进行散列运算，得到企业密钥，将所述企业密钥与所述用户名建立关联并保存。

8.根据权利要求7所述的方法，其特征在于，所述步骤T3中，根据所述用户名获取对应的服务器种子密钥，根据所述服务器种子密钥生成动态口令，具体包括：

步骤T3-1：所述云认证服务器根据所述用户名获取对应的所述企业密钥和所述加密服务器种子密钥；

步骤T3-2：所述云认证服务器根据所述企业密钥，应用预设解密算法对所述加密服务器种子密钥进行解密，得到服务器种子密钥；

步骤T3-3：所述云认证服务器根据所述服务器种子密钥，应用口令生成算法，生成动态口令。

9.根据权利要求1所述的方法，其特征在于，所述云认证服务器接收来自所述云认证管理平台的激活请求之前，还包括：

步骤a1：所述云认证管理平台等待接收管理员选择的需要激活的用户记录；

步骤a2：所述云认证管理平台根据所述用户记录中的用户名，生成激活请求；

步骤a3：所述云认证管理平台将所述激活请求发送给所述云认证服务器。

10.根据权利要求9所述的方法，其特征在于，所述步骤a1与所述步骤a2之间还包括：所述云认证管理平台根据所述用户记录，判断是否能够获取到对应的移动终端号码、邮箱账号和用户名，如果是，则执行步骤a2，否则提示信息不完整，结束。

11.根据权利要求10所述的方法，其特征在于，所述步骤S4中，所述云认证管理平台将所述二维码图片发送给所述客户端，具体为：所述云认证管理平台根据所述管理员选择的用户记录中保存的邮箱账号，将所述二维码图片通过邮件方式发送至所述客户端的邮件平台。

12.根据权利要求9所述的方法，其特征在于，所述步骤a1之前，还包括：

步骤b0：所述云认证管理平台将验证密码失败次数置为初值；

步骤b1：所述云认证管理平台等待接收管理员输入管理员账号和密码；

步骤b2：所述云认证管理平台判断接收到的管理员输入的管理员账号和密码是否正确，如果是，则执行步骤a1，否则执行步骤b3；

步骤b3：所述云认证管理平台更新所述验证密码失败次数，判断更新后的验证密码失败次数是否达到预设次数，如果是，则报错，锁定所述云认证管理平台，否则返回步骤b1。

13.根据权利要求9所述的方法，其特征在于，所述步骤a1与所述步骤a2之间还包括：所述云认证管理平台接收所述管理员点击的激活按钮，获取上次激活时间和当前系统时间，判断所述当前系统时间与所述上次激活时间之差是否大于预设时长，如果是，则允许再次激活，执行步骤a2，否则返回已激活响应，结束；

所述步骤a2具体为：所述云认证管理平台根据所述用户记录中的用户名和预设重新激活标识，生成激活请求。

14.根据权利要求13所述的方法，其特征在于，所述步骤S1具体包括：所述云认证服务器接收来自所述云认证管理平台的激活请求后，判断所述激活请求中是否有所述预设重新激活标识，如果是，则生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存，否则为所述激活请求中的用户名分配令牌序列号，并生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存。

15.根据权利要求1所述的方法，其特征在于，所述为所述激活请求中的用户名分配令牌序列号，具体为：所述云认证服务器根据令牌序列号生成方法，产生一个令牌序列号，将所述令牌序列号与所述用户名建立关联并保存。

16.根据权利要求1所述的方法，其特征在于，

所述步骤S1中，所述生成种子生成因子，具体为：所述云认证服务器调用随机数生成算法，生成第一随机数，将所述第一随机数作为所述种子生成因子；

所述步骤S3中，所述生成激活验证码，具体为：所述云认证服务器调用随机数生成算法，生成第二随机数，将所述第二随机数作为所述激活验证码。

17.根据权利要求1所述的方法，其特征在于，所述步骤S4中，所述根据所述加密激活码生成二维码图片，具体为：所述云认证管理平台根据所述加密激活码调用二维码图片生成函数，生成二维码图片。

18.根据权利要求1所述的方法，其特征在于，

所述步骤S4还包括：所述云认证管理平台将所述加密激活码发送给所述客户端；

所述步骤S5还包括：所述客户端显示所述加密激活码；

所述步骤S6还可以为，所述移动终端令牌接收用户输入所述加密激活码和所述激活验证码，根据所述激活验证码对所述加密激活码进行解密，得到激活码。

19.根据权利要求1所述的方法，其特征在于，所述步骤S2具体为：所述云认证服务器根据预设拼接组合方式，将所述令牌序列号与所述种子生成因子依序拼接，得到激活码。

20.根据权利要求19所述的方法，其特征在于，所述将所述令牌序列号与所述种子生成因子依序拼接，得到激活码，具体为：

判断移动终端令牌是否需要接收短信验证码，如果需要，则将所述激活码的第一位数据置为1，如果不需要，则将所述激活码的第一位数据设置为0；

判断口令生成算法，如果是第一预设算法，则将所述激活码的第二位数据设置为1，如果是第二预设算法，则将所述激活码的第二位数据设置为0；

将所述激活码的第三位至第十二位数据设置为所述种子生成因子；

将所述激活码的第十三位至第二十二位数据设置为所述令牌序列号；

对所述种子生成因子进行校验，得到第一校验值，将所述激活码的第二十三位数据设置为所述第一校验值；

对所述激活码的前二十三位进行校验计算，得到第二校验值，将所述激活码的第二十四位数据设置为所述第二校验值；

将所述激活码的第二十五位数据作为预设填充位，设置为0。

21.根据权利要求20所述的方法，其特征在于，所述步骤S7中，所述从所述激活码中获取所述种子生成因子和所述令牌序列号，具体为：所述移动终端令牌根据所述预设拆分方式，从所述激活码中分解得到所述种子生成因子和所述令牌序列号。

22.根据权利要求21所述的方法，其特征在于，所述根据所述预设拆分方式，从所述激活码中分解得到所述种子生成因子和所述令牌序列号，具体为：所述移动终端令牌获取所述激活码中第三位至第十二位的数据，作为所述种子生成因子，将所述激活码中第十三位至第二十二位的数据，作为所述令牌序列号。

23.根据权利要求1所述的方法，其特征在于，

所述步骤S3中，所述根据所述激活验证码对所述激活码进行加密，得到加密激活码，还可以为：所述云认证服务器根据所述用户名获取对应的移动终端号码，应用所述移动终端号码和所述激活验证码，对所述激活码进行加密，得到加密激活码；

所述步骤S6中，所述根据所述激活验证码对所述加密激活码进行解密，得到激活码，还可以为：所述移动终端令牌获取所述移动终端号码，根据所述移动终端号码和所述激活验证码，对所述加密激活码进行解密，得到激活码。

24.根据权利要求1所述的方法，其特征在于，

所述步骤S3中，所述根据所述激活验证码对所述激活码进行加密，得到加密激活码，还可以为：所述云认证服务器根据所述用户名获取预先保存的移动终端特征数据，应用所述移动终端特征数据和所述激活验证码，对所述激活码进行加密，得到加密激活码；

所述步骤S6中，所述根据所述激活验证码对所述加密激活码进行解密，得到激活码，还可以为：所述移动终端令牌获取所述移动终端特征数据，根据所述移动终端特征数据和所述激活验证码，对所述加密激活码进行解密，得到激活码。

25.根据权利要求1所述的方法，其特征在于，

所述步骤S2中，所述根据所述令牌序列号和所述种子生成因子，生成激活码，还可以为：所述云认证服务器根据所述用户名获取对应的移动终端号码，根据所述令牌序列号、所述种子生成因子和所述移动终端号码生成激活码；

所述步骤S7之前还包括：所述移动终端令牌从所述激活码中分解得到移动终端号码，并截取本机移动终端号码，判断所述激活码中的移动终端号码与截取到的移动终端号码是否匹配，如果是，则执行步骤S7，否则提示非本移动终端匹配激活信息，结束。

26.根据权利要求1所述的方法，其特征在于，

所述步骤S2中，所述根据所述令牌序列号和所述种子生成因子，生成激活码，还可以为：所述云认证服务器根据所述用户名获取对应的移动终端特征数据，根据所述令牌序列号、所述种子生成因子和所述移动终端特征数据生成激活码；

所述步骤S7之前还包括：所述移动终端令牌从所述激活码中分解得到移动终端特征数据，并获取本机移动终端特征数据，判断所述激活码中的移动终端特征数据，与获取到的移动终端特征数据是否匹配，如果是，则执行步骤S7，否则提示非本移动终端匹配激活信息，结束。

一种激活移动终端令牌的方法

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种激活移动终端令牌的方法。

背景技术

[0002] 移动终端令牌，全称动态密码移动终端令牌，是用来生成动态口令的移动终端客户端软件，移动终端令牌是由运行在移动终端上的程序产生动态口令，动态口令与移动终端绑定进行身份认证，口令的生成过程不产生通信及费用，具有使用简单、安全性高、低成本、无需携带额外设备、容易获取、无物流等优势，移动终端令牌是3G时代动态密码身份认证的发展趋势。

[0003] 云认证服务器是基于SaaS模式的身份认证平台，部署在互联网上，为个人、家庭和企业提供可靠的身份认证基础设施，云认证服务器为网站提供独立的基于云的服务，通过简单集成，使用免费的移动终端令牌，即可极大的增强网站登录的安全性。

[0004] 二维码，又称二维条码，它是用特定的几何图形按照一定规律在平米上分布的黑白相间的图形，是所有信息数据的一把钥匙，应用相当广泛。

[0005] 现有技术中，动态口令的获取是通过硬件令牌与服务器验证完成，而硬件令牌又需要消耗大量的人力物力，移动终端令牌就是在这样的情形下应运而生的。

发明内容

[0006] 为解决现有技术中提供的问题，本发明提供了一种激活移动终端令牌的方法。

[0007] 本发明采用的技术方案是：一种激活移动终端令牌的方法，应用于包括云认证管理平台、云认证服务器、客户端和移动终端令牌组成的系统中，所述方法包括：

[0008] 步骤S1：所述云认证服务器接收来自所述云认证管理平台的激活请求，为所述激活请求中的用户名分配令牌序列号，并生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存；

[0009] 步骤S2：所述云认证服务器根据所述令牌序列号和所述种子生成因子，生成激活码并保存；

[0010] 步骤S3：所述云认证服务器生成激活验证码，将所述激活验证码发送给对应的移动终端，并根据所述激活验证码对所述激活码进行加密，得到加密激活码，将所述加密激活码发送给所述云认证管理平台；

[0011] 步骤S4：所述云认证管理平台根据所述加密激活码生成二维码图片，将所述二维码图片发送给所述客户端；

[0012] 步骤S5：所述客户端显示所述二维码图片；

[0013] 步骤S6：当所述移动终端令牌获取到所述二维码图片和所述激活验证码后，解析所述二维码图片，得到加密激活码，根据所述激活验证码对所述加密激活码进行解密，得到激活码；

[0014] 步骤S7：所述移动终端令牌从所述激活码中获取所述种子生成因子和所述令牌序

列号，将所述令牌序列号保存；

[0015] 步骤S8：所述移动终端令牌根据所述种子生成因子得到令牌种子密钥并保存。

[0016] 所述步骤S8之后，还包括：

[0017] 步骤T1：所述移动终端令牌根据所述令牌种子密钥生成动态口令，显示所述动态口令；

[0018] 步骤T2：所述客户端接收用户输入的用户名和所述动态口令，将所述用户名和所述动态口令发送给所述云认证服务器；

[0019] 步骤T3：所述云认证服务器根据所述用户名获取对应的服务器种子密钥，根据所述服务器种子密钥生成动态口令，判断生成的动态口令与接收到的动态口令是否匹配，如果是，则向所述客户端返回认证成功响应，结束；否则向所述客户端返回认证失败响应，结束。

[0020] 所述步骤S8具体包括：

[0021] 步骤S8-1：所述移动终端令牌应用预设推导算法对所述种子生成因子进行推导，得到令牌种子密钥；

[0022] 步骤S8-2：所述移动终端令牌应用所述令牌序列号对所述令牌种子密钥进行加密，得到加密令牌种子密钥并保存。

[0023] 所述步骤T1，具体包括：

[0024] 步骤T1-1：所述移动终端令牌获取内部保存的所述令牌序列号和所述加密令牌种子密钥，应用所述令牌序列号对所述加密令牌种子密钥进行解密，得到令牌种子密钥；

[0025] 步骤T1-2：所述移动终端令牌应用口令生成算法，对所述令牌种子密钥和动态因子生成动态口令，显示所述动态口令。

[0026] 所述步骤S1中，所述云认证服务器接收到所述激活请求后，还包括：根据所述激活请求中的用户名获取对应的激活标识，判断所述激活标识，如果是已激活，则向所述云认证管理平台返回已激活响应，结束，如果是激活未确认，则获取保存的激活码，执行步骤S3，如果是未激活，则为所述激活请求中的用户名分配令牌序列号，并生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存，执行步骤S2；

[0027] 所述步骤S2还包括：将所述激活标识置为激活未确认；

[0028] 所述步骤T3中，所述向客户端返回激活成功响应，还包括：将所述激活标识置为已激活。

[0029] 所述步骤T2具体包括：

[0030] 步骤T2-1：所述客户端接收用户输入的用户名、密码和所述动态口令；

[0031] 步骤T2-2：所述客户端判断接收到的用户名和密码是否正确，如果是，则执行步骤T2-3，否则报错，结束；

[0032] 步骤T2-3：所述客户端将所述用户名和所述动态口令发送给所述云认证服务器。

[0033] 所述云认证服务器根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存，具体包括：

[0034] 步骤c1：所述云认证服务器应用预设推导算法，对所述种子生成因子进行推导，得到服务器种子密钥；

[0035] 步骤c2：所述云认证服务器根据所述用户名获取对应的企业密钥，应用所述企业

密钥对所述服务器种子密钥进行加密，得到加密服务器种子密钥，将所述加密服务器种子密钥与所述用户名建立关联并保存。

[0036] 所述步骤c2之前，还包括：

[0037] 步骤d1：密钥运维平台接收密钥持有者的管理员密钥；

[0038] 步骤d2：所述密钥运维平台对所述管理员密钥进行预设运算，得到主密钥，将所述主密钥保存；

[0039] 步骤d3：所述云认证服务器定时向所述密钥运维平台获取主密钥，判断获取到的主密钥与保存的主密钥是否相同，如果是，则执行步骤d4，否则用所述获取到的主密钥更新所述保存的主密钥，执行步骤d4；

[0040] 步骤d4：所述云认证服务器所述根据用户名获取对应的企业ID，对所述主密钥和所述企业ID进行散列运算，得到企业密钥，将所述企业密钥与所述用户名建立关联并保存。

[0041] 所述步骤T3中，根据所述用户名获取对应的服务器种子密钥，根据所述服务器种子密钥生成动态口令，具体包括：

[0042] 步骤T3-1：所述云认证服务器根据所述用户名获取对应的所述企业密钥和所述加密服务器种子密钥；

[0043] 步骤T3-2：所述云认证服务器根据所述企业密钥，应用预设解密算法对所述加密服务器种子密钥进行解密，得到服务器种子密钥；

[0044] 步骤T3-3：所述云认证服务器根据所述服务器种子密钥，应用口令生成算法，生成动态口令。

[0045] 所述云认证服务器接收来自所述云认证管理平台的激活请求之前，还包括：

[0046] 步骤a1：所述云认证管理平台等待接收管理员选择的需要激活的用户记录；

[0047] 步骤a2：所述云认证管理平台根据所述用户记录中的用户名，生成激活请求；

[0048] 步骤a3：所述云认证管理平台将所述激活请求发送给所述云认证服务器。

[0049] 所述步骤a1与所述步骤a2之间还包括：所述云认证管理平台根据所述用户记录，判断是否能够获取到对应的移动终端号码、邮箱账号和用户名，如果是，则执行步骤a2，否则提示信息不完整，结束。

[0050] 所述步骤S4中，所述云认证管理平台将所述二维码图片发送给所述客户端，具体为：所述云认证管理平台根据所述管理员选择的用户记录中保存的邮箱账号，将所述二维码图片通过邮件方式发送至所述客户端的邮件平台。

[0051] 所述步骤a1之前，还包括：

[0052] 步骤b0：所述云认证管理平台将验证密码失败次数置为初值；

[0053] 步骤b1：所述云认证管理平台等待接收管理员输入管理员账号和密码；

[0054] 步骤b2：所述云认证管理平台判断接收到的管理员输入的管理员账号和密码是否正确，如果是，则执行步骤a1，否则执行步骤b3；

[0055] 步骤b3：所述云认证管理平台更新所述验证密码失败次数，判断更新后的验证密码失败次数是否达到预设次数，如果是，则报错，锁定所述云认证管理平台，否则返回步骤b1。

[0056] 所述步骤a1与所述步骤a2之间还包括：所述云认证管理平台接收所述管理员点击的激活按钮，获取上次激活时间和当前系统时间，判断所述当前系统时间与所述上次激活

时间之差是否大于预设时长，如果是，则允许再次激活，执行步骤a2，否则返回已激活响应，结束；

[0057] 所述步骤a2具体为：所述云认证管理平台根据所述用户记录中的用户名和预设重新激活标识，生成激活请求。

[0058] 所述步骤S1具体包括：所述云认证服务器接收来自所述云认证管理平台的激活请求后，判断所述激活请求中是否有所述预设重新激活标识，如果是，则生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存，否则为所述激活请求中的用户名分配令牌序列号，并生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存。

[0059] 所述为所述激活请求中的用户名分配令牌序列号，具体为：所述云认证服务器根据令牌序列号生成方法，产生一个令牌序列号，将所述令牌序列号与所述用户名建立关联并保存。

[0060] 所述步骤S1中，所述生成种子生成因子，具体为：所述云认证服务器调用随机数生成算法，生成第一随机数，将所述第一随机数作为所述种子生成因子；

[0061] 所述步骤S3中，所述生成激活验证码，具体为：所述云认证服务器调用随机数生成算法，生成第二随机数，将所述第二随机数作为所述激活验证码。

[0062] 所述步骤S4中，所述根据所述加密激活码生成二维码图片，具体为：所述云认证管理平台根据所述加密激活码调用二维码图片生成函数，生成二维码图片。

[0063] 所述步骤S4还包括：所述云认证管理平台将所述加密激活码发送给所述客户端；

[0064] 所述步骤S5还包括：所述客户端显示所述加密激活码；

[0065] 所述步骤S6还可以为，所述移动终端令牌接收用户输入所述加密激活码和所述激活验证码，根据所述激活验证码对所述加密激活码进行解密，得到激活码。

[0066] 所述步骤S2具体为：所述云认证服务器根据预设拼接组合方式，将所述令牌序列号与所述种子生成因子依序拼接，得到激活码。

[0067] 所述将所述令牌序列号与所述种子生成因子依序拼接，得到激活码，具体为：

[0068] 判断移动终端令牌是否需要接收短信验证码，如果需要，则将所述激活码的第一位数据置为1，如果不需要，则将所述激活码的第一位数据设置为0；

[0069] 判断口令生成算法，如果是第一预设算法，则将所述激活码的第二位数据设置为1，如果是第二预设算法，则将所述激活码的第二位数据设置为0；

[0070] 将所述激活码的第三位至第十二位数据设置为所述种子生成因子；

[0071] 将所述激活码的第十三位至第二十二位数据设置为所述令牌序列号；

[0072] 对所述种子生成因子进行校验，得到第一校验值，将所述激活码的第二十三位数据设置为所述第一校验值；

[0073] 对所述激活码的前二十三位进行校验计算，得到第二校验值，将所述激活码的第二十四位数据设置为所述第二校验值；

[0074] 将所述激活码的第二十五位数据作为预设填充位，设置为0。

[0075] 所述步骤S7中，所述从所述激活码中获取所述种子生成因子和所述令牌序列号，具体为：所述移动终端令牌根据所述预设拆分方式，从所述激活码中分解得到所述种子生成因子和所述令牌序列号。

[0076] 所述根据所述预设拆分方式，从所述激活码中分解得到所述种子生成因子和所述令牌序列号，具体为：所述移动终端令牌获取所述激活码中第三位至第十二位的数据，作为所述种子生成因子，将所述激活码中第十三位至第二十二位的数据，作为所述令牌序列号。

[0077] 所述步骤S3中，所述根据所述激活验证码对所述激活码进行加密，得到加密激活码，还可以为：所述云认证服务器根据所述用户名获取对应的移动终端号码，应用所述移动终端号码和所述激活验证码，对所述激活码进行加密，得到加密激活码；

[0078] 所述步骤S6中，所述根据所述激活验证码对所述加密激活码进行解密，得到激活码，还可以为：所述移动终端令牌获取所述移动终端号码，根据所述移动终端号码和所述激活验证码，对所述加密激活码进行解密，得到激活码。

[0079] 所述步骤S3中，所述根据所述激活验证码对所述激活码进行加密，得到加密激活码，还可以为：所述云认证服务器根据所述用户名获取预先保存的移动终端特征数据，应用所述移动终端特征数据和所述激活验证码，对所述激活码进行加密，得到加密激活码；

[0080] 所述步骤S6中，所述根据所述激活验证码对所述加密激活码进行解密，得到激活码，还可以为：所述移动终端令牌获取所述移动终端特征数据，根据所述移动终端特征数据和所述激活验证码，对所述加密激活码进行解密，得到激活码。

[0081] 所述步骤S2中，所述根据所述令牌序列号和所述种子生成因子，生成激活码，还可以为：所述云认证服务器根据所述用户名获取对应的移动终端号码，根据所述令牌序列号、所述种子生成因子和所述移动终端号码生成激活码；

[0082] 所述步骤S7之前还包括：所述移动终端令牌从所述激活码中分解得到移动终端号码，并截取本机移动终端号码，判断所述激活码中的移动终端号码与截取到的移动终端号码是否匹配，如果是，则执行步骤S7，否则提示非本移动终端匹配激活信息，结束。

[0083] 所述步骤S2中，所述根据所述令牌序列号和所述种子生成因子，生成激活码，还可以为：所述云认证服务器根据所述用户名获取对应的移动终端特征数据，根据所述令牌序列号、所述种子生成因子和所述移动终端特征数据生成激活码；

[0084] 所述步骤S7之前还包括：所述移动终端令牌从所述激活码中分解得到移动终端特征数据，并获取本机移动终端特征数据，判断所述激活码中的移动终端特征数据，与获取到的移动终端特征数据是否匹配，如果是，则执行步骤S7，否则提示非本移动终端匹配激活信息，结束。

[0085] 本发明取得的有益效果是：采用本发明的技术方案，能够实现在移动终端处于没有网络离线的情况下，仍能够对移动终端令牌进行激活，应用更加广泛，而且允许对移动终端令牌重新激活，则导入移动终端令牌中的种子密钥也可以不同，且服务器端的种子密钥和导入移动终端令牌的种子密钥均为加密存储，保证种子的正确性，更加增加了移动终端令牌的安全性。

附图说明

[0086] 为了更清楚的说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单的介绍，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他的附图。

[0087] 图1是本发明实施例1提供的一种激活移动终端令牌的方法中激活过程流程图；

[0088] 图2和图3是本发明实施例2提供的一种激活移动终端令牌的方法中激活过程流程图；

[0089] 图4是本发明实施例2提供的一种激活移动终端令牌的方法中口令首次认证流程图。

具体实施方式

[0090] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动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。

[0091] 本发明实施例提供了一种激活移动终端令牌的方法，包括激活过程和口令首次验证过程，应用于包括终端和服务器的系统中，其中，服务器包括云认证管理平台和云认证服务器，终端包括客户端和移动终端，其中，客户端为能接收邮件的设备，包括主机PC或平板电脑等，其中，移动终端可以为手机、平板等设备，移动终端令牌为手机中的应用程序。

[0092] 本发明的激活过程是由云认证管理平台的管理员触发激活，口令首次验证是由客户端的用户触发验证完成。

[0093] 实施例1

[0094] 本发明实施例1提供了一种激活移动终端令牌的方法，应用于包括云认证管理平台、云认证服务器、客户端和移动终端令牌组成的系统中，如图1所示，包括：

[0095] 步骤S1：所述云认证服务器接收来自所述云认证管理平台的激活请求，为所述激活请求中的用户名分配令牌序列号，并生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存；

[0096] 步骤S2：所述云认证服务器根据所述令牌序列号和所述种子生成因子，生成激活码；

[0097] 步骤S3：所述云认证服务器生成激活验证码，将所述激活验证码发送给对应的移动终端，并根据所述激活验证码对所述激活码进行加密，得到加密激活码，将所述加密激活码发送给所述云认证管理平台；

[0098] 步骤S4：所述云认证管理平台根据所述加密激活码生成二维码图片，将所述二维码图片发送给所述客户端；

[0099] 步骤S5：所述客户端显示所述二维码图片；

[0100] 步骤S6：当所述移动终端令牌获取到所述二维码图片和所述激活验证码后，解析所述二维码图片，得到加密激活码，根据所述激活验证码对所述加密激活码进行解密，得到激活码；

[0101] 步骤S7：所述移动终端令牌从所述激活码中获取所述种子生成因子和所述令牌序列号，将所述令牌序列号保存；

[0102] 步骤S8：所述移动终端令牌根据所述种子生成因子得到令牌种子密钥并保存；

[0103] 本实施例中，服务器种子密钥和令牌种子密钥可以为加密存储或直接存储；

[0104] 本实施例中，步骤S8之后，还包括：

[0105] 步骤T1：所述移动终端令牌根据所述令牌种子密钥生成动态口令，显示所述动态口令；

[0106] 步骤T2：所述客户端接收用户输入的用户名和所述动态口令，将所述用户名和所述动态口令发送给所述云认证服务器；

[0107] 步骤T3：所述云认证服务器根据所述用户名获取对应的服务器种子密钥，根据所述服务器种子密钥生成动态口令，判断生成的动态口令与接收到的动态口令是否匹配，如果是，则向所述客户端返回认证成功响应，结束；否则向所述客户端返回认证失败响应，结束。

[0108] 实施例2

[0109] 本发明实施例2提供了一种激活移动终端令牌的方法，包括激活过程和首次认证过程，如图2和图3所示，包括：

[0110] 本实施例中，激活过程应用于包括云认证管理平台、客户端、云认证服务器和移动终端令牌组成的系统中，预先在云认证管理平台中注册有多组用户记录(包括用户名、移动终端号码、邮箱账号等)所述激活过程具体包括：

[0111] 步骤101：云认证管理平台等待接收管理员选择的需要激活的用户记录；

[0112] 本实施例中，步骤101之前还包括：

[0113] A：云认证管理平台将验证密码失败次数置为初值0；

[0114] B：云认证管理平台等待接收管理员输入管理员账号和密码；

[0115] C：云认证管理平台判断接收到的管理员输入的管理员账号和密码是否正确，如果是，则执行101，否则执行D；

[0116] D：云认证管理平台更新验证密码失败次数，判断更新后的验证密码失败次数是否达到预设次数，如果是，则报错，锁定云认证管理平台，否则返回步骤B；

[0117] 进一步的，管理员认证方式可预先进行配置，即可采用验证账号密码方式，也可配置为双因素认证；

[0118] 其中，双因素认证过程为：先进行账号密码验证，当账号密码匹配时，显示获取短信口令按钮和短信口令输入框，当管理员点击获取短信口令按钮后，等待管理员输入短信口令，当接收到短信口令后，判断短信口令是否正确，如果是，则登录成功，执行步骤101，否则累计短信口令验证次数，当达到预设次数(优选为10次)时，暂时锁定云认证管理平台，间隔预设时长(优选为30分钟)自动解锁；

[0119] 步骤102：云认证管理平台根据用户记录，判断是否能够获取对应的移动终端号码、邮箱账号、用户名，如果是，则执行步骤103，否则提示信息不完整，结束；

[0120] 本实施例中，用户记录包括用户名、移动终端号码、邮箱账号等；

[0121] 例如，云认证管理平台接收到管理员选择的用户记录为：

[0122] 用户名：abc

[0123] 用户邮箱：123456789@126.com

[0124] 移动终端号码：18912345678

[0125] 其中，云认证管理平台根据获取到的移动终端号码可判定该用户名已绑定移动终端令牌；

[0126] 步骤103：云认证管理平台根据用户记录中的用户名，生成激活请求；

[0127] 本步骤之前还包括：云认证管理平台接收管理员点击的激活按钮，云认证管理平台获取上次激活时间，判断当前系统时间与上次激活时间之差是否大于预设时长，如果是，则允许再次激活，执行步骤103，否则返回已激活响应，结束；

[0128] 其中，如果允许再次激活，则云认证管理平台根据用户记录中的用户名，另外还有预设重新激活标识，共同生成激活请求；如果为首次激活，则只根据用户名生成激活请求；

[0129] 步骤104：云认证管理平台将激活请求发送给云认证服务器；

[0130] 步骤105：云认证服务器接收到激活请求后，获取激活请求中的用户名；

[0131] 本实施例中，认证服务器存储区中保存的数据包括：一一对应的用户名、激活标识、移动终端号码、移动终端特征数据、加密种子密钥、令牌序列号和企业密钥等；

[0132] 步骤106：云认证服务器根据用户名获取服务器存储区中保存的激活标识，判断激活标识，如果是已激活，则执行步骤107，如果是激活未确认，则获取服务器存储区中保存的对应的激活码，执行步骤113，如果是未激活，则执行步骤108；

[0133] 优选的，当激活标识为0时，标识未激活，当激活标识为1时，标识激活未确认，当激活标识为2时，标识已激活；

[0134] 本实施例中，本步骤之前还包括：云认证服务器判断是否能够获取到预设重新激活标识，如果是，则不需要再重新生成令牌序列号，获取激活请求中的用户名，然后执行步骤109，否则执行步骤106；

[0135] 步骤107：云认证服务器向云认证管理平台发送已激活响应，结束；

[0136] 步骤108：云认证服务器根据令牌序列号生成方法，产生一个令牌序列号，将令牌序列号与用户名建立关联并保存至服务器存储区中；

[0137] 本实施例中，优选的，OTP云认证中心根据令牌序列号的生成顺序，生成一个长度为10位的令牌序列号；

[0138] 其中，优选的，所述令牌序列号生成方法，具体为：根据令牌序列号的生成顺序，按照从0000000001开始每次增加1的顺序产生一个令牌序列号，例如，已激活的令牌序列号为1000000000，则本次生成的令牌序列号为1000000001；

[0139] 步骤109：云认证服务器调用随机数生成函数，生成第一随机数，将该第一随机数作为种子生成因子；

[0140] 本实施例中，优选的，OTP云认证中心调用随机数生成函数，Random.nextInt(10)，生成长度为10位十进制的第一随机数，作为种子生成因子；

[0141] 例如，云认证服务器生成的第一随机数，即种子生成因子为6595781253；

[0142] 步骤110：云认证服务器应用预设推导算法，对种子生成因子进行推导，得到服务器种子密钥；

[0143] 本实施例中，优选的，OTP云认证中心应用PBKDF2推导算法，得到20个字节的服务器种子密钥，除此之外，还可以为BF推导算法等；

[0144] 例如，OTP云认证中心生成的第一随机数，即种子生成因子为6595781253，对种子生成因子进行推导，得到的服务器种子密钥为FB80ECDA5EDF464CF7715EE66A25ED079122D429；

[0145] 步骤111：云认证服务器根据用户名获取对应的企业密钥，应用企业密钥对服务器种子密钥进行加密，得到加密服务器种子密钥，将加密服务器种子密钥与用户名建立关联

并保存至服务器存储区中；

[0146] 具体为：OTP云认证中心根据令牌序列号，使用预设加密算法对服务器种子密钥进行加密，得到二进制的加密服务器种子密钥，然后对二进制的加密服务器种子密钥进行Base64转换，得到字符串，优选的，预设加密算法为3DES算法，除此之外，还可以为DES、RSA算法等；

[0147] 例如，OTP云认证中心获取到的企业密钥为1F3D4E3A12459372B8371931779137 82，应用企业密钥对服务器种子密钥加密且转换后得到的加密服务器种子密钥为PL96EUSWSdPP2gj8fr6m-YXBpLWE0OTJjN2Q3LmR1b3N1Y3VyaXR5LmNvbQ；

[0148] 本步骤之前，还包括：

[0149] 步骤1：密钥运维平台接收密钥持有者的管理员密钥；

[0150] 其中，为保证管理员密钥的安全性，密钥持有者的管理员密钥需要定期更换；

[0151] 步骤2：密钥运维平台对管理员密钥进行预设运算，得到主密钥，将主密钥保存至存储区中；

[0152] 步骤3：云认证服务器定时向密钥运维平台获取主密钥，判断获取到的主密钥与服务器存储区中保存的主密钥是否相同，如果是，则执行步骤4，否则更新服务器存储区中的主密钥，执行步骤4；

[0153] 本实施例中，由于管理员密钥需要定期更换，因此优选的，云认证服务器每隔2分钟向密钥运维平台发送获取主密钥的请求，接收密钥运维平台返回的当前主密钥；

[0154] 步骤4：云认证服务器根据用户名获取对应的企业ID，对主密钥和企业ID进行散列运算，得到企业密钥，将企业密钥保存至服务器存储区中；

[0155] 其中，企业ID是在管理员注册时，云认证管理平台为该企业随机分配的企业ID，并与多个用户名建立关联并保存至服务器存储区中；

[0156] 本实施例中，由于服务器种子密钥是使用企业ID进行加密的，因此当某个服务器种子密钥被破解时，其他企业的服务器种子密钥也不能够被同时破解，安全性更佳；

[0157] 步骤112：云认证服务器根据令牌序列号和种子生成因子，应用预设组成方式，生成激活码，将激活码与用户名建立关联并保存至服务器存储区中，并将激活标识置为激活未确认；

[0158] 本实施例中，根据令牌序列号和种子生成因子，应用预设激活码组成方式生成激活码，具体为：将令牌序列号和种子生成因子进行预设拼接组合，得到激活码；

[0159] 优选的，应用预设组成方式生成的激活码是由25位数字组成：

[0160] 其中，令牌序列号和种子生成因子进行预设拼接组合，得到激活码，具体为：

[0161] 1：判断移动终端令牌是否需要接收短信验证码，如果需要，则将所述激活码的第一位数据置为1，如果不需要，则将所述激活码的第一位数据设置为0；

[0162] 2：判断口令生成算法，如果是第一预设算法，则将所述激活码的第二位数据设置为1，如果是第二预设算法，则将所述激活码的第二位数据设置为0；

[0163] 3：将所述激活码的第三位至第十二位数据设置为所述种子生成因子；

[0164] 4：将所述激活码的第十三位至第二十二位数据设置为所述令牌序列号；

[0165] 5：对所述种子生成因子进行校验，得到第一校验值，将所述激活码的第二十三位数据设置为所述第一校验值；

[0166] 6:对所述激活码的前二十三位进行校验计算,得到第二校验值,将所述激活码的第二十四位数据设置为所述第二校验值;

[0167] 7:将所述激活码的第二十五位数据作为预设填充位,设置为0;

[0168] 例如,根据令牌序列号和种子生成因子,应用预设激活码组成方式生成的25位的激活码为1165957812531000000001350;

[0169] 除此之外,本实施例中,应用预设组成方法生成激活码,还可以为:

[0170] 其中,第一位标识移动终端令牌激活是否需要短信验证码,如果需要,则将第一位置为1,如果不需要,则将第一位置为0;

[0171] 第二位标识动态口令产生算法,如果使用SM3算法,则将第二位置为0,如果是国际AUTH算法,则将第二位置为1;

[0172] 第三位至第十二位为种子生成因子;

[0173] 第十三位至第二十二位为令牌序列号;

[0174] 第二十三位至第二十八位为移动终端号码后六位,或者获取移动终端特征数据,获取移动终端特征数据的预设长度的数据,设置激活码的第二十三位至第二十八位;

[0175] 第二十九位为对种子生成因子进行校验计算得到的校验值;

[0176] 第三十位为对前二十九位进行校验计算得到的校验值;

[0177] 第三十一位为预留填充位,设置为0;

[0178] 步骤113:云认证服务器调用随机数生成算法,生成第二随机数,将该第二随机数作为激活验证码;

[0179] 优选的,OTP云认证中心调用随机数生成算法Random.nextInt(6),随机生成6位十进制数据作为激活验证码;

[0180] 例如,OTP云认证中心生成的6位第二随机数,即激活验证码为551896;

[0181] 步骤114:云认证服务器根据激活验证码,应用预设加密算法,对激活码进行加密,得到加密激活码;

[0182] 本实施例中,OTP云认证中心应用激活验证码对激活码进行置换,得到乱序的加密激活码,优选的,预设加密算法为3DES算法,除此之外,还可以为DES、RSA算法等;

[0183] 本步骤,优选的,还可以为:云认证服务器根据用户名获取对应的移动终端号码,应用移动终端号码的后六位和激活验证码对激活码进行加密,得到加密激活码;

[0184] 进一步的,除此之外,还可以为:预先在云认证管理平台注册用户时需要用户输入移动终端特征数据(如蓝牙mac地址、默认随机数或移动终端内部版本号等);则本步骤还可以为:云认证服务器获取移动终端特征数据,应用移动终端特征数据和激活验证码对激活码进行加密,得到加密激活码;

[0185] 例如,OTP云认证中心应用3DES算法对激活码进行加密,得到的加密激活码为25310000000001116595781350;

[0186] 步骤115:云认证服务器根据用户名获取对应的移动终端号码;

[0187] 步骤116:云认证服务器将激活验证码以短信形式发送至移动终端号码对应的移动终端上,并将加密激活码发送给云认证管理平台;

[0188] 步骤117:云认证管理平台根据接收到的加密激活码生成二维码图片;

[0189] 具体的,云认证管理平台根据加密激活码调用二维码图片生成函数,生成二维码

图片；

[0190] 步骤118：云认证管理平台从用户记录中获取对应的邮箱账号，根据邮箱账号将二维码图片和加密激活码通过邮件方式发送至客户端的邮件平台；

[0191] 步骤119：客户端接收到邮件后，显示邮件中的二维码图片和加密激活码；

[0192] 本实施例中，由于有些用户的移动终端不具备扫描二维码功能，为解决此类问题，提供了由用户直接输入加密激活码的激活方式；

[0193] 步骤120：移动终端令牌等待接收用户扫描二维码图片或等待用户输入加密激活码；

[0194] 当移动终端令牌接收到用户扫描的二维码图片时，解析二维码图片得到加密激活码，执行步骤121；

[0195] 具体的，移动终端令牌调用解析二维码图片函数，得到加密激活码253100000000011116595781350；

[0196] 当移动终端令牌接收到用户输入的加密激活码时，执行步骤121；

[0197] 具体的，移动终端令牌接收用户输入的加密激活码253100000000011116595781350；

[0198] 步骤121：移动终端令牌接收用户输入的激活验证码；

[0199] 具体的，移动终端令牌接收用户输入的激活验证码551896；

[0200] 步骤122：移动终端令牌根据激活验证码，应用预设解密算法对加密激活码进行解密，得到激活码；

[0201] 本实施例中，移动终端令牌应用激活验证码对激活码进行反置换，得到激活码，优选的，预设加密算法为3DES算法，除此之外，还可以为DES、RSA算法等；

[0202] 本步骤还可以为：移动终端令牌根据激活验证码和移动终端号码后六位，对加密激活码进行解密，判断是否能够解密成功，如果是，则解密得到激活码，否则提示本移动终端非匹配激活移动终端信息，结束；

[0203] 进一步的，除此之外，本步骤还可以为：移动终端令牌获取移动终端特征数据，应用移动终端特征数据和激活验证码对加密激活码进行解密，判断是否能够解密成功，如果是，则解密得到激活码，否则提示本移动终端非匹配激活移动终端信息，结束；

[0204] 本实施例中，在二维码图片的生成过程中加入了移动终端号码和/或移动终端特征数据，能够使得一个二维码图片只能够被一个移动终端扫描得到种子密钥，其他移动终端不能使用，增加了离线激活的安全性；

[0205] 例如，移动终端令牌根据激活验证码551896，应用3DES算法对加密激活码进行解密，得到的激活码为116595781253100000000001350；

[0206] 步骤123：移动终端令牌根据预设组成方式，从激活码中分解得到种子生成因子和令牌序列号，将令牌序列号保存；

[0207] 本实施例中，移动终端令牌根据预设激活码组成方式，从激活码中分解得到种子生成因子，具体为：从激活码中获取第三位至第十二位的数据，即为种子生成因子；从激活码中获取第十三位至第二十二位的数据，即为令牌序列号；

[0208] 例如，移动终端令牌根据预设激活码组成方式，从激活码中分解得到的种子生成因子为6595781253；从激活码中分解得到的令牌序列号为1000000001；

[0209] 本实施例中，步骤124之前还可以包括：从激活码中获取第二十三位至第二十八位

的数据，并获取本机移动终端号码，判断激活码中第二十三位至第二十八位的数据与移动终端号码的后六位是否匹配，如果是，则执行步骤124，否则提示本移动终端非匹配激活移动终端信息，结束；

[0210] 或者，从激活码中获取第二十三位至第二十八位的数据，并获取本机移动终端特征数据，判断激活码中第二十三位至第二十八位的数据和本机特征数据是否匹配，如果是，则执行步骤124，否则提示本移动终端非匹配激活移动终端信息，结束；

[0211] 步骤124：移动终端令牌应用预设推导算法对种子生成因子进行推导，得到令牌种子密钥；

[0212] 优选的，移动终端令牌应用PBKDF2推导算法，得到20个字节的令牌种子密钥，除此之外，还可以为BF推导算法等；

[0213] 例如，移动终端令牌对种子生成因子进行推导，得到的令牌种子密钥为FB80ECDA5EDF464CF7715EE66A25ED079122D429；

[0214] 步骤125：移动终端令牌应用令牌序列号对令牌种子密钥进行加密，得到加密令牌种子密钥，将加密令牌种子密钥和令牌序列号保存至令牌存储区中；

[0215] 优选的，所述口令生成算法为OATH时间型算法，除此之外还可以为国密时间型算法SM3算法等；

[0216] 例如，移动终端令牌根据令牌种子密钥，应用OATH时间型算法，生成6位的动态口令651255；

[0217] 如图4所示，本实施例中，口令首次验证过程应用于包括云认证服务器、客户端和移动终端令牌组成的系统中，所述方法包括：当客户端启动某个需要验证动态口令的应用时，客户端显示输入用户名、密码和动态口令框，执行以下操作：

[0218] 步骤201：当移动终端令牌启动时，获取内部保存的令牌序列号和加密令牌种子密钥；

[0219] 例如，移动终端令牌获取到的令牌序列号为1000000001，加密种子密钥为PL96EUSWSdPP2gj8fr6m-YXBpLWE0OTJjN2Q3LmR1b3N1Y3VyaXR5LmNvbQ；

[0220] 步骤202：移动终端令牌根据令牌序列号，应用预设解密算法对加密令牌种子密钥进行解密，得到令牌种子密钥；

[0221] 具体为：移动终端令牌根据令牌序列号，使用预设解密算法对加密令牌种子密钥进行解密，得到令牌种子密钥，然后对令牌种子密钥进行Base64转换，得到字符串，优选的，预设解密算法为3DES算法，除此之外，还可以为DES、RSA算法等；

[0222] 例如，移动终端令牌根据令牌序列号对加密激活码解密得到的令牌种子密钥为FB80ECDA5EDF464CF7715EE66A25ED079122D429；

[0223] 步骤203：移动终端令牌根据令牌种子密钥，应用口令生成算法，生成动态口令，显示动态口令；

[0224] 例如，移动终端令牌根据令牌种子密钥FB80ECDA5EDF464CF7715EE66A25ED079122D429和口令生成算法SM3算法，生成动态口令569145；

[0225] 步骤204：客户端等待接收用户输入用户名、密码和动态口令；

[0226] 例如，客户端接收到的用户名为ft，密码为123，动态口令为569145；

[0227] 步骤205：客户端判断接收到的用户名和密码是否正确，如果是，则执行步骤206，否则报错，结束；

[0228] 其中，当客户端验证用户名和密码不正确时，还包括：判断验证用户名和密码是否达到预设次数(优选为3次)，如果是，则锁定客户端应用，否则返回步骤204；

[0229] 步骤206：客户端将用户名和接收到的动态口令发送给云认证服务器；

[0230] 例如，客户端将用户名ft和动态口令569145发送给云认证服务器；

[0231] 步骤207：云认证服务器根据用户名获取对应的加密服务器种子密钥和企业密钥；

[0232] 例如，云认证服务器根据用户名ft获取到对应的加密种子服务器密钥为PL96EUSWSdPP2gj8fr6m-YXBpLWE0OTJjN2Q3LmR1b3NlY3VyaXR5LmNvbQ，获取到的企业密钥为1F3D4E3A12459372B837193177913782；

[0233] 步骤208：云认证服务器根据企业密钥，应用预设解密算法对加密服务器种子密钥进行解密，得到服务器种子密钥；

[0234] 其中，优选的，预设解密算法为3DES算法，除此之外，还可以为DES、RSA算法等；

[0235] 例如，云认证服务器应用企业密钥对加密服务器种子密钥进行解密，得到服务器种子密钥为FB80ECDA5EDF464CF7715EE66A25ED 079122D429；

[0236] 步骤209：云认证服务器根据服务器种子密钥，应用口令生成算法，生成动态口令；

[0237] 例如，云认证服务器根据服务器种子密钥，生成的动态口令窗口中包括动态口令569145；

[0238] 步骤210：云认证服务器判断生成的动态口令与接收到的动态口令是否匹配，如果是，则执行步骤211，否则向所述客户端返回认证失败响应，结束；

[0239] 本步骤中，当云认证服务器向客户端返回口令错误响应后，客户端显示口令错误，如果客户端接收到用户输入的口令错误次数达到预设值时，提示用户联系管理员重新激活；

[0240] 步骤211：云认证服务器将激活标识置为已激活，并向客户端返回激活成功响应，结束；

[0241] 本步骤中，当云认证服务器向客户端返回激活成功响应后，客户端显示激活成功信息。

[0242] 以上所述，仅为本发明较佳的具体实施方式，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公开的技术范围内，可轻易想到的变化或替换，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该以权利要求的保护范围为准。

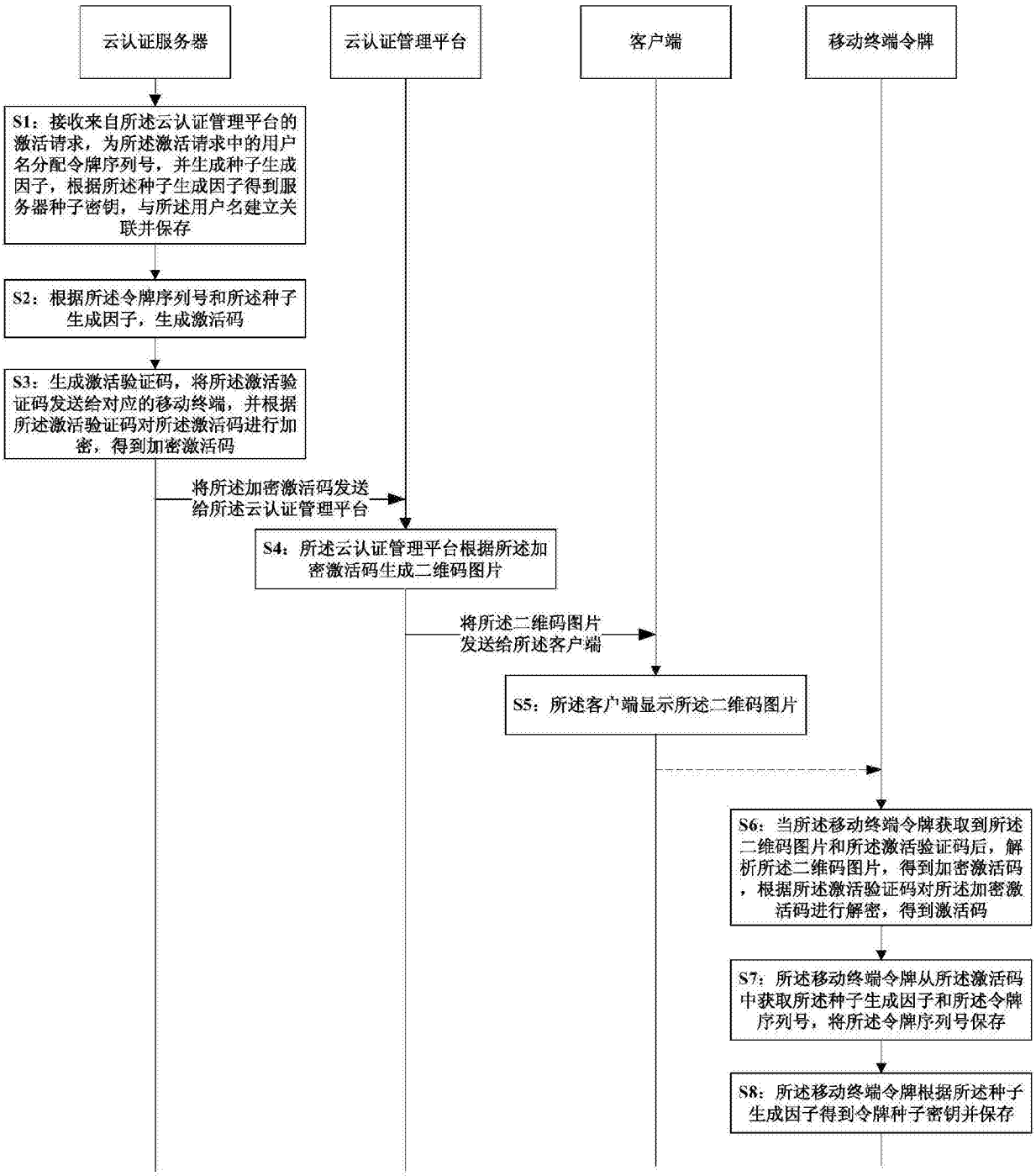

云认证服务器
云认证管理平台
客户端
移动终端令牌
S1：接收来自所述云认证管理平台的激活请求，为所述激活请求中的用户名分配令牌序列号，并生成种子生成因子，根据所述种子生成因子得到服务器种子密钥，与所述用户名建立关联并保存
S2：根据所述令牌序列号和所述种子生成因子，生成激活码
S3：生成激活验证码，将所述激活验证码发送给对应的移动终端，并根据所述激活验证码对所述激活码进行加密，得到加密激活码
将所述加密激活码发送给所述云认证管理平台
S4：所述云认证管理平台根据所述加密激活码生成二维码图片
将所述二维码图片发送给所述客户端
S5：所述客户端显示所述二维码图片
S6：当所述移动终端令牌获取到所述二维码图片和所述激活验证码后，解析所述二维码图片，得到加密激活码，根据所述激活验证码对所述加密激活码进行解密，得到激活码
S7：所述移动终端令牌从所述激活码中获取所述种子生成因子和所述令牌序列号，将所述令牌序列号保存
S8：所述移动终端令牌根据所述种子生成因子得到令牌种子密钥并保存

图1

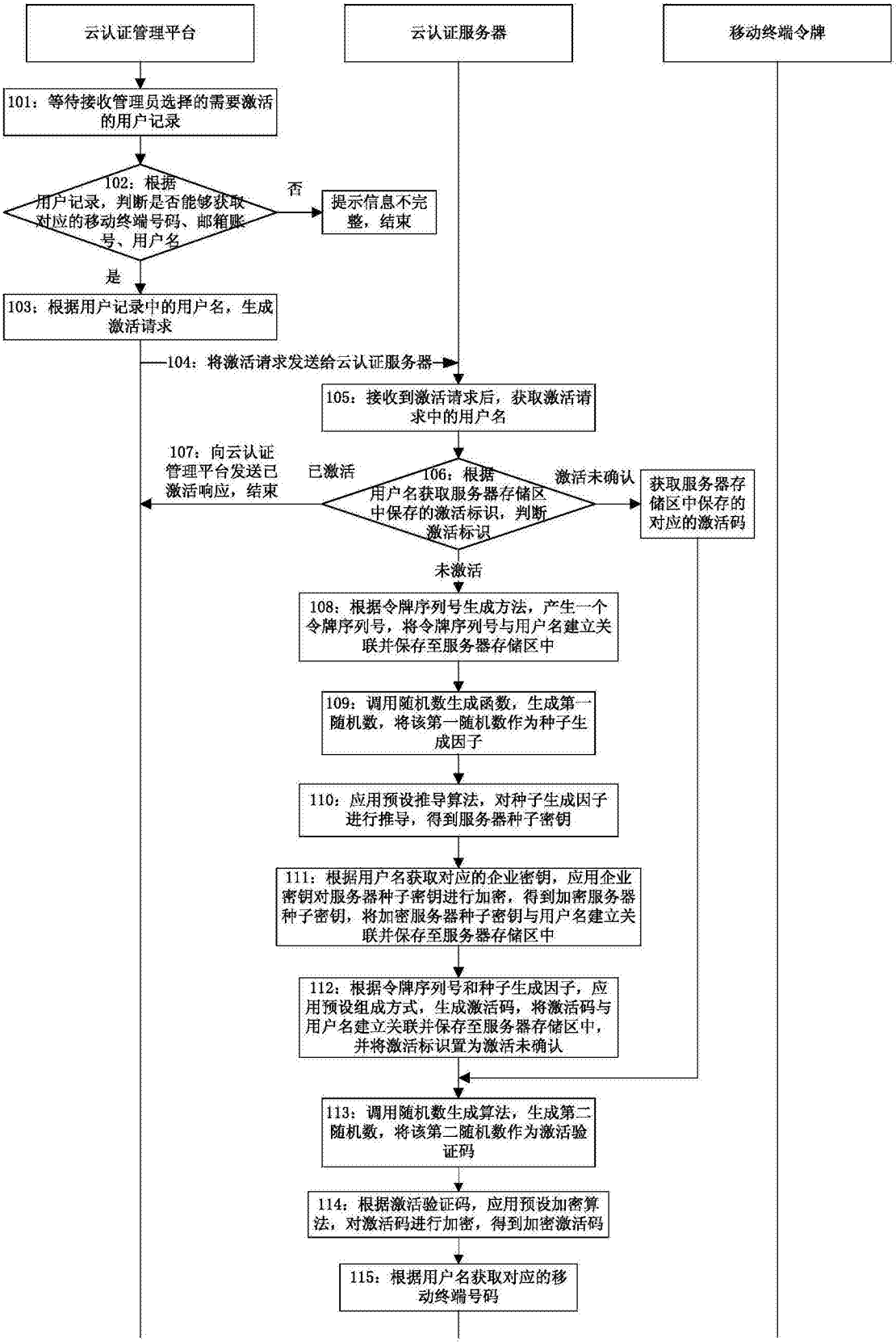

云认证管理平台
云认证服务器
移动终端令牌
101：等待接收管理员选择的需要激活的用户记录
102：根据用户记录，判断是否能够获取对应的移动终端号码、邮箱账号、用户名
否
提示信息不完整，结束
是
103：根据用户记录中的用户名，生成激活请求
104：将激活请求发送给云认证服务器
105：接收到激活请求后，获取激活请求中的用户名
106：根据用户名获取服务器存储区中保存的激活标识，判断激活标识
已激活
107：向云认证管理平台发送已激活响应，结束
激活未确认
获取服务器存储区中保存的对应的激活码
未激活
108：根据令牌序列号生成方法，产生一个令牌序列号，将令牌序列号与用户名建立关联并保存至服务器存储区中
109：调用随机数生成函数，生成第一随机数，将该第一随机数作为种子生成因子
110：应用预设推导算法，对种子生成因子进行推导，得到服务器种子密钥
111：根据用户名获取对应的企业密钥，应用企业密钥对服务器种子密钥进行加密，得到加密服务器种子密钥，将加密服务器种子密钥与用户名建立关联并保存至服务器存储区中
112：根据令牌序列号和种子生成因子，应用预设组成方式，生成激活码，将激活码与用户名建立关联并保存至服务器存储区中，并将激活标识置为激活未确认
113：调用随机数生成算法，生成第二随机数，将该第二随机数作为激活验证码
114：根据激活验证码，应用预设加密算法，对激活码进行加密，得到加密激活码
115：根据用户名获取对应的移动终端号码

图2

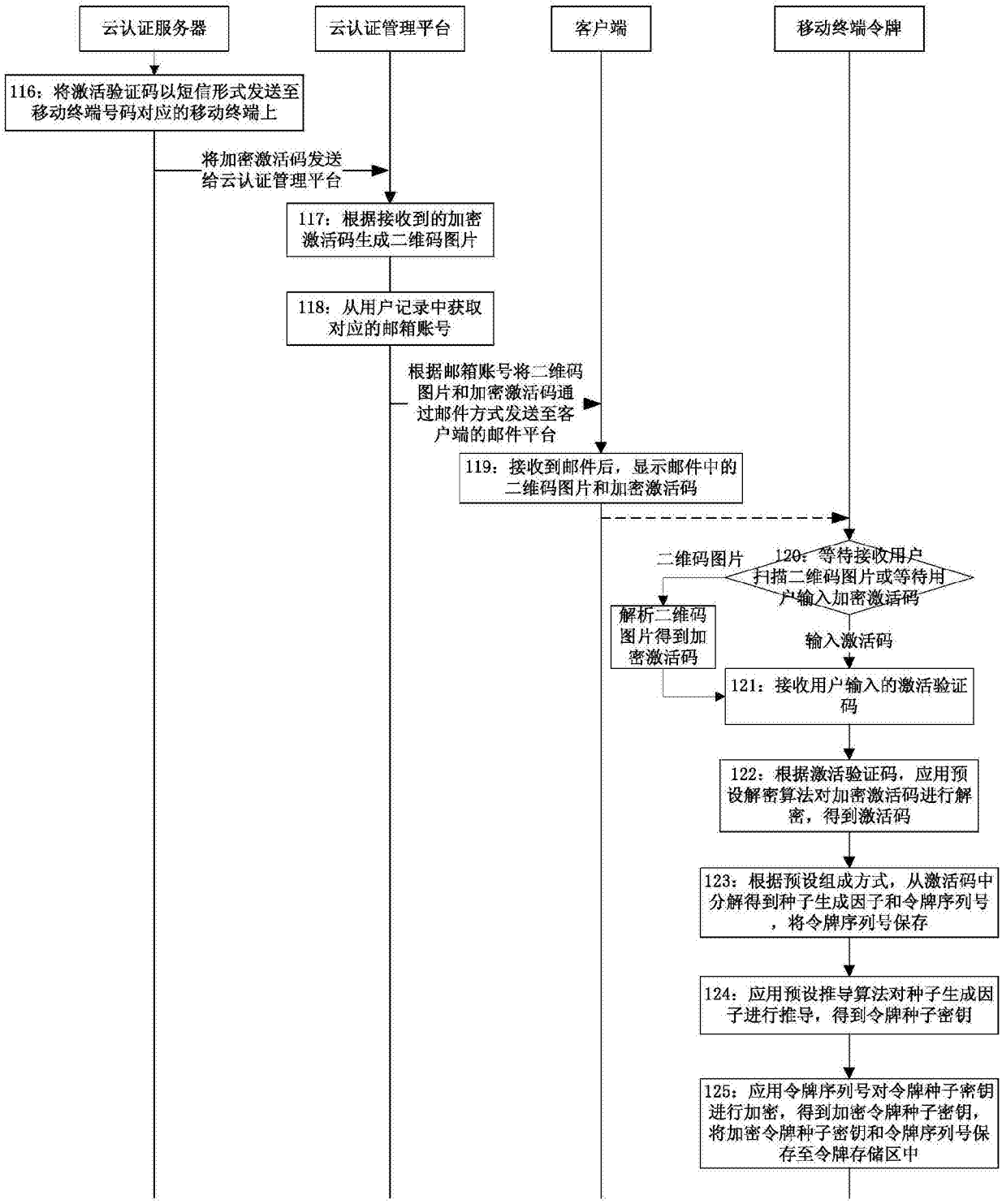

云认证服务器
云认证管理平台
客户端
移动终端令牌
116：将激活验证码以短信形式发送至移动终端号码对应的移动终端上
将加密激活码发送给云认证管理平台
117：根据接收到的加密激活码生成二维码图片
118：从用户记录中获取对应的邮箱账号
根据邮箱账号将二维码图片和加密激活码通过邮件方式发送至客户端的邮件平台
119：接收到邮件后，显示邮件中的二维码图片和加密激活码
二维码图片
120：等待接收用户扫描二维码图片或等待用户输入加密激活码
解析二维码图片得到加密激活码
输入激活码
121：接收用户输入的激活验证码
122：根据激活验证码，应用预设解密算法对加密激活码进行解密，得到激活码
123：根据预设组成方式，从激活码中分解得到种子生成因子和令牌序列号，将令牌序列号保存
124：应用预设推导算法对种子生成因子进行推导，得到令牌种子密钥
125：应用令牌序列号对令牌种子密钥进行加密，得到加密令牌种子密钥，将加密令牌种子密钥和令牌序列号保存至令牌存储区中

图3

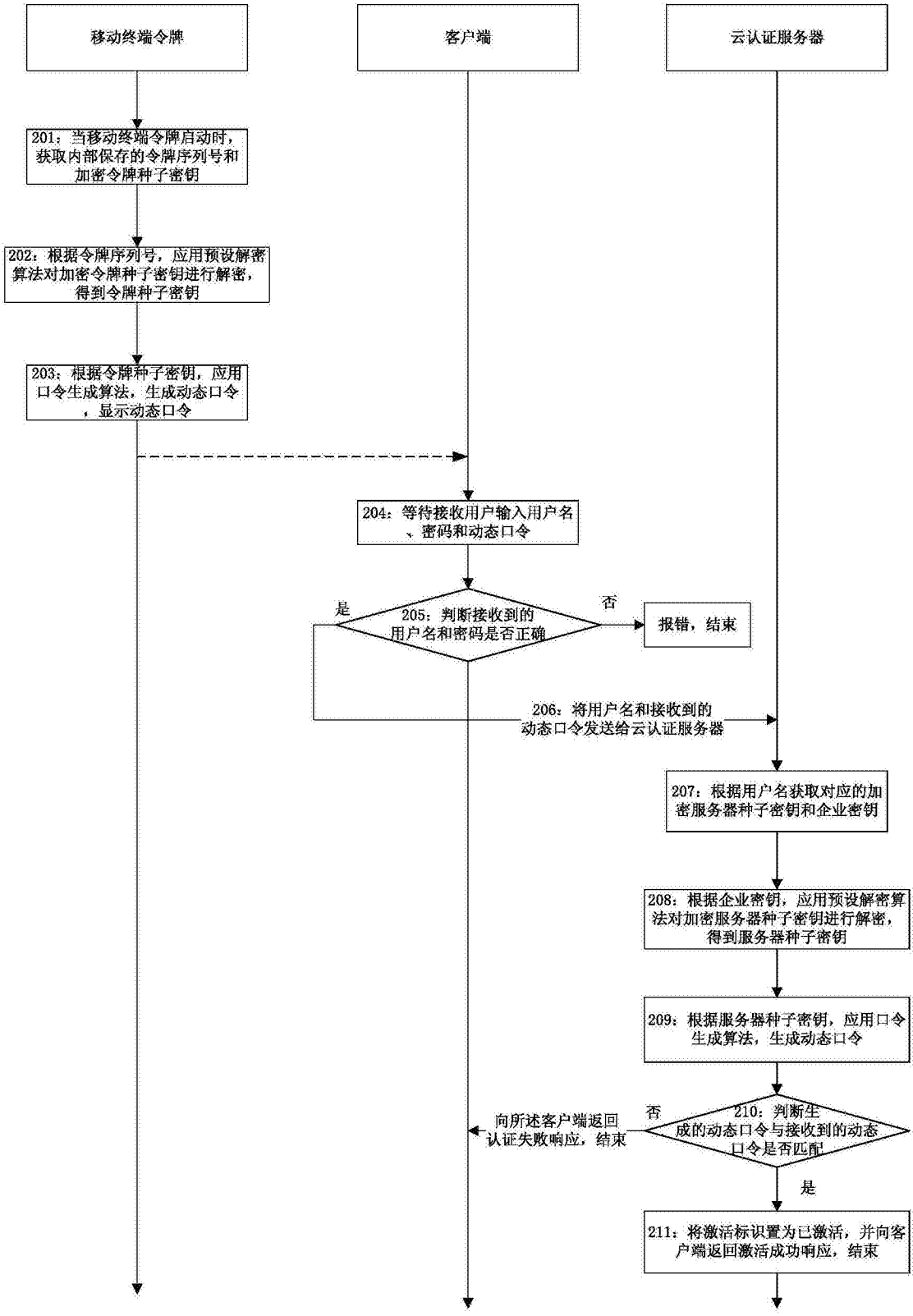

移动终端令牌
客户端
云认证服务器
201：当移动终端令牌启动时，获取内部保存的令牌序列号和加密令牌种子密钥
202：根据令牌序列号，应用预设解密算法对加密令牌种子密钥进行解密，得到令牌种子密钥
203：根据令牌种子密钥，应用口令生成算法，生成动态口令，显示动态口令
204：等待接收用户输入用户名、密码和动态口令
是
205：判断接收到的用户名和密码是否正确
否
报错，结束
206：将用户名和接收到的动态口令发送给云认证服务器
207：根据用户名获取对应的加密服务器种子密钥和企业密钥
208：根据企业密钥，应用预设解密算法对加密服务器种子密钥进行解密，得到服务器种子密钥
209：根据服务器种子密钥，应用口令生成算法，生成动态口令
否
210：判断生成的动态口令与接收到的动态口令是否匹配
向所述客户端返回认证失败响应，结束
是
211：将激活标识置为已激活，并向客户端返回激活成功响应，结束

图4