(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 104660416 B
(45)授权公告日 2018.08.28

(21)申请号 201510077143.7

(22)申请日 2015.02.13

(65)同一申请的已公布的文献号
申请公布号 CN 104660416 A

(43)申请公布日 2015.05.27

(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 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 102780674 A,2012.11.14,
CN 102780674 A,2012.11.14,
CN 102611793 A,2012.07.25,
CN 204103934 U,2015.01.14,
EP 1679578 A1,2006.07.12,
CN 103663088 A,2014.06.26,

审查员 何花

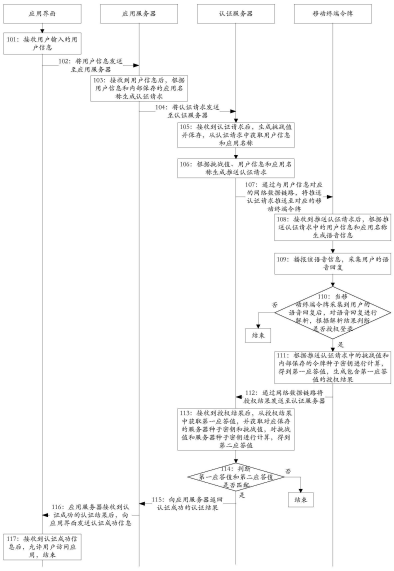
权利要求书6页 说明书14页 附图8页

(54)发明名称

一种语音认证系统和设备的工作方法

(57)摘要

本发明公开一种语音认证系统和设备的工作方法，属于信息安全领域，所述方法包括：应用服务器将应用界面发送来的用户信息和保存的应用名称发送至认证服务器，认证服务器根据生成的挑战值、用户信息和应用名称生成推送认证请求发送至移动终端令牌，移动终端令牌根据推送认证请求生成语音信息，采集用户的语音回复，根据语音回复判定能授权登录时，根据挑战值生成第一应答值并发送至认证服务器，认证服务器根据挑战值生成第二应答值，当两个应答值相同时，返回认证成功。采用本发明的技术方案，通过语音的方式告知用户认证信息，语音信息由挑战值生成，防止由于用户失误导致的点击错误，方便提醒用户当前信息，避免认证延时，增加了安全性。



CN 104660416 B

1.一种语音认证系统的工作方法，应用于包括应用界面、应用服务器、认证服务器和移动终端令牌组成的系统中，其特征在于，当用户访问应用时，所述方法包括：

步骤S1：所述应用界面接收用户输入的用户信息，将所述用户信息发送至所述应用服务器；

步骤S2：所述应用服务器接收到所述用户信息后，根据所述用户信息和内部保存的应用名称生成认证请求，将所述认证请求发送至所述认证服务器；

步骤S3：所述认证服务器接收到所述认证请求后，生成挑战值并保存，从所述认证请求中获取用户信息和应用名称；

步骤S4：所述认证服务器根据所述挑战值、所述用户信息和所述应用名称生成推送认证请求，通过与所述用户信息对应的网络数据链路，将所述推送认证请求推送至对应的移动终端令牌；

步骤S5：所述移动终端令牌接收到所述推送认证请求后，根据所述推送认证请求中的用户信息和应用名称生成语音信息；

步骤S6：所述移动终端令牌播报所述语音信息，采集用户的语音回复；

步骤S7：当所述移动终端令牌采集到用户的语音回复后，根据所述语音回复判断是否授权登录，如果是，则执行步骤S8，否则结束；

步骤S8：所述移动终端令牌根据所述推送认证请求中的挑战值和内部保存的令牌种子密钥进行计算，得到第一应答值，生成包含所述第一应答值的授权结果，通过所述网络数据链路将所述授权结果发送至所述认证服务器；

步骤S9：所述认证服务器接收到所述授权结果后，从所述授权结果中获取第一应答值，并获取保存的服务器种子密钥和挑战值，对所述挑战值和所述服务器种子密钥进行计算，得到第二应答值；

步骤S10：所述认证服务器判断所述第一应答值和所述第二应答值是否匹配，是则向所述应用服务器返回认证成功的认证结果，执行步骤S11，否则向所述应用服务器返回认证失败的认证结果，执行步骤S11；

步骤S11：所述应用服务器判断接收到的认证结果，如果是认证成功，则允许用户访问所述应用，如果是认证失败，则禁止用户访问所述应用；

所述步骤S1，具体包括：所述应用界面接收用户输入的用户信息，并接收用户对认证类型的选择，当用户选择语音认证类型时，将所述用户信息和语音认证类型发送至应用服务器；

所述步骤S2，具体为：所述应用服务器根据所述语音认证类型、所述用户信息和内部保存的应用标识生成认证请求，将所述认证请求发送至所述认证服务器；

所述步骤S4，具体为：所述认证服务器根据所述认证请求中的语音认证类型，将认证类型设置为预设语音认证类型，根据所述预设语音认证类型、所述挑战值、所述用户信息和所述应用名称生成推送认证请求；

所述步骤S5中，所述接收到所述推送认证请求后，还包括：所述移动终端令牌从所述推送认证请求中获取认证类型，判断所述认证类型是否为预设语音认证类型，如果是，则继续，否则报错，结束。

2.根据权利要求1所述的方法，其特征在于，所述步骤S7中，所述根据所述语音回复判

断是否授权登录，具体为：所述移动终端令牌判断所述语音回复是否为预设授权登录信息，如果是，则执行步骤S8，否则结束。

3.根据权利要求1所述的方法，其特征在于，所述步骤S5至步骤S7，具体包括：

步骤a1：所述移动终端令牌从所述推送认证请求中获取挑战值、用户信息和应用名称；

步骤a2：所述移动终端令牌根据所述挑战值、所述用户信息和所述应用名称生成语音信息，播报所述语音信息，采集用户的语音回复；

步骤a3：当所述移动终端令牌采集到用户的语音回复后，判断所述语音回复与所述挑战值是否匹配，如果是，则授权登录，执行步骤S8，否则结束。

4.根据权利要求3所述的方法，其特征在于，所述判断所述语音回复与所述挑战值是否匹配，具体为：判断所述语音回复与所述挑战值是否相同，如果是，则授权登录，执行步骤S8，否则结束。

5.根据权利要求3所述的方法，其特征在于，所述根据所述挑战值、所述用户信息和所述应用名称生成语音信息，具体为：根据预设格式对所述挑战值、所述用户信息和所述应用名称进行组合，得到语音信息。

6.根据权利要求3所述的方法，其特征在于，

所述步骤a2，具体包括：所述移动终端令牌获取所述挑战值的预设位上的数据，将其作为第一匹配数据，根据所述第一匹配数据、所述用户信息和所述应用名称生成语音信息，播报所述语音信息，采集用户的语音回复；

所述步骤a3中，所述判断所述语音回复与所述挑战值是否匹配，具体为：判断所述语音回复与所述第一匹配数据是否相同，如果是，则授权登录，执行步骤S8，否则结束。

7.根据权利要求6所述的方法，其特征在于，所述根据所述第一匹配数据、所述用户信息和所述应用名称生成语音信息，具体为：根据预设格式对所述第一匹配数据、所述用户信息和所述应用名称进行组合，得到语音信息。

8.根据权利要求6所述的方法，其特征在于，所述步骤S7中，所述根据所述语音回复判断是否授权登录，具体包括：

步骤b1：所述移动终端令牌对所述语音回复进行解析，得到解析结果，判断所述解析结果中是否存在与所述第一匹配数据相同的第一数据，如果是，则执行步骤b2，否则结束；

步骤b2：所述移动终端令牌判断在所述解析结果中的所述第一数据之前和所述第一数据之后是否存在预设字符，如果是，则执行步骤S8，否则结束。

9.根据权利要求3所述的方法，其特征在于，

所述步骤a2，具体包括：所述移动终端令牌对所述挑战值进行预设计算，生成第二匹配数据，根据所述第二匹配数据、所述用户信息和所述应用名称生成语音信息，播报所述语音信息，采集用户的语音回复；

所述步骤a3中，所述判断所述语音回复与所述挑战值是否匹配，具体为：判断所述语音回复与所述第二匹配数据是否相同，如果是，则授权登录，执行步骤S8，否则结束。

10.根据权利要求9所述的方法，其特征在于，所述根据所述第二匹配数据、所述用户信息和所述应用名称生成语音信息，具体为：根据预设格式对所述第二匹配数据、所述用户信息和所述应用名称进行组合，得到语音信息。

11.根据权利要求9所述的方法，其特征在于，所述步骤S7中，所述根据所述语音回复判

断是否授权登录，具体包括：

步骤c1：所述移动终端令牌对所述语音回复进行解析，得到解析结果，判断所述解析结果中是否存在与所述第二匹配数据相同的第二数据，如果是，则执行步骤c2，否则结束；

步骤c2：所述移动终端令牌判断在所述解析结果中的所述第二数据之前和所述第二数据之后是否存在预设字符，如果是，则执行步骤S8，否则结束。

12.根据权利要求1所述的方法，其特征在于，所述步骤S7，具体为：

步骤S7-1：所述移动终端令牌每隔预设时长监听采集到的用户的语音回复，判断采集到的用户的语音回复的长度是否发生变化，如果是，则执行步骤S7-2，否则执行步骤S7-3；

步骤S7-2：所述移动终端令牌对采集到的用户的语音回复进行解析，得到解析结果，根据解析结果判断是否授权登录，如果是，则执行步骤S8，否则执行步骤S7-3；

步骤S7-3：所述移动终端令牌判断录音时间是否达到预设时长，如果是，则输出语音回复不正确的提示信息，结束，否则返回步骤S7-1。

13.根据权利要求1所述的方法，其特征在于，

所述步骤S6之前还包括：所述移动终端令牌将语音播报错误次数置为初值；

所述步骤S7，还包括：

步骤d1：所述移动终端令牌判断在预设时间内是否接收到用户的语音回复，如果是，则对所述语音回复进行解析，否则执行步骤d2；

步骤d2：所述移动终端令牌判断所述语音播报错误次数是否达到预设次数，如果是，则结束，否则更新所述语音播报错误次数，返回步骤S6。

14.根据权利要求1所述的方法，其特征在于，所述步骤S5中，所述移动终端令牌接收到所述推送认证请求后，还包括：从推送认证请求中获取认证类型，判断所述认证类型，如果是预设语音认证类型，则继续，否则执行相应类型的认证。

15.根据权利要求1所述的方法，其特征在于，所述方法还包括：当移动终端令牌启动时，根据内部保存的访问地址，访问所述认证服务器，建立所述移动终端令牌与所述认证服务器之间的网络数据链路。

16.根据权利要求1所述的方法，其特征在于，所述步骤S3中，所述生成挑战值，具体为：所述认证服务器调用随机数生成函数，生成随机数，将所述随机数作为挑战值；或者，所述认证服务器根据所述认证请求中的用户信息获取对应保存的服务器种子密钥，对所述服务器种子密钥进行计算，得到挑战值。

17.根据权利要求1所述的方法，其特征在于，

所述步骤S2中，所述根据用户信息和内部保存的应用名称生成认证请求，替换为：所述应用服务器根据用户信息和内部保存的应用标识生成认证请求；

所述步骤S3中，所述从所述认证请求中获取用户信息和应用名称，具体为：从所述认证请求中获取应用标识，根据所述应用标识获取对应的应用名称。

18.根据权利要求1所述的方法，其特征在于，

所述步骤S4中，所述根据所述挑战值、所述用户信息和所述应用名称生成推送认证请求，具体包括：所述认证服务器生成认证请求ID，与所述用户信息建立关联并保存，根据所述挑战值、所述用户信息、所述应用名称和所述认证请求ID生成推送认证请求；

所述步骤S8中，所述生成包含所述第一应答值的授权结果，具体包括：生成包含所述第

一应答值、所述认证请求ID的授权结果；

所述步骤S9之前还包括：所述认证服务器从所述授权结果中获取认证请求ID，并获取保存的认证请求ID，判断所述授权结果中的认证请求ID与保存的认证请求ID是否相同，如果是，则执行步骤S9，否则将所述保存的认证请求ID删除，结束。

19.根据权利要求18所述的方法，其特征在于，

所述步骤S4还包括：所述认证服务器获取当前服务器时间，将其作为认证请求ID生成时间并保存；

所述步骤S9之前还包括：所述认证服务器获取保存的认证请求ID生成时间并获取接收到授权结果时的服务器时间，判断该服务器时间与所述认证请求ID生成时间之差是否在预设时间内，如果是，则所述认证请求ID有效，执行步骤S9，否则将所述保存的认证请求ID删除，结束。

20.一种语音认证系统中认证服务器的工作方法，其特征在于，包括：

步骤T1：认证服务器接收到来自应用服务器的认证请求后，生成挑战值并保存，从所述认证请求中获取用户信息、应用标识和语音认证类型；

步骤T2：所述认证服务器根据所述用户信息查找对应的网络数据链路，并根据所述应用标识获取对应的应用名称；

步骤T3：所述认证服务器根据所述语音认证类型，将认证类型设置为预设语音认证类型，根据所述预设语音认证类型、所述挑战值、所述用户信息和所述应用名称生成推送认证请求，并通过所述网络数据链路推送至对应的移动终端令牌；所述推送认证请求用于所述移动终端令牌根据所述推送认证请求中的信息生成语音信息，播报所述语音信息，播报完成后，开启录音采集用户的语音回复并进行解析；

步骤T4：所述认证服务器接收到所述移动终端返回的授权结果，从所述授权结果中获取第一应答值，并获取对应保存的服务器种子密钥和挑战值，对所述挑战值和所述服务器种子密钥进行计算，得到第二应答值；

步骤T5：所述认证服务器判断所述第一应答值和所述第二应答值是否匹配，是则向所述应用服务器返回认证成功的认证结果，结束，否则向所述应用服务器返回认证失败的认证结果，结束。

21.根据权利要求20所述的方法，其特征在于，

所述步骤T2，还包括：所述认证服务器根据所述用户信息获取对应的令牌信息；

所述步骤T3，具体包括：所述认证服务器根据所述挑战值、所述令牌信息、所述用户信息和所述应用名称生成推送认证请求，并通过所述网络数据链路将所述推送认证请求推送至移动终端令牌。

22.根据权利要求21所述的方法，其特征在于，所述令牌信息包括令牌序列号；

所述将所述推送认证请求推送至移动终端令牌，具体为：所述认证服务器根据所述令牌序列号获取对应的移动终端令牌，将所述推送认证请求推送至所述移动终端令牌。

23.根据权利要求21所述的方法，其特征在于，所述令牌信息包括令牌标识码；

所述根据所述挑战值、所述令牌信息、所述用户信息和所述应用名称生成推送认证请求，具体包括：所述认证服务器应用所述令牌标识码对所述挑战值进行加密，得到挑战值密文，根据所述挑战值密文、所述令牌信息、所述用户信息和所述应用名称生成推送认证请

求。

24.根据权利要求20所述的方法，其特征在于，所述步骤T1中，所述生成挑战值，具体为：所述认证服务器调用随机数生成函数，生成随机数，将所述随机数作为挑战值；或者，所述认证服务器根据所述认证请求中的用户信息获取对应保存的服务器种子密钥，对所述服务器种子密钥进行计算，得到挑战值。

25.根据权利要求20所述的方法，其特征在于，所述步骤T4中，所述对所述挑战值和所述服务器种子密钥进行计算，得到第二应答值，具体包括：所述认证服务器获取服务器当前时间，应用预设口令生成算法，对所述服务器当前时间、所述挑战值、所述服务器种子密钥和动态因子进行计算，得到第二应答值。

26.根据权利要求20所述的方法，其特征在于，所述步骤T2中，所述根据所述用户信息查找对应的网络数据链路，具体包括：所述认证服务器判断根据所述用户信息是否能够查找到对应的网络数据链路，如果是，则查找得到对应的网络数据链路，否则向所述应用服务器返回错误响应，结束。

27.一种语音认证系统中移动终端令牌的工作方法，其特征在于，包括：

步骤K1：移动终端令牌接收来自认证服务器的推送认证请求；

步骤K2：所述移动终端令牌从所述推送认证请求中获取用户信息和应用名称，根据所述用户信息和所述应用名称生成语音信息；

步骤K3：所述移动终端令牌播报所述语音信息，采集用户的语音回复；

步骤K4：当所述移动终端令牌采集到用户的语音回复后，根据所述语音回复判断是否授权登录，如果是，则执行步骤K5，否则结束；

步骤K5：所述移动终端令牌根据所述推送认证请求中的挑战值和内部保存的令牌种子密钥进行计算，得到第一应答值，生成包含所述第一应答值的授权结果，通过网络数据链路将所述授权结果发送至所述认证服务器，令牌操作结束；

所述步骤K1中，所述移动终端令牌接收到所述推送认证请求后，还包括：所述移动终端令牌从所述推送认证请求中获取认证类型，判断所述认证类型是否为预设语音认证类型，如果是，则继续，否则报错，结束。

28.根据权利要求27所述的方法，其特征在于，所述步骤K4中，所述根据所述语音回复判断是否授权登录，具体为：所述移动终端令牌判断所述语音回复是否为预设授权登录信息，如果是，则关闭录音，执行步骤K5，否则结束。

29.根据权利要求27所述的方法，其特征在于，所述步骤K2至步骤K4，具体包括：

步骤a1：所述移动终端令牌从所述推送认证请求中获取挑战值、用户信息和应用名称；

步骤a2：所述移动终端令牌根据所述挑战值、所述用户信息和所述应用名称生成语音信息，播报所述语音信息，采集用户的语音回复；

步骤a3：当所述移动终端令牌采集到用户的语音回复后，根据所述语音回复判断是否授权登录，如果是，则授权登录，执行步骤K5，否则结束。

30.根据权利要求29所述的方法，其特征在于，所述判断所述语音回复与所述挑战值是否匹配，具体为：判断所述语音回复与所述挑战值是否相同，如果是，则授权登录，执行步骤K5，否则结束。

31.根据权利要求29所述的方法，其特征在于，

所述步骤a2，具体包括：所述移动终端令牌获取所述挑战值的预设位上的数据，将其作为第一匹配数据，根据所述第一匹配数据、所述用户信息和所述应用名称生成语音信息，播报所述语音信息，采集用户的语音回复；

所述步骤a3中，所述判断所述语音回复与所述挑战值是否匹配，具体为：判断所述语音回复与所述第一匹配数据是否匹配，如果是，则授权登录，执行步骤K5，否则结束。

32.根据权利要求31所述的方法，其特征在于，所述步骤K4中，所述根据所述语音回复判断是否授权登录，具体包括：

步骤b1：所述移动终端令牌对所述语音回复进行解析，得到解析结果，判断所述解析结果中是否存在与所述第一匹配数据相同的第一数据，如果是，则执行步骤b2，否则结束；

步骤b2：所述移动终端令牌判断在所述解析结果中的所述第一数据之前和所述第一数据之后是否存在预设字符，如果是，则执行步骤K5，否则结束。

33.根据权利要求29所述的方法，其特征在于，

所述步骤a2，具体包括：所述移动终端令牌从所述推送认证请求中获取挑战值，对所述挑战值进行预设计算，生成第二匹配数据，根据所述第二匹配数据、所述用户信息和所述应用名称生成语音信息，播报所述语音信息，采集用户的语音回复；

所述步骤a3中，所述判断所述语音回复与所述挑战值是否匹配，具体为：判断所述语音回复与所述第二匹配数据是否匹配，如果是，则授权登录，执行步骤K5，否则结束。

34.根据权利要求33所述的方法，其特征在于，所述步骤K4中，所述根据所述语音回复判断是否授权登录，具体包括：

步骤c1：所述移动终端令牌对所述语音回复进行解析，得到解析结果，判断所述解析结果中是否存在与所述第二匹配数据相同的第二数据，如果是，则执行步骤c2，否则结束；

步骤c2：所述移动终端令牌判断在所述解析结果中的所述第二数据之前和所述第二数据之后是否存在预设字符，如果是，则执行步骤K5，否则结束。

35.根据权利要求27所述的方法，其特征在于，所述步骤K4，具体为：

步骤K4-1：所述移动终端令牌每隔预设时长监听采集到的用户的语音回复，判断采集到的语音回复的长度是否发生变化，如果是，则执行步骤K4-2，否则执行步骤K4-3；

步骤K4-2：所述移动终端令牌对采集到的语音回复进行解析，得到解析结果，根据解析结果判断是否授权登录，如果是，则执行步骤K5，否则执行步骤K4-3；

步骤K4-3：所述移动终端令牌判断录音时间是否达到预设时长，如果是，则输出语音回复不正确的提示信息，结束，否则返回步骤K4-1。

36.根据权利要求27所述的方法，其特征在于，所述方法还包括：当移动终端令牌启动时，根据内部保存的访问地址，访问所述认证服务器，建立所述移动终端令牌与所述认证服务器之间的网络数据链路。

一种语音认证系统和设备的工作方法

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种语音认证系统和设备的工作方法。

背景技术

[0002] 移动终端令牌，全称动态密码移动设备(包括手机、pad等)令牌，是用来生成动态口令的移动设备客户端软件，移动终端令牌是由运行在移动设备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] 现有技术在认证过程中，当消息推送至移动终端令牌时，令牌通过显示的方式告知用户，接收用户触发选项按钮，这种方式可能存在由于用户失误导致点击错误，如果刚好是黑客登录应用时，造成无法弥补的损失，安全性较低，且通过显示的方式通知用户，不能引起用户重视，导致用户未及时响应信息，造成认证过程的延时。

发明内容

[0004] 为解决现有技术中提供的问题，本发明提供了一种语音认证系统和设备的工作方法。

[0005] 本发明采用的技术方案是：一种语音认证系统的工作方法，应用于包括应用界面、应用服务器、认证服务器和移动终端令牌组成的系统中，所述方法包括：

[0006] 步骤S1：所述应用界面接收用户输入的用户信息，将所述用户信息发送至所述应用服务器；

[0007] 步骤S2：所述应用服务器接收到所述用户信息后，根据所述用户信息和内部保存的应用名称生成认证请求，将所述认证请求发送至所述认证服务器；

[0008] 步骤S3：所述认证服务器接收到所述认证请求后，生成挑战值并保存，从所述认证请求中获取用户信息和应用名称；

[0009] 步骤S4：所述认证服务器根据所述挑战值、所述用户信息和所述应用名称生成推送认证请求，通过与所述用户信息对应的网络数据链路，将所述推送认证请求推送至对应的移动终端令牌；

[0010] 步骤S5：所述移动终端令牌接收到所述推送认证请求后，根据所述推送认证请求中的用户信息和应用名称生成语音信息；

[0011] 步骤S6：所述移动终端令牌播报所述语音信息，采集用户的语音回复；

[0012] 步骤S7：当所述移动终端令牌采集到用户的语音回复后，对所述语音回复进行解析，根据解析结果判断是否授权登录，如果是，则执行步骤S8，否则结束；

[0013] 步骤S8：所述移动终端令牌根据所述推送认证请求中的挑战值和内部保存的令牌种子密钥进行计算，得到第一应答值，生成包含所述第一应答值的授权结果，通过所述网络数据链路将所述授权结果发送至所述认证服务器；

[0014] 步骤S9:所述认证服务器接收到所述授权结果后,从所述授权结果中获取第一应答值,并获取保存的服务器种子密钥和挑战值,对所述挑战值和所述服务器种子密钥进行计算,得到第二应答值;

[0015] 步骤S10:所述认证服务器判断所述第一应答值和所述第二应答值是否匹配,是则向所述应用服务器返回认证成功的认证结果,执行步骤S11,否则结束;

[0016] 步骤S11:所述应用服务器接收到所述认证成功的认证结果后,向所述应用界面发送认证成功信息;

[0017] 步骤S12:所述应用界面接收到所述认证成功信息后,允许用户访问应用,结束。

[0018] 一种语音认证系统中认证服务器的工作方法,包括:

[0019] 步骤T1:所述认证服务器接收到来自应用服务器的认证请求后,生成挑战值并保存,从所述认证请求中获取用户信息和应用标识;

[0020] 步骤T2:所述认证服务器根据所述用户信息获取对应的网络数据链路,并根据所述应用标识获取对应的应用名称;

[0021] 步骤T3:所述认证服务器根据所述挑战值、所述用户信息和所述应用名称生成推送认证请求,并通过所述网络数据链路推送至对应的移动终端令牌;

[0022] 步骤T4:所述认证服务器接收到所述移动终端返回的授权结果,从所述授权结果中获取第一应答值,并获取对应保存的服务器种子密钥和挑战值,对所述挑战值和所述服务器种子密钥进行计算,得到第二应答值;

[0023] 步骤T5:所述认证服务器判断所述第一应答值和所述第二应答值是否匹配,是则向所述应用服务器返回认证成功的认证结果,结束,否则向所述应用服务器返回认证失败的认证结果,结束。

[0024] 一种语音认证系统中移动终端令牌的工作方法,包括:

[0025] 步骤K1:所述移动终端令牌接收来自认证服务器的推送认证请求;

[0026] 步骤K2:所述移动终端令牌从所述推送认证请求中获取用户信息和应用名称,根据所述用户信息和所述应用名称生成语音信息;

[0027] 步骤K3:所述移动终端令牌播报所述语音信息,采集用户的语音回复;

[0028] 步骤K4:当所述移动终端令牌采集到用户的语音回复后,对所述语音回复进行解析,根据解析结果判断是否授权登录,如果是,则关闭录音,执行步骤K5,否则结束;

[0029] 步骤K5:所述移动终端令牌根据所述推送认证请求中的挑战值和内部保存的令牌种子密钥进行计算,得到第一应答值,生成包含所述第一应答值的授权结果,通过所述网络数据链路将所述授权结果发送至所述认证服务器,令牌操作结束。

[0030] 本发明取得的有益效果是:采用本发明的技术方案,移动终端令牌通过语音的方式告知用户认证信息,且要求用户返回的语音信息是由挑战值生成的,因此可以防止由于用户失误导致的点击错误,而且方便提醒用户当前信息,避免认证延时,且增加了安全性。

附图说明

[0031] 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。

[0032] 图1是本发明实施例1提供的一种语音认证系统的工作方法流程图；

[0033] 图2、图3和图4是本发明实施例2提供的一种语音认证系统的工作方法流程图；

[0034] 图5是本发明实施例2中步骤219至步骤221的细化流程图；

[0035] 图6是本发明实施例2提供的另一种语音认证系统的工作方法流程图；

[0036] 图7是本发明实施例3提供的一种语音认证系统中认证服务器的工作方法流程图；

[0037] 图8是本发明实施例4提供的一种语音认证系统中移动终端令牌的工作方法流程图。

具体实施方式

[0038] 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。

[0039] 本发明中，语音认证系统包括应用界面、应用服务器、认证服务器和移动终端令牌，语音认证设备包括认证服务器和移动终端令牌。

[0040] 本发明中，认证服务器对移动终端令牌激活过程中，建立两者之间的网络数据链路，且在认证服务器中保存有用户信息与网络数据链路的对应关系，之后每次当移动终端令牌启动时，获取内部保存的访问地址，根据访问地址访问认证服务器，重新建立起移动终端令牌与认证服务器之间的网络数据链路(优选为TCP协议的网络数据链路)，移动终端令牌通过该网络数据链路将令牌信息发送至认证服务器，认证服务器接收到令牌信息后，获取服务器存储区中对应保存的令牌信息，若接收到的令牌信息与保存的令牌信息不相同，则更新保存的令牌信息为接收到的令牌信息；

[0041] 其中，令牌信息包括：令牌序列号、令牌标识码、移动终端操作系统；

[0042] 例如，移动终端令牌内部保存的访问地址为api-dfserv.cloudentify.com:1843；

[0043] 移动终端令牌发送至认证服务器的令牌信息为：

[0044] {"tokens":["1000000006","1000000003"],"os":"1",udid":"57987117827971672588""reqtype":"1"}。

[0045] 实施例1

[0046] 本发明实施例1提供了一种语音认证系统的工作方法，应用于包括应用界面、应用服务器、认证服务器和移动终端令牌组成的系统中，如图1所示，包括：

[0047] 步骤101：应用界面接收用户输入的用户信息；

[0048] 其中，用户信息可以为用户名，也可以为用户名和密码，本实施例以用户信息为用户名为例来说明。

[0049] 步骤102：应用界面将用户信息发送至应用服务器。

[0050] 步骤103：应用服务器接收到用户信息后，根据用户信息和内部保存的应用名称生成认证请求。

[0051] 步骤104：应用服务器将认证请求发送至认证服务器。

[0052] 步骤105：认证服务器接收到认证请求后，生成挑战值并保存，从认证请求中获取

用户信息和应用名称；

[0053] 步骤106：认证服务器根据挑战值、用户信息和应用名称生成推送认证请求；

[0054] 步骤107：认证服务器通过与用户信息对应的网络数据链路，将推送认证请求推送至对应的移动终端令牌；

[0055] 步骤108：移动终端令牌接收到推送认证请求后，根据推送认证请求中的用户信息和应用名称生成语音信息；

[0056] 步骤109：移动终端令牌播报该语音信息，采集用户的语音回复；

[0057] 本步骤中，播报语音信息之后还可以包括：开启录音；

[0058] 步骤110：当移动终端令牌采集到用户的语音回复后，对语音回复进行解析，根据解析结果判断是否授权登录，如果是，则执行步骤111，否则结束；

[0059] 本步骤中，判断为是时，还可以包括：关闭录音；

[0060] 本实施例中，根据解析结果判断是否授权登录，具体为：移动终端令牌判断解析结果是否为预设授权登录信息，如果是，则执行步骤108，否则结束；

[0061] 其中，预设授权登录信息可以为“是”、“确认”、“YES”等授权信息。

[0062] 步骤111：移动终端令牌根据推送认证请求中的挑战值和内部保存的令牌种子密钥进行计算，得到第一应答值，生成包含第一应答值的授权结果；

[0063] 步骤112：移动终端令牌通过网络数据链路将授权结果发送至认证服务器；

[0064] 步骤113：认证服务器接收到授权结果后，从授权结果中获取第一应答值，并获取对应保存的服务器种子密钥和挑战值，对挑战值和服务器种子密钥进行计算，得到第二应答值；

[0065] 步骤114：认证服务器判断第一应答值和第二应答值是否匹配，是则执行步骤115，否则结束；

[0066] 步骤115：认证服务器向应用服务器返回认证成功的认证结果；

[0067] 步骤116：应用服务器接收到认证成功的认证结果后，向应用界面发送认证成功信息；

[0068] 步骤117：应用界面接收到认证成功信息后，允许用户访问应用，结束。

[0069] 实施例2

[0070] 本发明实施例2提供一种语音认证的方法，应用于包括应用界面、应用服务器、认证服务器和移动终端令牌组成的系统中，如图2、图3和图4所示，包括：

[0071] 步骤201：应用界面接收用户输入的用户信息，包括用户名和密码；

[0072] 其中，用户信息可以为用户名，也可以为用户名和密码，本实施例以用户信息为用户名和密码为例来说明；

[0073] 例如，用户信息包括：用户名abc@test.com，密码168408afag。

[0074] 步骤202：应用界面将用户名和密码发送至应用服务器。

[0075] 步骤203：应用服务器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，否则执行步骤204；

[0076] 具体包括，应用服务器判断从应用服务器存储区中是否能够获取与接收到的用户名对应的用户信息，如果能够获取到，则判断应用服务器存储区中用户信息中的密码与接收到的密码是否相同，如果是，则用户名和密码正确，否则用户名和密码不正确，执行步骤

204，如果不能够获取到，则向应用界面返回用户名不正确响应。

[0077] 步骤204：应用服务器向应用界面返回用户信息不正确响应。

[0078] 步骤205：应用界面接收到用户信息不正确响应后，输出用户信息不正确的提示信息，结束；

[0079] 本实施例中，步骤205之前还包括：初始化验证次数；本步骤中，当接收到用户信息不正确响应时，还包括：更新验证次数，判断更新后的验证次数是否达到预设次数，如果是，则报错，结束，否则返回步骤201；其中，验证次数的初值为0，更新验证次数优选是将验证次数自加1，预设次数优选为3次；

[0080] 进一步地，本实施例中，应用界面输出用户信息不正确的提示信息之后，还可以包括输出提示重新输入用户信息，等待接收用户输入的用户信息，返回步骤201。

[0081] 步骤206：应用服务器根据用户名和内部保存的应用标识生成认证请求；

[0082] 本步骤还可以包括：应用服务器应用第一预设协商密钥对认证请求进行加密，得到认证请求密文；

[0083] 其中，应用第一预设协商密钥对认证请求进行加密，具体为：应用服务器根据预设加密算法，使用第一预设协商密钥对认证请求进行加密；优选的，预设加密算法为DES算法，除此之外还可以为RSA算法等；

[0084] 例如，应用界面为WEBSDK登录界面，对应的应用标识为yiwnzh-ajg。

[0085] 步骤207：应用服务器将认证请求发送至认证服务器；

[0086] 本步骤具体为：应用服务器将认证请求发送至认证代理，认证代理接收到认证请求后，将认证请求转发至认证服务器；

[0087] 还可以为：应用服务器将认证请求密文发送至认证代理，认证代理接收到认证请求密文后，将认证请求密文转发至认证服务器。

[0088] 步骤208：认证服务器接收到认证请求后，获取认证请求中的用户名和应用标识；

[0089] 本步骤还可以为：认证服务器接收到认证请求密文后，根据第一预设协商密钥对认证请求密文进行解密，得到认证请求，获取认证请求中的用户名和应用标识；

[0090] 其中，根据第一预设协商密钥对认证请求密文进行解密，具体为：认证服务器根据预设解密算法，使用第一预设协商密钥对认证请求密文进行解密；优选的，预设解密算法为DES算法，除此之外还可以为RSA算法等。

[0091] 步骤209：认证服务器根据用户名从服务器存储区中获取对应的令牌信息，并查找与用户名对应的网络数据链路；

[0092] 本实施例中，认证服务器从认证请求中获取用户名之后，还包括：判断从服务器存储区中是否能够找到与用户名对应的用户记录，如果是，则继续，否则向应用服务器返回用户未注册信息；

[0093] 本实施例中，服务器存储区中保存的用户记录包括：用户名、服务器种子密钥、应用名称和令牌信息，其中，令牌信息包括令牌标识码、令牌序列号、移动终端操作系统。

[0094] 步骤210：认证服务器根据应用标识，从服务器存储区中获取对应的应用名称；

[0095] 本步骤还包括：判断从服务器存储区中是否能够找到与应用标识对应的应用名称，如果是，则继续，否则向应用服务器返回应用未注册信息；

[0096] 步骤211：认证服务器生成预设长度的挑战值，与用户信息建立关联并保存至服务

器存储区中；

[0097] 优选的，预设长度为6位十进制数据；

[0098] 本实施例中，生成挑战值可以为调用随机数生成函数生成随机数，将随机数作为挑战值，也可以为：根据用户名从服务器存储区中获取对应的服务器种子密钥，对服务器种子密钥进行计算，生成挑战值；

[0099] 其中，对服务器种子密钥进行计算，生成挑战值，具体为：应用预设算法对服务器种子密钥进行计算，生成长度为6位的十进制的挑战值，优选的，预设算法为SM3算法，还可以为OATH算法等；

[0100] 例如，生成的挑战值为308962；

[0101] 本实施例中，步骤209、步骤210和步骤211无先后顺序，可同时执行。

[0102] 步骤212：认证服务器获取服务器时间，根据服务器时间、挑战值、用户信息和应用名称生成推送认证请求；

[0103] 其中，根据服务器时间、挑战值、用户信息和应用名称生成推送认证请求，具体包括：根据服务器时间、挑战值、令牌信息、用户信息和应用名称生成推送认证请求；

[0104] 本步骤还可以为：认证服务器从服务器存储区中获取令牌标识码，应用令牌标识码对挑战值进行加密，得到挑战值密文，根据服务器时间、挑战值密文、用户信息和应用名称生成推送认证请求；

[0105] 本步骤还可以包括：认证服务器应用第二预设协商密钥对推送认证请求进行加密，得到推送认证请求密文；

[0106] 其中，应用第二预设协商密钥对推送认证请求进行加密，具体为：根据预设加密算法，使用第二预设协商密钥对推送认证请求进行加密；优选的，预设加密算法为DES算法，除此之外还可以为RSA算法等；

[0107] 本步骤之前还包括：认证服务器调用随机数生成函数，生成第一随机数，将第一随机数作为认证请求ID，与用户信息建立关联并保存至服务器存储区中；

[0108] 进一步的，还包括：认证服务器获取当前服务器时间，将当前服务器时间作为认证请求ID的生成时间保存至服务器存储区中；

[0109] 例如，认证服务器生成的认证请求ID为：

[0110] 02c0e8b4-be19-49f6-aab6-273b38522cea；

[0111] 认证请求ID的生成时间为1419325026；

[0112] 根据服务器时间、挑战值、用户信息和应用名称生成推送认证请求，具体为：根据服务器时间、挑战值、用户信息、应用名称和认证请求ID生成推送认证请求；

[0113] 例如，生成的推送认证请求为：

[0114] {"appname":"WEBSDK","challenge":"308962","pushtype":"2","reqid":"02c0e8b4-be19-49f6-aab6-273b38522cea","time":"1419325027","token":"1000000003","userid":"abc@test.com"}；其中，当pushtype为2时，表示认证类型为预设语音认证类型；

[0115] 加密后得到的推送认证请求密文为：

[0116] {"data":"a539f8d217b3c05cb5a5340c7b8c8842bcfcace3180c6da9f595015a087c1612e39110fc2e75debc3e435e974a2d7907fa50df880b26ce9ecf1ed4988c9b1c5ad3d00d494

2efcd06f83df5624b35769c00f770fd2bb4ada37e0b9c1ac74513ef1e83fc519cb88a66651a875e7423ed4ff7aa546c07bc96251683d617ec8cf03f007f3287352646ee92edcfd08dced63cd916018ea7596a3b2ccd44f958a6e2245a6dc863230d1940333430703a798eef″,″mac″:″3531e1c344107efd1bee06dac2c15f9f71467a3f″}。

[0117] 步骤213:认证服务器根据令牌信息中的令牌序列号查找对应的移动终端令牌;

[0118] 具体的,认证服务器根据用户名获取对应的令牌序列号,根据令牌序列号获取到对应的网络数据链路,根据网络数据链路查找到对应的移动终端令牌。

[0119] 步骤214:认证服务器通过网络数据链路将推送认证请求推送至该移动终端令牌;

[0120] 本步骤还可以为:认证服务器通过网络数据链路将推送认证请求密文推送至该移动终端令牌。

[0121] 步骤215:移动终端令牌接收到推送认证请求后,从推送认证请求中获取认证类型,判断认证类型,如果是预设语音认证类型,则执行步骤216,否则执行相应类型的认证;

[0122] 本步骤之前还包括:移动终端令牌接收到推送认证密文后,应用第二预设协商密钥对推送认证请求密文进行解密,得到推送认证请求;

[0123] 具体的,应用第二预设协商密钥对推送认证请求密文进行解密,具体为:认证服务器应用预设解密算法,根据第二预设协商密钥对推送认证请求密文进行解密;优选的,预设解密算法为DES算法,除此之外还可以为RSA算法等;

[0124] 优选的,移动终端令牌判断认证类型是否为2,如果是,则认证类型为预设语音认证类型,否则认证类型不为预设语音认证类型;

[0125] 进一步的,需要说明的是,非预设语音认证类型的认证不在本发明的限制范围内。

[0126] 步骤216:移动终端令牌从推送认证请求中获取挑战值,根据挑战值得到挑战值匹配数据并保存;

[0127] 本实施例中,从推送认证请求中获取挑战值,还可以为:移动终端令牌从推送认证请求中获取挑战值密文,并从移动终端令牌中获取令牌标识码,应用令牌标识码对挑战值密文进行解密,得到挑战值;

[0128] 本步骤中,根据挑战值得到挑战值匹配数据,具体包括下述几种情况:

[0129] 1、将挑战值中预设位上的数据作为第一匹配数据,即挑战值匹配数据;

[0130] 例如,挑战值为308962,则获取挑战值中第2、4、6位上的数据092,作为第一匹配数据,即挑战值匹配数据;

[0131] 2、对挑战值进行预设计算,生成第二匹配数据,即挑战值匹配数据;

[0132] 例如,挑战值为308962,则对挑战值进行计算,生成第二匹配数据621,即挑战值匹配数据;

[0133] 3、将挑战值作为挑战值匹配数据;

[0134] 例如,将挑战值308962作为挑战值匹配数据;

[0135] 步骤217:移动终端令牌从推送认证请求中获取用户名和应用名称,根据预设格式对挑战值匹配数据、用户信息和应用名称进行组合,得到语音信息;

[0136] 本实施例中,预设格式为:亲爱的XXX(用户名),您的账号于XXX(令牌当前时间)登录XXX(应用名称),请语音回复XXX(挑战值匹配数据)确认登录,语音回复NO拒绝登录。

[0137] 步骤218:移动终端令牌根据语音信息,调用预设语音系统函数,播报该语音信息,

播报完成后，调用预设录音系统函数，开启录音，采集用户的语音回复；

[0138] 本实施例中，开启录音，具体为：移动终端令牌分配录音存储区，调用操作系统中的录音函数，将录音存储区的首地址传入录音函数中，开启录音，按照预设采样频率和预设采样大小及预设声道，接收录音数据；

[0139] 例如，在Windows操作系统中，通过构造WAVEFORMATEX结构，传入采样频率为44100，采样大小为16位，声道为单声道，调用waveInOpen函数，传入WAVEFORMATEX结构，得到HWAVEIN句柄，构造WAVEHDR结构，传入录音缓存地址，调用waveInPrepareHeader函数，传入WAVEHDR结构准备录音，调用waveInAddBuffer函数，传入WAVEHDR结构通知录音设备录音缓存地址，调用waveInStart函数，传入WAVEIN句柄开始录音；

[0140] 在Android操作系统中，通过构造AudioRecord对象，传入采样频率为44100，采样大小为16位，声道为单声道，调用AudioTrack类的read方法，开始录音；

[0141] 在iOS操作系统中，通过创建QueueState对象，传入采样频率为44100，采样大小为16位，声道为单声道，调用AudioQueueNewInput函数，传入QueueState对象，调用AudioQueueAllocateBuffer函数，分配录音存储区，调用AudioQueueEnqueueBuffer函数，将缓存加入录音队列，调用AudioQueueStart，开始录音；

[0142] 在Windows Phone 7操作系统中，通过创建Microphone对象，传入采样频率为44100，采样大小为16位，声道为单声道，调用Microphone类的Start方法，开始录音。

[0143] 步骤219：移动终端令牌判断在预设时间内是否接收到用户的语音回复，如果是，则执行步骤220，否则超时，结束；

[0144] 优选的，预设时间为30s；

[0145] 本步骤中，进一步的，当移动终端令牌在预设时间内未接收到用户的语音回复时，输出提示超时的提示信息，并向认证服务器返回超时的授权结果，认证服务器接收到超时的授权结果后，向应用服务器返回超时的认证结果，应用服务器接收到超时的认证结果后，将超时的认证结果返回给应用界面，应用界面输出提示超时的提示信息，结束；

[0146] 步骤220：移动终端令牌对接收到的语音回复进行解析，得到解析结果；

[0147] 本实施例中，对数据存储区中的录音数据进行解析，得到解析结果，具体为：将接收到的语音回复进行滤波操作、隔直操作、低通滤波操作、转换操作后，得到解析结果；

[0148] 步骤221：移动终端令牌获取保存的挑战值匹配数据，判断解析结果与挑战值匹配数据是否匹配，如果是，则执行步骤222，否则结束；

[0149] 本实施例中，对应步骤216，则获取保存的挑战值匹配数据，判断解析结果与挑战值匹配数据是否匹配，具体包括以下情况：

[0150] 1、获取保存的第一匹配数据，判断解析结果与第一匹配数据是否匹配，如果是，则解析结果与挑战值匹配数据匹配，授权登录，否则解析结果与挑战值匹配数据不匹配；

[0151] 2、获取保存的第二匹配数据，判断解析结果与第二匹配数据是否匹配，如果是，则解析结果与挑战值匹配数据匹配，授权登录，否则解析结果与挑战值匹配数据不匹配；

[0152] 2、获取保存的挑战值，判断解析结果与挑战值是否匹配，如果是，则解析结果与挑战值匹配数据匹配，授权登录，否则解析结果与挑战值匹配数据不匹配；

[0153] 本步骤中，当移动终端令牌判断解析结果与挑战值匹配数据不相同时，输出语音回复不正确的提示信息，并向认证服务器返回语音回复错误的授权结果，认证服务器接收

到语音回复错误的授权结果后，向应用服务器返回失败的认证结果，应用服务器接收到失败的认证结果后，将失败的认证结果返回给应用界面，应用界面输出认证失败的提示信息，结束；

[0154] 参见图5，本实施例中，步骤219至步骤221，具体包括：

[0155] 步骤a1：移动终端令牌每隔预设时长监听录音存储区中的数据，判断录音存储区中的数据长度是否发生变化，如果是，则执行步骤a2，否则执行步骤a5；

[0156] 本步骤还可以包括：每隔预设时长监听录音存储区中的数据长度，如果长度未发生变化，则更新采集失败次数，返回步骤218，当采集失败次数达到预设次数(优选为2)时，关闭录音，结束；

[0157] 步骤a2：移动终端令牌采集录音存储区中的数据，对录音存储区中的数据进行解析，得到解析结果；

[0158] 例如，得到的解析结果为1230922540；

[0159] 步骤a3：移动终端令牌判断该解析结果中是否存在与挑战值匹配数据相同的匹配数据，如果是，则执行步骤a4，否则执行步骤a5；

[0160] 例如，该解析结果中存在与挑战值匹配数据相同的匹配数据092；

[0161] 步骤a4：移动终端令牌判断在匹配数据之前和匹配数据之后是否存在预设字符，如果是，则执行步骤222，否则执行步骤a5；

[0162] 优选的，预设字符为空格；

[0163] 例如，该解析结果中匹配数据092之前与之后均存在空格；

[0164] 步骤a5：移动终端令牌判断录音时间是否达到预设时长，如果是，则输出语音回复不正确的提示信息，执行步骤218，否则返回步骤a1；

[0165] 优选的，预设时长为30s，如果录音时间达到预设时长，则还可以包括重复播报语音信息，即返回步骤218；

[0166] 进一步的，当移动终端令牌输出语音回复不正确的提示信息后，还可以包括：

[0167] 获取语音回复的错误次数，判断该错误次数是否达到预设值，如果是，则向认证服务器返回语音回复错误的授权信息，否则更新该错误次数，返回继续执行步骤218；相应的，步骤218之前还包括：初始化语音回复的错误次数为0；

[0168] 例如，移动终端令牌得到的解析结果为092，与保存的挑战值匹配数据相同，即接收到用户的语音回复正确；

[0169] 更进一步的，移动终端令牌组织的语音信息中包括播报“如需重复，请语音回复‘重复播报’”，当对接收到的语音回复解析得到的解析结果为“重复播报”时，返回步骤218。

[0170] 步骤222：移动终端令牌从推送认证请求中获取服务器时间，并从令牌存储区中获取保存的令牌种子密钥。

[0171] 步骤223：移动终端令牌应用预设口令生成算法，对挑战值、服务器时间和令牌种子密钥进行计算，生成第一应答值；

[0172] 优选的，本实施例中，移动终端令牌生成预设长度的第一应答值，预设长度优选为6位十进制数据；

[0173] 具体的，移动终端令牌应用预设口令生成算法，对挑战值、服务器时间、令牌种子密钥和动态因子进行计算，生成第一应答值；

[0174] 例如，移动终端令牌生成的第一应答值为677165。

[0175] 步骤224：移动终端令牌生成包含第一应答值的允许登录的授权结果，执行步骤225；

[0176] 本步骤还可以包括：移动终端令牌应用第二预设协商密钥对授权结果进行解密，得到授权结果密文；

[0177] 具体的，生成包含第一应答值的允许登录的授权结果，具体包括：根据第一应答值、令牌信息和认证请求ID生成允许登录的授权结果；

[0178] 例如，移动终端令牌生成的允许登录的授权结果为：

[0179] {"result":"1","time":"1419325027","reqtype":"2","otp":"677165","token":"1000000003","reqid":"02c0e8b4-be19-49f6-aab6-273b38522cea"}；

[0180] 加密得到的授权结果密文为：

[0181] {"data":"4fbd9ef79abbb78b59b7b4364b93db26527dc3a4c0b5dcadd34428de3649fc0f4e07a7f4282b5b88c21500f1b4c8bed324ec80f3815264787ea90a4723e024fb3a4e6cb09b7b44f801c9cc64cd50334fc8f037206d706dfc40727d08a3f67d91174db8396b7574fa1fbc09da25d861d9b945f3c7dc9654455ef0e168eb826f8b8e56a928e274f033079bdfb336848b78","app_version":"2.6","mac":"ba7ab1a123c930ca73ad5944d4fd0cf8ee4f0667"}；

[0182] 本实施例中，如果步骤223中所述动态因子中包含事件型动态因子，则在步骤224执行完毕后，移动终端令牌更新事件型动态因子，优选为将事件型动态因子加1，该事件型动态因子初始值为0。

[0183] 步骤225：移动终端令牌通过网络数据链路将授权结果上送至认证服务器；

[0184] 本步骤还可以包括：移动终端令牌通过网络数据链路将授权结果密文上送至认证服务器。

[0185] 步骤226：认证服务器接收到授权结果后，判断授权结果，如果为允许登录，则执行步骤228，否则执行步骤227；

[0186] 本实施例中，如果判断授权结果中的返回结果为1时，则为允许登录，如果判断授权结果中的返回结果为0时，则为取消登录；

[0187] 本步骤之前还可以包括：认证服务器接收到授权结果密文后，应用第二预设协商密钥对授权结果密文进行解密，得到授权结果；

[0188] 具体的，本步骤之前还包括：认证服务器从授权结果中获取认证请求ID，判断认证请求ID是否正确且有效，如果是，则执行步骤226，否则删除服务器存储区中保存的认证请求ID，并向应用服务器返回失败响应，结束；

[0189] 其中，判断认证请求ID是否正确且有效，具体为：认证服务器从获取服务器当前时间，并从服务器存储区中获取保存的认证请求ID和认证请求ID的生成时间，判断授权结果中的认证请求ID与服务器存储区中保存的认证请求ID是否相同，如果是，则认证请求ID正确，否则认证请求ID不正确；判断服务器当前时间与认证请求ID的生成时间之差是否在预设时长内，如果是，则认证请求ID有效，否则认证请求ID无效，优选的，当认证请求ID不正确或无效时，还包括：删除服务器存储区中保存的认证请求ID和认证请求ID的生成时间。

[0190] 步骤227：认证服务器生成登录失败的认证结果，执行步骤233；

[0191] 本步骤还可以包括：认证服务器应用第一预设协商密钥对认证结果进行加密，得

到认证结果密文。

[0192] 步骤228:认证服务器从授权结果中获取第一应答值;

[0193] 本步骤具体包括:认证服务器从授权结果中获取第一应答值和令牌信息;

[0194] 例如,认证服务器从授权结果中获取到的令牌序列号为1000000003、第一应答值为677165。

[0195] 步骤229:认证服务器根据令牌信息从服务器存储区中获取对应的挑战值和服务器种子密钥,并获取当前服务器时间;

[0196] 例如,认证服务器获取的当前服务器时间为1419325029。

[0197] 步骤230:认证服务器应用口令生成算法,对挑战值、服务器种子密钥和当前服务器时间进行计算,得到第二应答值;

[0198] 具体的:认证服务器应用口令生成算法,对挑战值、服务器种子密钥、当前服务器时间和动态因子进行计算,得到第二应答值;

[0199] 例如,认证服务器生成的第二应答值为677165。

[0200] 步骤231:认证服务器判断第一应答值和第二应答值是否匹配,如果是,则生成认证成功的认证结果,执行步骤233,否则执行步骤232;

[0201] 步骤232:认证服务器生成认证失败的认证结果,执行步骤233;

[0202] 本步骤还可以包括:认证服务器应用第一预设协商密钥对认证结果进行加密,得到认证结果密文;

[0203] 本实施例中,如果步骤230中所述动态因子中包含事件型动态因子,则在步骤232执行完毕后,证服务器更新事件型动态因子,优选为将事件型动态因子加1,该事件型动态因子初始值为0。

[0204] 步骤233:认证服务器将认证结果发送至应用服务器;

[0205] 本步骤还可以包括:认证服务器将认证结果密文发送至认证服务器;

[0206] 本步骤具体为:认证服务器将认证结果发送至认证代理,认证代理接收到认证结果后,将认证结果发送至应用服务器。

[0207] 步骤234:应用服务器接收到认证结果后,将认证结果发送至应用界面;

[0208] 本步骤还可以包括:应用界面将认证结果密文发送至应用界面。

[0209] 步骤235:应用界面接收到认证结果后,判断认证结果,如果是登录失败,则执行步骤236,如果是认证失败,则执行步骤237,如果是认证成功,则执行步骤238;

[0210] 本步骤还可以包括:应用界面接收到认证结果密文后,应用第一预设协商密钥对认证结果密文进行解密,得到认证结果;

[0211] 步骤236:应用界面显示登录失败的提示信息,应用登录认证流程结束;

[0212] 步骤237:应用界面显示认证失败的提示信息,应用登录认证流程结束;

[0213] 步骤238:应用界面允许用户访问应用,并显示应用登录成功后的界面,应用登录认证流程结束;

[0214] 其中,当应用登陆认证流程结束且登陆成功之后,客户端可根据用户输入的操作请求执行相应操作以完成用户对应用的访问,直至用户退出登陆,需要说明的是,应用登陆认证流程结束后的操作不在本发明的限制范围内。

[0215] 本实施例中,步骤201还包括:客户端开启超时定时器,并实时检测超时定时器的

值是否达到预设时长，如果是，则提示认证超时的提示信息，应用登录认证流程结束。

[0216] 如图6所示，本实施例中，步骤201至步骤215还可以为：

[0217] 步骤301：应用界面接收用户输入的用户名和密码，并接收用户对认证类型的选择，当用户选择语音认证类型时，执行步骤302，否则执行其他推送认证，结束；

[0218] 需要说明的是，其他推送认证流程不在本发明限制范围内；

[0219] 步骤302：应用界面将用户信息和语音认证类型发送至应用服务器；

[0220] 步骤303：应用服务器判断接收到的用户名和密码是否正确，如果是，则执行步骤304，否则结束；

[0221] 步骤304：应用服务器根据用户名、语音认证类型和内部保存的应用标识生成认证请求；

[0222] 步骤305：应用服务器将认证请求发送至认证服务器；

[0223] 步骤306：认证服务器接收到认证请求后，获取认证请求中的用户名、语音认证类型和应用标识；

[0224] 步骤307：认证服务器根据用户名从服务器存储区中查找对应的令牌信息和网络数据链路，并根据应用标识从服务器存储区中获取对应的应用名称；

[0225] 步骤308：认证服务器生成预设长度的挑战值，与用户信息建立关联并保存至服务器存储区中；

[0226] 步骤309：认证服务器根据语音认证类型，将认证类型设置为预设语音认证类型，获取服务器时间，根据预设语音认证类型、挑战值、令牌信息、用户信息和应用名称生成推送认证请求；

[0227] 步骤310：认证服务器根据令牌信息中的令牌序列号查找对应的移动终端令牌；

[0228] 步骤311：认证服务器通过网络数据链路将推送认证请求推送至该移动终端令牌；

[0229] 步骤312：移动终端令牌接收到推送认证请求后，从推送认证请求中获取认证类型，判断认证类型是否为预设语音认证类型，如果是，则执行步骤216，否则报错，结束；

[0230] 本实施例中，除实施例中的传输方式外，应用界面与应用服务器、应用服务器与认证代理、认证代理与认证服务器、认证服务器与移动终端令牌之间的通信数据是经过双方预先协商的算法和密钥处理过的；进一步的，它们之间的通信数据还可以包含长度和校验位，接收方通过通信数据中的长度和校验位判断接收到的通信数据是否正确，若正确则进行正常操作流程，若不正确则通知发送方数据错误，发送方重新发送通信数据；更进一步地，它们之间的通信数据还可以进行网络加密或者采用私密软件传输等，以保证应用服务器和交互界面之间的通信数据的安全性。

[0231] 实施例3

[0232] 本发明实施例3提供了一种语音认证系统中认证服务器的工作方法，如图7所示，包括：

[0233] 步骤401：认证服务器接收到来自应用服务器的认证请求后，生成挑战值并保存，从认证请求中获取用户信息和应用名称；

[0234] 本实施例中，生成挑战值，具体为：调用随机数生成函数，生成随机数，将该随机数作为挑战值；或者，根据认证请求中的用户信息获取对应保存的服务器种子密钥，对服务器种子密钥进行计算，生成挑战值。

[0235] 步骤402:认证服务器根据用户信息查找对应的网络数据链路;

[0236] 本步骤还包括:认证服务器根据用户信息获取对应的令牌信息;

[0237] 进一步的,根据用户信息查找对应的网络数据链路,具体包括:判断根据用户信息是否能够查找到对应的网络数据链路,如果是,则查找得到对应的网络数据链路,否则向应用服务器返回错误响应,结束。

[0238] 步骤403:认证服务器根据挑战值、用户信息和应用名称生成推送认证请求,并通过与用户信息对应的网络数据链路推送至对应的移动终端令牌;

[0239] 本步骤具体包括:认证服务器根据挑战值、令牌信息、用户信息和应用名称生成推送认证请求,并通过网络数据链路将推送认证请求推送至移动终端令牌;

[0240] 本步骤中,根据挑战值、用户信息和应用名称生成推送认证请求,还可以包括:认证服务器应用令牌标识码对所述挑战值进行加密,得到挑战值密文,根据挑战值密文、令牌信息、用户信息和应用名称生成推送认证请求;

[0241] 其中,令牌信息包括令牌序列号;则将推送认证请求推送至移动终端令牌,具体为:认证服务器根据令牌序列号获取对应的移动终端令牌,将推送认证请求推送至该移动终端令牌。

[0242] 步骤404:认证服务器接收到移动终端令牌返回的授权结果,从授权结果中获取第一应答值,并获取对应保存的服务器种子密钥和挑战值,对挑战值和服务器种子密钥进行计算,得到第二应答值;

[0243] 本实施例中,对挑战值和服务器种子密钥进行计算,得到第二应答值,具体包括:获取服务器当前时间,应用预设口令生成算法,对服务器当前时间、挑战值、服务器种子密钥和动态因子进行计算,得到第二应答值。

[0244] 步骤405:认证服务器判断第一应答值和第二应答值是否匹配,是则向应用服务器返回认证成功的认证结果,结束,否则向应用服务器返回认证失败的认证结果,结束。

[0245] 实施例4

[0246] 本发明实施例4提供了一种语音认证系统中移动终端令牌的工作方法,如图8所示,包括:

[0247] 步骤501:移动终端令牌接收来自认证服务器的推送认证请求;

[0248] 步骤502:移动终端令牌从推送认证请求中获取用户信息和应用名称,根据用户信息和应用名称生成语音信息;

[0249] 步骤503:移动终端令牌播报语音信息,采集用户的语音回复;

[0250] 步骤504:当移动终端令牌采集到用户的语音回复后,对语音回复进行解析,根据解析结果判断是否授权登录,如果是,则执行步骤505,否则结束;

[0251] 本实施例中,根据解析结果判断是否授权登录,具体为:移动终端令牌判断解析结果是否为预设授权登录信息,如果是,则执行步骤505,否则结束;

[0252] 本实施例中,步骤502至步骤504具体包括:

[0253] 步骤a1:移动终端令牌从推送认证请求中获取挑战值、用户信息和应用名称;

[0254] 步骤a2:移动终端令牌根据挑战值、用户信息和应用名称生成语音信息,播报语音信息,采集用户的语音回复;

[0255] 本步骤具体包括:移动终端令牌从推送认证请求中获取挑战值,获取挑战值的预

设位上的数据，将其作为第一匹配数据，根据第一匹配数据、用户信息和应用名称生成语音信息，播报语音信息，采集用户的语音回复；

[0256] 或者，移动终端令牌从推送认证请求中获取挑战值，对挑战值进行预设计算，生成第二匹配数据，根据第二匹配数据、用户信息和应用名称生成语音信息，播报语音信息，采集用户的语音回复；

[0257] 或者，移动终端令牌从推送认证请求中获取挑战值，根据挑战值、用户信息和应用名称生成语音信息，播报语音信息，采集用户的语音回复；

[0258] 步骤a3：当移动终端令牌采集到用户的语音回复后，对语音回复进行解析，判断解析结果与挑战值是否匹配，如果是，则授权登录，执行步骤505，否则结束；

[0259] 本步骤中，判断解析结果与挑战值是否匹配，具体为：判断解析结果与第一匹配数据是否匹配，如果是，则授权登录，执行步骤505，否则结束；

[0260] 具体为：判断解析结果中是否存在与第一匹配数据相同的第一数据，判断在第一数据之前和第一数据之后是否存在预设字符，如果均为是，则执行步骤505，否则结束；

[0261] 或者，判断解析结果与第二匹配数据是否匹配，如果是，则授权登录，执行步骤505，否则结束；

[0262] 具体为：判断解析结果中是否存在与第二匹配数据相同的第二数据，判断在第二数据之前和第二数据之后是否存在预设字符，如果均为是，则执行步骤505，否则结束；

[0263] 或者，判断解析结果与挑战值是否匹配，如果是，则授权登录，执行步骤505，否则结束；

[0264] 步骤505：移动终端令牌根据推送认证请求中的挑战值和内部保存的令牌种子密钥进行计算，得到第一应答值，生成包含第一应答值的授权结果，通过网络数据链路将授权结果发送至认证服务器，令牌操作结束；

[0265] 本实施例中，步骤504对语音回复进行解析，根据解析结果判断是否授权登录，具体包括：

[0266] 步骤1：移动终端令牌每隔预设时长监听采集到的音频数据，判断采集到的音频数据的长度是否发生变化，如果是，则执行步骤2，否则执行步骤3；

[0267] 步骤2：移动终端令牌对采集到的音频数据进行解析，得到解析结果，根据解析结果判断是否授权登录，如果是，则执行步骤505，否则执行步骤3；

[0268] 步骤3：移动终端令牌判断录音时间是否达到预设时长，如果是，则输出语音回复不正确的提示信息，结束，否则返回步骤1。

[0269] 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。

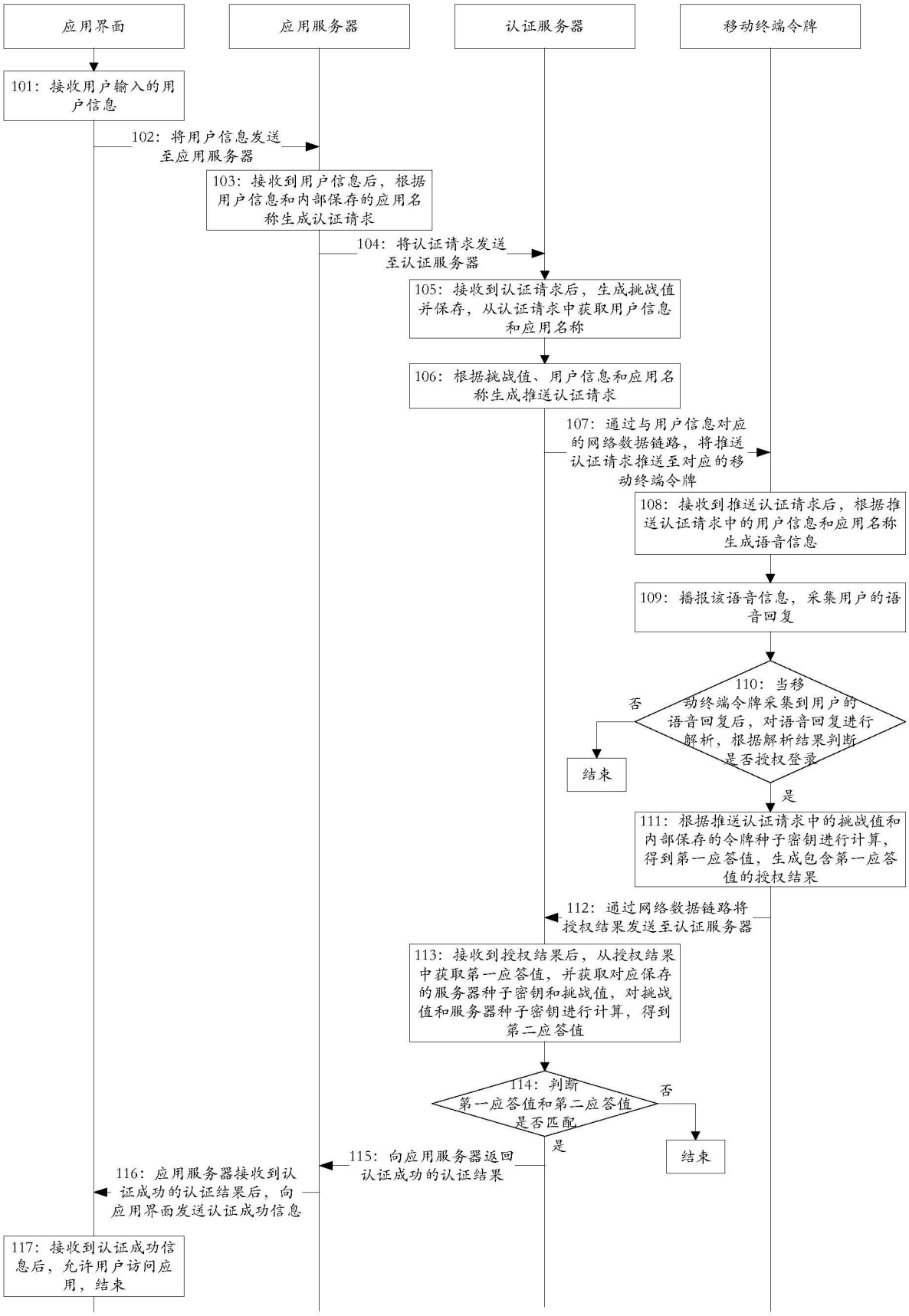

应用界面
应用服务器
认证服务器
移动终端令牌
101：接收用户输入的用户信息
102：将用户信息发送至应用服务器
103：接收到用户信息后，根据用户信息和内部保存的应用名称生成认证请求
104：将认证请求发送至认证服务器
105：接收到认证请求后，生成挑战值并保存，从认证请求中获取用户信息和应用名称
106：根据挑战值、用户信息和应用名称生成推送认证请求
107：通过与用户信息对应的网络数据链路，将推送认证请求推送至对应的移动终端令牌
108：接收到推送认证请求后，根据推送认证请求中的用户信息和应用名称生成语音信息
109：播报该语音信息，采集用户的语音回复
110：当移动终端令牌采集到用户的语音回复后，对语音回复进行解析，根据解析结果判断是否授权登录
否
结束
是
111：根据推送认证请求中的挑战值和内部保存的令牌种子密钥进行计算，得到第一应答值，生成包含第一应答值的授权结果
112：通过网络数据链路将授权结果发送至认证服务器
113：接收到授权结果后，从授权结果中获取第一应答值，并获取对应保存的服务器种子密钥和挑战值，对挑战值和服务器种子密钥进行计算，得到第二应答值
114：判断第一应答值和第二应答值是否匹配
否
结束
是
115：向应用服务器返回认证成功的认证结果
116：应用服务器接收到认证成功的认证结果后，向应用界面发送认证成功信息
117：接收到认证成功信息后，允许用户访问应用，结束

图1

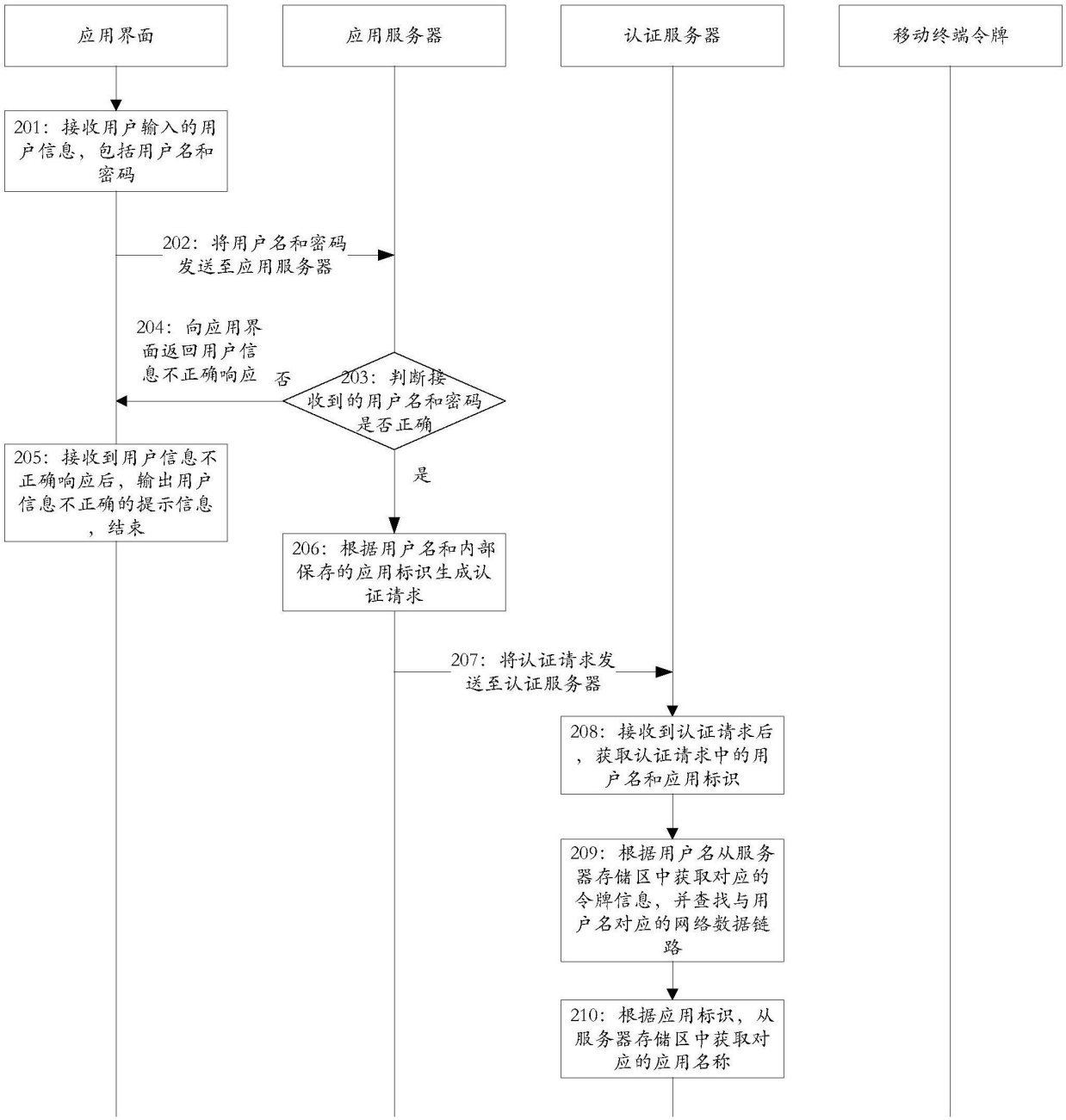

应用界面
应用服务器
认证服务器
移动终端令牌
201：接收用户输入的用户信息，包括用户名和密码
202：将用户名和密码发送至应用服务器
204：向应用界面返回用户信息不正确响应
否
203：判断接收到的用户名和密码是否正确
是
205：接收到用户信息不正确响应后，输出用户信息不正确的提示信息，结束
206：根据用户名和内部保存的应用标识生成认证请求
207：将认证请求发送至认证服务器
208：接收到认证请求后，获取认证请求中的用户名和应用标识
209：根据用户名从服务器存储区中获取对应的令牌信息，并查找与用户名对应的网络数据链路
210：根据应用标识，从服务器存储区中获取对应的应用名称

图2

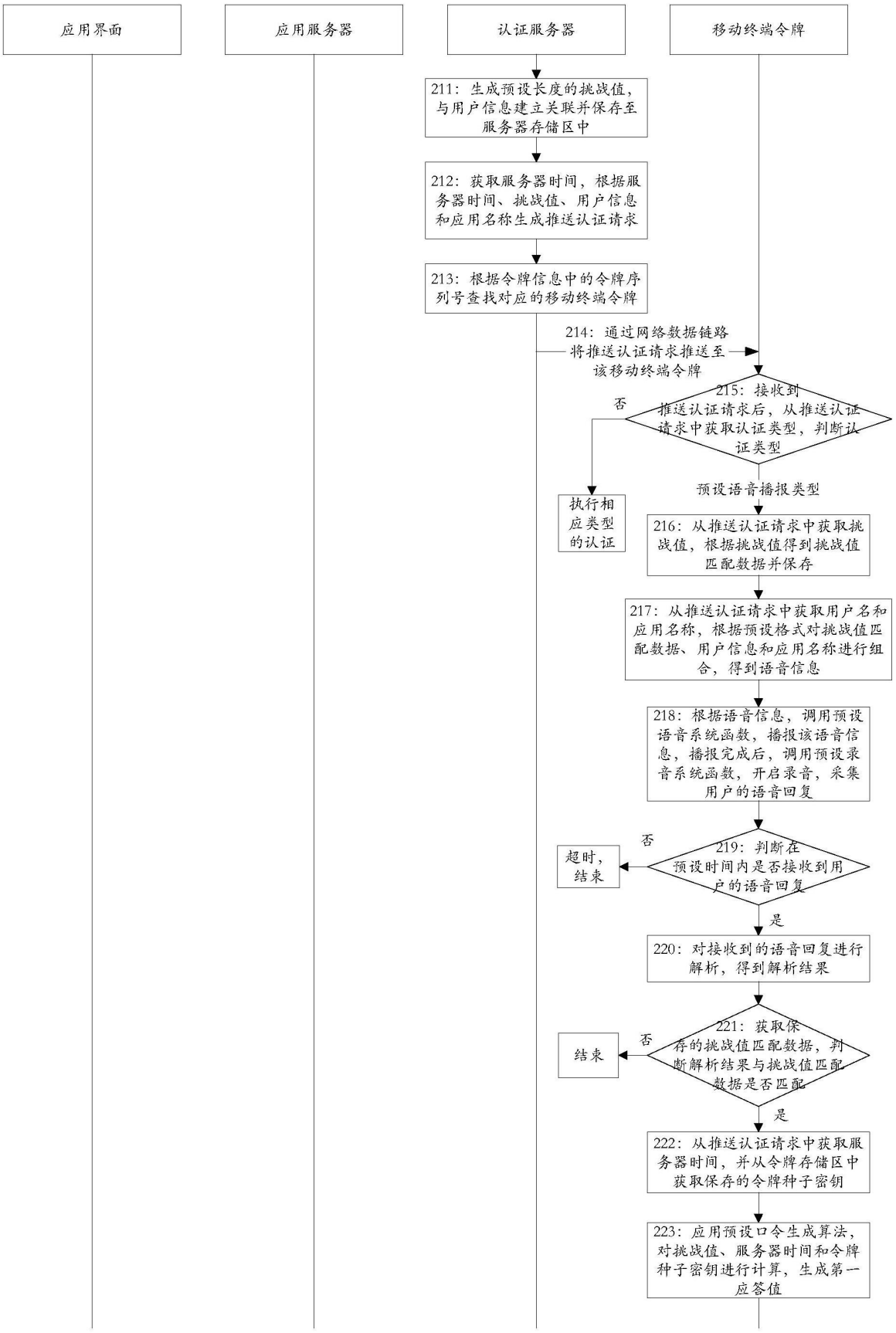

应用界面
应用服务器
认证服务器
移动终端令牌
211：生成预设长度的挑战值，与用户信息建立关联并保存至服务器存储区中
212：获取服务器时间，根据服务器时间、挑战值、用户信息和应用名称生成推送认证请求
213：根据令牌信息中的令牌序列号查找对应的移动终端令牌
214：通过网络数据链路将推送认证请求推送至该移动终端令牌
215：接收到推送认证请求后，从推送认证请求中获取认证类型，判断认证类型
否
执行相应类型的认证
预设语音播报类型
216：从推送认证请求中获取挑战值，根据挑战值得到挑战值匹配数据并保存
217：从推送认证请求中获取用户名和应用名称，根据预设格式对挑战值匹配数据、用户信息和应用名称进行组合，得到语音信息
218：根据语音信息，调用预设语音系统函数，播报该语音信息，播报完成后，调用预设录音系统函数，开启录音，采集用户的语音回复
否
超时，结束
219：判断在预设时间内是否接收到用户的语音回复
是
220：对接收到的语音回复进行解析，得到解析结果
否
结束
221：获取保存的挑战值匹配数据，判断解析结果与挑战值匹配数据是否匹配
是
222：从推送认证请求中获取服务器时间，并从令牌存储区中获取保存的令牌种子密钥
223：应用预设口令生成算法，对挑战值、服务器时间和令牌种子密钥进行计算，生成第一应答值

图3

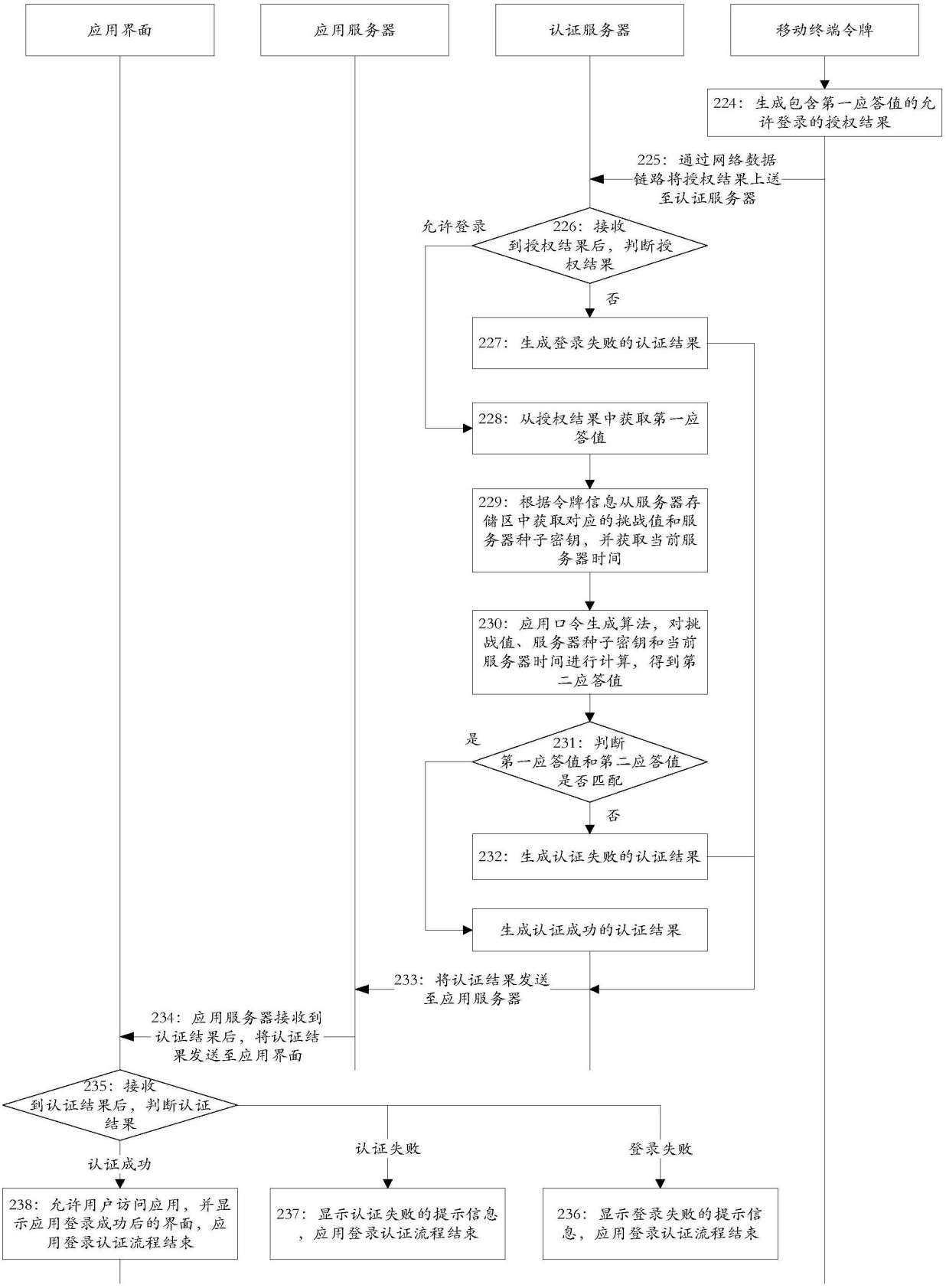

应用界面
应用服务器
认证服务器
移动终端令牌
224：生成包含第一应答值的允许登录的授权结果
225：通过网络数据链路将授权结果上送至认证服务器
允许登录
226：接收到授权结果后，判断授权结果
否
227：生成登录失败的认证结果
228：从授权结果中获取第一应答值
229：根据令牌信息从服务器存储区中获取对应的挑战值和服务器种子密钥，并获取当前服务器时间
230：应用口令生成算法，对挑战值、服务器种子密钥和当前服务器时间进行计算，得到第二应答值
是
231：判断第一应答值和第二应答值是否匹配
否
232：生成认证失败的认证结果
生成认证成功的认证结果
233：将认证结果发送至应用服务器
234：应用服务器接收到认证结果后，将认证结果发送至应用界面
235：接收到认证结果后，判断认证结果
认证成功
认证失败
登录失败
238：允许用户访问应用，并显示应用登录成功后的界面，应用登录认证流程结束
237：显示认证失败的提示信息，应用登录认证流程结束
236：显示登录失败的提示信息，应用登录认证流程结束

图4

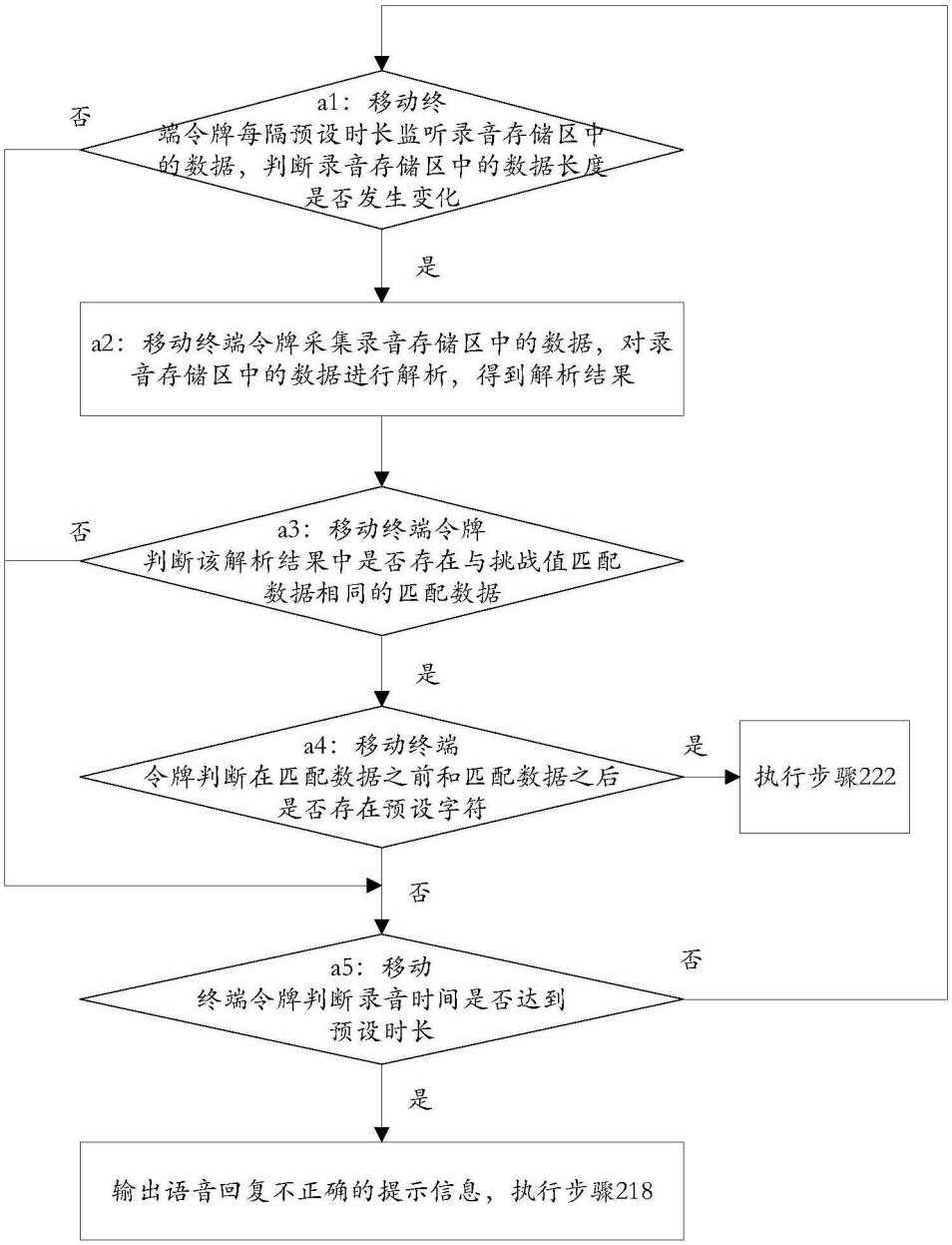

a1：移动终端令牌每隔预设时长监听录音存储区中的数据，判断录音存储区中的数据长度是否发生变化
否
是
a2：移动终端令牌采集录音存储区中的数据，对录音存储区中的数据进行解析，得到解析结果
a3：移动终端令牌判断该解析结果中是否存在与挑战值匹配数据相同的匹配数据
否
是
a4：移动终端令牌判断在匹配数据之前和匹配数据之后是否存在预设字符
是
执行步骤222
否
a5：移动终端令牌判断录音时间是否达到预设时长
否
是
输出语音回复不正确的提示信息，执行步骤218

图5

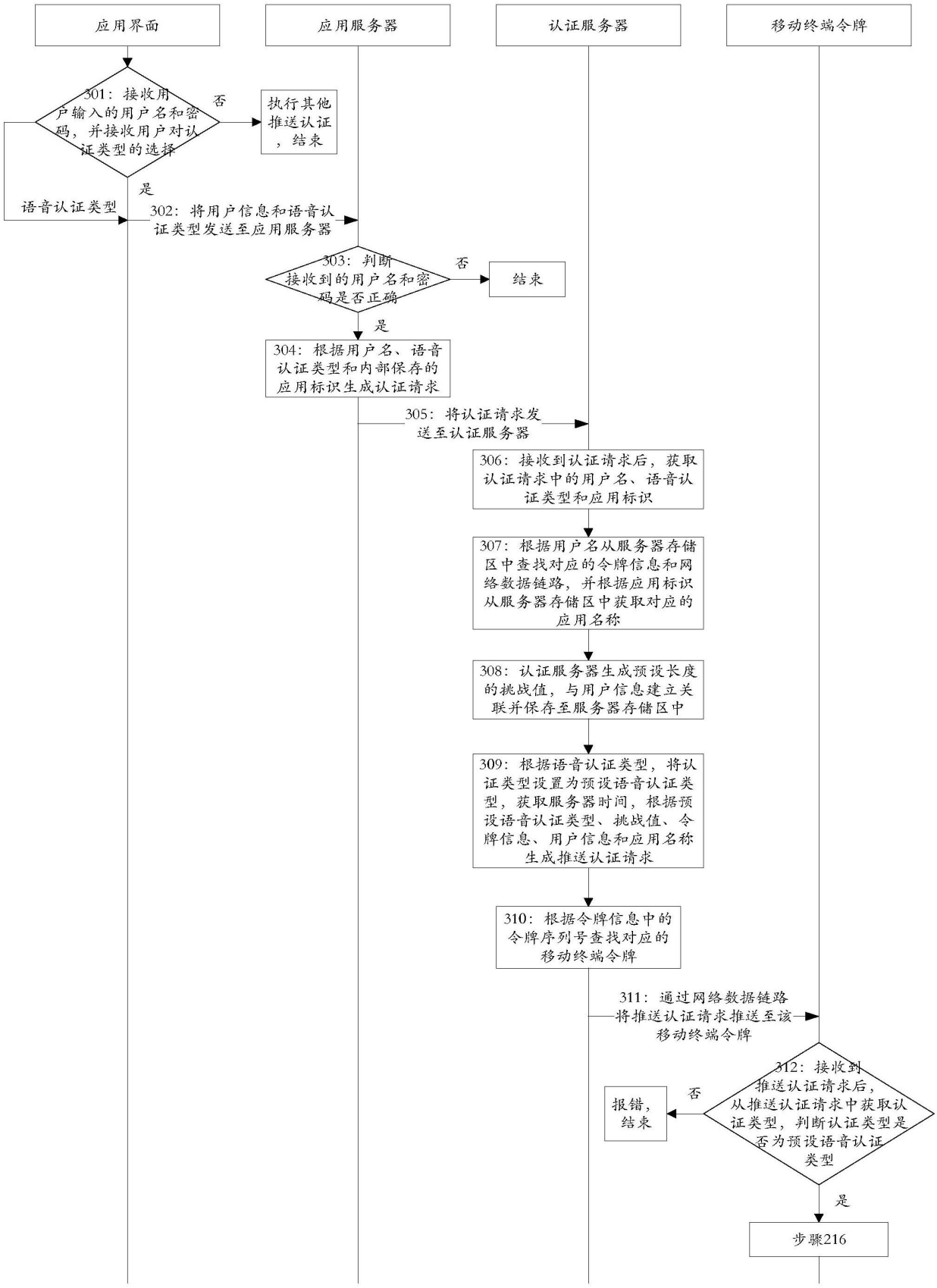

应用界面
应用服务器
认证服务器
移动终端令牌
301：接收用户输入的用户名和密码，并接收用户对认证类型的选择
否
执行其他推送认证，结束
是
语音认证类型
302：将用户信息和语音认证类型发送至应用服务器
303：判断接收到的用户名和密码是否正确
否
结束
是
304：根据用户名、语音认证类型和内部保存的应用标识生成认证请求
305：将认证请求发送至认证服务器
306：接收到认证请求后，获取认证请求中的用户名、语音认证类型和应用标识
307：根据用户名从服务器存储区中查找对应的令牌信息和网络数据链路，并根据应用标识从服务器存储区中获取对应的应用名称
308：认证服务器生成预设长度的挑战值，与用户信息建立关联并保存至服务器存储区中
309：根据语音认证类型，将认证类型设置为预设语音认证类型，获取服务器时间，根据预设语音认证类型、挑战值、令牌信息、用户信息和应用名称生成推送认证请求
310：根据令牌信息中的令牌序列号查找对应的移动终端令牌
311：通过网络数据链路将推送认证请求推送至该移动终端令牌
312：接收到推送认证请求后，从推送认证请求中获取认证类型，判断认证类型是否为预设语音认证类型
否
报错，结束
是
步骤216

图6

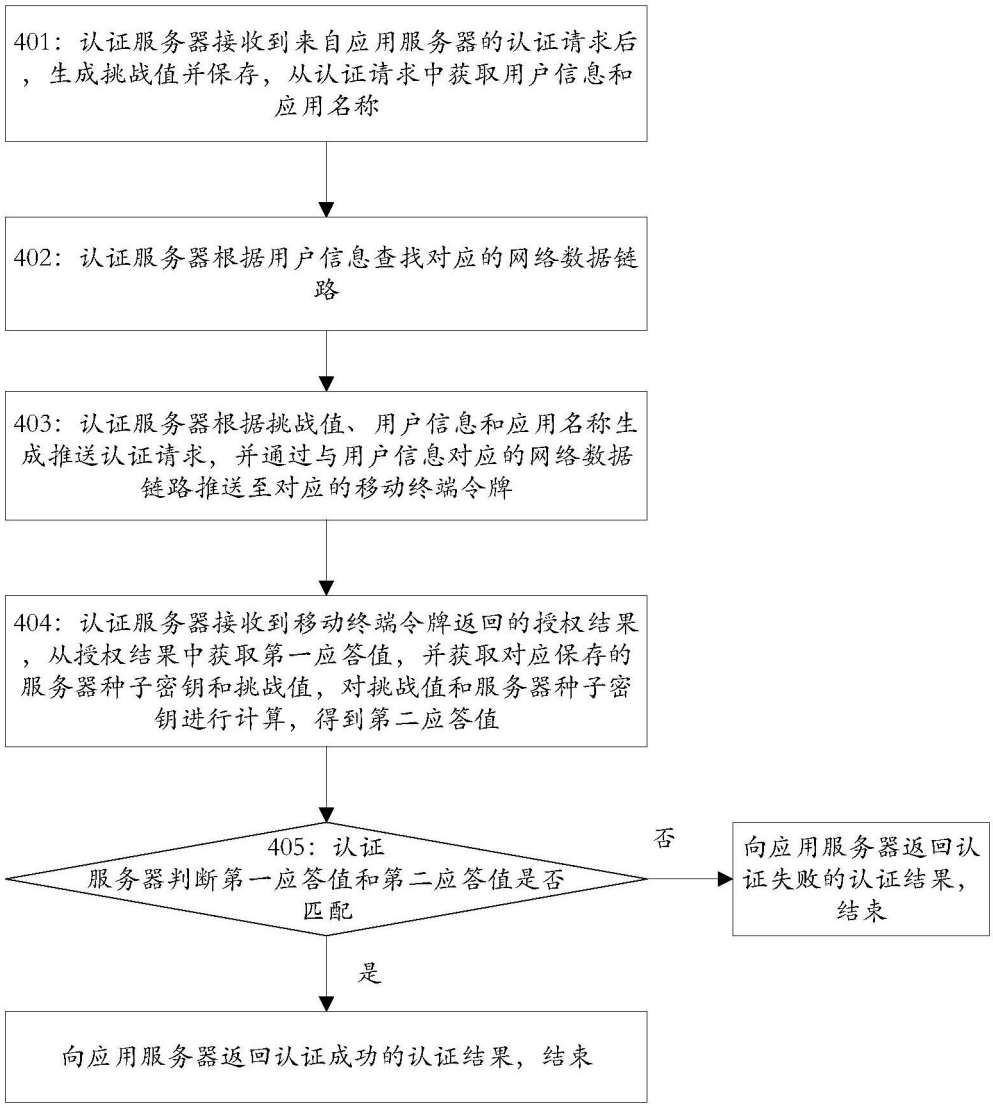

401：认证服务器接收到来自应用服务器的认证请求后，生成挑战值并保存，从认证请求中获取用户信息和应用名称
402：认证服务器根据用户信息查找对应的网络数据链路
403：认证服务器根据挑战值、用户信息和应用名称生成推送认证请求，并通过与用户信息对应的网络数据链路推送至对应的移动终端令牌
404：认证服务器接收到移动终端令牌返回的授权结果，从授权结果中获取第一应答值，并获取对应保存的服务器种子密钥和挑战值，对挑战值和服务器种子密钥进行计算，得到第二应答值
405：认证服务器判断第一应答值和第二应答值是否匹配
否
向应用服务器返回认证失败的认证结果，结束
是
向应用服务器返回认证成功的认证结果，结束

图7

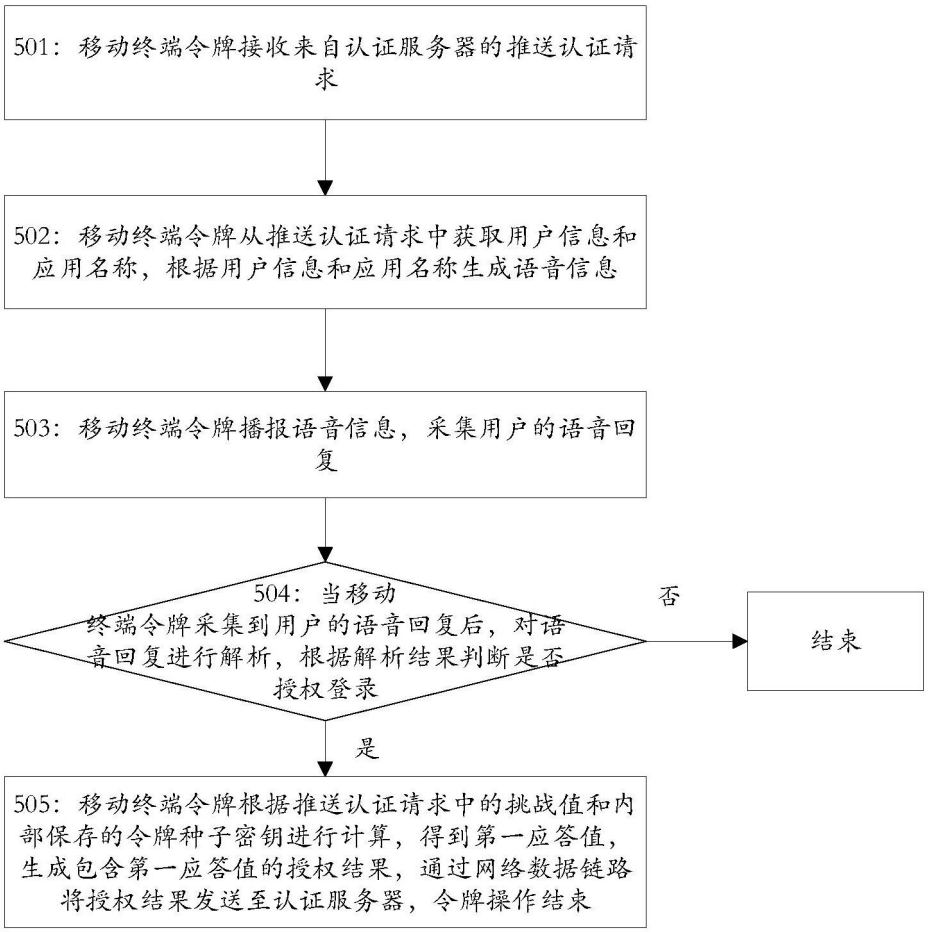

501：移动终端令牌接收来自认证服务器的推送认证请求
502：移动终端令牌从推送认证请求中获取用户信息和应用名称，根据用户信息和应用名称生成语音信息
503：移动终端令牌播报语音信息，采集用户的语音回复
504：当移动终端令牌采集到用户的语音回复后，对语音回复进行解析，根据解析结果判断是否授权登录
否
结束
是
505：移动终端令牌根据推送认证请求中的挑战值和内部保存的令牌种子密钥进行计算，得到第一应答值，生成包含第一应答值的授权结果，通过网络数据链路将授权结果发送至认证服务器，令牌操作结束

图8