(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 101335619 B
(45)授权公告日 2010.10.13

(21)申请号 200710024804.5
(22)申请日 2007.06.27
审查员 刘冬生

(73)专利权人 刘建军
地址 225600 江苏省高邮市北门大街 158 号
(72)发明人 刘建军

(51)Int.Cl.
H04L 9/32(2006.01)
H04M 3/42(2006.01)
H04W 88/00(2006.01)

(56)对比文件
CN 1925398 A,2007.03.07, 全文.
US 2004/0083393 A1,2004.04.29, 全文.
CN 1622508 A,2005.06.01, 全文.
CN 1435985 A,2003.08.13, 全文.

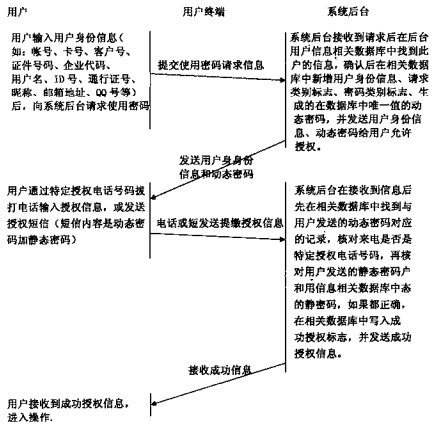
权利要求书 1 页 说明书 5 页 附图 5 页

(54)发明名称

一次性动态密码电话或短信授权使用方法

(57)摘要

本发明公开了一次性动态密码电话或短信授权使用方法，网络用户在网上发起新建、使用、修改静态密码的申请，系统后台在接收到申请后，在相关数据库中新增用户身份信息、生成的在数据库中唯一值的动态密码或非唯一值的动态密码、请求类别标志、密码类别标志，并发送用户身份信息、动态密码和允许授权信息给用户，授权时效5分钟，用户通过特定授权电话号码或任一部电话拨打电话或发送短信给系统后台进行动态密码授权，授权信息内容包含动态密码和静态密码，其它信息可以根据需要定制，后台通过对授权信息的核实，实现动态密码与静态密码之间的相互授权，解决了网络用户使用密码安全问题，广泛适用于所有使用密码进行用户身份确认的网络用户。



CN 101335619 B

1. 一种一次性动态密码授权使用方法，通过用户特定授权电话号码拔打或短信发送授权信息与系统后台进行联络对用户申请的一次性动态密码进行授权使用，特定授权电话号码是用户在系统后台预留的用于授权的电话号码，只有用户用此号码拔打授权电话或发送授权短信息，系统后台才允许授权，一次性动态密码通过特定授权电话号码拔打电话授权使用、以及一次性动态密码通过特定授权电话号码发送短信息授权使用方法使用范围包括所有使用密码进行身份确认的网络用户，其特征在于：用户根据自己的身份发起新建、使用、修改静态密码的请求，系统后台根据用户请求，核对用户身份信息后，在相关数据库中加入用户身份信息、生成在数据库中唯一值的动态密码、请求类别标志和密码类别标志，请求类别标志包括新建请求标志、使用请求标志、修改请求标志，由用户所选操作决定，密码类别标志包括登录密码标志、通讯密码标志、交易密码标志、超级用户密码标志，各种密码级别由系统后台设定，由用户所选操作决定，根据需要设定授权等待时间，超出时间将删除相关数据库中的授权记录，停止授权，并发送用户身份信息、动态密码和允许授权信息给用户，用户通过特定授权电话号码拔打授权电话，根据提示输入授权信息，或短信发送授权信息，授权信息内容根据系统要求设定，包括动态密码和静态密码，系统后台接收到用户的授权信息后通过用户授权信息中的动态密码和相关数据库中唯一值的动态密码建立用户授权信息和系统后台用户信息之间的对应关系，根据请求类别标志进行分类操作：对使用静态密码的授权，即静态密码对动态密码授权，需核对用户的特定授权电话号码，根据密码类别标志核对相应静态密码，完全正确后，在相关数据库中写入授权成功标志，生成授权成功信息，用户接收到授权成功信息后即可进行所需操作，在相关数据库中的已被授权使用过的动态密码被失效删除；对新建、修改静态密码的授权，即动态密码对静态密码授权，需要进行两次授权以确定静态密码输入的正确性，两次授权内容相同，系统后台核对特定授权电话号码，核对两次授权信息中的静态密码，完全正确后，根据密码类别标志在用户信息相关数据库中变更用户相应静态密码，在相关数据库中写入授权成功标志，生成授权成功信息，用户接收到授权成功信息后即可使用新的静态密码，在相关数据库中的已被授权使用过的动态密码被失效删除，在以上所述中，电话包括固定电话、移动电话、网络电话，密码与口令意义相同，动态密码与动态口令意义相同，静态密码与静态口令意义相同。

2. 根据权利要求 1 所述方法，其特征在于：将用户在系统后台预留的特定授权电话号码替换为任意一个电话号码进行授权，这样减少了对用户真实身份的一次认证。

3. 根据权利要求 1 所述方法，其特征在于：将生成在数据库中唯一值的动态密码替换为在数据库中不是唯一值的动态密码，这样在授权信息中增加用户身份信息来确定用户授权信息和系统后台用户信息之间的对应关系，用户身份信息和静态密码需在电话设备中同时输入。

4. 根据权利要求 2 所述方法，其特征在于：将生成在数据库中唯一值的动态密码替换为在数据库中不是唯一值的动态密码，这样在授权信息中增加用户身份信息来确定用户授权信息和系统后台用户信息之间的对应关系，用户身份信息和静态密码需在电话设备中同时输入。

5. 根据权利要求 1 到 4 任一项所述方法，其特征在于：系统后台不先预留动态密码，根据用户申请生成动态密码，授权后才能使用，且只能使用一次。

一次性动态密码电话或短信授权使用方法

[0001] 技术领域：本发明涉及一种一次性动态密码电话或短信授权使用方法，具体说：涉及到一种应用在所有网络上新建、使用、修改静态密码的所有网络用户使用一次性动态密码电话或短信授权使用方法

[0002] 背景技术：在现有的技术中：网络上所有需要通过密码确认身份的用户在使用静态密码或动态密码时，虽然输入过程中提供了各种加密方法，但静态密码因多次使用还是容易被盗取并解码，对用户造成信息和资金损失，动态密码在一定程度上减少了被盗问题，但动态密码的记录介质（动态口令卡、动态口令令牌等）、不易携带、容易丢失、被盗，这都会给用户的使用带来不便，用户的信息、资金安全受到威胁，总之现在的密码使用方法存在较大的安全隐患。

[0003] 发明内容：本发明的目的在于提供一种一次性动态密码电话或短信授权使用方法，用户在使用过程中只要记住你的用户身份信息（如：帐号、卡号、客户号、证件号码、企业代码、用户名、ID 号、通行证号、昵称、邮箱地址、QQ 号等）和静态密码，无需在操作介面中同时输入你的用户身份信息和静态密码，也不需要携带动态密码记录介质，有效地防止了用户信息和资金的被盗用，为用户提供了一种更方便安全的密码使用方法。

[0004] 为了达到上述目的，本发明提供了如下的技术方案：采用一次性动态密码电话或短信授权使用方法，用户在新建、使用、修改静态密码时，用户在操作介面中输入用户身份信息（如：帐号、卡号、客户号、证件号码、企业代码、用户名、ID 号、通行证号、昵称、邮箱地址、QQ 号等）和相关信息后，给系统后台发送用户信息、请求类别标志（如：新建请求标志、使用请求标志、修改请求标志等）和密码类别标志（如：登录密码、通讯密码、交易密码、超级用户密码等，各种密码级别由系统后台设定），请求动态密码授权，请求类别标志和密码类别标志由用户所选操作确定，系统后台接收到用户发送的信息后，与系统中的用户信息进行核对（如果是新建用户密码则在用户注册信息得到系统后台确认后，最后才能进行密码新建），如核对相同，系统在相关数据库中加入用户身份信息、生成的在数据库中唯一值的动态密码（也可以不是唯一值，但在用户的授权权信息中就要包含用户身份信息，来关联授权信息和系统后台用户信息之间的关系，会使用户身份信息和静态密码同时出现在电话设备中，降低用户安全）、请求类别标志、密码类别标志等，设定此动态密码的授权有效时间为 5 分钟（超出时间，系统后台将删除此条授权信息，时间可以根据实际需要设定），并发送用户信息、动态密码和允许授权信息到用户操作介面，用户在操作介面中接收到用户信息和动态密码后，用户用特定授权电话号码（特定授权电话号码是用户在系统后台预先设定的一部或几部电话号码，只有用此号码拔打输入和短信发送的信息，系统后台才允许授权，如果在系统后台没有设定特定授权电话号码，可以使用任何一部电话拔打授权电话或发送授权信息，会减少对用户真实身份的一次核实，用户的安全性会降低）拔打授权电话，或发送授权信息，拔打授权电话时根据提示输入动态密码和静态密码或动态密码加旧静态密码加新静态密码，发送短信息的内容是动态密码加静态密码或动态密码加旧静态密码新静态密码（它们之间可以用分隔符隔开），具体的授权信息内容可以根据需要进行定制；根据请求类别标志分为使用静态密码授权（即静态密码对动态密码授权）和新建、修改

静态密码授权（即动态密码对静态密码授权）；静态密码对动态密码授权时，系统后台接收到授权信息后，通过用户授权信息中的动态密码和相关数据库中唯一值的动态密码建立用户授权信息和系统后台用户信息之间的对应关系，再确认是否是特定授权电话号码进行的授权，如果不是则系统认定为无效授权信息，系统不作任何动作，如果是特定授权电话号码进行的授权，则根据密码类别标志核对用户信息相关数据库中的相应静态密码和授权信息中的静态密码，如果核对相同，则在相关数据库中写入授权成功标志，用户接收到成功信息后，用户即可进行所需操作，如果核对不相同，则用户接收到授权失败信息；动态密码对静态密码授权时，需要两次授权，授权内容两次相同，以确定授权信息的正确性，系统后台接收到授权信息后，通过用户授权信息中的动态密码和相关数据库中唯一值的动态密码建立用户授权信息和系统后台用户信息之间的对应关系，也要先确认是否是特定授权电话号码进行的授权，再核对两次授权的静态密码，如果核对相同，则根据密码类别标志在用户信息相关数据库中变更用户的相应静态密码，在相关数据库中写入授权成功标志，用户接收到成功信息，用户即可进行所需操作，如果不正确，则用户接收到授权失败信息；用户在接收到成功信息并进行所需操作后或接收到不成功信息后，系统后台将删除相关数据库中这一动态密码记录。

[0005] 本发明较好的技术方案可以是，在使用电话或短信授权时，在系统后台必须设定授权用特定授权电话号码，用户只有用特定授权电话号码才能授权，加强了对用户身份真实性的论证；在用户请求动态密码授权时，在相关数据库中生成的动态密码必须是在数据库中是唯一值，避免了用户完整信息在用户操作介面或电话设备上同时输入，减少非法用户从单一设备盗取用户完整信息。

[0006] 与现有的静态密码新建、使用、修改方法相比较，本发明具有如下优点和效果：1、用户在使用静态密码时，用户不需要在操作介面中输入静态密码，只用电话和短信授权使用，就不可能被盗取，动态密码授权使用一次后即失效，可以有效地防止用户静态密码泄露；2、用户使用特定授权电话号码进行授权，系统对特定授权电话号码进行认证，电话号码具有唯一性，无法被复制，实际上就是对用户身份的一次真实性的论证，而现在的用户在使用电子证书、用户 IC 卡、U-KEY 等的身份论证过程中，容易被非法用户下载、复制、盗用，因此系统后台对特定授权电话号码论证更安全，真实、有效；3、用户在正常的操作中无需输入授权用特定授权电话号码信息，非法用户无法盗取用户特定授权电话号码信息，即是非法用户得到用户身份信息和静态密码，也无法知道用户特定授权电话号码信息，更无法授权，既是知道特定授权电话号码，也无法复制，更无法进行授权；4、在用户操作介面或电话设备中，都没有同时输入用户身份信息和静态密码，这样，非法用户从任何单一设备中都无法盗取到用户的完整信息，就无法正真实施盗窃 5、在使用本方法时，用户不需要随身设带动态口令卡、电子证书、动态口令令牌等物品，减少了丢失被盗风险。

[0007] 附图说明 以下是本发明的附图说明

[0008] 图 1 是一次性动态密码电话或短信授权使用方法在新注册用户时的流程图；

[0009] 图 2 是一次性动态密码电话或短信授权使用方法在用户登录使用时的流程图；

[0010] 图 3 是一次性动态密码电话或短信授权使用方法在用户修改静态密码时的流程图；

[0011] 图 4 是一次性动态密码电话或短信授权使用方法在银行网上银行进行交易时的

流程图；

[0012] 图 5 是一次性动态密码电话或短信授权使用方法在银行自助设备上进行交易时的流程图

[0013] 具体实施方式：以下通过具体的实施方式对本发明进行更详细的描述：

[0014] 实施例子 1 在新注册时的应用

[0015] 参照图 1，用户是新注册用户，在注册信息输入完成并得到系统后台认可后（包括特定授权电话号码），进入下一步后设定用户静态密码，后台系统在相关数据库中新增得到系统后台认可的用户身份信息、生成的在数据库中是唯一值的动态密码（目前由于在电话来电授权时不能输入字符，所以目前动态密码和静态密码以数字为主，纯短信授权用户可以不受此限制）请求类别标志和密码类别标志，设定此动态密码的授权有效时间为 5 分钟（时间可能根据实际需要设定），并发送用户身份信息和生成的动态密码到用户操作介面，用户拔打授权电话（如设定特定授权电话号码的要用特定授权电话号码拔打，），根据提示输入动态密码和静态密码，或发送授权短信，短信内容是动态密码加静态密码（两个密码之间可以加分隔符），系统后台根据授权信息中的动态密码和相关数据库中的唯一值的动态密码建立系统后台用户信息与授权信息之间关联，如设定特定授权电话号码，则需确认是特定授权电话号码的来电或发送的信息，为了确认用户输入的正解性，系统在进入下一步后要求再次拔打授权电话或发送授权短信，重新输入同相的动态密码和静态密码，系统确认正确后，根据密码类别标志在系统后台用户信息相关数据库中加入此用户的静态密码，发送新注册用户注册成功信息给用户，同时系统后台删除相关数据库中的此次授权的动态密码信息。

[0016] 实施例子 2 在登录时的应用

[0017] 参照图 2，用户在登录介面中输入你的用户身份信息（如：帐号、用户名、卡号、UID 号、通行证号、邮箱地址、QQ 号等），可以加入验证码，点击进入下一步，把用户身份信息和登录使用请求信息发送到系统后台，系统后台在用户信息相关数据库中找到对应信息后在相关数据库中插入此用户身份信息、生成的在数据库中是唯一值的动态密码（目前由于在电话来电授权时不能输入字符，所以目前动态密码和静态密码以数字为主，纯短信授权用户可以不受此限制）、请求类别标志和密码类别标志，设定此动态密码的授权有效时间为 5 分钟（时间可能根据实际需要设定），并把用户身份信息和生成的动态密码发送到用户操作介面上，用户在得到动态密码后，用电话拔打系统后台的授权电话进行动态密码授权，根据提示输入动态密码和静态密码，或发送授权短信，短信内容是动态密码加静态密码（两个密码之间可以加分隔符），系统后台在接收到授权信息后根据授权信息中的动态密码和相关数据库中的唯一值的动态密码建立系统后台用户信息与授权信息之间关联，用户设定用特定授权电话号码授权的，要核对来电号码是否为特定授权电话号码，如果不是，后台不作处理，等待特定授权电话号码的授权信息，如果是特定授权电话号码的授权信息，根据密码类别标志系统后台核对用户信息相关数据库中的静态密码与用户授权信息中的静态密码，如正确则在相关数据库中写入授权成功标志，系统后台发送成功授权并允许登录的信息给用户，用户成功登录使用，系统后台删除相关数据库中此次授权信息。

[0018] 实施例子 3 在修改密码时的应用

[0019] 参照图 3 如用户是修改静态密码，在用户登录进入自己的操作介面后，选择修改

密码操作，系统后台在接收到修改用户静态密码请求后，在相关数据库中增加用户身份信息、生成的在相关数据库中是唯一值的动态密码（目前由于在电话来电授权时不能输入字符，所以目前动态密码和静态密码以数字为主，纯短信授权用户可以不受此限制）、请求类别标志和密码类别标志，并发送用户身份信息和生成的动态密码到用户操作介面，用户拔打授权电话（如设定特定授权电话号码的要用特定授权电话号码拔打），根据提示输入动态密码和新的静态密码或动态密码加旧静态密码加新静态密码，或发送授权短信，短信内容是动态密码加新静态密码或动态密码加旧静态密码加新静态密码（两个密码之间可以加分隔符），为了确认用户输入的正解性，系统会要求再次拔打授权电话，重新输入同相授权内容，系统在每次接收到授权信息后根据授权信息中的动态密码和相关数据库中的唯一值的动态密码建立系统后台用户信息与授权信息之间关联，根据密码类别标志核对特定授权电话号码和旧静态密码，并核对两次授权信息中的新静态密码的一致性，系统确认正确后，在系统后台用户信息数据库中修改此用户的静态密码，同时系统后台删除相关数据库中此次授权信息，用户修改静态密码成功。

[0020] 实施例子 4 在银行网上银行的应用

[0021] 参照图 4 在银行网上银行进行交易时，用户按照实施例子 2 所述方法登录进入用户自己的操作介面后，输入交易要素（如：对方帐号，卡号，缴费信息等），并得到系统后台确认信息的真确性、完整性后，需提交交易密码进行真实资金划转时，用户发送用户信息和交易求请信息，后台在接收到信息后，在相关数据库中增加用户身份信息、生成的在相关数据库中是唯一值的动态密码（目前由于在电话来电授权时不能输入字符，所以目前动态密码和静态密码以数字为主，纯短信授权用户可以不受此限制）、请求类别标志和密码类别标志，并发送用户身份信息和生成的动态密码到用户操作介面，用户拔打授权电话（如设定特定授权电话号码的要用特定授权电话号码拔打），根据提示输入动态密码和静态密码，或发送授权短信，短信内容是动态密码和静态密码（两个密码之间可以加分隔符），系统后台在接收到授权信息后根据授权信息中的动态密码和相关数据库中的唯一值的动态密码建立系统后台用户信息与授权信息之间关联，用户是需要用特定授权电话号码授权的，要核对来电号码是否为特定授权电话号码，如果不是，后台不作处理，等待特定授权电话号码的授权信息，如果是特定授权电话号码的授权信息，根据密码类别标志系统后台核对用户信息相关数据库中的交易静态密码与用户授权信息中的静态密码，如正确则进行真实交易，并发送交易成功信息给用户。

[0022] 实施例子 5 在银行自助设备上的应用

[0023] 参照图 5 在银行自助设备进行交易时，用户插入用户帐户卡或存折，系统自动发送用户身份信息和登录使用请求信息，后台接收到信息，在用户信息相关数据库中找到对应信息后，在相关数据库中增加用户身份信息、生成的在相关数据库中是唯一值的动态密码（目前由于在电话来电授权时不能输入字符，所以目前动态密码和静态密码以数字为主，纯短信授权用户可以不受此限制）、请求类别标志和密码类别标志，并发送用户身份信息和生成的动态密码到用户操作介面，用户拔打授权电话（如设定特定授权电话号码的要用特定授权电话号码拔打），根据提示输入动态密码和静态密码，或发送授权短信，短信内容是动态密码和静态密码（两个密码之间可以加分隔符），系统后台在接收到授权信息后根据授权信息中的动态密码和相关数据库中的唯一值的动态密码建立系统后台用户信息

与授权信息之间关联，用户是需要用特定授权电话号码授权的，要核对来电号码是否为特定授权电话号码，如果不是，后台不作处理，等待特定授权电话号码的授权信息，如果是特定授权电话号码的授权信息，根据密码类别标志系统后台核对用户信息相关数据库中的静态密码与用户授权信息中的静态密码，如正确则允许登录使用，并发送授权登录成功信息给用户，自动进入用户操作介面，用户即可进行正常自助操作。

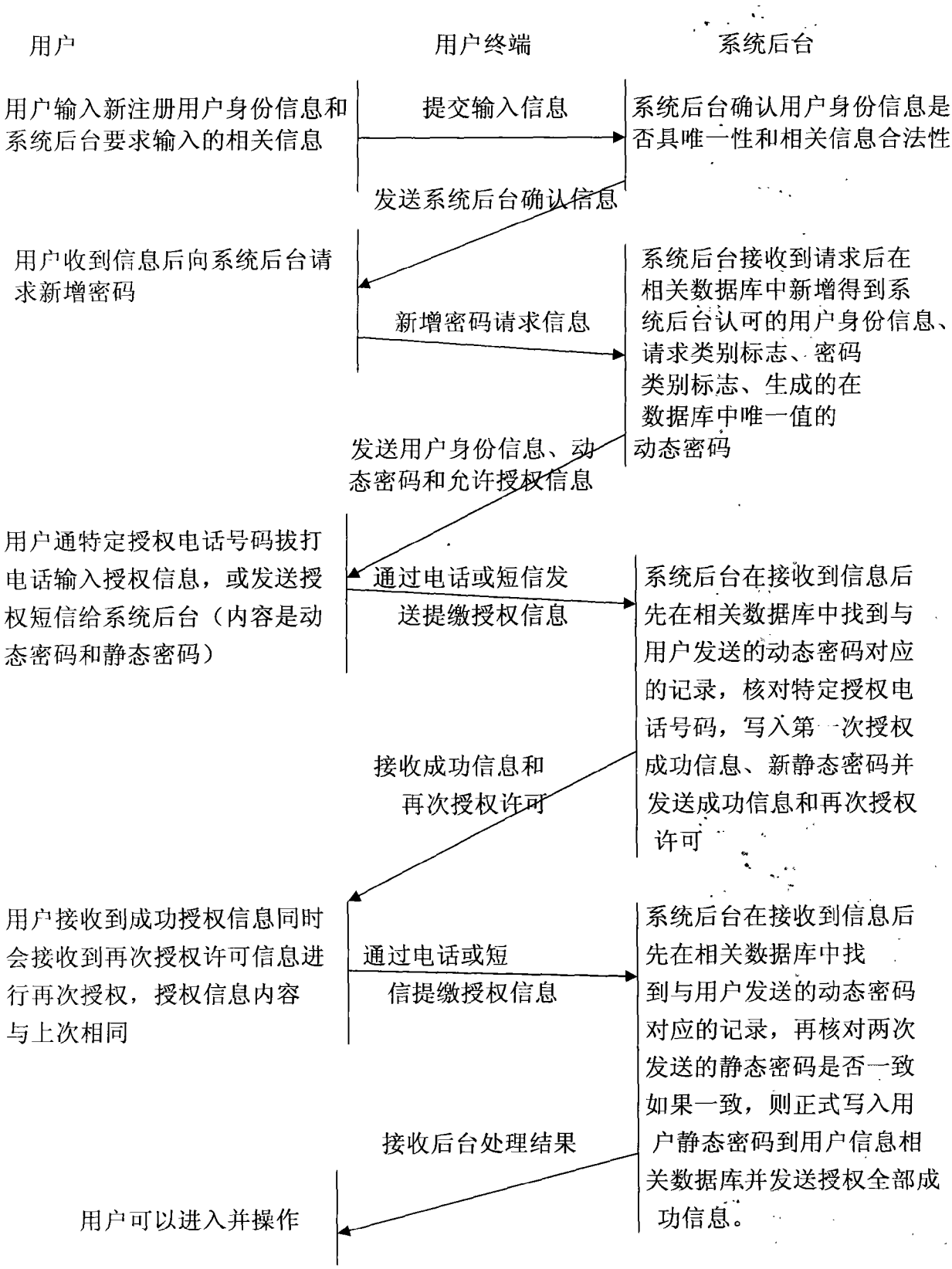

用户
用户终端
系统后台
用户输入新注册用户身份信息和系统后台要求输入的相关信息
提交输入信息
系统后台确认用户身份信息是否具唯一性和相关信息合法性
发送系统后台确认信息
用户收到信息后向系统后台请求新增密码
新增密码请求信息
系统后台接收到请求后在相关数据库中新增得到系统后台认可的用户身份信息、请求类别标志、密码类别标志、生成的在数据库中唯一值的动态密码
发送用户身份信息、动态密码和允许授权信息
用户通特定授权电话号码拨打电话输入授权信息，或发送授权短信给系统后台（内容是动态密码和静态密码）
通过电话或短信发送提缴授权信息
系统后台在接收到信息后先在相关数据库中找到与用户发送的动态密码对应的记录，核对特定授权电话号码，写入第一次授权成功信息、新静态密码并发送成功信息和再次授权许可
接收成功信息和再次授权许可
用户接收到成功授权信息同时会接收到再次授权许可信息进行再次授权，授权信息内容与上次相同
通过电话或短信提缴授权信息
系统后台在接收到信息后先在相关数据库中找到与用户发送的动态密码对应的记录，再核对两次发送的静态密码是否一致如果一致，则正式写入用户静态密码到用户信息相关数据库并发送授权全部成功信息。
接收后台处理结果
用户可以进入并操作

图 1

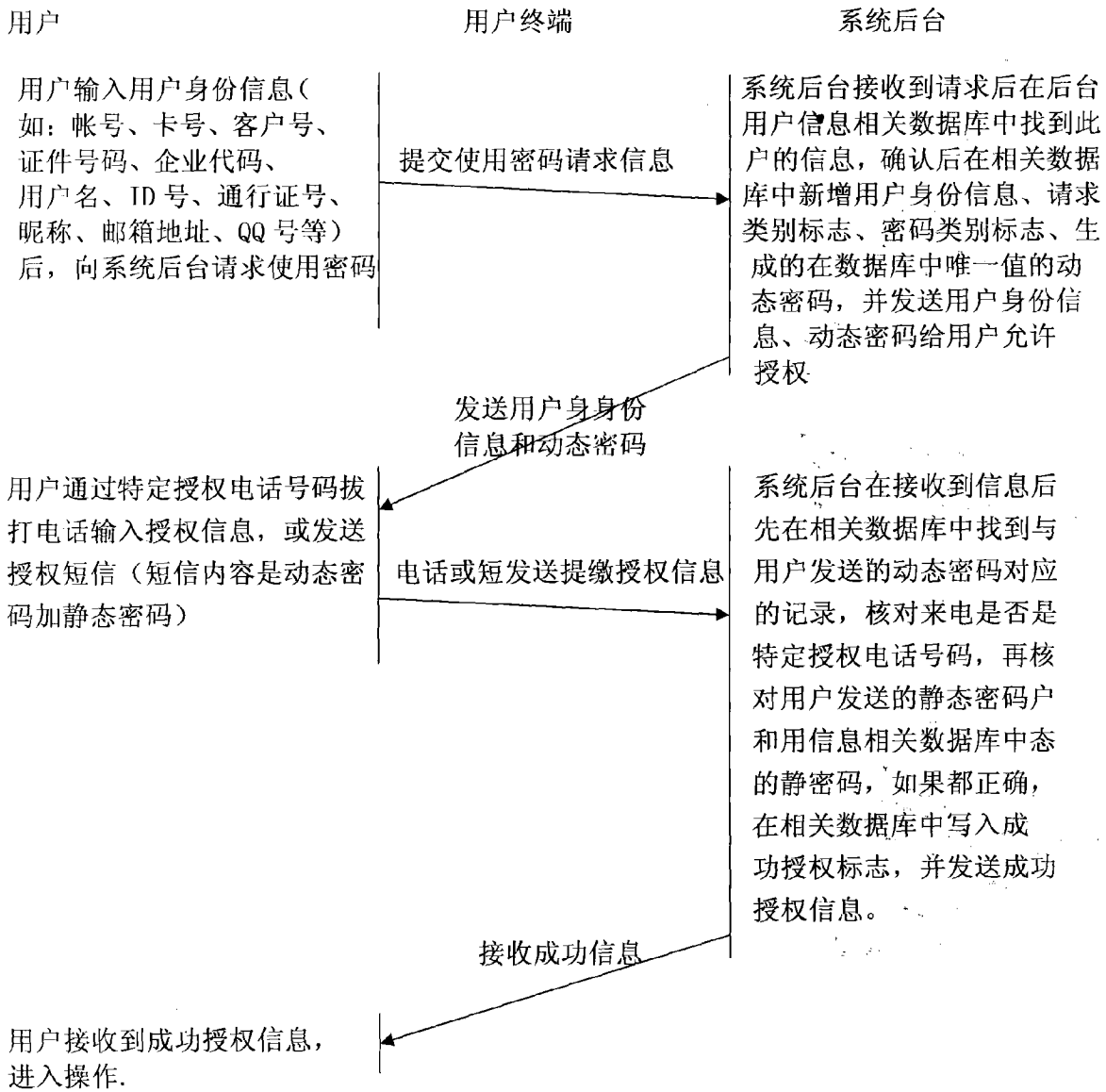

用户
用户终端
系统后台
用户输入用户身份信息(如：帐号、卡号、客户号、证件号码、企业代码、用户名、ID 号、通行证号、昵称、邮箱地址、QQ 号等)后，向系统后台请求使用密码
提交使用密码请求信息
系统后台接收到请求后在后台用户信息相关数据库中找到此户的信息，确认后在相关数据库中新增用户身份信息、请求类别标志、密码类别标志、生成的在数据库中唯一值的动态密码，并发送用户身份信息、动态密码给用户允许授权
发送用户身身份信息和动态密码
用户通过特定授权电话号码拨打电话输入授权信息，或发送授权短信（短信内容是动态密码加静态密码）
电话或短发送提缴授权信息
系统后台在接收到信息后先在相关数据库中找到与用户发送的动态密码对应的记录，核对来电是否是特定授权电话号码，再核对用户发送的静态密码户和用信息相关数据库中态的静密码，如果都正确，在相关数据库中写入成功授权标志，并发送成功授权信息。
接收成功信息
用户接收到成功授权信息，进入操作.

图 2

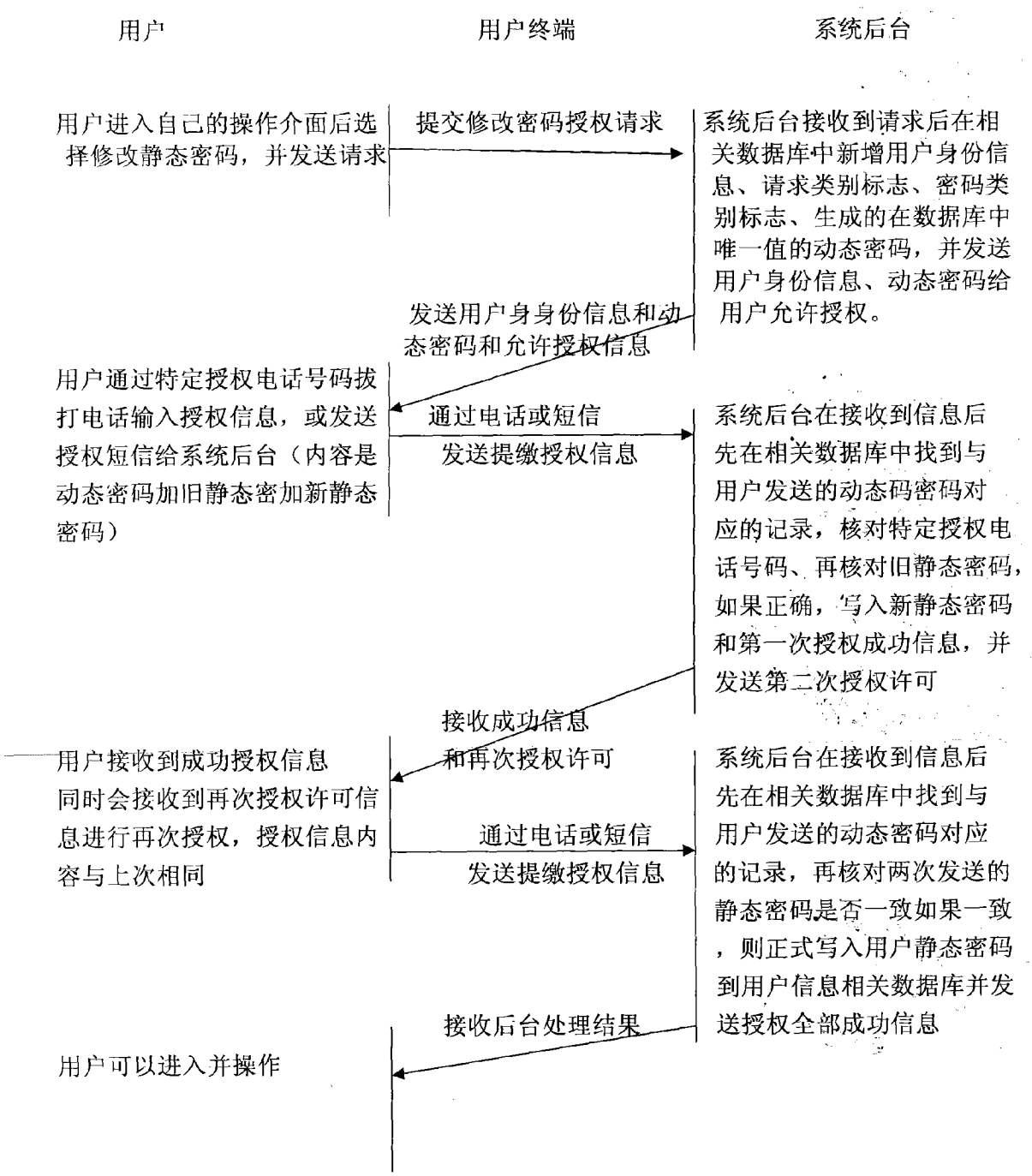

用户
用户终端
系统后台
用户进入自己的操作介面后选择修改静态密码，并发送请求
提交修改密码授权请求
系统后台接收到请求后在相关数据库中新增用户身份信息、请求类别标志、密码类别标志、生成的在数据库中唯一值的动态密码，并发送用户身份信息、动态密码给用户允许授权。
发送用户身身份信息和动态密码和允许授权信息
用户通过特定授权电话号码拨打电话输入授权信息，或发送授权短信给系统后台（内容是动态密码加旧静态密加新静态密码）
通过电话或短信
发送提缴授权信息
系统后台在接收到信息后先在相关数据库中找到与用户发送的动态码密码对应的记录，核对特定授权电话号码、再核对旧静态密码，如果正确，写入新静态密码和第一次授权成功信息，并发送第二次授权许可
接收成功信息和再次授权许可
用户接收到成功授权信息同时会接收到再次授权许可信息进行再次授权，授权信息内容与上次相同
通过电话或短信
发送提缴授权信息
系统后台在接收到信息后先在相关数据库中找到与用户发送的动态密码对应的记录，再核对两次发送的静态密码是否一致如果一致，则正式写入用户静态密码到用户信息相关数据库并发送授权全部成功信息
接收后台处理结果
用户可以进入并操作

图 3

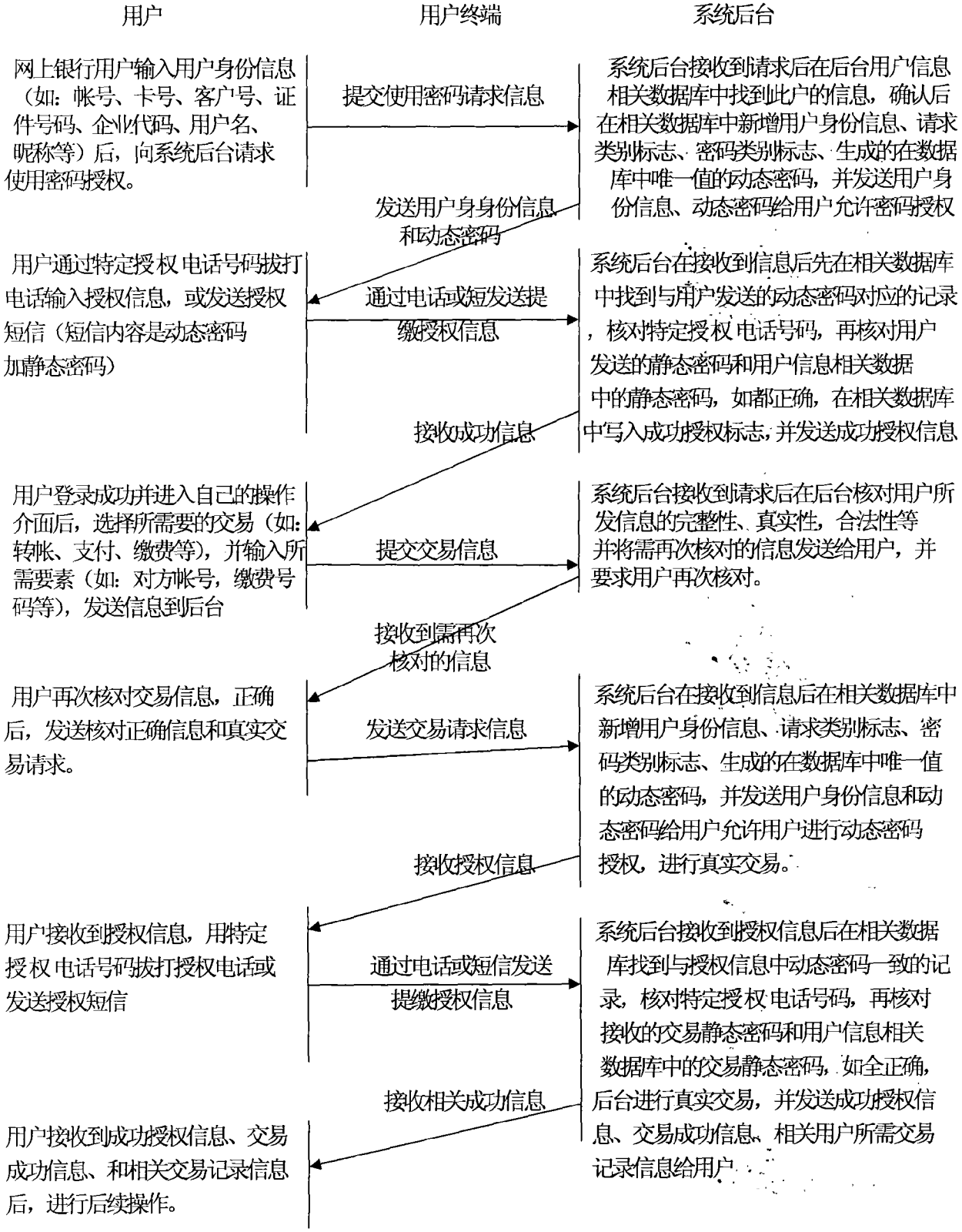

用户
用户终端
系统后台
网上银行用户输入用户身份信息（如：帐号、卡号、客户号、证件号码、企业代码、用户名、昵称等）后，向系统后台请求使用密码授权。
提交使用密码请求信息
系统后台接收到请求后在后台用户信息相关数据库中找到此户的信息，确认后在相关数据库中新增用户身份信息、请求类别标志、密码类别标志、生成的在数据库中唯一值的动态密码，并发送用户身份信息、动态密码给用户允许密码授权
发送用户身身份信息和动态密码
用户通过特定授权电话号码拨打电话输入授权信息，或发送授权短信（短信内容是动态密码加静态密码）
通过电话或短发送提缴授权信息
系统后台在接收到信息后先在相关数据库中找到与用户发送的动态密码对应的记录，核对特定授权电话号码，再核对用户发送的静态密码和用户信息相关数据中的静态密码，如都正确，在相关数据库中写入成功授权标志，并发送成功授权信息
接收成功信息
用户登录成功并进入自己的操作介面后，选择所需要的交易（如：转帐、支付、缴费等），并输入所需要素（如：对方帐号，缴费号码等），发送信息到后台
提交交易信息
系统后台接收到请求后在后台核对用户所发信息的完整性、真实性，合法性等并将需再次核对的信息发送给用户，并要求用户再次核对。
接收到需再次核对的信息
用户再次核对交易信息，正确后，发送核对正确信息和真实交易请求。
发送交易请求信息
系统后台在接收到信息后在相关数据库中新增用户身份信息、请求类别标志、密码类别标志、生成的在数据库中唯一值的动态密码，并发送用户身份信息和动态密码给用户允许用户进行动态密码授权，进行真实交易。
接收授权信息
用户接收到授权信息，用特定授权电话号码拨打授权电话或发送授权短信
通过电话或短信发送提缴授权信息
系统后台接收到授权信息后在相关数据库找到与授权信息中动态密码一致的记录，核对特定授权电话号码，再核对接收的交易静态密码和用户信息相关数据库中的交易静态密码，如全正确，后台进行真实交易，并发送成功授权信息、交易成功信息、相关用户所需交易记录信息给用户
接收相关成功信息
用户接收到成功授权信息、交易成功信息、和相关交易记录信息后，进行后续操作。

图 4

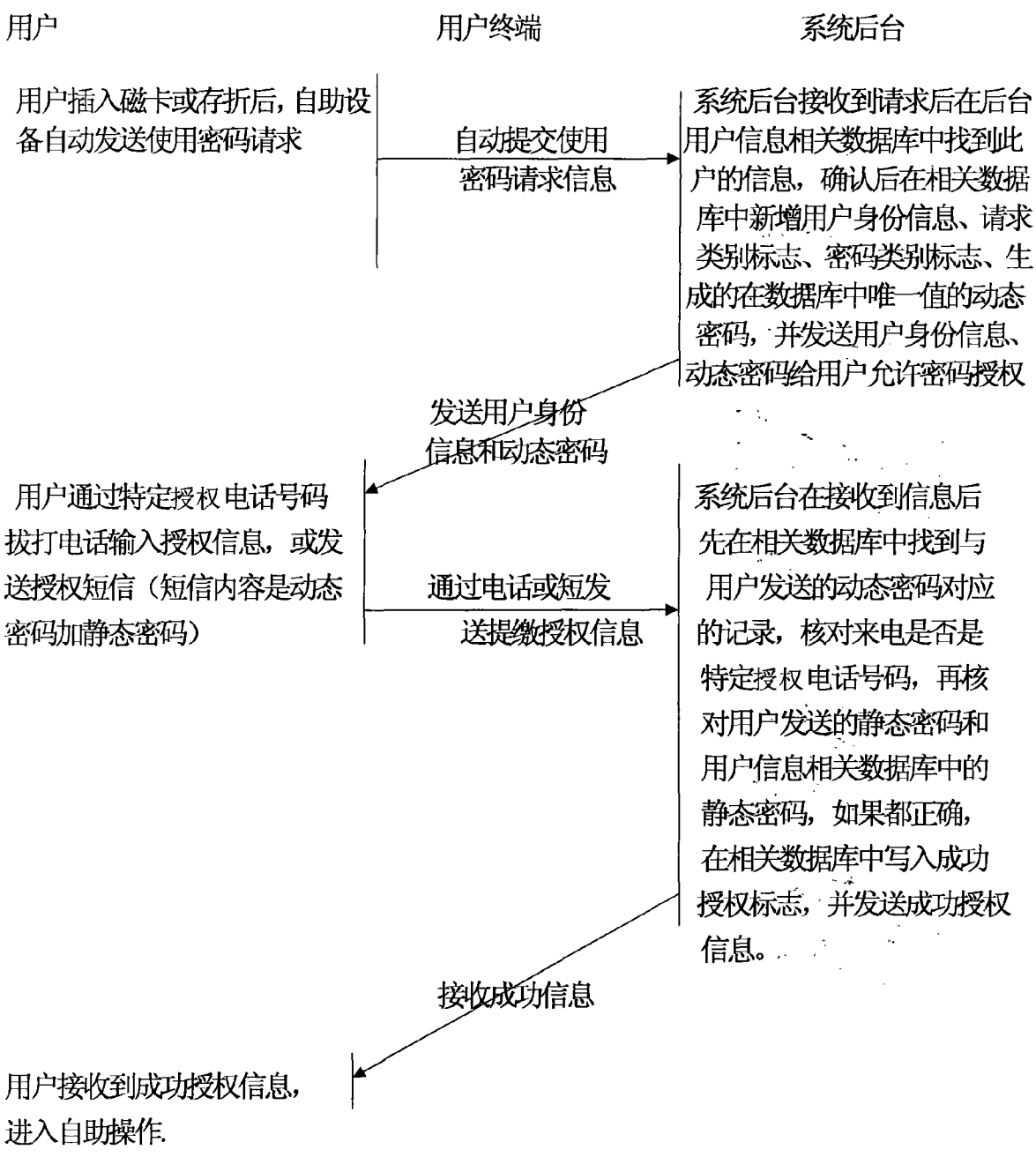

用户
用户终端
系统后台
用户插入磁卡或存折后，自助设备自动发送使用密码请求
自动提交使用密码请求信息
系统后台接收到请求后在后台用户信息相关数据库中找到此户的信息，确认后在相关数据库中新增用户身份信息、请求类别标志、密码类别标志、生成的在数据库中唯一值的动态密码，并发送用户身份信息、动态密码给用户允许密码授权
发送用户身份信息和动态密码
用户通过特定授权电话号码拔打电话输入授权信息，或发送授权短信（短信内容是动态密码加静态密码）
通过电话或短发送提缴授权信息
系统后台在接收到信息后先在相关数据库中找到与用户发送的动态密码对应的记录，核对来电是否是特定授权电话号码，再核对用户发送的静态密码和用户信息相关数据库中的静态密码，如果都正确，在相关数据库中写入成功授权标志，并发送成功授权信息。
接收成功信息
用户接收到成功授权信息，进入自助操作.

图 5