[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/32 (2006.01)
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 200310111571.4

[45] 授权公告日 2006 年 8 月 2 日

[11] 授权公告号 CN 1268157C

[22] 申请日 2003.12.12
[21] 申请号 200310111571.4
[71] 专利权人 华中科技大学
地址 430074 湖北省武汉市洪山区珞喻路 1037 号
[72] 发明人 胡汉平 王祖喜 吴晓刚 曾伟国 吴 俊 王凌斐 刘 博
审查员 张 慧

[74] 专利代理机构 华中科技大学专利中心
代理人 曹葆青

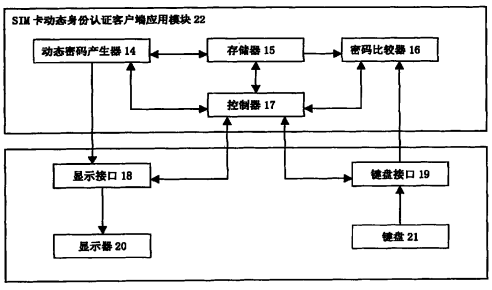
权利要求书 1 页 说明书 11 页 附图 8 页

[54] 发明名称

一种用于动态身份认证的手机

[57] 摘要

本发明公开了一种用于动态身份认证的手机，该手机的 SIM 卡中设置有动态身份认证客户端应用模块，可独立产生与认证服务器相同且同步的动态身份认证密码；存储器与动态密码产生器、密码比较器和控制器相连，动态密码产生器用于由当前工作密码 Ks 产生用户当前认证密码，该认证密码与服务器的相对应，并将该认证密码通过手机的输出装置告知用户；密码比较器用来判断手机用户是否合法；控制器用于控制各模块的协调工作。 该手机与现有的手机不同的是它可以产生动态身份认证密码，而且该手机可以与认证服务器共同完成认证系统安全协议。 通过安全协议，用户可以随时开启和取消动态身份认证服务、主动请求手机和认证系统同步、用户请求解锁等功能。



1、一种用于动态身份认证的手机，其特征在于：该手机的SIM卡中设置有动态身份认证客户端应用模块，该应用模块由动态密码产生器(14)、存储器(15)、密码比较器(16)和控制器(17)构成，可独立产生与认证服务器相同且同步的动态身份认证密码；

存储器(15)用于存储用户ID、用户身份证号、注册密码Pr、加密密钥Ke，并负责存储用于产生当前动态身份认证密码的当前工作密码Ks、客户应用模块的启动密码或手机令牌口令Pt和在令牌上连续错误地输入令牌访问密码的次数Nt；它与动态密码产生器(14)、密码比较器(16)和控制器(17)相连；

动态密码产生器(14)用于由当前工作密码Ks依据时间或事件的同步方式产生用户当前认证密码，该认证密码与服务器的当前认证密码相对应，并将该认证密码通过手机的输出装置告知用户；

密码比较器(16)用来判断手机用户是否合法；

控制器(17)用于控制上述各模块的协调工作，它根据预先确定的协议，控制手机通过所接收到的由服务器发送过来的工作密码修改存储器（15）中存储的当前工作密码Ks，校正由于用户的误操作或时间积累误差所导致的动态身份认证手机和服务器中动态密码产生器之间的失步；还控制手机用所接收到由服务器发送过来的加密密钥修改存储器（15）中存储的加密密钥Ke；控制器(17)控制手机与服务器之间传送预先定义的请求、应答信息，实现与之相对应的异地开启、取消和解锁的动态身份认证服务。

一种用于动态身份认证的手机

技术领域

本发明属于信息安全认证技术，它综合利用电子计算机、信息编码及移动通讯技术实现，可以应用于银行、证券等许多需要进行身份认证的系统和领域，具体涉及一种用于动态身份认证的手机。

背景技术

身份认证是实现网络安全的重要机制之一，在安全的网络通信中，涉及的通信各方必须通过某种形式的身份认证机制来验证他们的身份与所宣称的是否一致，然后才能实现对于不同用户的访问控制和记录。早在二十世纪七十年代初期，国际银行卡片协会就遇到了如何对用户进行身份认证以确保系统安全性的问题。随着信息技术的快速发展，窃听者可以采用低级的窥视方法获取口令；利用“Password 文件”系统的猜测口令、分析协议和滤出口令（利用嗅控程序）；用 TSR（终端驻留程序）监视和获得口令；用特洛伊木马程序截获口令等方法突破计算机安全机制进行非法访问；用电脑病毒（如： bugbear 病毒）从电脑上盗取信用卡号码、网上银行的资料和银行密码。比较有效的预防方法就是采用动态电子密码技术。其实质是按某种规律定时或每次使用之后更换密码，用户每次访问时输入的密码都不相同，这就给电子盗窃增加了难度。

利用上述技术的方法和系统我们已在“动态电子密码形成方法”（99116451.2）和“动态电子密码系统”（00114328.X）两项发明专利中提出。但是，由于用户密码卡与主机系统的同步主要是采用非接触式时钟同步技术，由此可能会导致时间上的误差积累，因此需要在一段时间之后校正双方的时钟；此外，用户密码卡的使用增加了用户的使用负担；而且这种带键盘和液晶显示屏的用户密码卡也会因使用不慎而损坏。为克服上述缺点，我们又提出了“动态密码无线传输方法”（99116517.9）的发明专利。但是，由于该方法中动态密码以明文方式传输，窃听者可以很方便的截获身份认证密码。而且，该方法在无线网络通信拥挤时无法保证认证的实时

性。本发明人发明了一种新的动态身份认证方法，见本申请人另一专利申请“一种动态身份认证方法和系统”。该方法既可有效防范通过窥视或猜测认证密码来进行的非法登录，又可有效防范通过截获传输数据来进行的非法登录，可大幅度提高系统的安全性，而且认证过程中的动态密码不需要使用无线网络传输，保证了认证的实时性。该方法在使用过程中需采用一种专用手机作为身份令牌。

发明内容

本发明的目的在于提供一种用于动态身份认证的手机，该手机可以作为身份令牌，在动态身份认证中使用，以提高认证的安全性和实时性。

本发明提供的一种用于动态身份认证的手机，其特征在于：该手机的SIM卡中设置有动态身份认证客户端应用模块，该应用模块由动态密码产生器、存储器、密码比较器和控制器构成，可独立产生与认证服务器相同且同步的动态身份认证密码；

存储器用于存储用户ID、用户身份证号、注册密码Pr、加密密钥Ke，并负责存储用于产生当前动态身份认证密码的当前工作密码Ks、客户应用模块的启动密码或手机令牌口令Pt和在令牌上连续错误地输入令牌访问密码的次数Nt；它与动态密码产生器、密码比较器和控制器相连；

动态密码产生器用于由当前工作密码Ks依据时间或事件的同步方式产生用户当前认证密码，该认证密码与服务器的当前认证密码相对应，并将该认证密码通过手机的输出装置告知用户；

密码比较器用来判断手机用户是否合法；

控制器用于控制上述各模块的协调工作，它根据预先确定的协议，控制手机通过所接收到的由服务器发送过来的工作密码修改存储器中存储的当前工作密码Ks，校正由于用户的误操作或时间积累误差所导致的动态身份认证手机和服务器中动态密码产生器之间的失步；还控制手机用所接收到由服务器发送过来的加密密钥修改存储器中存储的加密密钥Ke；控制器控制手机与服务器之间传送预先定义的请求、应答信息，实现与之相对应的异地开启、取消和解锁的动态身份认证服务。

本发明提供的手机与现有的手机不同的是它可以产生动态身份认证密码,而且该手机可以与认证服务器共同完成认证系统安全协议。通过安全协议，用户可以随时开启和取消动态身份认证服务、主动请求手机和认证系统同步、用户请求解锁等功能。

附图说明

图 1 为本发明提供的手机的动态身份认证客户端应用模块的结构示意图；

图 2 为认证系统整体结构图；

图 3 为认证服务器软件体系结构图；

图 4 为动态身份认证过程图，其中 4.1 是手机端执行过程，4.2 是认证服务器端执行过程；

图 5 为启动动态身份认证服务过程图，其中 5.1 是手机端执行过程，5.2 是认证服务器端执行过程；

图 6 为申请系统同步过程图，其中 6.1 是手机端执行过程，6.2 是认证服务器端执行过程；

图 7 为申请用户帐号解锁过程图，其中 7.1 是手机端执行过程，7.2 是认证服务器端执行过程；

图 8 为取消动态身份认证服务过程图，其中 8.1 是手机端执行过程，8.2 是认证服务器端执行过程；

图 9 为安全协议消息格式说明图，其中 9.1 是协议消息头格式，9.2 是服务请求消息体格式，9.3 是服务应答消息体格式；

具体实施方式

本发明提供的手机可以在普通手机的 SIM 卡上写入动态身份认证客户端应用模块。手机的 SIM 卡具备 JAVA 程序运行环境，动态身份认证客户端应用模块是使用 JAVA 语言开发的嵌入式应用模块，可以由手机生产厂家或其它机构 SIM 卡写入设备(如 TY311)写入到手机的 SIM 卡中。如图 1 所示，22 是手机令牌中 SIM 卡部分结构图，23 是手机的接口部分结构图。手机中的动态身份认证客户端应用模块包括动态密码产生器 14、存储器 15、密码比较器 16 和控制器 17。存储器 15 用于存储用户 ID、用户身份证号、注册密码 Pr、加、解密密钥 Ke，并负责存储用于产生当前动态身份认证密码的

当前工作密码 Ks（与服务器中所存储当前工作密码是相同的）、客户应用模块的启动密码或手机口令 Pt 和在手机上连续错误地输入令牌访问密码的次数 Nt。加密密钥 Ke 和当前工作密码 Ks 是在用户申请服务时，认证服务器为用户手机分配的；客户应用模块的启动密码或手机口令 Pt 由用户提供并写入 SIM 卡。存储器 15 与动态密码产生器 14、密码比较器 16 和控制器 17 相连。动态密码产生器 14 用来由当前工作密码 Ks 产生用户当前认证密码，可以是 RC4 等流密码算法，与服务器认证密码相对应。动态密码产生器 14 通过手机的显示接口 18 与显示器 20 相连，将所产生的密码显示在显示屏上。密码比较器 16 用来判断手机用户是否合法，它通过键盘接口 19 与键盘 21 相连，这样用户通过键盘输入的密码与客户应用模块的启动密码或手机口令 Pt 相比较。控制器 17 用来控制各个模块的协调工作。

本发明只是在现有手机中加入上述模块，它不影响手机原来的结构、功能及工作过程，这些也不是本发明的内容，故在此不再赘述。下文中，我们将设置有上述应用模块的手机称之为“手机令牌”。

下面以银行系统为例，结合附图详细说明采用本发明提供的手机进行动态身份认证的系统结构和认证过程。

一、 系统结构说明

图 2 是认证系统整体结构图，包括用户终端 6、用户信息服务器 1、认证服务器 2 和手机令牌 5。用户信息服务器 1 是系统中的数据服务器，使用 oracle9i 数据库系统，其中存放按照身份认证协议所设定的表格，提供认证过程中所需要的每一用户信息。它包括如下字段：身份证号、用户 ID、注册密码 Pr、加、解密密钥 Ke、当前工作密码 Ks（与手机令牌中所存储当前工作密码是相同的）、帐号正被使用的标志（防止竞争攻击）和手机号等。用户信息服务器 1 接收认证服务器 2 的操作（查询和修改用户信息）请求，该操作请求使用 OLEDB 数据接口。认证服务器 2 是整个认证系统的 Server 端，负责接收和完成用户的服务请求。认证服务器中布置有认证服务器端的服务模块、密码产生模块 3、通信模块 4。密码产生模块 3 负责产生服务器端的动态身份认证密码，是“动态电子密码产生算法”的硬件实现，它使用服务器总线和认证服务器 2 通信。通信模块 4 使用 COM 口和认证服务器 2 通信，手机令牌 5 是能够完成认证令牌功能的用户手机，其 SIM 卡具备 JAVA 程序运行环境。动态身份认证客户端的应用模块是使用 JAVA

语言开发的嵌入式应用模块，它通过 SIM 卡写入设备 TY311 写入到手机令牌 5 的 SIM 卡中。手机令牌 5 中的动态身份认证客户端的应用模块和认证服务器中的密码产生模块 3 使用相同的动态密码产生算法，并独立产生同步的动态身份认证密码。用户终端 6(如 ATM 终端)通过银行内部网络 7 与身份认证服务器 2 通信。认证时由用户向认证服务器提交手机令牌产生的用户端动态身份认证密码，认证服务器将用户端动态身份认证密码和自己产生的服务器端动态身份认证密码进行比较，并根据比较结果判断用户是否通过身份认证。

图 3 是认证服务器端服务模块结构图。认证服务器端服务模块是认证系统的 Server 端软件，主要完成网络传输控制、认证系统安全协议处理、信息传输的加密和解密、用户信息访问和动态密码获取与暂存等功能。认证服务器端服务模块包括用户信息访问模块 8、动态密码访问模块 9、协议处理模块 10、核心管理模块 11、加密模块 12 和网络传输模块 13。用户信息访问模块 8 是后端用户信息服务器的访问模块，负责完成核心管理模块 11 的用户信息管理命令，包括建立新帐户、修改已有帐户信息、删除过期帐户信息、锁定或解锁用户帐号和控制用户访问权限等。动态密码访问模块 9 是认证服务中动态密码产生模块的访问模块，它接收核心管理模块 11 提供的用户密钥信息，产生认证过程中的动态密码，并将动态密码交给核心管理模块 11 暂存。协议处理模块 10 是动态身份认证系统安全协议的 Server 处理端，它接收核心管理模块 11 提供的安全协议信息，并将处理结果返回给核心管理模块 11。核心管理模块 11 是整个认证服务器端软件的核心，负责协调其他模块之间的相互关系和信息传递。加密模块 12 主要完成核心管理模块 11 的信息加解密请求。网络传输模块 13 主要完成服务器端的信息传输任务，它接收银行专有网络的信息和认证服务器中通信模块的信息。它同时也处理核心管理模块的信息传输请求，将不同类型的信息发送到不同的通信网络中。

二、认证过程

如图 4 所示，认证过程包括以下步骤：

（1）用户在 ATM 终端插入银行卡，提交用户信息，并向身份认证服务器发送身份认证请求；

（2）身份认证服务器接收到认证请求后，首先验证用户信息的合法性。如果该用户是合法用户（该用户的信息已经保存在用户信息数据库），身份认证服务器产生服务器端动态身份认证密码并暂存，并在用户终端提示用户输入用户端动态身份认证密码。此步骤的详细处理过程如下：

(2.1)身份认证服务器中的网络传输模块接收到认证请求后，向核心管理模块提交用户请求。

(2.2)核心管理模块通过用户信息访问模块查询用户信息数据库，如果用户信息数据库中没有该用户的信息，核心管理模块生成错误报文，并通过网络传输模块传输给 ATM 终端，终端收到该报文后向用户提示：用户信息错误。如果用户信息数据库中有该用户的信息，那么用户信息管理模块向核心管理模块返回该用户的用户信息，并查看其中的 Identification_Mode 字段值（字段值为 0 表示用户使用静态密码认证，为 1 则表示使用动态密码认证）。

(2.3)如果 Identification_Mode＝1，则核心管理模块查询此用户的 Lock_State 字段(字段值为 0 表示用户为被锁定，为 1 表示用户已被锁定)，如果 Lock_State＝1，核心管理模块向 ATM 终端发送信息，提示该用户已被锁定，并退出认证过程，否则核心管理模块向动态密码访问模块传递该用户的当前工作密码，动态密码产生模块根据当前工作密码产生该用户此次动态认证密码并返回给核心管理模块，核心管理模块将该用户的动态身份认证密码暂存，并向 ATM 终端发送信息，提示用户输入用户端动态身份认证密码。

合法用户如果发现自己的帐户被锁定，则可以通过手机令牌申请解锁，解锁的具体过程见动态身份认证安全协议的“用户申请解锁”部分。

(3)用户通过手机令牌产生用户端动态身份认证密码，显示在手机屏幕上。

必须强调的是，用户在使用银行提供的动态身份认证服务之前必须完成“手机令牌初始化”和“开启动态身份认证服务”两个过程。两个过程的详细细节见动态身份认证安全协议的“手机令牌初始化”和“开启动态身份认证服务”两部分。

(4)用户将手机屏幕上所显示用户端动态身份认证密码通过用户终端输入并传送到身份认证服务器，等待身份认证。

(5)如果身份认证服务器接收到的用户端动态身份认证密码与服务器端动态身份认证密码一致，则通过身份认证；否则，认证不通过。此步骤的详细过程如下：

(5.1)认证服务器的核心管理模块从网络传输模块得到该用户提交的用户端动态身份认证密码；

(5.2)核心管理模块比较用户端动态身份认证密码和暂存的服务器端动态身份认证密码，如果两者一致，则核心管理模块通过网络传输模块向ATM终端发送信息，提示用户认证成功，否则，核心管理模块通过用户信息网络模块修改用户信息数据库中用户信息，将此用户信息中的WrongPSW_Count字段加1(WrongPSW_Count达到临界值时该用户将被锁定)，并通过网络传输模块向ATM终端发送行信息，要求用户重新开始认证过程；

必须指出，如果合法用户发现通过正确的操作后无法通过认证，用户可以使用手机令牌请求系统同步，同步过程见动态身份认证安全协议的“用户申请系统同步”部分。

三．动态身份认证安全协议

基于手机令牌方式的动态身份认证方法是一种基于同步动态身份认证密码的认证方法，在实施过程中需要保证手机令牌和认证服务器的系统同步，本发明使用动态身份认证安全协议来实现该目的。动态身份认证安全协议是基于手机令牌方式的动态身份认证方法的支撑协议。它是一种基于短信的交互协议，定义了手机令牌和认证服务器之间交互的流程、交互的信息格式以及保障交互过程安全性的安全机制（包括交互信息加密方法、加密密钥管理方法以及交互信息的认证方法）。安全协议不但向用户提供了手机令牌和认证服务器端的系统同步功能，而且也支持用户能够使用手机令牌完成动态身份认证服务启动、用户解锁和用户取消动态身份认证服务等功能。下面从协议过程、安全机制和信息格式几方面详细介绍安全协议的基本原理。

（一）协议过程

1．手机令牌初始化

手机令牌初始化过程分为客户端应用模块写入、客户端应用模块初始化两个环节。客户端应用模块写入指使用 SIM 卡写入设备 TY311 在用户手

机 SIM 卡中写入基于 JAVA 嵌入式动态身份认证客户端应用模块。客户端应用模块初始化主要是对 SIM 卡中的客户端应用模块进行参数设置，包括设置用户身份信息、信息加、解密密钥、客户端的应用模块启动密码、当前工作密码和用户注册密码等参数。客户端的应用模块启动密码和注册密码由用户自己选定，并随时可以修改。客户端的应用模块启动密码用于保证只有合法的手机令牌使用者才可以使用手机令牌完成动态身份认证过程。注册密码用于保证只有合法用户才可以使用手机令牌完成“解锁”和“取消动态身份认证服务”功能；当前工作密码和信息加、解密密钥分为手机令牌端的当前工作密码和认证服务器端的当前工作密码，认证服务器端的当前工作密码和信息加、解密密钥也是用户信息的一部分，两端应具有相同的当前工作密码和信息加、解密密钥。在初始化时，由随机数产生器分别产生初始的当前工作密码和信息加、解密密钥，并将手机令牌中的当前工作密码、信息加、解密密钥和认证服务器端的当前工作密码、信息加、解密密钥设置为该初始的当前工作密码和该信息加、解密密钥；。

2. 用户开启动态身份认证服务

用户开启动态身份认证服务过程是指用户使用手机令牌向认证服务器端发出“开启动态身份认证服务请求”，认证服务器接到该请求后首先验证该用户的用户信息的合法性并做相应的处理，然后向该用户发送“开启动态身份认证服务应答”。详细过程如下：

1）用户输入手机令牌客户应用模块启动密码（手机令牌初始化时设定），通过手机令牌端的身份验证；

2）用户通过手机手机令牌向认证服务器发送“开启动态身份认证服务请求”信息；

3）认证服务器接收到“开启动态身份认证服务请求”信息后验证信息合法性（验证信息中的用户 ID 和注册密码，该注册密码是在用户手机初始化的时候确定）；

4）认证服务器在用户信息库中将该用户的认证方式标记为动态身份认证方式，然后向手机令牌发送“开启动态身份认证服务应答”信息；

5）手机令牌接收“开启动态身份认证服务应答”信息，提示动态身份认证服务已经开启。

用户开启动态身份认证服务时手机令牌端和认证服务器端的处理过程

见图 5 。

3．用户申请系统同步

前面提到过，用户能够通过认证服务器认证的关键是手机令牌和认证服务器保持系统同步。但由于存在使两端不同步的异常情况（例如用户认证过程中手机突然断电等），因此需要通过执行动态身份认证安全协议的“用户申请系统同步”恢复两端的系统同步状态。详细过程如下：

1）用户输入手机令牌客户应用模块启动密码，通过手机令牌端的身份验证；

2）用户通过手机手机令牌向认证服务器发送“申请系统同步请求”信息；

3）认证服务器接收到“申请系统同步请求”信息后验证信息合法性（验证信息中的用户 ID 和注册密码，该注册密码是在用户手机初始化的时候确定）；

4）认证服务器从用户信息库中取出服务器端的当前工作密码；

5）认证服务器生成“申请系统同步应答”信息，将服务器端的当前工作密码写入信息中的“服务方信息”字段，然后向用户发送应答信息；

6）手机令牌接收“申请系统同步应答”信息后提取信息中的当前工作密码，并将手机令牌端的动态电子密码当前工作密码设置为信息中所提取的当前工作密码，完成系统同步。

用户申请系统同步时手机令牌端和认证服务器端的处理过程见图 6。

4．用户申请解锁

如果用户发现自己的帐号被银行锁定，用户可以通过手机令牌申请解锁。详细过程如下：

1）用户输入手机令牌客户应用模块启动密码，通过手机令牌端的身份验证；

2）用户通过手机手机令牌向认证服务器发送“申请帐号解锁请求”信息；

3）认证服务器接收到“申请帐号解锁请求”信息后验证信息合法性（验证信息中的用户 ID 和注册密码，该注册密码是在用户手机初始化的时候确定）；

4）认证服务器在用户信息数据库中将该用户的“用户状态”字段设置

为解锁状态，然后向用户发送“申请帐号解锁应答”信息；

5）手机令牌接收“申请帐号解锁应答”信息，提示用户解锁成功。

用户申请解锁时手机令牌端和认证服务器端的处理过程见图 7。

5．用户取消动态身份认证服务

用户不但可以通过手机令牌开启动态身份认证服务，而且可以使用手机令牌取消动态身份认证服务。详细过程如下：

1）用户输入手机令牌客户应用模块启动密码，通过手机令牌端的身份验证；

2）用户通过手机手机令牌向认证服务器发送“取消动态身份认证服务请求”信息；

3）认证服务器接收到“取消动态身份认证服务请求”信息后验证信息合法性（验证信息中的用户 ID 和注册密码，该注册密码是在用户手机初始化的时候确定）；

4）认证服务器在用户信息库中将该用户的认证方式标记为固定密码身份认证方式，然后向手机令牌发送“取消动态身份认证服务应答”信息；

5）手机令牌接收“取消动态身份认证服务应答”信息，提示动态身份认证服务已经取消。

用户取消动态身份认证服务时手机令牌端和认证服务器端的处理过程见图 8。

（二）安全协议的安全机制

安全协议根据加、解密密钥和 DES（Data Encryption Standard）等分组密码算法对交互信息进行加、解密。

协议不但定义了交互信息的加、解密方法，也规定了相应的加、解密密钥管理细节。协议规定：在手机令牌初始化时写入加、解密密钥；使用基于信息使用次数的加、解密密钥更新方法，也即在用户手机端维护一个信息计数器，统计手机令牌发送的请求信息个数，当计数器达到门限值时，手机令牌自动在交互信息中设置密钥更新标志位，认证服务器接到该信息后就在应答信息中携带新的信息加、解密密钥，手机令牌接到新的密钥后就开始使用新的密钥对信息进行加、解密。

（三）安全协议信息格式

协议信息格式见图 9。信息分为服务请求信息和服务应答信息两种，每

信息又分为信息头和信息体两部分。具体格式说明如下：

（1）协议信息头

版本：协议的版本号；

头部长度：协议信息头的长度；

服务方 ID：使用唯一 ID 标识每一个提供动态认证服务的服务方；

总长度：信息的总长度，之所以设置该字段是因为考虑到以后信息体的扩展；

（2）服务请求信息体

服务类型：第 1 bit 指明信息类型；第 2 bit 指明客户是否请求信息加密密钥更新或者在应答信息中是否有携带更新的密钥；3-8 比特是信息类型比特；

验证码：信息使用字节求和验证；

序列号：标识每个请求信息，防止应答重放攻击；

用户 ID：用户认证帐号；

注册码：用户手机令牌初始化是生成，用户的私有数据。服务器使用用户 ID 和用户验证码对用户身份确认；

（3）服务应答信息体

服务类型：同上；

验证码：同上；

序列号：拷贝请求中的序列号，保证应答和请求的一一对应关系；

新密钥：携带协议信息加密新密钥；

服务方信息：服务方返回给用户的应答信息，例如算法当前工作密码；

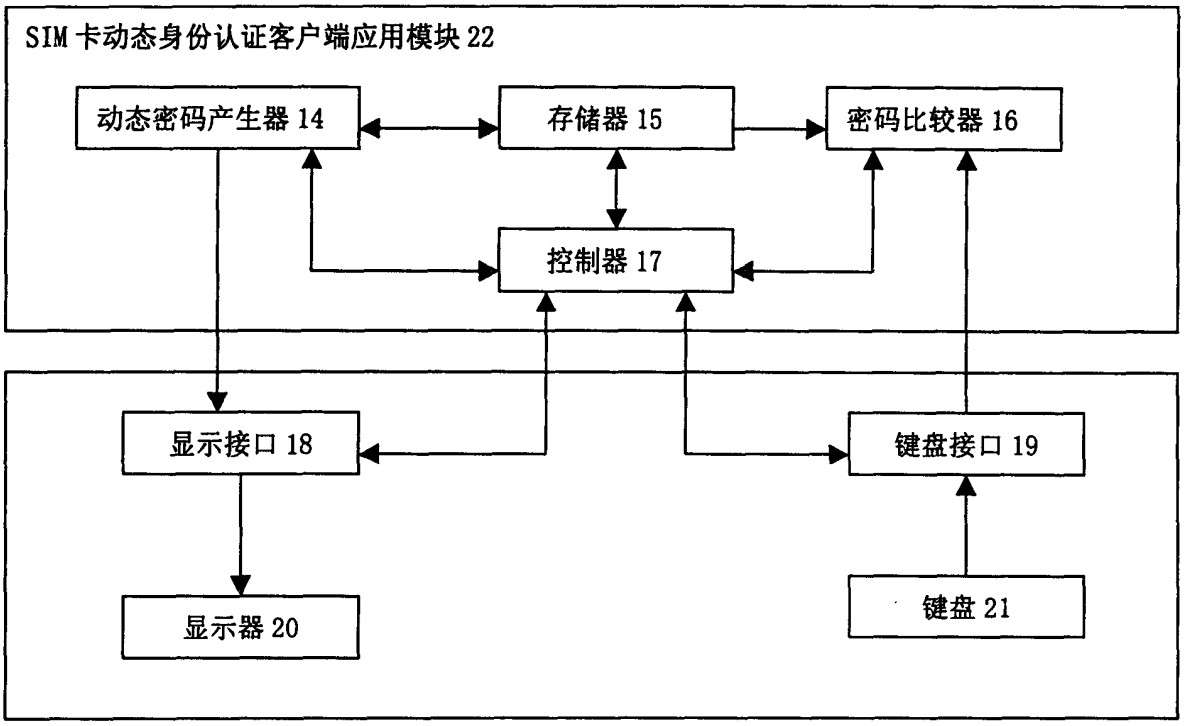

SIM 卡动态身份认证客户端应用模块 22
动态密码产生器 14
存储器 15
密码比较器 16
控制器 17
显示接口 18
键盘接口 19
显示器 20
键盘 21

图 1

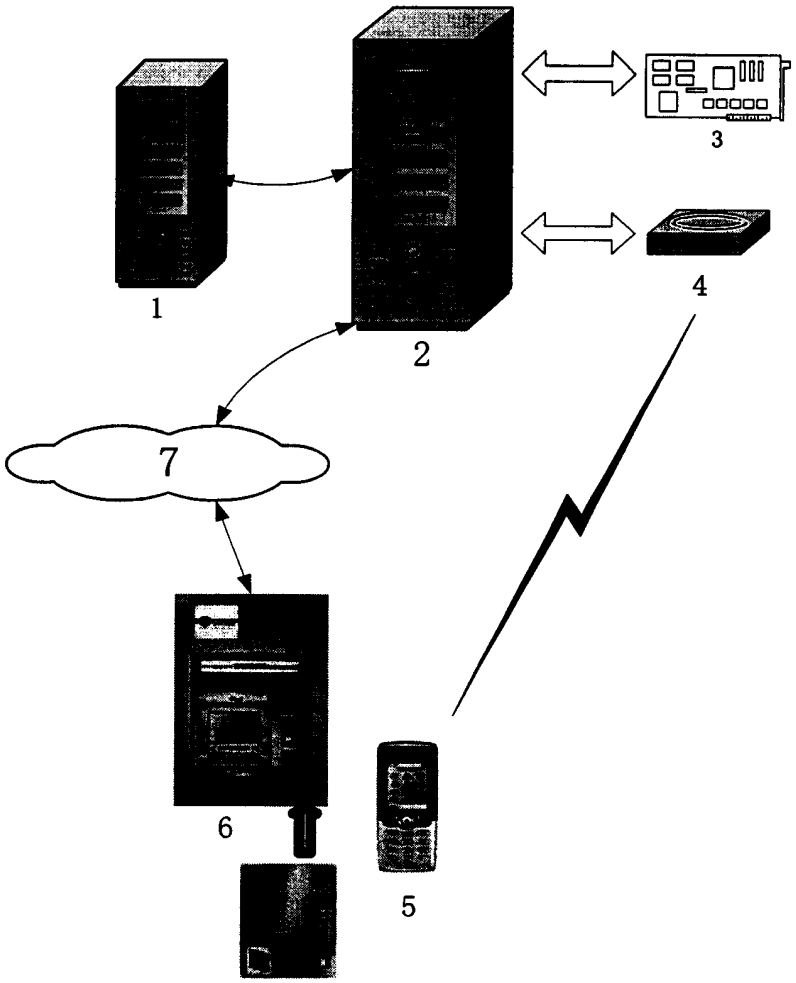

1
2
3
4
5
6
7

图 2

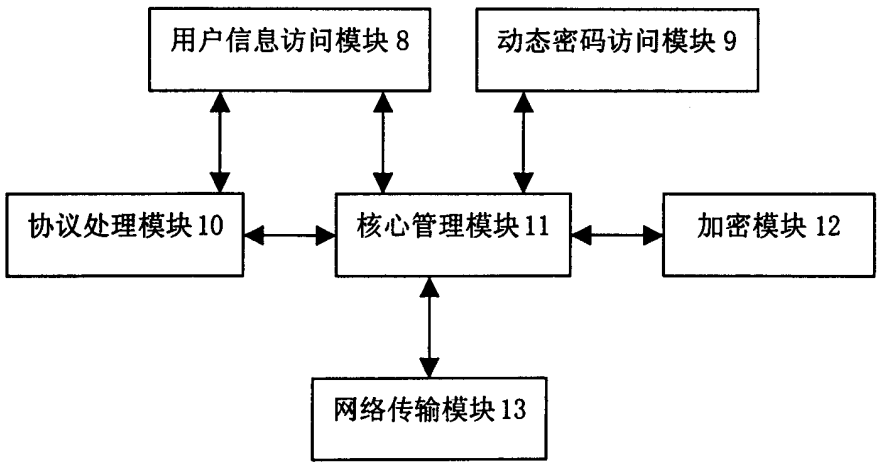
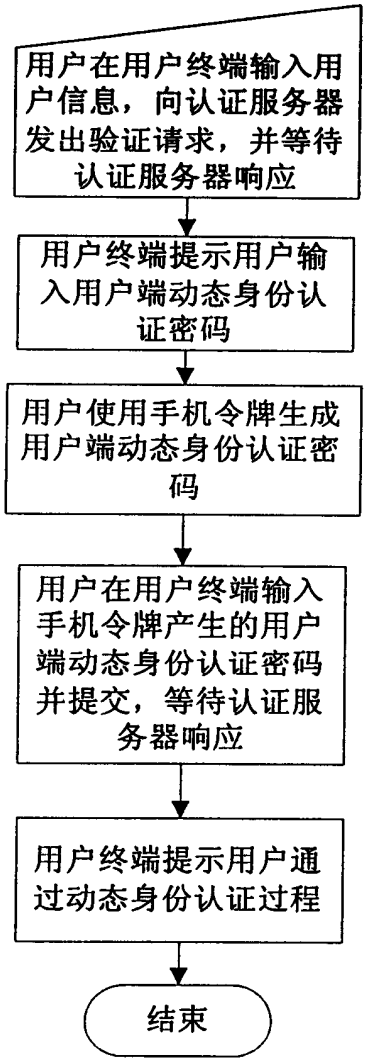
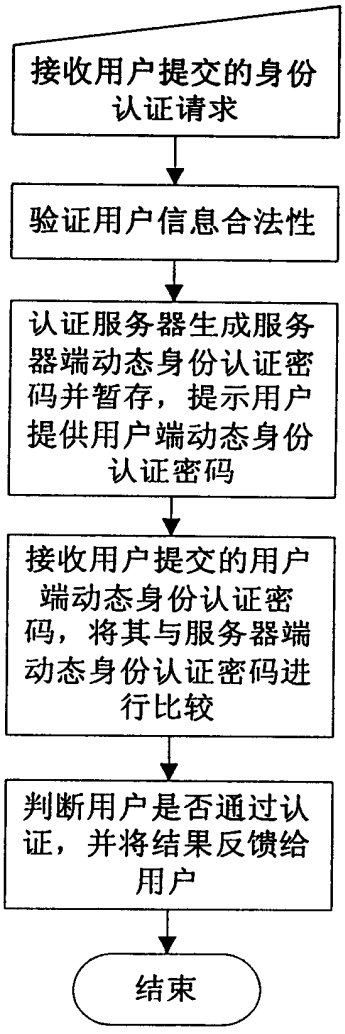

用户信息访问模块 8
动态密码访问模块 9
协议处理模块 10
核心管理模块 11
加密模块 12
网络传输模块 13

图 3

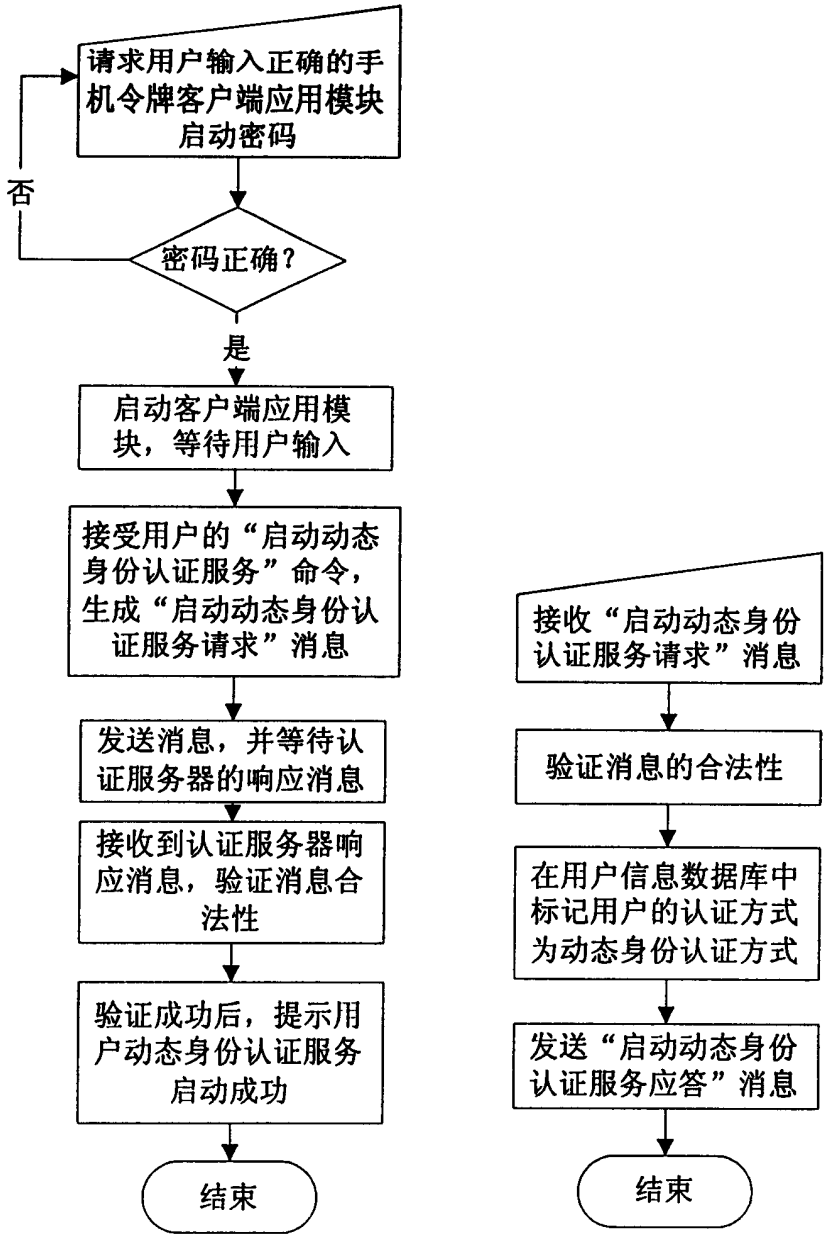

用户在用户终端输入用户信息，向认证服务器发出验证请求，并等待认证服务器响应
用户终端提示用户输入用户端动态身份认证密码
用户使用手机令牌生成用户端动态身份认证密码
用户在用户终端输入手机令牌产生的用户端动态身份认证密码并提交，等待认证服务器响应
用户终端提示用户通过动态身份认证过程
结束

4.1


接收用户提交的身份认证请求
验证用户信息合法性
认证服务器生成服务器端动态身份认证密码并暂存，提示用户提供用户端动态身份认证密码
接收用户提交的用户端动态身份认证密码，将其与服务器端动态身份认证密码进行比较
判断用户是否通过认证，并将结果反馈给用户
结束

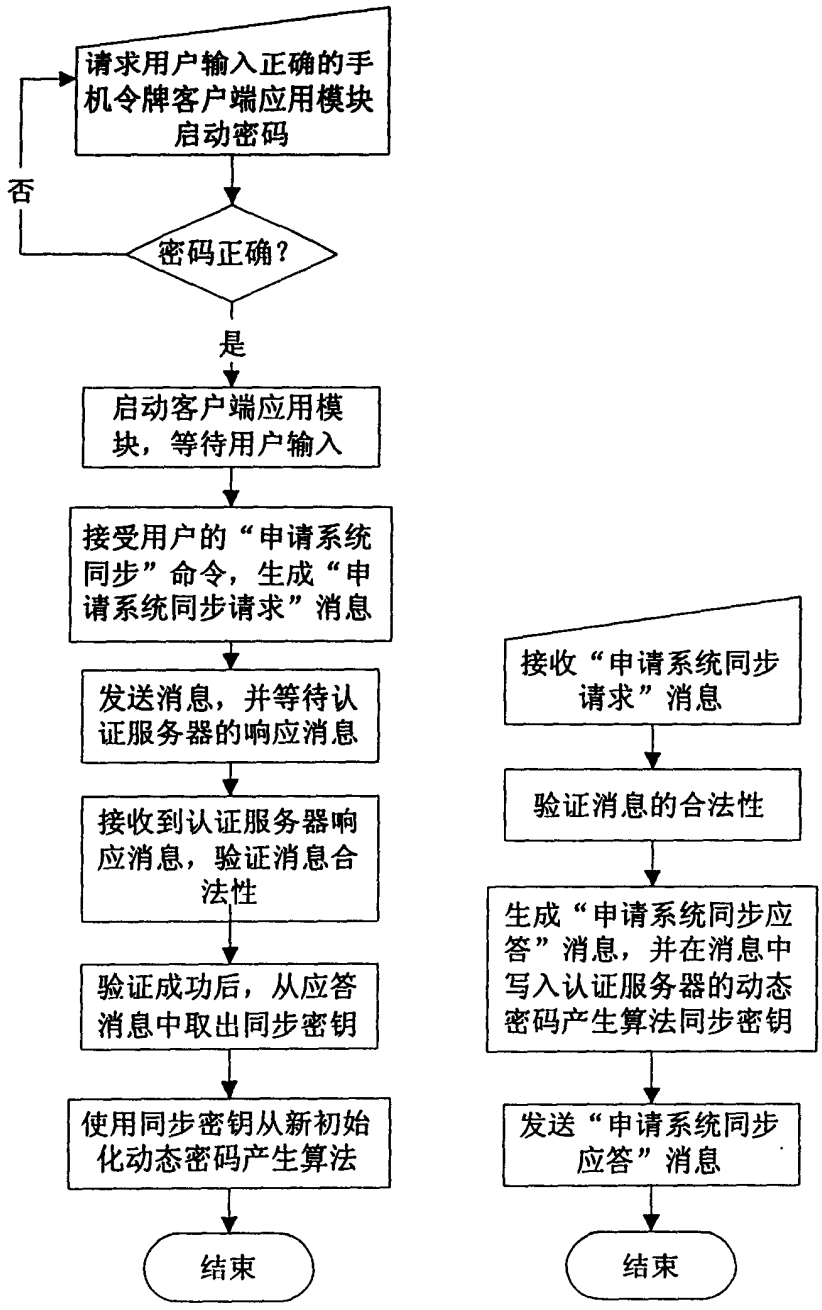
4.2

图 4


请求用户输入正确的手机令牌客户端应用模块启动密码
否
密码正确？
是
启动客户端应用模块，等待用户输入
接受用户的“启动动态身份认证服务”命令，生成“启动动态身份认证服务请求”消息
发送消息，并等待认证服务器的响应消息
接收到认证服务器响应消息，验证消息合法性
验证成功后，提示用户动态身份认证服务启动成功
结束
接收“启动动态身份认证服务请求”消息
验证消息的合法性
在用户信息数据库中标记用户的认证方式为动态身份认证方式
发送“启动动态身份认证服务应答”消息
结束

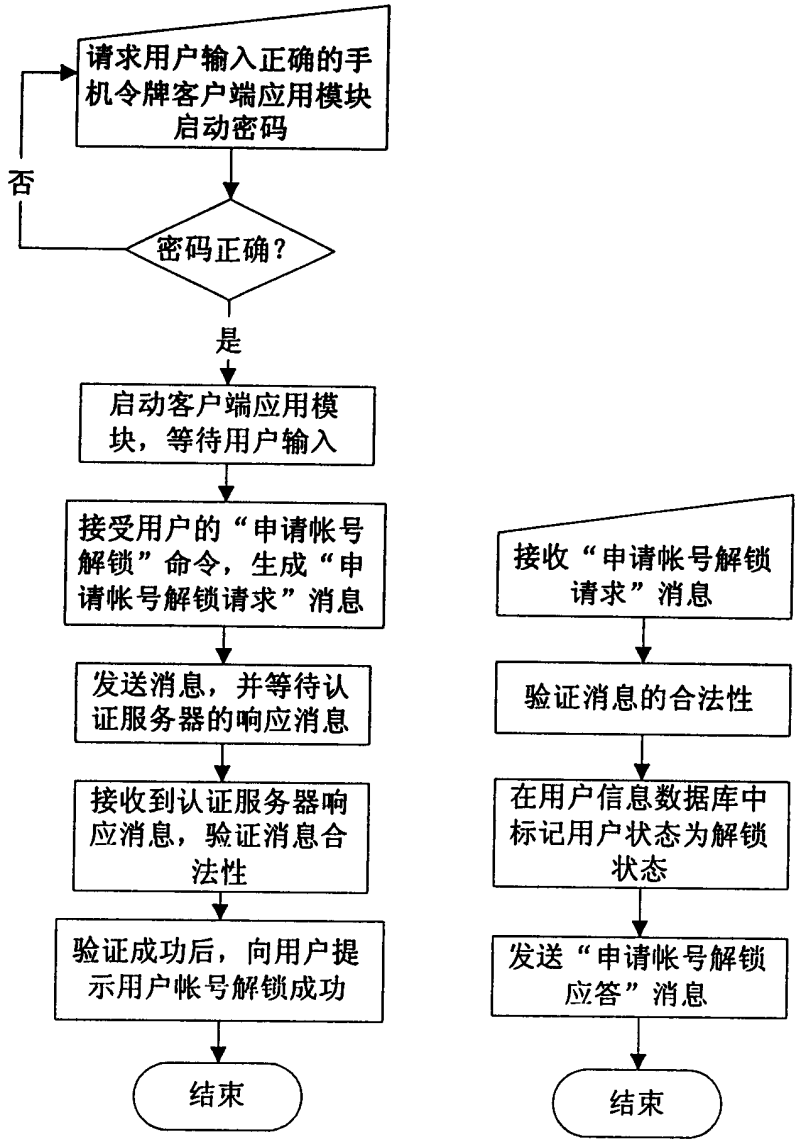
5.1 5.2

图 5


请求用户输入正确的手机令牌客户端应用模块启动密码
否
密码正确？
是
启动客户端应用模块，等待用户输入
接受用户的“申请系统同步”命令，生成“申请系统同步请求”消息
发送消息，并等待认证服务器的响应消息
接收到认证服务器响应消息，验证消息合法性
验证成功后，从应答消息中取出同步密钥
使用同步密钥从新初始化动态密码产生算法
结束
接收“申请系统同步请求”消息
验证消息的合法性
生成“申请系统同步应答”消息，并在消息中写入认证服务器的动态密码产生算法同步密钥
发送“申请系统同步应答”消息
结束

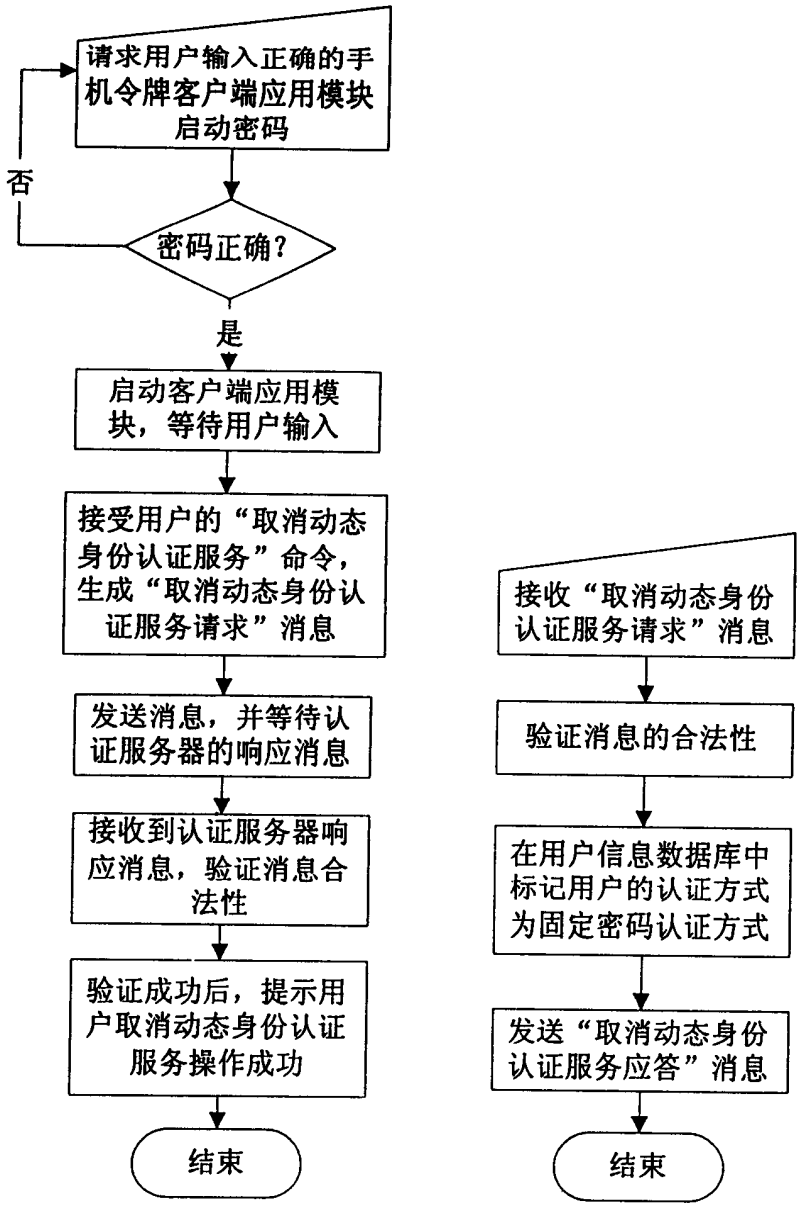
6.1 6.2

图 6


请求用户输入正确的手机令牌客户端应用模块启动密码
否
密码正确？
是
启动客户端应用模块，等待用户输入
接受用户的“申请帐号解锁”命令，生成“申请帐号解锁请求”消息
发送消息，并等待认证服务器的响应消息
接收到认证服务器响应消息，验证消息合法性
验证成功后，向用户提示用户帐号解锁成功
结束
接收“申请帐号解锁请求”消息
验证消息的合法性
在用户信息数据库中标记用户状态为解锁状态
发送“申请帐号解锁应答”消息
结束

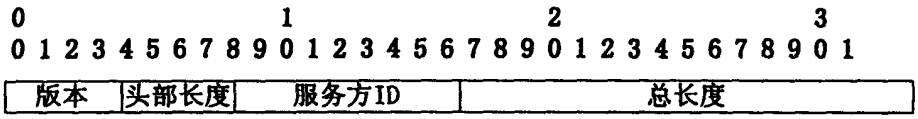
7.1 7.2

图 7

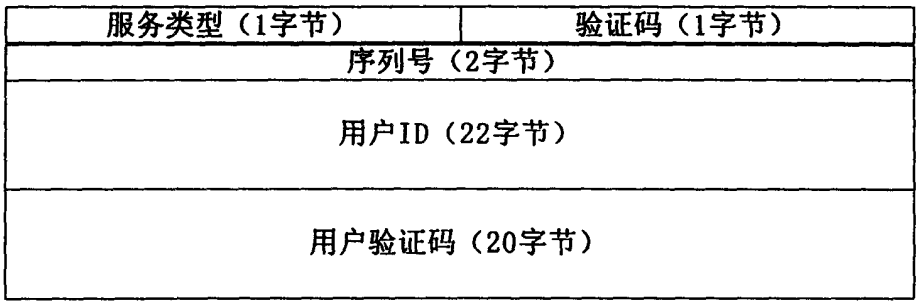

请求用户输入正确的手机令牌客户端应用模块启动密码
否
密码正确？
是
启动客户端应用模块，等待用户输入
接受用户的“取消动态身份认证服务”命令，生成“取消动态身份认证服务请求”消息
发送消息，并等待认证服务器的响应消息
接收到认证服务器响应消息，验证消息合法性
验证成功后，提示用户取消动态身份认证服务操作成功
结束
接收“取消动态身份认证服务请求”消息
验证消息的合法性
在用户信息数据库中标记用户的认证方式为固定密码认证方式
发送“取消动态身份认证服务应答”消息
结束

8.1 8.2

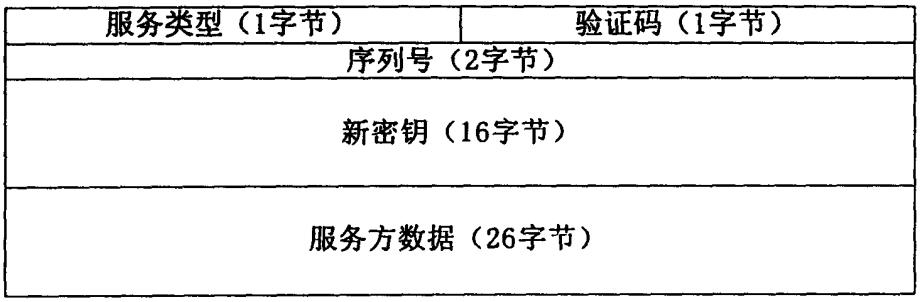
图 8


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
版本
头部长度
服务方ID
总长度

9.1


服务类型（1字节）
验证码（1字节）
序列号（2字节）
用户ID（22字节）
用户验证码（20字节）

9.2


服务类型（1字节）
验证码（1字节）
序列号（2字节）
新密钥（16字节）
服务方数据（26字节）

9.3

图 9