[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
H04Q 7/32 (2006.01)
H04Q 7/38 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610168591.9

[43] 公开日 2007 年 6 月 27 日

[11] 公开号 CN 1987885A

[22] 申请日 2006.12.21
[21] 申请号 200610168591.9
[30] 优先权
[32] 2005.12.22 [33] US [31] 11/317,136
[71] 申请人 三菱电机株式会社
地址 日本东京
[72] 发明人 乔纳斯·I·库基尔 梁 维

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 朱智勇

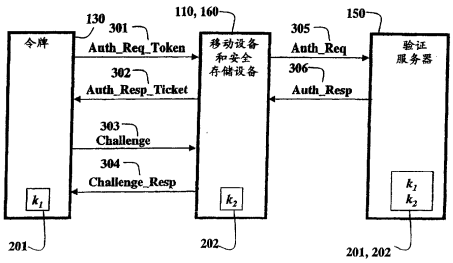
权利要求书 3 页 说明书 7 页 附图 4 页

[54] 发明名称

安全获取绑定密钥的计算机实现的方法和安全绑定系统

[57] 摘要

本发明涉及安全获取绑定密钥的计算机实现的方法和安全绑定系统，提出了一种使用可携带的令牌来保护移动设备的系统和方法，其中移动设备例如是膝上型电脑、PDA 和移动电话机等。 该方法执行令牌使能的验证以允许对移动设备的操作。 为了进行验证，在令牌和移动设备之间使用近程无线通信。



1. 一种计算机实现的用于安全获取令牌设备和安全存储设备的绑定密钥的方法，包括以下步骤：

在令牌设备内存储令牌密钥；

在移动设备的安全存储设备内存储安全存储设备密钥；

由验证服务器访问令牌密钥和安全存储设备密钥以产生绑定密钥；以及

在令牌设备和安全存储设备内存储该绑定密钥。

2. 权利要求 1 所述的方法，还包括以下步骤：

从令牌设备向移动设备发送第一验证请求消息 **Auth_Req_Token**，其中第一验证请求消息被定义为：

（**Auth_Req_Token={ID_t，AuthReq}**），

其中，ID_t 是该令牌设备的标识，**AuthReq** 表示第一验证请求消息是用于与移动设备进行初始验证；

作为对接收到第一验证请求消息的响应，在移动设备中产生第二验证请求消息 **Auth_Req**，其中第二验证请求消息被定义为：

（**Auth_Req ={ID_t，ID_s，AuthReq}**），

其中，ID_s 是移动设备的安全存储设备的标识；

把第二验证请求消息发送至验证服务器；

以第一验证响应消息 **Auth_Resp** 响应，第一验证响应消息被定义为：

（**Auth_Resp={ID_s，k_b，$\{ID_t, k_b\}^{k_1}\}^{k_2}$**），

其中该第一验证响应消息是用安全存储设备密钥 k_2 加密的，令牌设备的标识和绑定密钥 k_b 是用令牌密钥 k_1 和安全存储设备密钥 k_2 加密的；

由安全存储设备对第一验证响应消息进行解密；

把绑定密钥 k_b 存储在安全存储设备中；

把第二验证响应消息 **Auth_Resp_Ticket** 转发给令牌设备，其中第二验证响应消息被定义为：

（$\mathbf{Auth_Resp_Ticket} = \{\mathbf{ID}_t, k_b\}^{k_1}$）；

由令牌设备对第二验证响应消息进行解密；以及

把绑定密钥 k_b 存储在令牌设备中。

3. 一种计算机实现的用于安全获取令牌设备和安全存储设备的绑定密钥的方法，包括以下步骤：

在令牌设备内存储令牌密钥；

在移动设备的安全存储设备内存储安全存储设备密钥；

由用户利用令牌密钥和安全存储设备密钥访问令牌设备和安全存储设备；

在安全存储设备中产生绑定密钥；

在安全存储设备中存储绑定密钥；以及

在令牌设备和安全存储设备内存储该绑定密钥。

4. 权利要求 3 所述的方法，还包括以下步骤：

从用户向安全存储设备发送第一验证请求消息 **Auth_Req_S**，其中第一验证请求消息被定义为：

（$\mathbf{Auth_Req_S} = \{k_2\}^{k_2}$），

其中，k_2 是安全存储设备密钥；

作为对接收到第一验证请求消息的响应，在移动设备中产生第一验证响应消息 **Auth_Resp_S**，其中第一验证响应消息被定义为：

（$\mathbf{Auth_Resp_S} = \{\mathbf{AuthResp}\}$），

其中 **AuthResp** 表示验证成功；

从移动设备向令牌设备发送第二验证请求消息 **Auth_Req_T**，其中该第二验证请求消息被定义为：

（$\mathbf{Auth_Req_T} = \{k_1\}^{k_1}$），

其中，k_1 是令牌设备密钥；

作为对接收到第二验证请求消息的响应，在令牌设备中产生第二验证响应消息 **Auth_Resp_T**，其中该第二验证响应消息被定义为：

（$\mathbf{Auth_Resp_T} = \{\mathbf{AuthResp}\}$），

其中 **AuthResp** 表示验证成功；

在安全存储设备中产生绑定密钥;

把绑定密钥存储在安全存储设备中;

用缺省绑定密钥加密上述绑定密钥;

把加密的绑定密钥发送给令牌设备;

用缺省绑定密钥对所述加密的绑定密钥进行解密,以恢复该绑定密钥;以及

把该绑定密钥存储在令牌设备中。

5. 一种用于安全地绑定令牌设备和安全存储设备的系统,包括:

存储令牌设备密钥的令牌设备;和

存储安全存储设备密钥的安全存储设备。

6. 权利要求 **5** 所述的系统,还包括:

验证服务器。

安全获取绑定密钥的计算机实现的方法和安全绑定系统

技术领域

本发明一般涉及保护数据和设备，具体涉及保护诸如膝上型电脑、PDA、照相机和移动电话机的移动设备免遭未授权使用。

背景技术

随着共享数据、执行商业交易和移动计算的需求的增加，小型移动设备的使用越来越广泛。移动设备容易遗失或失窃。因此，有必要提高移动设备的安全性。

使用诸如密码、生物测定和基于非对称密钥的验证的验证机制可以降低移动设备的脆弱性。但是这些方法给用户带来负担，并且在验证过程中会降低设备的性能。

使用密码验证时，用户通常要提供用户名和密码。记忆和输入用户名和密码就是一种负担。在用户已被验证后，在验证后获得对移动设备的物理控制的任何人仍然能对存储在移动设备中的数据进行未授权访问。如果使用诸如脸或指纹验证的生物测定验证，则误检出差错率是一个问题。而且，生物测定验证需要耗能的扫描器。

Noble 等人的美国专利申请 **No. 2003/0005300** 描述了一种利用一个令牌（授权服务器）来保护存储在膝上型电脑（客户机）中的文件的方法和系统。当该令牌靠近膝上型电脑时，要先执行 **Rijindael** 对称密钥交换才能访问文件。

Jones 等人的美国专利 **No. 5,623,637** 提供了一种用于存储访问密码和加密密钥的智能卡。若要访问数据，必须把该智能卡插入存储数据的设备中。该系统的问题在于一旦把卡插进去，就可能危及该设备的安全。

Cyras等人的美国专利No. 5,889,866描述了一种存有密码的集成电路（IC）卡。当这种IC卡插入计算机设备时，就能执行密码验证，以允许操作该计算机设备。

下述美国专利也一般涉及数据保护：美国专利 No. 5,012,514; 5,091,939; 5,226,080; 5,375,243; 5,657,470; 6,189,099; 6,070,240; 6,088,450; 5,757,916; 5,544,321; 5,611,050 和 5,836,010。

发明内容

一种系统和方法利用可携带的令牌来保护移动设备，所述移动设备例如是膝上型电脑、PDA和移动电话机等。

此方法执行令牌使能的验证来允许对移动设备的操作。为了进行验证，在令牌和移动设备之间采用近程无线通信。

附图说明

图1是根据本发明的实施例的用于保护移动设备的系统和方法的框图；

图2是根据本发明的实施例的利用绑定密钥保护移动设备的系统和方法的框图；

图3是根据本发明的实施例的验证交换的示意图；以及

图4是根据本发明的另一个实施例的验证交换的示意图。

具体实施方式

本文所述的验证方法采用了两个阶段：一个初始化阶段和一个正常使用阶段。初始化阶段是利用下述两种方法之一来完成的。正常使用阶段是一种通过现时（nonce）执行的周期性验证，同时检验授权令牌的存在和防止重放攻击。

移动设备、安全存储设备和令牌

图1示出了一种用于保护诸如PDA、膝上型电脑、照相机、可移动的数据存储设备或移动电话机的移动设备110的系统和方法。令

牌（或令牌设备）130 存储了一个令牌密钥 k_1 201 和一个绑定密钥 k_b 203。安全存储设备密钥 k_2 202 和绑定密钥 k_b 203 通过一个安全存储设备 160 安全地存储在移动设备 110 内。

在优选实施例中，可以对存储的令牌密钥 k_1 201 和安全存储设备密钥 k_2 202 进行加密，比如加密成散列值，以避免在安全存储设备 160 或令牌 130 遗失、失窃或处于其它不安全状况下时暴露。密钥 k_1 和 k_2 是由一个源例如零售商或制造商存储在令牌和安全存储设备中的。绑定密钥 k_b 203 则是在初始化阶段产生的。

通常，令牌 130 是处于用户 120 的物理控制下的。例如，用户在口袋中携带该令牌，或用带子把令牌系在用户身上。

移动设备 110 可以通过无线信道 140 与令牌 130 以及与安全存储设备 160 通信。该无线信道是一个近程通信链路，例如符合蓝牙规范，IEEE 802.15.1 标准（2002 年 6 月 14 日）的链路，该标准在此并入作为参考。不同类别的蓝牙设备的射程根据能量级别而可能在 10cm 到 100m 之间变化。因此，可能要求令牌 130 必须在物理上非常靠近移动设备 110 才允许操作该移动设备。

正常使用

图 1 描述了正常使用阶段。移动设备 110 通过无线信道 140 上的一个无线电信号，例如载波，检测令牌 130 的存在。移动设备 110 在安全存储设备 160 的指导下周期性生成一个现时并期望来自令牌的响应，以便进行验证。如果由令牌提供的该现时的响应满足该安全存储设备所要求的响应，则允许对该移动设备进行操作。

应当理解的是，安全存储设备可以存储多个绑定密钥 k_b 203，这些密钥可被不同的令牌和不同的用户启用。还应当理解的是，不同的密钥和密码可以允许对存储在移动设备的安全存储器中的不同数据、或该移动设备的特定应用或不同硬件功能的访问。在另一个变型中，令牌能启动与令牌存储了相同的绑定密钥 k_b 203 的多个设备。在另一个变型中，令牌针对不同的安全存储设备存储多个绑定密钥 k_b 203。

利用验证服务器的初始化阶段

图 2 示出了一种使用验证服务器 150 的本发明实施例。令牌 130 存储令牌密钥 k_1 201，移动设备 110 中的安全存储设备 160 存储安全存储设备密钥 k_2 202。当用户 120 得到该令牌和安全存储设备时，用户可以通过一个验证服务器 150 绑定来自相应源的设备 130 和 160。验证服务器 150 通过其令牌密钥 k_1 201 访问令牌 130，通过其安全存储设备密钥 k_2 202 访问安全存储设备 160，以便在令牌 130 和安全存储设备 160 中放置一个绑定密钥 k_b 203。其结果就是无需用户 120 的干预就把令牌 130 和安全存储设备 160 彼此绑定。

绑定密钥 k_b 203 存储在令牌和安全存储设备中用于正常使用阶段。该绑定密钥被存储在令牌和安全存储设备中，直到通过解除令牌和安全存储设备的绑定而移除该绑定密钥。解除绑定可能出于以下原因：访问权已改变，令牌或移动设备的所有权改变，或是令牌或设备遗失或失窃。

在令牌与安全存储设备绑定后，安全存储设备拒绝任何进一步的绑定变化，除非至少有一个初始合法令牌存在。这能防止被盗的安全存储设备与任何令牌绑定。

利用验证服务器密钥交换的初始化阶段

安全存储设备和令牌可以如图 3 所示“绑定”。为了进行初始验证，令牌 130 向移动设备 110 发送第一验证请求消息 Auth_Req_Token 301。消息 Auth_Req_Token 被定义为：

（Auth_Req_Token={ID_t，AuthReq}），

其中，ID_t 是该令牌的标识，AuthReq 表示该消息用于与移动设备进行初始验证。

作为对接收到验证请求消息 Auth_Req_Token 的响应，移动设备 110 向该消息添加安全存储设备的标识 ID_s，从而产生 Auth_Req 305，其被定义为：

（Auth_Req ={ID_t，ID_s，AuthReq}），

其中，ID_s 是移动设备 110 的安全存储设备 160 的标识。此消息被转发至验证服务器 150。验证服务器查找两个 ID，并以验证响应消息

Auth_Resp 306 响应。Auth_Resp 的消息结构被定义为：

（Auth_Resp ={ ID_s， k_b ，{ID_t， k_b}^{k_1}}^{k_2}），

其中该消息和消息的部分是利用令牌密钥 k_1 和安全存储设备密钥 k_2 加密的。ID_t 是令牌的标识，ID_s 是安全存储设备的标识，k_1 是令牌设备密钥 201，k_2 是安全存储设备密钥 202，k_b 是绑定令牌和安全存储设备的绑定密钥 203。安全存储设备对消息 Auth_Resp 中其自己的部分进行解密，存储绑定密钥 k_b 203，然后把消息的剩余部分 Auth_Resp_Ticket 302 转发给令牌。Auth_Resp_Ticket 被定义为：

（Auth_Resp_Ticket = {ID_t， k_b}^{k_1} ）。

令牌对这个消息进行解密，也存储绑定密钥 k_b 203。然后令牌利用一个现时发送一个询问消息 Challenge 303。这个现时是令牌利用一个随机数 R 产生的。利用绑定密钥 k_b 203 对随机数 R 加密，表示如下：

（Challenge = {R}^{k_b} ）。

安全存储设备通过对该现时进行解密、计算现时的响应以及用绑定密钥 k_b 203 加密该现时的响应，以 Challenge_Resp 304 对该询问响应，表示如下：

（Challenge_Resp = {R-1}^{k_b} ）。

令牌解密这个现时的响应，如果该现时的响应满足令牌的要求，那么该安全存储设备和该令牌就通过绑定密钥 k_b 203 绑定在一起了。

没有验证服务器的初始化阶段

图 4 示出了本发明的另一个实施例，该实施例涉及用户 120。令牌 130 存储令牌密钥 k_1 201，移动设备 110 中的安全存储设备 160 存储安全存储设备密钥 k_2 202。两个设备还存储了缺省绑定密钥 k_{b0}。当用户获得该令牌和安全存储设备时，用户还从相应源获得密钥 201-202 的加密信息。用户 120 通过内嵌令牌密钥 k_1 201 的消息访问令牌 130，通过内嵌安全存储设备密钥 k_2 202 的消息访问安全存储设备 160，以便把绑定密钥 k_b 203 存储在令牌 130 和安全存储设备 160 中。其结果就是令牌 130 和安全存储设备 160 彼此绑定在一起。

绑定密钥 k_b 203 存储在令牌和安全存储设备中用于正常使用阶

段。该绑定密钥被存储在令牌和移动设备中，直到通过解除令牌和移动设备的绑定而移除该绑定密钥。解除绑定可能出于以下原因：访问权已改变，令牌或移动设备的所有权改变，或是令牌或设备遗失或失窃。

没有验证服务器密钥交换的初始化阶段

安全存储设备和令牌还能如图4所示"绑定"。为了进行初始验证，用户 120 向安全存储设备 160 发送第一验证请求消息 Auth_Req_S 403。任何通信设备都可以用来发送此消息。消息 Auth_Req_S 被定义为：

（Auth_Req_S =$\{k_2\}^{k_2}$），

其中 k_2 是安全存储设备 160 的安全存储设备密钥 202，该消息表示用户的与安全存储设备进行初始验证的请求。

作为对接收到验证请求消息 Auth_Req_S 的响应，安全存储设备 160 发送一个验证响应消息 Auth_Resp_S 404。该消息 Auth_Resp_S 被定义为：

（Auth_Resp_S = {AuthResp}），

其中 AuthResp 表示验证成功。

用户 120 通过发送消息 Auth_Req_T 405 经由安全存储设备 160 向令牌 130 提交验证请求，消息 Auth_Req_T 被定义为：

（Auth_Req_T =$\{k_1\}^{k_1}$），

其中 k_1 是令牌 130 的令牌密钥 201，该消息表示用户的与令牌进行初始验证的请求。

作为对接收到验证请求消息 Auth_Req_T 的响应，令牌 130 发送一个验证响应消息 Auth_Resp_T 406。该消息 Auth_Resp_T 被定义为：

（Auth_Resp_T = {AuthResp}），

其中 AuthResp 表示验证成功。

然后安全存储设备利用一个现时发送一个询问消息 Challenge 401，该现时也成为新的绑定密钥 k_b。这个现时是安全存储设备利用随机数产生的，并用缺省绑定密钥 k_{b0} 加密，表示如下：

（$\mathbf{Challenge} = \{k_b\}^{k_{b0}}$）。

令牌通过解密该现时、计算现时的响应以及用缺省绑定密钥 k_{b0} 加密该响应，以 **Challenge_Resp 402** 对该询问响应，表示如下：

（$\mathbf{Challenge_Resp} = \{k_b\text{-}1\}^{k_{b0}}$）。

安全存储设备解密这个现时的响应。如果该现时的响应满足安全存储设备的要求，那么该安全存储设备和该令牌就通过新的绑定密钥 k_b 绑定在一起了。这时紧接着用于正常使用的询问交换。

尽管已经通过优选实施例描述了本发明，但是应当理解的是在本发明的精神和范围内可以作其他各种适配和修改。因此，所附的权利要求书的目标就是包含在本发明的真正精神和范围内的所有这些变型和修改。

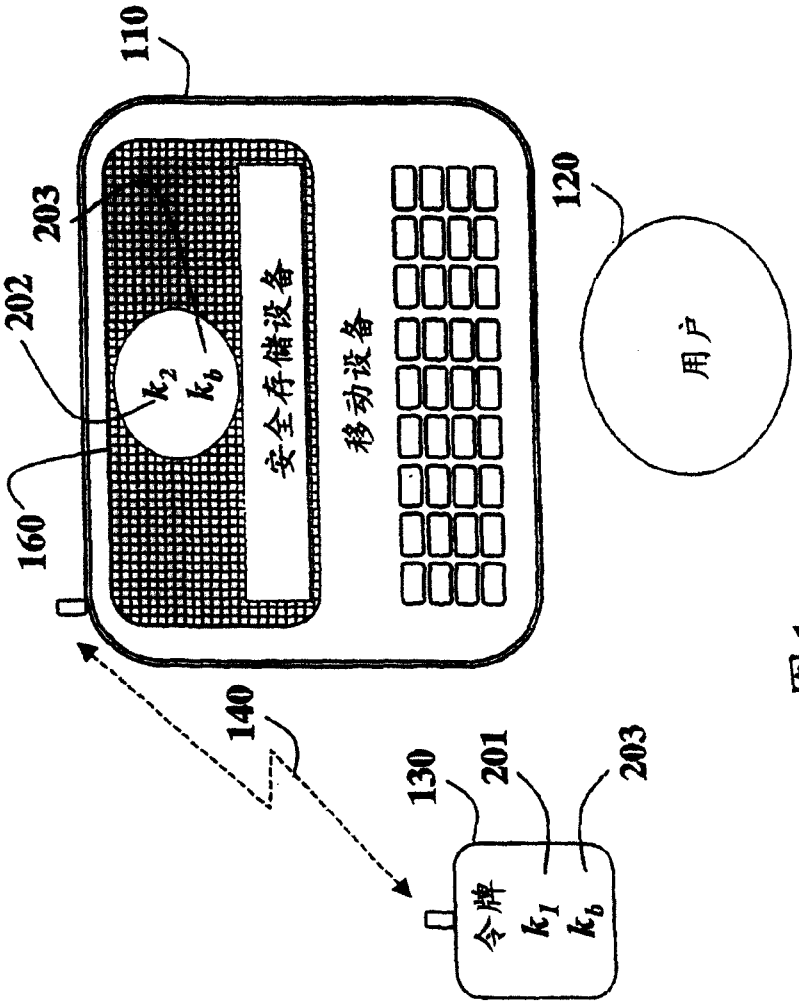


图 1

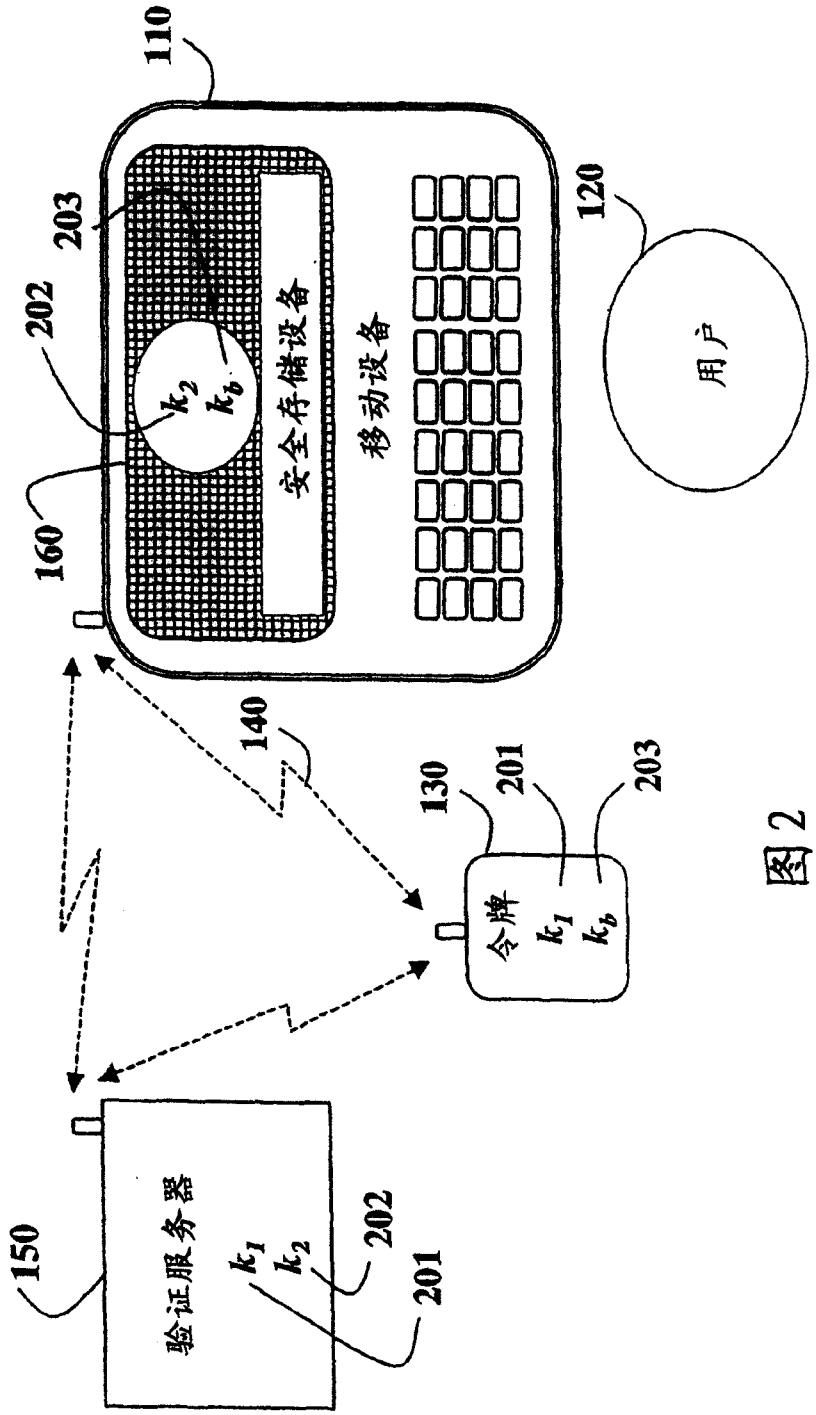

110
203
202
160
150
140
130
201
203
120
k_2
k_b
安全存储设备
移动设备
用户
令牌
k_1
k_b
验证服务器
k_1
k_2
202
201

图 2

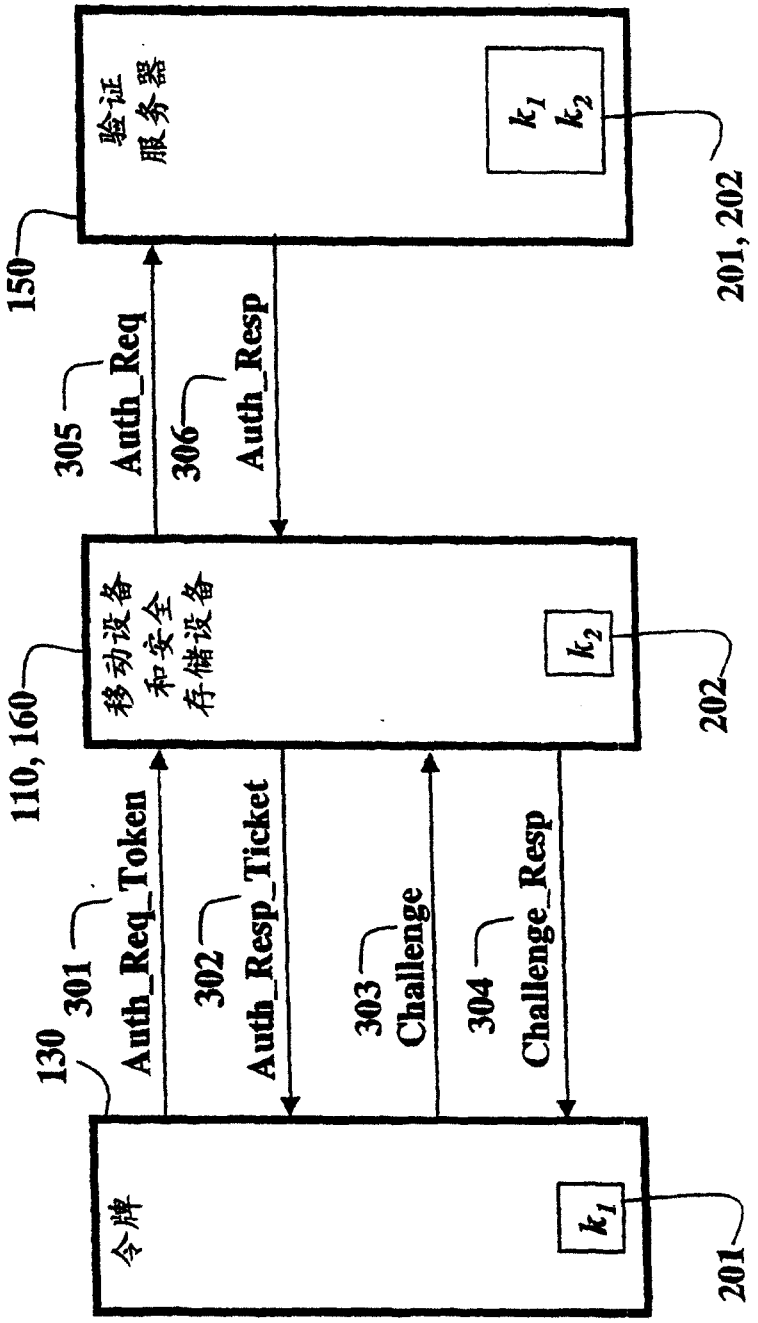

验证服务器
k_1 k_2
150
201, 202
305 Auth_Req
306 Auth_Resp
移动设备和安全存储设备
k_2
110, 160
202
301 Auth_Req_Token
302 Auth_Resp_Ticket
303 Challenge
304 Challenge_Resp
令牌
k_1
130
201

图 3

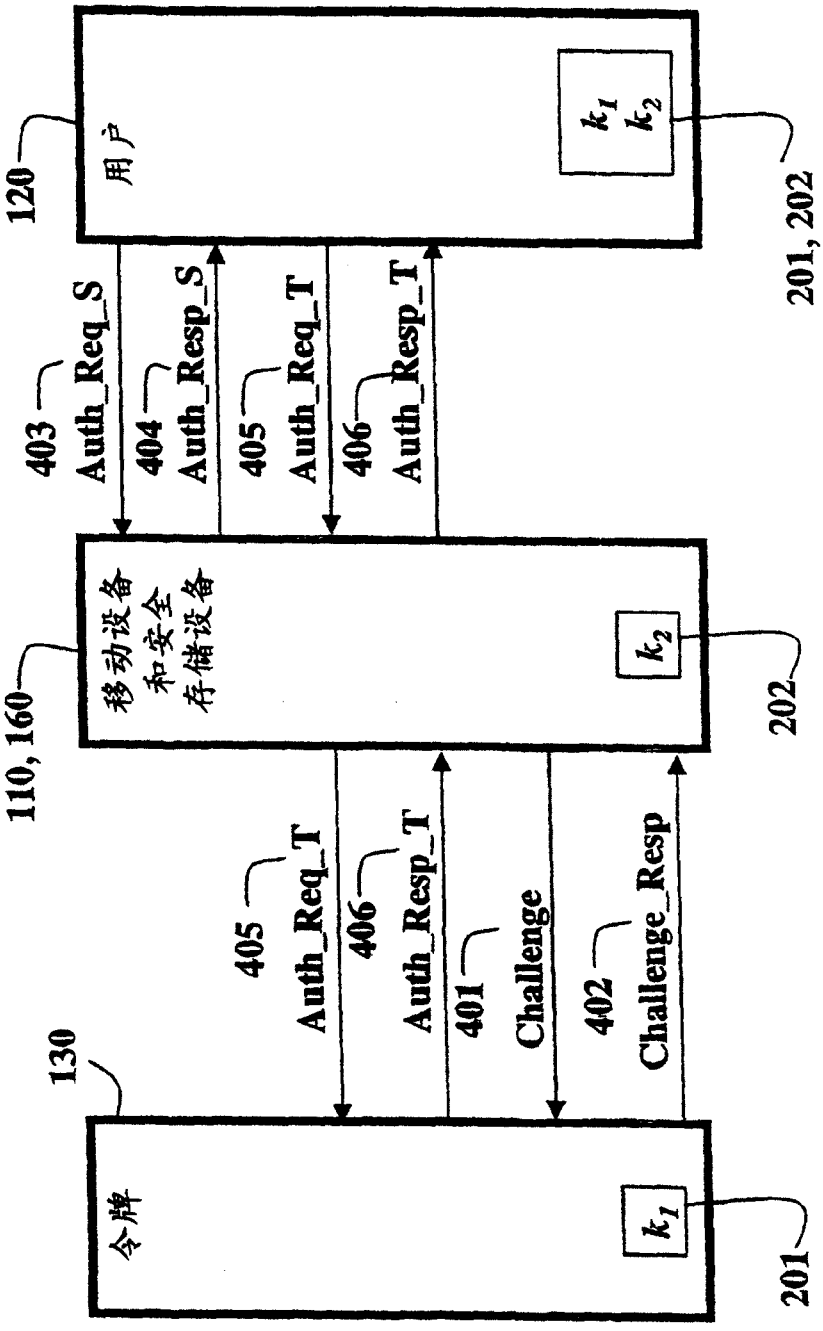

120
用户
k_1
k_2
201, 202
403
Auth_Req_S
404
Auth_Resp_S
405
Auth_Req_T
406
Auth_Resp_T
110, 160
移动设备
和安全
存储设备
k_2
202
405
Auth_Req_T
406
Auth_Resp_T
401
Challenge
402
Challenge_Resp
130
令牌
k_1
201

图 4