(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104410968 A
(43)申请公布日 2015.03.11

(21)申请号 201410653530.6

(22)申请日 2014.11.18

(71)申请人 王家城
地址 100192 北京市朝阳区林萃西里 26 号楼 6 单元 602

(72)发明人 王家城

(51)Int.Cl.
H04W 12/06(2009.01)
H04L 29/06(2006.01)

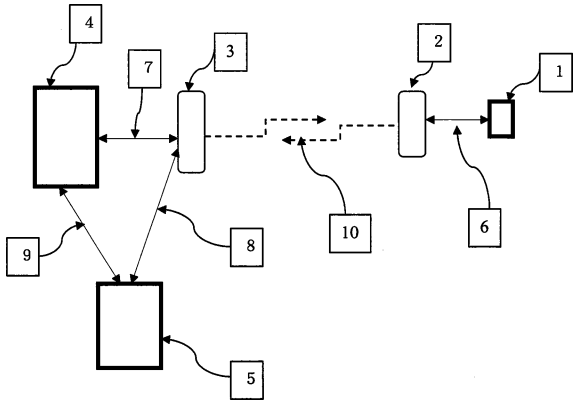
权利要求书3页 说明书9页 附图2页

(54)发明名称

一种便携式 UICC 卡用户终端设备及其身份认证系统

(57)摘要

本发明属于智能卡技术领域。本发明公开了一种便携式 UICC 卡用户终端设备及其身份认证方法和系统。通过充分利用 UICC 卡在用户身份认证中的安全性和无线通信在用户使用过程中的方便性，使得用户的身份认证在保持安全的同时，使用更为方便。用户在使用过程中不需要提供用户密码，也不需要把 UICC 卡提供给业务部门供查验。其身份认证的安全性和现有的接触式 IC 卡是等同的，还省略了读卡器设备。可以替代现有互联网中广泛使用的“用户名－密码”身份认证方式，在不需要用户密码的同时大大地提高了用户身份认证的安全性。可穿戴式的用户终端设备更进一步地加强了设备安全性和使用方便性。



CN 104410968 A

1. 一种基于通用集成电路卡 (UICC 卡,IC 卡) 的用户身份认证系统,其特征在于 :上述用户身份认证系统包括如下功能模块 :

1) 用户身份标识 IC 卡,

2) 具有无线通信功能的可穿戴式的用户 IC 卡接口设备,

3) 网络接口设备,

4) 用户身份认证服务器,

5) 用户数据服务器。

2. 根据权利要求 1 所述的用户 IC 卡接口设备,其特征在于 :上述用户 IC 卡接口设备具有如下功能模块 :

1) 接触式 IC 卡读卡接口,使得用户身份标识 IC 卡能够插入该设备中,并能够读取 IC 卡的相关数据,

2) 无线通信模块,能够通过无线传输方式 (或者通过无线通信和其它有线通信相结合的传输方式) 把从用户身份标识 IC 卡读取的数据传送给网络云端服务器,也能够把网络云端服务器的数据传送给用户身份标识 IC 卡,

3) 安全控制模块,能够提供用户 IC 卡接口设备和网络云端服务器的通信安全性和用户身份标识 IC 卡内部数据的访问安全性,

4) 能源供应模块如电池等,使得用户 IC 卡接口设备成为一个移动设备而可以独立工作,

5) 便于用户随身携带的配件如腕表式携带的表带等,成为可穿戴式设备而和用户随时随地同在,加强设备本身的安全性。

3. 根据权利要求 1 所述的网络接口设备,其特征在于 :上述网络接口设备具有如下功能模块 :

1) 无线通信模块,提供无线通信连接于用户 IC 卡接口设备,使得用户 IC 卡接口设备能够方便地连接于网络身份认证服务器,完成用户身份认证过程,

2) 连接于用户身份认证服务器,能够把用户身份认证服务器的数据转发给用户 IC 卡接口设备,也能够把用户 IC 卡接口设备的数据转发给用户身份认证服务器,

3) 连接于用户数据服务器,在需要的时候能够读取与用户身份相关联的业务数据。

4. 根据权利要求 1 所述的用户身份认证系统,其特征在于 :上述用户身份认证系统中的用户身份标识 IC 卡和用户身份认证服务器有一个用户数据的初始化过程,在用户开始使用用户身份标识 IC 卡之前就需要完成所述用户数据的初始化过程,上述初始化过程包括 :

1) 在用户身份标识 IC 卡和用户身份认证服务器中都写入一个唯一的用户身份号码,用户 ID 号,这个用户 ID 号不需要保密,是公开的,任何第三方在需要的时候,获得适当的授权后就可以获得,

2) 在用户身份标识 IC 卡和用户身份认证服务器中都写入一个能够标识业务服务提供部门的业务 ID 号,该业务 ID 号不需要保密,是公开的,

3) 在用户身份标识 IC 卡和用户身份认证服务器中都写入一个由业务服务提供部门提供的,唯一的,高度保密的身份认证密码 Kw, Kw 只能在用户身份认证服务器内部被用户身份认证服务器读取,或者在用户身份标识 IC 卡内部被用户身份标识 IC 卡读取,任何第三方

都不能读取，

4) 在用户身份标识 IC 卡和用户身份认证服务器中都写入一个由用户提供的，唯一的，高度保密的身份认证密码 Ky，Ky 只能在用户身份认证服务器内部被用户身份认证服务器读取，或者在用户身份标识 IC 卡内部被用户身份标识 IC 卡读取，任何第三方都不能读取，

5) 在用户身份标识 IC 卡和用户身份认证服务器中都写入一个由业务服务提供部门提供的，高度保密的加密算法 Am，Am 只能在用户身份认证服务器内部被用户身份认证服务器读取，或者在用户身份标识 IC 卡内部被用户身份标识 IC 卡读取，任何第三方都不能读取，Am 的输入数据包括 Kw，Ky 和一个在使用的时候才生成的，一次性使用的随机数序列 Ri，而其输出的数据则是一个身份认证鉴权数据序列 Si。

5. 根据权利要求 4 所述的用户数据的初始化过程，其特征在于：上述用户数据的初始化数据的写入只能在特定的地点，用特定的设备写入需要保密的数据，包括身份认证密码 Kw，Ky 和加密算法 Am，任何第三方都不能改写这些数据，也不能读取这些数据，这种安全性保障是通过用户身份标识 IC 卡和用户身份认证服务器设备本身提供的。

6. 根据权利要求 1 所述的用户身份认证系统，其特征在于：上述用户身份认证系统通过如下的步骤完成对用户的身份认证鉴权过程：

1) 用户 IC 卡接口设备读取存储在用户身份标识 IC 卡中的用户 ID 号，并通过网络接口设备，把用户 ID 号传送给用户身份认证服务器，申请用户身份认证，

2) 用户身份认证服务器收到用户 ID 号后，读取自身的安全数据库，得到该用户 ID 号所对应的用户身份认证密码 Kw 和 Ky，与此同时，生成一个临时的，一次性使用的随机数序列 Riw，

3) 在用户身份认证服务器内部运行加密算法 Am，以 Kw，Ky 和临时生成的随机数序列 Riw 为输入，得到一个用户身份认证鉴权数据序列 Siw，存储于用户身份认证服务器，等待使用，

4) 用户身份认证服务器把随机数序列 Riw，通过网络接口设备传送给用户 IC 卡接口设备，用户 IC 卡接口设备再把 Riw 传送给用户身份标识 IC 卡，

5) 用户身份标识 IC 卡收到随机数序列 Riw 后，读取存储于其内部的用户身份认证密码 Kw 和 Ky，并在 IC 卡内部运行加密算法 Am，得到用户端的身份认证鉴权数据序列 Siy，

6) 用户 IC 卡接口设备读取用户身份标识 IC 卡生成的用户身份认证鉴权数据序列 Siy，并通过网络接口设备，传送给用户身份认证服务器，

7) 用户身份认证服务器收到身份认证鉴权数据序列 Siy 后，和自己先前生成的数据序列 Siw 进行对比，如果一致，则完成对用户的身份认证过程，确认该用户 ID 号是真实的可信用户，如果不一致，则中断用户的身份认证过程，拒绝提供进一步的服务，

8) 用户身份认证服务器通过网络接口设备以及用户 IC 卡接口设备，发送确认消息给用户身份标识 IC 卡，通知其网络云端的用户身份认证过程已完成，并提供其自身的业务 ID 号，通知用户身份标识 IC 卡可以启动对网络的身份认证，

9) 用户身份标识 IC 卡在收到确认消息后，在 IC 卡内部生成一个临时的，一次性使用的随机数序列 Rjy，并通过用户 IC 卡接口设备，网络接口设备传送给用户身份认证服务器，

10) 用户身份标识 IC 卡在其内部运行加密算法 Am，以 Kw，Ky 和 Rjy 为输入数据，生成一个网络身份认证鉴权数据序列 Sjy，存储于用户身份标识 IC 卡内部，等待使用，

11) 用户身份认证服务器收到随机数序列 Rjy 后，读取自身的安全数据库，得到该用户 ID 号所对应的用户身份认证密码 Kw 和 Ky，

12) 在用户身份认证服务器内部运行加密算法 Am，以 Kw，Ky 和收到的 Rjy 为输入数据，生成一个网络身份认证鉴权数据序列 Sjw，

13) 用户身份认证服务器通过网络接口设备以及用户 IC 卡接口设备，把自己生成的数据序列 Sjw 传送给用户身份标识 IC 卡，

14) 用户身份标识 IC 卡收到数据序列 Sjw 后，和自身先前生成的网络身份认证鉴权数据序列 Sjy 进行对比，如果一致，则完成对业务网络的身份认证，如果不一致，则中断对网络的身份认证过程，拒绝和网络的进一步连接和数据交换，

15) 用户身份标识 IC 卡在完成对业务网络的身份认证后，通过用户 IC 卡接口设备，网络接口设备，发送消息给用户身份认证服务器，确认对业务网络的身份认证，

16) 用户身份的认证鉴权过程完成后，用户身份认证服务器发送确认消息给网络接口设备和用户数据服务器，可以使用和该用户 ID 号所对应的业务数据，

17) 在使用业务数据的时候，用户可选地使用附加的业务密码，进一步加强业务数据的使用安全性。

7. 根据权利要求 1 所述的用户 IC 卡接口设备的无线通信功能模块，其特征在于：上述无线通信模块是蓝牙 (Bluetooth) 通信功能模块。

8. 根据权利要求 1 所述的用户 IC 卡接口设备的无线通信模块，其特征在于：上述无线通信模块是能够接入蜂窝移动通信网络的 2G 通信系统如 GSM/GPRS/EDGE，CDMA 等，3G 通信的 WCDMA，CDMA2000，TD-SCDMA 等通信系统，LTE FDD，TD-LTE 等 4G 移动通信系统的通信功能模块。

9. 根据权利要求 1 所述的用户 IC 卡接口设备的无线通信模块，其特征在于：上述无线通信模块是无线局域网 (WLAN，WiFi) 通信功能模块。

10. 根据权利要求 3 所述的网络接口设备的无线通信模块，其特征在于：上述无线通信模块提供一种或多种的无线通信连接方式，包括蓝牙通信，无线局域网通信，蜂窝移动通信广域网络的移动互网接入，使得如根据权利要求 2 所述的用户 IC 卡接口设备能够方便的连接于用户身份认证服务器。

一种便携式 UICC 卡用户终端设备及其身份认证系统

技术领域

[0001] 本发明属于智能卡（也称芯片卡,UICC 卡,IC 卡）技术领域。具体地说,本发明涉及一种使用方便并安全的用户身份认证设备及方法,同时也涉及适用于这种用户身份认证的网络云端系统及其身份认证鉴权协议。

背景技术

[0002] 目前,通用集成电路卡 (UICC,Universal Integrated Circuit Card,简称 IC 卡）广泛应用于用户的身份认证系统。如移动通信系统的 SIM 卡和 USIM 卡,银行系统中用户帐户数据的金融 IC 卡,还包括各种社会保障卡如医保卡和公民的居民身份证系统。由于 IC 卡采用集成电路技术,使得其内部可以具有独立的 CPU（中央处理器）,存储系统和通信接口,其安全性得到大大增强。同时,由于 IC 卡的标准化和小型化,也利于随身携带,其使用也更为方便。

[0003] 根据 IC 卡和读卡器之间的信息交换方式,可以分为接触式 IC 卡和非接触式 IC 卡。然而,无论是接触式还是非接触式 IC 卡,都需要用户的 IC 卡和读卡器配合,才能完成用户的身份认证（非接触式 IC 卡和读卡器一般也需要 5mm-10mm 的距离）。例如,用户的银行账户的金融 IC 卡需要插入银行系统的读卡器,才能获得用户信息。这种用户身份标识 IC 卡和业务服务提供部门的读卡器之间需要物理地近距离接触的使用方式,给用户的使用带来一定程度的不方便。用户在使用业务时,需要前往业务服务提供部门,用专业的读卡器,读取用户的 IC 卡数据。这样,IC 卡的安全性和用户的使用方便性不能很好的共存,也不能满足人们在不同应用场景的使用需求。

[0004] 随着移动互联网和智能终端（如智能手机,平板电脑等）的发展,其应用也越来越深入人们生活的各个方面。例如手机钱包,使得人们可以随时随地完成移动支付而不需要使用现金,银行卡或者其他实体的支付凭证,给人们的日常生活带来极大的方便。作为用户的身份认证方式,在互联网系统中广泛使用的是“用户名 - 密码”的登陆方式,其唯一的用户身份标识就是登陆密码（用户名作为公开的信息可以很容易地获得）。也就是说,只要用户能够正确地输入密码,就认为该用户是真实的合法用户。

[0005] 这种“用户名 - 密码”的身份认证方式有其固有的不安全性和使用的不方便性。一方面,如果用户的登陆密码被泄露,这种用户身份认证方式就毫无安全性可言,任何人都可以使用其密码而冒充真实的用户。另一方面,用户需要记住密码,使得每次使用的时候能够被正确地认证。安全性需要密码越复杂越好,但是用户对密码记忆的方便性却是越简单越好。安全的登陆密码的复杂性,难记忆性和用户使用的方便性成为了一对矛盾,不可能同时兼顾。用户在每次使用业务时,需要输入密码以供身份验证,这种多次地重复使用相同的密码也增加了密码泄露的风险。在不同业务系统中的不同用户密码也增加了用户记忆密码的难度。

[0006] 尽管“用户名 - 密码”的身份认证方式有着天然的不安全性,但从实际的使用情况看来,人们往往选择了方便性,而忽略了安全性。使用简单的密码,方便地完成用户身份认

证。这样的使用方式存在极大的安全隐患，特别和用户的个人金融等唯一身份认证信息相关联的时候，这种安全性就显得更为重要。所以，提供一种用户方便使用的，同时又具有充分安全性保障的用户身份认证方式就显得非常重要。

[0007] 在现有市场中，有一种消除用户对“用户名－密码”身份认证的安全性顾虑的方式，即“用户资金安全保障”的附加保险。如果用户由于使用“用户名－密码”的方式使得其身份被盗用，使得其账户资金有损失，可以得到资金损失赔付。从用户的角度来看，好像足解决了其安全性问题。但足，这实际上只是一种风险转移，并没有解决其安全性问题，并且这种风险转移的成本最终还是由用户支付。

[0008] 在现有市场中，还有一种利用用户的生物特征如指纹等作为用户身份认证的标识。这种身份认证方式很好的解决了用户身份认证的唯一性问题。但是，由于用户的生物特征是有变化的，这种身份认证方式就存在识别的准确性和确定性问题。在用户的生物特征发生变化时，就不能很好的识别用户。在以确定性为基础的计算机和网络系统中，需要一种确定的唯一身份标识。并且用户的生物特征如指纹等也有可能被复制，进而使用复制的身份数据，假冒真实的用户而使用用户的业务数据，存在安全性隐患。

[0009] 本发明的核心功能就是公开了一种安全的，方便使用的用户身份认证设备，方法和系统。用户相关的具体业务信息，如用户在银行的账户信息，在医院的身体健康信息都存储在网络云端，而用户只需要提供唯一的，不可更改和复制的身份信息，就可以获得与此用户身份相关联的业务信息。用户不需要提供密码，也不需要把用于身份标识的 IC 卡提供给具体的业务部门（如银行等）供验证。大大地方便了用户的使用，也极大地提高了用户数据的安全性。

发明内容

[0010] 本发明的关键之处在于综合利用 IC 卡在用户身份认证中的安全性和无线通信在用户使用中的方便性，为用户和具体的业务提供部门提供一种安全的，方便的用户身份认证设备，方法和系统。

[0011] 本发明的用户身份认证系统包括如下部分：

[0012] 1) 用户身份标识 IC 卡。主要是接触式 IC 卡，提供通信传输接口，其通信数据接口满足智能卡传输协议 ISO-7816 标准。在其内部的存储系统中，根据使用的需要，有一个或者多个存储区域，每一个存储区域存储有具体的与不同业务相关联的用户身份标识相关信息。每一个存储区域的数据访问受到安全控制，需要相应的业务授权才能访问。存储区域之间的数据互相访问也需要相应的授权。每一个存储区域的数据满足不同业务的数据格式标准，例如，用于移动通信的用户身份标识的 SIM/USIM 卡满足 ETSI TS 102.211，3GPP TS 31.101，3GPP TS11.11 等标准；用于银行帐户的用户身份标识的金融 IC 卡满足金融 IC 卡的标准 ISO-10202 等。

[0013] 2) 用户 IC 卡接口设备。主要完成用户身份标识 IC 卡数据的读取和传输，有如下的功能模块：

[0014] a) 接触式 IC 卡读卡接口，使得用户身份标识 IC 卡能够插入该设备中，并能够读取 IC 卡的相关数据。其读卡接口满足 ISO-7816 传输协议标准。

[0015] b) 无线通信模块，能够通过无线传输方式（或者无线和有线相结合的传输方式）

把从用户身份标识 IC 卡读取的数据传送给网络云端服务器，也能够把网络云端服务器的数据传送给用户身份标识 IC 卡。

[0016] c) 安全控制模块，主要是确保用户 IC 卡接口设备和网络云端服务器之间的通信安全性和用户身份标识 IC 卡数据的访问安全性。

[0017] d) 能源供应模块如电池等，主要是使得用户 IC 卡接口设备成为一个移动设备而和用户随时随地同在，增加使用的方便性。

[0018] e) 便于用户随身携带的配件如腕表式携带的表带等，成为可穿戴式设备而不容易被丢失，进一步加强设备的安全性。

[0019] 3) 网络接口设备。主要是连接网络云端服务器和用户 IC 卡接口设备，能够把云端服务器的数据转发给用户 IC 卡接口设备，也能够把用户 IC 卡接口设备的数据转发给网络云端服务器。有如下的功能模块：

[0020] a) 连接于用户身份认证服务器，该服务器能够完成对用户的身份认证。

[0021] b) 连接于用户数据服务器，在需要的时候能够读取与用户身份相关联的业务数据。

[0022] c) 无线通信模块，提供无线通信连接（或者无线通信和有线通信相结合）使得用户 IC 卡接口设备能够方便地连接于网络身份认证服务器，完成用户身份认证过程。

[0023] 4) 用户身份认证服务器。主要是能够安全地完成对用户的身份认证，确保用户身份的真实性；并能够被用户身份标识 IC 卡认证，使得用户确信是接入一个真实的网络，而不是一个虚假的冒充网络。有如下的功能模块：

[0024] a) 连接于网络接口设备，使得用户身份认证服务器和用户身份标识 IC 卡能够建立可靠而安全的通信连接。它们之间的通信连接时通过网络接口设备，用户 IC 卡接口设备的转接完成的。

[0025] b) 连接于用户数据服务器，使得用户的业务数据和用户的身份标识能够建立起唯一的对应关系。在需要的时候，能够根据用户的身份标识 ID 号得到其相应的业务数据。

[0026] c) 用户身份认证鉴权模块，能够安全地完成对用户的身份认证，确保用户身份的真实性。这种对用户身份的认证主要是通过对用户身份标识 IC 卡内的数据完整性，算法的真实性的确认来完成的。

[0027] d) 网络自身业务的身份标识模块，能够被用户身份标识 IC 卡认证，使得用户确信是接入一个真实的网络，而不是一个虚假的冒充网络。

[0028] 5) 用户数据服务器。主要存储用户的业务数据，确保真实用户的合法数据访问，并拒绝假冒用户的非法数据访问。有如下的功能模块：

[0029] a) 连接于网络接口设备，在需要的时候提供用户的具体业务数据。

[0030] b) 连接于用户身份认证服务器，使得用户的业务数据和用户的身份标识能够建立起唯一的对应关系。

[0031] c) 数据访问安全控制模块，使得在任何情况下对用户的业务数据的访问，都必须在用户身份被正确地认证鉴权后，在用户身份认证服务器的授权下才能进行。

[0032] 通过如上所述的各个功能部分的协同工作，为用户和具体的业务部门（如银行，医院，电信等）提供方便的，安全的用户身份认证服务。其具体的过程可以分为两个主要部分，包括用户身份标识 IC 卡数据的初始化和用户身份的真实性认证。

[0033] 用户身份标识 IC 卡数据的初始化过程包括：

[0034] 1) 根据业务的需要，在用户身份标识 IC 卡内的存储设备中，选择一个存储区域，与此业务相关的用户身份标识信息都只存储在该区域中。并且对该区域的数据访问受到安全性控制，不同的数据具有不同访问权限。有些安全性敏感数据甚至不能被外部设备读取，只能在 IC 卡内部被 IC 卡自身读取。

[0035] 2) 用户需要使用业务部门提供的服务时，业务服务提供部门分配给用户一个唯一的业务用户身份号码，称为用户 ID 号。根据业务需要，用户 ID 号可以是全球唯一的，也可以是区域性唯一的，也可以重用其他业务的用户 ID 号（如居民身份证号码等）。其主要目的是和使用该业务的其他用户号码唯一地区分。当然，这种用户 ID 号的编码方式中，可以提供一些额外的信息，如快速地定位为用户身份标识 IC 卡提供身份认证服务的网络云端服务器的信息。这个用户 ID 号不需要保密，是公开的，任何第三方在需要的时候，获得适当的授权后就可以获得。用户 ID 号在用户身份标识 IC 卡数据的初始化过程中被写入 IC 卡中，能够被用户 IC 卡接口设备读取，并在需要的时候传送给网络云端服务器。

[0036] 3) 业务服务提供部门为用户提供一个其自身的业务 ID 号。同用户 ID 号一样，这个业务 ID 号也不需要保密，是公开的。在用户身份标识 IC 卡数据的初始化过程中，这个业务 ID 号被写入用户身份标识 IC 卡中，能够被用户 IC 卡接口设备读取。

[0037] 4) 在用户身份认证服务器上，分配给用户一个唯一的身份认证密码 Kw。Kw 和用户 ID 号是一一对应的，不同的用户具有不同的 Kw。并且 Kw 是高度保密的，作为一个高度机密的商业秘密被业务服务提供部门保存。只能被用户身份认证服务器读取，任何第三方，包括用户本人都不能读取。在用户身份标识 IC 卡数据的初始化过程中，Kw 被用户身份认证服务器写入用户身份标识 IC 卡中。这种写入是一次性的，不能被改写，只能在需要的时候，由用户身份认证服务器重新为用户分配一个新的 Kw，再重新写入用户身份标识 IC 卡。同样，写入用户身份标识 IC 卡的 Kw 只能在 IC 卡的内部被 IC 卡读取，任何第三方，包括用户 IC 卡接口设备都不能读取。这样，Kw 只共享于用户身份标识 IC 卡和用户身份认证服务器，成为它们之间进行身份认证的安全性保障的一部分。Kw 具有足够的长度，使得它不可能通过遍历的方式被猜测出来。

[0038] 5) 在用户身份标识 IC 卡数据的初始化过程中，用户通过安全的输入设备，输入一个用户端的身份认证密码 Ky。同样 Ky 具有足够的长度，使得它不可能通过遍历的方式被猜测出来。用户身份认证服务器接收 Ky 后，进行唯一性检查，确保用户 Ky 的唯一性。如果 Ky 不是唯一的，提示用户重新输入，直到 Ky 在整个业务中是唯一的为止。用户身份认证密码 Ky 也和用户 ID 号一一对应，以高度保密的方式存储于用户身份认证服务器上，并被用户身份认证服务器写入用户身份标识 IC 卡，安全地存储于 IC 卡中。任何第三方包括业务服务提供部门，都不能读取 Ky，只能在网络云端被用户身份认证服务器读取，或者只能在 IC 卡的内部被 IC 卡读取。Ky 虽然是用户输入的，但用户并不需要记住 Ky，并且由于其复杂性，大多数情况下很快就会被用户忘记。Ky 只是在初始化阶段一次性地输入，或者在需要的时候重复如上所述过程而重新输入一个新的 Ky，而不需要用户在每次使用业务时重复输入，大大加强了 Ky 的保密性。和 Kw 一样，Ky 只共享于用户身份标识 IC 卡和用户身份认证服务器，成为它们之间进行身份认证的安全性保障的一部分。

[0039] 6) 业务服务提供部门提供一个用户身份认证鉴权的加密算法 Am，作为一个高度

机密的商业秘密被业务服务提供部门保存。在用户身份标识 IC 卡数据的初始化过程中，加密算法 Am 被写入用户身份认证服务器和用户身份标识 IC 卡中，并被安全的存储。同 Kw 和 Ky 一样，加密算法 Am 不能被任何第三方读取，只能在网络云端被用户身份认证服务器读取，或者只能在 IC 卡的内部被 IC 卡读取。加密算法 Am 的输入数据包括 Kw，Ky 和一个临时生成的随机数序列 Ri，而其输出的数据则是一个身份认证鉴权数据序列 Si。除了业务服务提供部门，加密算法 Am 只共享于用户身份标识 IC 卡和用户身份认证服务器，成为它们之间进行身份认证的安全性保障的一部分。

[0040] 7) 在整个用户身份标识 IC 卡数据的初始化过程中，为了加强安全性数据 Kw，Ky 和 Am 的保密性，其生成和写入应当在特定的地点，用特定的设备写入。避免通过数据的传输，以远程的方式写入。减少在数据传输过程中安全性数据泄露的风险。由于这种写入是一次性的，并没有增加用户或者业务服务提供部门在使用过程中的复杂性。

[0041] 当用户身份标识 IC 卡完成数据的初始化后，就可以提供给用户使用。用户身份标识 IC 卡插入用户 IC 卡接口设备，而用户 IC 卡接口设备可以作为可穿戴设备而和用户随时随地同在。这样，用户身份标识 IC 卡就作为一个物理的实体凭证而和用户随时随地同在，用于标识用户的身份 ID。而作为可穿戴设备，就不容易被用户丢失，同时也提高了用户身份标识 IC 卡的物理安全性。

[0042] 当用户需要身份认证的时候，通过如下的步骤完成用户身份的认证鉴权过程：

[0043] 1) 用户 IC 卡接口设备读取存储在用户身份标识 IC 卡中的用户 ID 号，并通过网络接口设备，把用户 ID 号传送给用户身份认证服务器，申请用户身份认证，以确认使用该用户 ID 号的用户确实是真实合法的用户。

[0044] 2) 用户身份认证服务器收到用户 ID 号后，读取自身的安全数据库，得到该用户 ID 号所对应的用户身份认证密码 Kw 和 Ky。与此同时，生成一个临时的，一次性使用的随机数序列 Riw。

[0045] 3) 在用户身份认证服务器内部运行加密算法 Am。以 Kw，Ky 和临时生成的随机数序列 Riw 为输入，得到一个用户身份认证鉴权数据序列 Siw，存储于用户身份认证服务器，等待使用，以完成对用户的身份认证。

[0046] 4) 用户身份认证服务器把随机数序列 Riw，通过网络接口设备传送给用户 IC 卡接口设备，用户 IC 卡接口设备再把 Riw 传送给用户身份标识 IC 卡。

[0047] 5) 用户身份标识 IC 卡收到随机数序列 Riw 后，读取存储于其内部的用户身份认证密码 Kw 和 Ky，并在 IC 卡内部运行加密算法 Am，得到用户端的身份认证鉴权数据序列 Siy。由于使用了和用户身份认证服务器端相同的加密算法 Am，也使用了相同的 Kw 和 Ky，以及相同的随机数序列 Riw，所以得到的身份认证鉴权数据序列 Siy 就和用户身份认证服务器的用户身份认证鉴权数据序列 Siw 是一致的。并且由于加密算法 Am，用户身份认证密码 Kw 和 Ky 只是共享于用户身份标识 IC 卡和用户身份认证服务器，任何第三方即使窃取到随机数序列 Riw，也不可能的到相同的用户身份认证鉴权数据序列 Siy。另一方面，随机数序列 Riw 是一次性使用的，每次进行用户身份标识认证的鉴权数据序列 Siy 就是不同的，所以，即使鉴权数据序列 Siy 被泄露，对用户以后的身份标识认证也没有任何影响。

[0048] 6) 用户 IC 卡接口设备读取户身份标识 IC 卡生成的用户身份认证鉴权数据序列 Siy，并通过网络接口设备，传送给用户身份认证服务器。

[0049] 7) 用户身份认证服务器收到身份认证鉴权数据序列 Siy 后，和自己先前生成的数据序列 Siw 进行对比。如果一致，则完成对用户的身份认证过程，确认使用该用户 ID 号的用户是真实的合法可信用户。如果不一致，则中断用户的身份认证过程，拒绝提供进一步的服务。

[0050] 8) 用户身份认证服务器通过网络接口设备以及用户 IC 卡接口设备，发送确认消息给用户身份标识 IC 卡，通知其网络云端的用户身份认证过程已完成。并提供其自身的业务 ID 号，通知用户身份标识 IC 卡可以启动对网络的身份认证。防止用户接入虚假的冒充网络。

[0051] 9) 用户身份标识 IC 卡在收到确认消息后，启动对网络的业务 ID 身份认证。在 IC 卡内部生成一个临时的，一次性使用的随机数序列 Rjy，并通过用户 IC 卡接口设备，网络接口设备传送给用户身份认证服务器。

[0052] 10) 用户身份标识 IC 卡在其内部运行加密算法 Am，以 Kw，Ky 和 Rjy 为输入数据，生成一个网络身份认证鉴权数据序列 Sjy。存储于用户身份标识 IC 卡内部，等待使用，以完成对用户身份认证服务器的身份认证。

[0053] 11) 用户身份认证服务器收到随机数序列 Rjy 后，读取自身的安全数据库，得到该用户 ID 号所对应的用户身份认证密码 Kw 和 Ky。

[0054] 12) 在用户身份认证服务器内部运行加密算法 Am，以 Kw，Ky 和收到的 Rjy 为输入数据，生成一个网络身份认证鉴权数据序列 Sjw。

[0055] 13) 用户身份认证服务器通过网络接口设备以及用户 IC 卡接口设备，把自己生成的数据序列 Sjw 传送给用户身份标识 IC 卡。

[0056] 14) 用户身份标识 IC 卡收到数据序列 Sjw 后，和自身先前生成的网络身份认证鉴权数据序列 Sjy 进行对比。如果一致，则完成对业务网络的身份认证，确信接入的是一个真实的合法业务网络。如果不一致，则中断对网络的身份认证过程，拒绝和网络的进一步连接和数据交换。

[0057] 15) 用户身份标识 IC 卡在完成对业务网络的身份认证后，通过用户 IC 卡接口设备，网络接口设备，发送消息给用户身份认证服务器，确认对业务网络的身份认证。

[0058] 16) 整个用户身份的认证鉴权过程完成后，用户身份认证服务器发送消息给网络接口设备和用户数据服务器，授权可以进一步使用和该用户 ID 号所对应的业务数据。

[0059] 17) 在使用业务数据的时候，用户可以使用附加的业务密码，进一步加强业务数据的使用安全性。当然，由于最重要的身份的认证鉴权过程已经完成，这个附加的业务密码是可选的。

[0060] 在整个身份认证鉴权过程中，由于加密算法和身份认证密码只存在于网络的两端，并不需要在它们之间传送，极大地提高了身份认证鉴权的安全性。即使用于身份认证的数据 (Ri，Si) 在传输过程中有泄漏，得到数据的任何第三方也无法完成身份认证鉴权过程，并对用户以后的身份认证鉴权过程没有任何影响。

[0061] 由于用户 IC 卡接口设备和网络接口设备之间的通信连接是无线通信，或者是有线和无线通信的结合，使得在用户端的使用变得非常方便。用户不需要把用户身份标识 IC 卡插入或者靠近业务服务提供部门的读卡器设备，就能够完成用户身份认证。例如这种无线通信可以是短距离的蓝牙通信，其通信范围可以是几十米。在银行或者医院的服务大厅

的任何一个地方就可以接入其业务网络，完成用户身份认证和网络的身份认证。这种无线通信也可以是广域网的蜂窝式移动通信网络和有线的互联网的结合，在世界的任何一个地方就可以接入其业务网络，完成用户身份认证和网络的身份认证。并不需要用户身份标识IC卡和业务服务提供部门的读卡器的物理近距离接触，使得新兴的互联网业务服务提供部门可以快速的开展业务，即使没有大规模的业务服务网点。

[0062] 发明的效果

[0063] 在本发明的技术实施方案中，充分利用了UICC卡在用户身份认证中的安全性和无线通信在用户使用过程中的方便性，成功地兼顾了在用户业务数据使用过程中的安全性和方便性。其身份认证的安全性和现有的接触式IC卡是等同的，并且对现有的业务数据和IC卡身份数据没有任何影响，只需要增加与身份认证相关的设备，如用户身份认证服务器，网络接口设备和用户IC卡接口设备。对历史的业务数据可以很好的继承和使用，同时省略了业务服务提供部门的读卡器设备。本发明的身份认证方法可以替代现有互联网络（包括固定的因特网和移动互联网）中广泛使用的“用户名－密码”身份认证方式，从而加强用户身份认证的安全性，促进与用户身份认证相关的业务如移动金融的发展。

附图说明

[0064] 图1是本发明的各个功能模块示意图和它们之间的通信连接图。模块1是UICC卡，即用户身份标识IC卡。模块2是用户IC卡接口设备，该模块可以是一个可穿戴的移动设备，并且通常情况下模块1是插入模块2中，方便用户的移动使用。模块3是网络接口设备，模块4是用户身份认证服务器，模块5是用户数据服务器。模块1和模块2通过模块6进行通信连接，它们之间的数据传输是现有标准的接触式UICC卡传输协议。模块3和模块4之间通过模块7进行通信连接，可以是有线通信，也可以是无线通信，由具体的业务服务提供部门决定和提供。模块3和模块5通过模块8进行通信连接，模块4和模块5通过模块9进行通信连接。同模块7一样，模块8和模块9可以是有线通信，也可以是无线通信，由具体的业务服务提供部门决定和提供。无线传输通信模块10提供模块2（用户IC卡接口设备）和模块3（网络接口设备）之间的连接，为用户接入具体业务服务网路提供方便的通信连接。当然，通信模块10也可以是无线通信和有线通信的结合，主要是在用户端（模块2，用户IC卡接口设备）提供无线通信连接，方便用户的使用。

[0065] 图2是本发明的用户身份标识IC卡的数据初始化过程。包括在用户身份认证服务器和用户身份标识IC卡中同时写入用户ID号，业务ID号，网络端的身份认证密码Kw，用户端的身份认证密码Ky，加密算法Am。其中用户ID号和业务ID号是公开的，不需要保密。而网络端的身份认证密码Kw，用户端的身份认证密码Ky和加密算法Am是高度保密的，只能在用户身份认证服务器内部或者在用户身份标识IC卡内部被读取，任何外部设备都不能读取这些安全性数据。

[0066] 图3是本发明的用户身份认证鉴权消息流程图。包括用户身份认证服务器对用户身份标识IC卡的认证，确信使用该用户ID号的用户一个真实的合法用户。也包括用户身份标识IC卡对用户身份认证服务器的认证，确信用户接入的是一个真实的合法业务网络，而不是一个虚假的冒充网络。

具体实施方式

[0067] 根据不同的服务业务类型以及不同的无线通信方式，本发明的用户身份标识 IC 卡及其身份认证系统可以有不同的具体实施方式。下面就结合几个不同的具体实施例子来进一步对本发明进行说明。

[0068] 实施例子 1

[0069] 本实施例子的应用场景是用户身份标识 IC 卡为用户的银行账户，用户需要使用的业务是在银行的自动取款机上支取其个人帐户的现金。

[0070] 作为用户个人银行账户的用户身份标识 IC 卡，在用户向银行申请金融业务服务时，银行为用户设立银行账户，分配给用户一个唯一的个人银行账户号码，作为用户 ID 号，写入用户的帐户金融 IC 卡。同时，也把银行自身的业务 ID 号写入用户的帐户金融 IC 卡。用户的帐户 ID 号和银行的业务 ID 号作为公开的信息，可以用另外的书面形式提供给用户，方便用户在使用银行业务时使用相关 ID 号。作为用户银行账户的安全性数据，银行提供给用户的身份认证密码 Kw 和加密算法 Am 是在银行的业务窗口，用专门的写卡设备，写入用户的账户金融 IC 卡。与此同时，用户通过银行业务窗口的密码键盘，输入用户的身份认证密码 Ky，并确保 Ky 的唯一性，也用专门的写卡设备，写入用户的账户金融 IC 卡。在银行的后台业务网络中，Kw，Ky 和 Am 也被安全的写入用户帐户身份认证服务器，并完成其它的业务数据初始化。这样，用户的金融 IC 卡作为用户个人银行账户的用户身份标识 IC 卡，就可以交付给用户使用。

[0071] 用户 IC 卡接口设备是一个腕表式设备，被用户穿戴而和用户随时随地同在。作为银行账户的用户身份标识 IC 卡插入腕表中，也和用户随时随地同在。作为用户 IC 卡接口设备的腕表具有无线蓝牙通信模块，银行的自动取款机上也具有无线蓝牙通信模块，它们之间通过蓝牙通信能够建立起无线连接。

[0072] 作为联网设备，自动取款机具有另外一个通信链路连接于银行的后台网络系统，包括用户帐户身份的真实性认证鉴权服务器，用于认证将要进行现金支取业务的用户是合法真实的用户；也包括用户帐户数据服务器，存储有与用户帐户数据相关的信息，例如帐户余额等。这样，自动取款机就提供了一个在本发明中的网络接口设备的功能。

[0073] 当用户靠近自动取款机，在蓝牙通信的有效距离范围内时，就可以操作腕表，使其连接于自动取款机。或者根据用户预先的设定，腕表自动检测有效的自动取款机（例如用户经常使用的某个固定的自动取款机），并自动地建立蓝牙通信连接，完成双向的身份认证鉴权过程，确保用户和网络双方都是合法真实有效的。这样，当用户到达自动取款机时，就可以直接地支取现金，而不需要把作为自己的银行账户的金融 IC 卡插入自动取款机。甚至连银行通常使用的取款密码也不需要，因为作为安全性检查的身份认证过程已经完成，其安全性已经得到充分保障。当然，作为安全性补充，用户可以为现金支取业务设定一个业务附加密码，在完成现金支取密码验证后才能支取现金，这就和现有的自动取款机业务一样了。不过作为用户帐户身份的认证过程，已经大为简化了，极大地方便了用户的使用。在整个现金支取业务过程中，用户也不用担心接入一个虚假的冒充网络，因为根据本发明的身份认证鉴权机制，任何第三方的网络都不可能通过用户身份标识 IC 卡对网络的身份认证过程。并且一旦用户在使用中（或者银行的例行性安全检查中）发现异常，银行能够迅速行动，消除其安全隐患。同样，任何虚假的无效用户也不可能通过用户身份认证服务器对用

户的身份认证鉴权过程，保障了银行的自动取款机上的现金支取业务的安全性。

[0074] 这样，通过本发明的用户身份标识 IC 卡的认证方法，设备和系统，使得银行自动取款机上的现金支取业务比现有的使用用户密码的方式更为安全。而另一方面，对用户的使用来说，也更为方便，其取款过程也大为简化。

[0075] 实施例子 2

[0076] 本实施例子的应用场景是移动支付。同实施例子 1 一样，用户身份标识 IC 卡为用户的银行账户。而用户需要使用的业务是在超市购物的支付结算。

[0077] 超市的支付结算系统在获得用户 ID 号后，连接于银行的账户系统，请求银行账户系统从该用户 ID 号的帐户中划转结算资金。银行的用户身份认证服务器通过网络接口设备（连接于移动互联网的服务器），通过广域网的蜂窝式移动互联网（例如，2G 通信系统如 GSM/GPRS/EDGE，CDMA 等，3G 通信的 WCDMA，CDMA2000，TD-SCDMA 等通信系统，LTE FDD，TD-LTE 等 4G 移动通信系统），连接于用户的腕表，和用户的银行账户金融 IC 卡建立连接，完成双向的身份认证鉴权过程，确保用户和网络双方都是合法真实有效的。然后银行的账户数据服务器向用户发送支付消息，得到用户确认后，向超市的支付结算系统划转结算资金。这样，在整个支付过程中，用户只需要确认支付，而没有其他任何额外的步骤，极大地方便了用户的使用，移动支付过程也更为流畅。同时避免了在互联网中广为使用的“用户名 - 密码”身份认证方式，其安全性也大为增强，同时保护了银行和用户双方的数据。

[0078] 另一方面，超市的支付结算系统可以提供网络接口设备的部分功能，其一方面连接于银行的网络接口设备，另一方面具有短距离的无线蓝牙通信连接于用户的腕表。这样超市的支付结算系统就是银行的网络接口设备和用户的 IC 卡接口设备之间的一个桥梁。当银行的用户身份认证服务器完成身份认证鉴权后，超市的支付结算系统就可以收到确认消息，能够直接收到银行的账户数据服务器的结算资金。这样，连用户的支付确认步骤都可以省略，其使用也更为方便流畅。例如，当用户完成购物后，或者在购物过程中，直接通过超市的远距离支付结算系统，自动地完成购物支付，而不需要在超市的收银台作任何停留，用户的购物体验也更为完美。

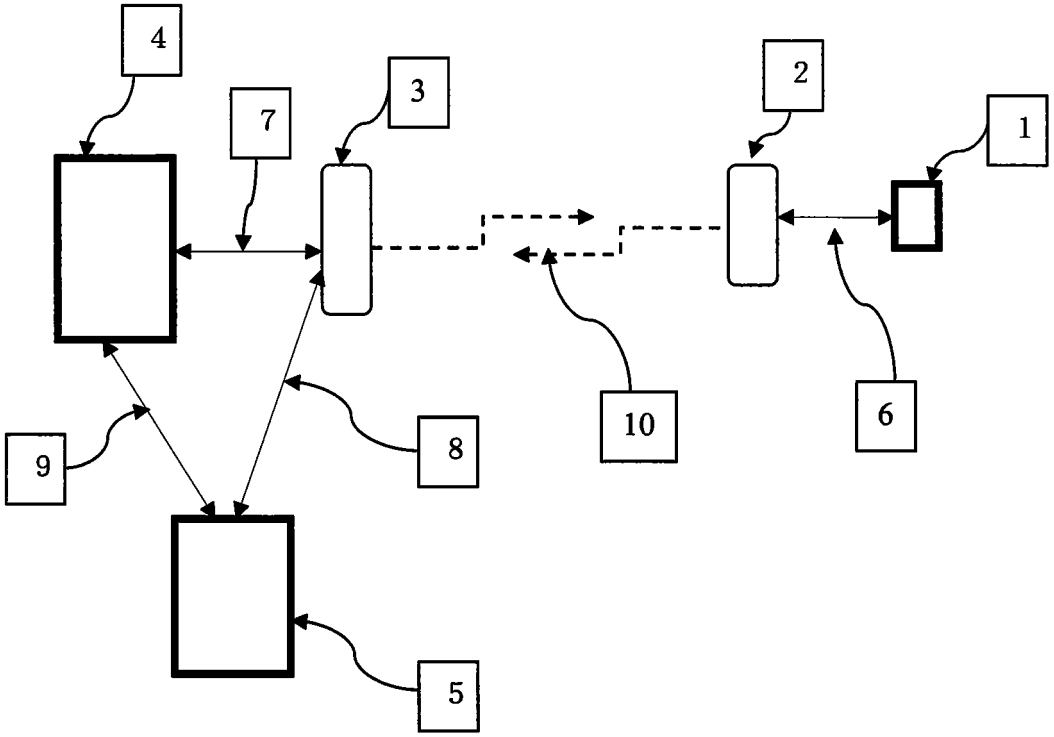

4
7
3
2
1
10
6
9
8
5

图 1

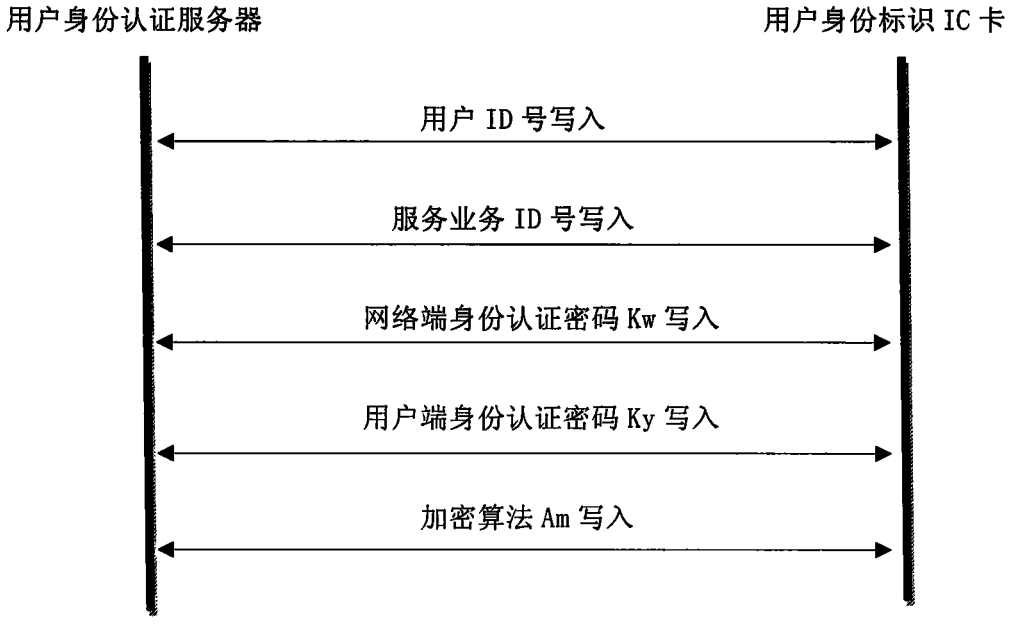

用户身份认证服务器
用户身份标识 IC 卡
用户 ID 号写入
服务业务 ID 号写入
网络端身份认证密码 Kw 写入
用户端身份认证密码 Ky 写入
加密算法 Am 写入

图 2

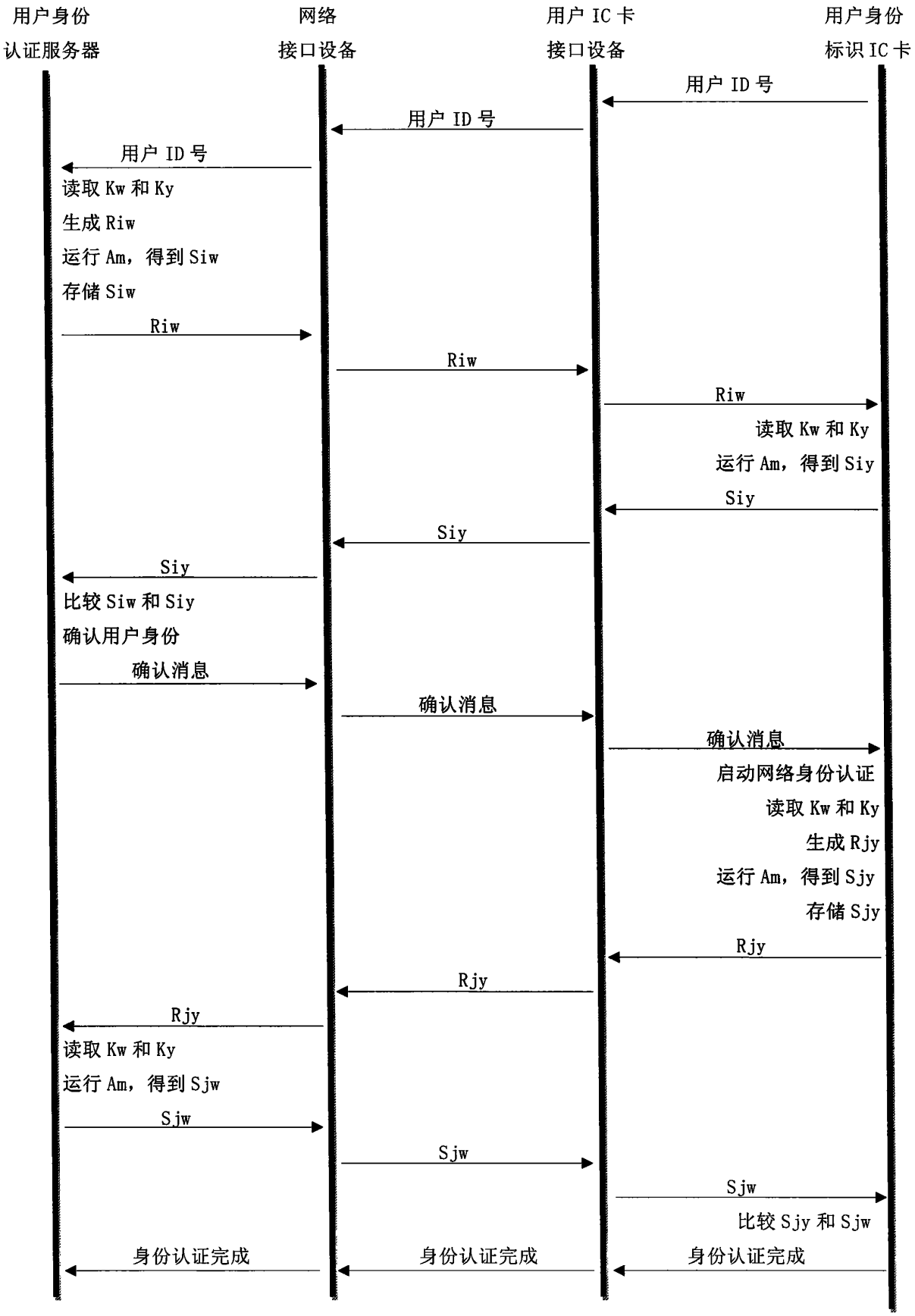

用户身份
认证服务器
网络
接口设备
用户 IC 卡
接口设备
用户身份
标识 IC 卡
用户 ID 号
用户 ID 号
用户 ID 号
读取 Kw 和 Ky
生成 Riw
运行 Am，得到 Siw
存储 Siw
Riw
Riw
Riw
读取 Kw 和 Ky
运行 Am，得到 Siy
Siy
Siy
Siy
比较 Siw 和 Siy
确认用户身份
确认消息
确认消息
确认消息
启动网络身份认证
读取 Kw 和 Ky
生成 Rjy
运行 Am，得到 Sjy
存储 Sjy
Rjy
Rjy
Rjy
读取 Kw 和 Ky
运行 Am，得到 Sjw
Sjw
Sjw
Sjw
比较 Sjy 和 Sjw
身份认证完成
身份认证完成
身份认证完成

图 3