

[12] 发明专利说明书

[21] ZL 专利号 95194608.0

[45] 授权公告日 2002 年 5 月 15 日

[11] 授权公告号 CN 1085025C

[22] 申请日 1995. 6. 14

[21] 申请号 95194608.0

[30] 优先权

[32] 1994. 6. 24 [33] US [31] 08/264,939

[86] 国际申请 PCT/SE95/00719 1995. 6. 14

[87] 国际公布 WO96/00485 英 1996. 1. 4

[85] 进入国家阶段日期 1997. 2. 14

[73] 专利权人 艾利森电话股份有限公司

地址 瑞典斯德哥尔摩

[72] 发明人 B·E·R·容森 J·P·发尔克

[56] 参考文献

EP 0506637A 1992. 9. 30 H04Q7/04

GB 2190820A 1987. 11. 25 H04L9/00

US 5287545 1994. 2. 15 H04Q7/04

WO 9317529A 1993. 9. 2 H04Q7/26

审查员 程 东

[74] 专利代理机构 中国专利代理(香港)有限公司

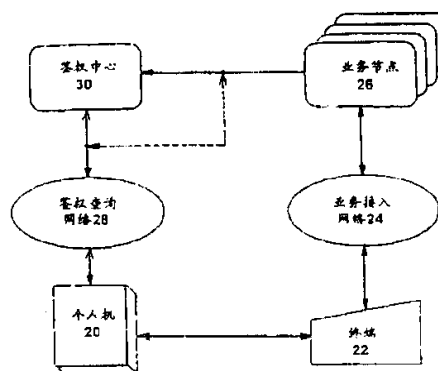
代理人 董 巍 董江雄

权利要求书 4 页 说明书 10 页 附图页数 3 页

[54] 发明名称 用户鉴权的方法和设备

[57] 摘要

用一个改进的寻呼机,基于一个被发送的查询码、一个被输入的个人识别号码和一个内部密钥,对该查询码算出唯一的响应码,对某一用户使用一项业务提供鉴权。该响应码被输入进一个简单的终端如电话机,如果该唯一的响应码是可接受的,这个用户就可以访问期望的业务如无现金交易或长途电话业务。



权 利 要 求 书

1.对一项电子业务的一个预期的用户鉴权的一个方法,该用户有一个个人机,所说的方法包括的步骤为:

发送一个查询码;

5 所说的个人机接收所说的查询码;

所说的个人机中,基于至少以所说的查询码和一个用户输入为变量的算法产生一个响应码;

产生一个输出码,它包括一个所说的响应码,适合被输入到一个物理上处于所说的用户位置但与所说的个人机是分离的终端,所说的终端与所
10 说的电子业务连接才生效;

把所说的响应码与一个期望的响应码比较;

仅当所说的比较结果可以接受时,才容许访问所说的电子业务。

2.按照权利要求1的一个方法,进一步又包括的步骤为:

在接收到所说的查询码之前,请求访问所说的电子业务,其中响应所
15 说的访问请求,发送和接收所说的查询码。

3.按照权利要求1的一个方法,进一步又包括的步骤为:

在所说的个人机存储一个或多个接收到的查询码;

在所说的查询码接收到并存储后请求访问所说的电子业务,其中在产生一个响应码时,所说的算法使用至少一个所说的存储的查询码和一个用
20 户输入作为变量。

4.按照权利要求1的一个方法,进一步又包括的步骤为:

通过键盘接收所说的用户输入。

5.按照权利要求1的一个方法,进一步又包括的步骤为:

通过一个笔迹识别装置接收所说的用户输入。

25 6.一个个人机包括:

一个用于接收查询码的接收机;

用于键入一个用户输入的一个输入装置;

一个响应码产生装置,它与所说的接收机和所说的输入装置连接才生效,用于按照一个接收的查询码和一个用户输入产生一个响应码;

30 一个输出装置,用于产生一个适合输入到终端的输出码,该终端连接到一项外部电子业务,所说的个人机物理上是与所说的终端分离的并且所说的终端处于用户的位置。

7.按照权利要求6的一个个人机,其中所说的接收机包括一个无线电波接收机。

8.按照权利要求7的一个个人机,其中所说的接收机包括常规的寻呼机电路。

5 9.按照权利要求6的一个个人机,其中所说的用户输入是一个个人身份号码。

10.按照权利要求6的一个个人机,其中所说的输入装置包括一个键盘。

10 11.按照权利要求6的一个个人机,其中所说的输入装置包括一个字符识别装置。

12.按照权利要求6的一个个人机,其中所说的输出装置包括一个显示器。

13.按照权利要求6的一个个人机,其中所说的输出装置包括一个音频发生器。

15 14.按照权利要求13的一个个人机,其中所说的音频发生器包括一个双音多频发生器。

15.按照权利要求6的一个个人机,其中所说的输出装置包括一个光学发生器。

20 16.按照权利要求13的一个个人机,其中所说的光学发生器至少包括红外线发生器、可见光发生器和紫外线发生器中的一个。

17.按照权利要求6的一个个人机,其中所说的输出装置包括至少一个电子感应耦合器。

18.按照权利要求17的一个个人机,其中所说的至少一个电子感应耦合器包括至少一个感应线圈。

25 19.按照权利要求6的一个个人机,其中所说的输出装置包括至少一个无线发射机。

20.按照权利要求6的一个个人机,其中所说的响应码发生器装置按照一个算法计算出一个响应码,其中所说的接收到的查询码、所说的用户输入和存储在所说的个人机的密钥在算法中是变量。

30 21.一个系统包括:

一个个人机用于接收一个查询码,接收一个用户输入,以及按照一个接收到的查询码和一个用户输入产生一个响应码;

一个与一个鉴权中心连接才生效的终端，所说的终端能接收所说的响应码并且物理上是与所说的个人机是分离的；

当访问一项业务时发送所说的查询码的一个网络，以及从所说的个人机接收所说的响应码，所说的网络又包括：

- 5 用于将所说的个人机产生的所说的响应码与期望的响应码进行比较的比较装置，及

仅当个人机产生的所说的响应码与所说的期望响应码比较的结果是可接受时，才容许访问所说的业务的容许装置。

22.按照权利要求 21 的一个系统，其中所说的网络包括：

- 10 一个业务接入网络，用于发送一个请求访问一项业务；

一个鉴权查询网络，与所说的鉴权中心连接才生效，用于把所说的查询码发送到所说的便携式，

所说的系统又包括：

- 15 至少一个业务节点提供一项业务，包括通过所说的业务接入网络与一个用户交换业务数据，以及用于接收所说的访问一项业务的请求，使鉴权中心响应所说的访问一项业务的请求产生一个响应码。

23.按照权利要求 22 的一个系统，其中所说的业务接入网络又包括用于发送所说的响应码到所说的比较装置的装置。

- 20 24.按照权利要求 22 的一个系统，其中所说的鉴权查询网络又包括用于把所说的响应码发送到所说的比较装置的装置。

25.按照权利要求 23 的一个系统，其中所说的比较装置位于所说的鉴权中心。

26.按照权利要求 24 的一个系统，其中所说的比较装置位于所说的鉴权中心。

- 25 27.按照权利要求 23 的一个系统，其中所说的比较装置位于所说的至少一个业务节点。

28.按照权利要求 24 的一个系统，其中所说的比较装置位于所说的至少一个业务节点。

- 30 29.按照权利要求 21 的一个系统，其中所说的响应码按照存储在所说的个人机中的一个算法产生。

30.按照权利要求 22 的一个系统，其中所说的业务接入网络包括一个有线电话系统。

31.按照权利要求 22 的一个系统，其中所说的业务节点提供一项或多项从下列业务中选出的业务：银行业务、信用卡业务、自动柜员机业务、帐户信息业务、一般信息业务、保密业务以及长途电话业务。

5 32.按照权利要求 22 的一个系统，其中所说的鉴权查询网络包括一个无线发射机。

33.按照权利要求 22 的一个系统，其中所说的鉴权查询网络包括一个蜂窝电话网络。

34.按照权利要求 22 的一个系统，其中所说的鉴权查询网络包括一个寻呼机网络。

10 35.按照权利要求 22 的一个系统，其中所说的个人机包括一个响应码发生器装置。

36.按照权利要求 29 的一个系统，其中所说的响应码发生器根据所说的接收到的查询码、所说的用户输入和存储在所说的个人机的一个密钥产生所说的响应码。

说明书

用户鉴权的方法和设备

本发明的背景

5 1)本发明的领域

本发明涉及到对一个试图访问一项电子业务的用户鉴权的一个方法和设备。具体地说是提供一个与已有系统分离的鉴权单元。

2)相关技术的描述

10 非常需要有效的鉴权方法和设备防止对业务的盗用。在当今信息时代，随着电子业务爆炸式地发展，这种要求也不断增长。诸如银行业务、信用卡业务、自动柜员机(ATM)业务、帐户信息业务如抵押、存款和投资帐户、一般信息业务如数据库业务和网络、保密业务、和长途电话业务之类的电子业务，为了保密、正确计费 and 避免盗用的目的都要求准确地识别用户。最近，蜂窝移动电话业中的盗用对有效的鉴权方法产生了非常大的需求，因此对一个用于蜂窝移动系统的协议作了标准化。见这儿引入作为参考的欧洲电信标准机构(ETSD)的 GSM 03.20 1993 年 19-29 页和美国专利号 5282250。

20 然而，常规的鉴权系统要求具有诸如 ATM 或信用卡读卡器的专门配备终端、加油站终端、使用登录程序的数据终端、或具有内置鉴权能力的蜂窝移动无线台。具有磁条的信用卡仅提供最低程度的保密，除了可能把该卡上一个未鉴权的签名与该用户的签名对比外，通常容许该卡的持卡人不用进一步鉴别该用户的身份进行业务处理。甚至在需要签名的业务处理中，对用户身份的确认度也是最低的。

25 其它的身份卡如 ATM 卡需要一个使用口令或 PIN 的登录过程。但一旦 PIN 被无权用户知道，如果这个用户能复制该 ATM 卡，则对鉴别该用户不能提供保密性。

30 这些鉴权方法需要专门配备的常常是专用的终端，这增加了成本并减低了相关的电子业务的可用性。换句话说，现有技术的保密系统常常需要专用的或按需改制的终端或对现存的终端进行改进，这大大地限制了把保密系统用到具体的场合。而且，一个用户可能使用几种电子业务，每种业务需要一种鉴权过程和/或个人身份号码(PIN)或口令，每种过程或口令与其

它的不同。当一个用户使用几种电子业务，可能难以记住众多的口令。更糟糕的是，他或她可能被要求周期性地改变这些口令，因此必须记住某个口令是否仍然有效。

而且，使用相对简单的终端如电话机，非常难以进行需要确定性比较高的鉴权的业务处理。例如，使用电话机的家庭银行业务被限制在涉及银行顾客自己的帐户或仅使用顾客自己的电话机。

本发明的概要

本发明通过一个鉴权过程克服这样或那样的问题，其中用户持有一个个人机，并不限制要使用任何特定的电子业务的终端或物理上与任何特定的电子业务的终端连接。该个人机可以通过与多种多样的电子业务联系的多种多样的终端，用来鉴别一个用户的身份。

该个人机含有一个接收器和一个算法单元，接收器接收被发出的查询码，算法单元根据预先存储的算法，对该查询码、一个用户输入如个人身份号码(PIN)或电子可识别的签名、和一个内部存储的密钥处理，算出一个响应码。然后该响应码送到业务节点，如果它是可接受的，批准访问该项业务。

基本方法涉及到从一个系统接收一个查询码，用户输入一个个人身份号码或其它的可识别输入，以及该个人机产生一个基于内部存储的算法的响应码。PIN或其它用户输入随时可能改变，查询码和响应码对每一次业务处理是唯一的。便携机可能接收、存储多个查询码供以后使用。

某种电子业务基本上任何现存的终端都可以使用个人机，而不需要对现存终端改进或按需改制。例如，个人机可以与一部标准电话配合使用，无论是一部无线电话或有线电话。用户可以通过电话机键盘输入显示在个人机上的响应码或个人机可以包括一个DTMF发射机，直接把响应码输入到电话机的麦克风。结果，任何业务终端(例如连接到一台业务计算机的数据终端)的键盘可以用作输入响应码。如果在终端中使用某些其它的输入装置如声音输入、感应耦合输入、光输入、无线发射机(具体的是如果该终端被旁路了，响应码被直接发送到鉴权中心)等，个人机可以包括一个兼容的输出装置。换句话说，个人机可以改进或配备成与现存的或可能的终端兼容，而不是必须改进终端以适应鉴权过程。

相同的基本鉴权过程可以用于用户希望申请的所有的业务，该过程可以被修改以适应电子业务的任何特定的要求。用户可能对所有他希望申请

的所有业务仅有一个个人机或几个个人机，每个个人机用作一项或几项该用户申请的部分业务。

附图的简短描述

现在将参考附图描述本发明，其中：

5 图 1 是一个按照本发明的鉴权寻呼系统的简要图；

图 1A 是一个按照本发明的参考具体的通信方式的鉴权寻呼系统的简要图；

图 2 是一个按照本发明的个人机的透视图；

图 3 是按照本发明的概述鉴权过程的流程图。

10 优选实施方案的详细描述

系统的硬件

参考图 1，本发明包括一个个人机 20 用作产生响应码，一个终端 22 用作发起业务访问和实施业务，以及用作把响应码输入到业务接入网络 24 或直接输入到一个独立的鉴权中心 30。业务接入网络在终端 22 和业务节点 26 间传送数据。业务节点 26 产生一个查询码，并且请求该查询码通过一个鉴权查询网络 28 被发送到个人机 20。另一种方法是，独立的鉴权中心 30 在业务节点 26 的请求下产生查询码。终端 22 可以是有线电话机、无线电话机、ATM、带 modem(调制解调器)的计算机、传真机或基本上任何其它类型的能直接接收输入或间接地从便携机接收输入并把信息中转到业务节点 26 的终端。

业务节点 26 可能是任何形式的电子业务，如银行或金融业务、信用卡业务、长途电话业务、信息业务等。所提供的业务的类型与本发明没有紧密的关系。本发明的便携机的一个优点是它可以被用作对任何类型业务的用户鉴权。

25 在一个示范的实现方案中，鉴权中心 30，不管是独立的还是业务节点 26 的一部分，包括一台无线发射机、存储一个或多个算法的存储器和一个比较接收到的响应码与期望的响应码的比较器。鉴权中心 30 可以以附加在前在的寻呼系统或其它的无线通信系统上的外加软件的形式实现。独立的鉴权中心 30 使许多业务节点或网络能够使用一个鉴权中心 30。这容许为所有的应用在一个位置改变鉴权程序并容许一个鉴权程序用于多个业务也许是所有的用户已申请的业务。

业务接入网络 24 可以是任何形式的通信系统如公用或专用电话网、电

报、或其它有线系统、蜂窝无线网络、或其它无线通信网络。业务接入网络 24 的形式可以是能从终端 22 发送信息到业务节点 26 的任何形式。下面某些例子中的业务接入网络 24 是以现存的电话网的形式提供的。

5 鉴权查询网络 28 可以与业务接入网络 24 是同一个网络，或最好是一个独立的、不同的网络。鉴权查询网络 28 可以是任何通信系统，如公用或专用电话网、电报、或其它有线系统、蜂窝无线网络、或其它无线通信网络。鉴权查询网络 28 可以是能从业务节点 26(或鉴权中心 30)发送信息到个人机 20 的任何形式。在一个实施方案中，鉴权网络是已有的广域寻呼系统，能广播个人机识别号码和额外的信息如至少能广播查询码。至少可以发送被提示将呼叫的用户的电话号码的现有的寻呼系统，足以和这里所公开的
10 个人机一起使用。任何形式的无线通信系统可以达到本发明所提供的最优的保密性，因为当输入正确的 PIN 或其它类似的号码时，仅一个特定的接收机正确地产生期望的响应。然而，如果要通过一个交互的业务接入网络 24，用户可能被要求手动键入一个查询码。

15 在图 2 所示的示范的实施方案中，个人机 20 包含一个接收机单元 21a 用于接收查询码，和一个算法单元 21b，它连接到接收机单元 21a 才生效，并且最好包括一个输入装置接收作用户输入，如 PIN 这样的保密号码(图 2)。接收机单元 21a 可以是寻呼机的形式，具有数字显示功能能显示呼叫者的电话号码或类似的号码。个人机 20 基本上可以是一台常规的寻呼机，
20 它被改进成包括如一个接收机 21b、一个输入键盘 21c 和一个可选用的双音多频(DTMF)发生器 21d(当终端 22 连接到某种形式的语音通信网络，如果要求自动输入显示的响应码，最好使用这种装置)。在业务接入网络包括一条无线上行链路或响应码直接发送到鉴权中心 30 或业务节点 26 的实现方案中，个人机 20 可能包括一个发射机 21f。算法单元 21b 按照接收到的
25 查询码、一个合适的被输入的保密码和可选用的一个在申请业务时写入个人机的存储器中的密钥(个人机的供应商提供的一个保密号码)计算出一个响应码。这种类型的算法有现成的技术或从中可以得到。见 GSM 03.20，附录 c.2，如算法 A3。用在给定的实施方案中的具体的算法与本发明无密切的关系。提供存储器 21e 存贮该算法、密钥、接收的查询码和计算机程序因为一个具体的实现方案说明起来比较方便。寻呼机单元可以用微处
30 理器驱动的。

这提供了对用户的身份的三重检验，要求信息来自 3 个不同的来源(用

户: PIN, 业务节点或鉴权中心: 查询码, 个人机的供应商: 密钥), 因此增加了业务处理的相对保密性, 以防止盗用或其它无权使用。

在本发明的一个优选的实施方案中, 个人机是一个独立的单元, 因此减少了或避免了按需改制通信设备如蜂窝电话的需要。接收机单元、输入装置和执行必要计算的能力在常规电话和个人通信机中都是存在的, 这样容许本发明通过软件来实现。

查询码可以对一次确定的业务处理是唯一的或是广播形式的, 例如在确定的时刻对所有这样的个人机进行广播。响应码对这两种情况的每一次业务处理都是唯一的。而且, 在这两种情况中, 查询码应该周期性地或随机地改变, 对业务处理提供额外的保密性。相似的情况, 用户输入, 如 PIN 可以由用户决定或有规律地更新。甚至算法可以随时改变, 或个人机 20 中可以存储多于一个算法, 它可以以预先确定的顺序循环使用或在预先确定次数的使用后改变。只要鉴权中心 30 可以决定对给定的业务处理使用什么算法、什么密钥(如果使用)以及什么用户输入, 用户就可以被鉴权。

算法单元 21b 基于接收的查询码、用户输入(如 PIN)和可选用的密钥算出一个响应码。因此, 如果要保证访问某项业务, 要产生一个正确的响应码, 查询码、用户输入和密钥(如果使用)必须与业务节点 26 或鉴权中心 30 的期望一致。提供足够的信息给业务节点 26 或鉴权中心 30, 供其预测正确的响应码。因此, 要使一次业务处理被授权, 用户必须知道合适的用户输入(如 PIN), 持有正确的个人机并且接收合适的查询码。

为了输入图 2 所示的用户输入, 最好提供常规的 12 个按钮(1-9, *和#)的键盘 21c。另一种选择是, 可以根据提供较少还是较多的保密性, 使用精减的或扩展的键盘。可以识别签名或其它笔迹的字符识别装置可以用作用户输入装置。而且, 在适当的场合为增加保密性可以使用指纹或视网膜扫描器。

例如, 查询码可以具有 10 个十进制数字, 密钥具有 12 个十进制数字, PIN 具有 4 个十进制数字, 以及响应码具有 8 个十进制数字。

鉴权过程

某用户使用终端 22 通过业务接入网络 24 发送请求到业务节点 26, 发起对一项业务的访问。业务节点 26 不立即提供该项业务。而是, 它产生一个查询码或使鉴权中心 30 产生一个查询码。查询码通过一个鉴权查询网络 28 发送到便携机。

当便携机 20 接收到一个鉴权查询码, 它提示用户输入一个 PIN 或其它识别信息, 并且通过一个使用查询码、内部密码和 PIN 作为变量的算法产生一个响应码。另一种方法, 可以接收几个查询码并存储在个人机, 当用户试图访问一项电子业务时, 用户被提示进行用户输入。用户输入, 如通过键盘键入, 一个 PIN。然而, 已知的字符识别装置可以用作识别签名或一般的笔迹, 它是通过一个书写人在一本便笺上输入的。其它的可能性包括指纹或视网膜扫描装置, 尽管这些装置的成本使该实现方案实用化不太可能, 除非该业务处理需要最高形式的保密。

基于查询码、用户输入和可选用的密钥, 内部存储的算法产生一个响应码。

响应码或者在显示器 20a 上显示, 用作人工输入到终端 22, 或者以电子、声音或光学输入到终端 22, 它又透明地把响应码通过业务接入网络 24 发送到业务节点 26。另一种也是额外的方法, 响应码可以通过鉴权网络 28 发送到鉴权中心 30, 然后它可能把响应码发送到业务节点 26, 或把响应码与期望的响应码比较并且把结果转发到业务节点 26。如果该响应码是可接受的, 业务节点 26 容许用户访问它提供的业务。该响应码与期望的响应码比较, 在示范的实施方案中, 期望的响应码可能是预先存储的或用同样的算法和变量产生的。因为鉴权查询网络中的通信链路以及业务接入网络可能受噪声(如无线电干扰)的影响, 对比较的结果给出一些容限。换句话说, 为了访问该项业务, 该响应码和期望的响应码没有必要正好是相同的, 特别是当使用模拟而不是数字传输格式时。

参考图 3 的流程图, 示范的鉴权过程从步骤 S10 开始, 用户通过业务接入网络 24 发起与业务节点 26 的通信。这可以很简单如摘机并且拨适当的电话号码, 它可以是预先存储在个人机中的。在步骤 S12, 该过程可以包括键入一个用户号码或身份, 如用作数据业务的那种号码。如步骤 S14 所示, 业务接入网络 24 透明地把来自用户的访问请求送到业务节点 26。业务节点 26 响应访问请求, 通过经鉴权查询网络 28 发送一个查询码(或者在独立的查询中心 30 或在业务节点 26 产生)到用户的个人机 20 请求鉴权, 如步骤 S18 所示。另一种方法, 一个或多个查询码可以被预先发送到个人机。个人机 20 可能显示一条提示语, 提示用户键入如一个密码, 如 PIN, 或由终端 22 提供提示语。得到用户输入, 个人机 20 的算法单元 21b 算出并发送一个响应码到显示器或到双音多频发生器, 或两者。可以采用其它

输出装置如无线电波(如无线发射机或收发信机)、红外线、可见光或紫外线发生器(如 LED 或半导体激光器), 电子感应耦合器(如感应线圈), 或除 DTMF 发生器外的各种形式的声学装置。

5 然后用户或者把显示的响应码手动键入到终端 22 , 或在使用不同类型的输出装置的情况下便携机 20 直接把响应码输入。例如, 当通信系统中使用双音多频(DTMF)发生器时, 用户把产生的音频信号送给该系统的麦克风。

10 业务接入网络 24 透明地把响应码发送到业务节点 26 , 它决定该响应码是否可接受。如果鉴权中心 30 对接收到的响应码与期望的响应码进行比较, 业务节点 26 将把响应码发送到鉴权中心 30 。另一种方法是, 个人机可以通过无线传输把响应码直接发送到鉴权中心 30 , 且鉴权中心 30 把结果通知业务节点 26 。如果响应码不可接受, 用户访问该项业务被拒绝, 则鉴权程序返回到启动整个程序或重新请求识别信息。可选用的是, 如果预先确定次数的访问请求被拒绝或如果已经报告个人机 20 被盗, 系统可以使
15 该个人机无效。

如果响应码是可接受的, 该项业务被访问, 并且用户可以通过业务节点执行希望的、可用的功能。

参考图 1A , 参考一个示范的实施方案的具体的、编号的通信步骤, 检验基本的程序。

20 (1)键入用户身份命令: PTOEXAN

(2)业务节点接收来自 PROEXAN 的对某项业务的请求。该用户身份送到专利和商标办公室检查员 Andersson 。业务节点发送鉴权请求: “请对这个用户鉴权: 检查员 Andersson ”。

(3)查询码被发送到检查员 Andersson 的鉴权寻呼机。

25 (4)键入口令, 该口令从业务节点发送到数据终端。

(5)检查员 Andersson 键入 PIN 号码, 激活个人机中对响应码的计算。响应码在便携机的显示器上显示, 然后被手动键入到数据终端。另一种方法是, 响应码通过无线链路直接发送到鉴权中心。

(6)响应码从业务节点发送到鉴权中心。

30 (7)鉴权中心把接收到的响应码与期望的响应码比较, 并且发送一条消息到业务节点, 通知节点已经鉴权还是未鉴权。

(8)对该用户的鉴权得到同意或未同意。

作为本发明的一个具体的例子，将描述家庭银行的应用。在该应用中，目的在于把钱从主人的帐户转移到一个不同的帐户，如一个债权人的帐户。用户可以在家里用一部电话机和一个个人机支付帐单。在该例中，用户所执行的所有的鉴权步骤都是手动的。相应的问答方式如下：

5 用户：通过呼叫一个银行的付款业务电话号码发起一次电话呼叫。

 银行：“键入你的帐号。”

 用户：“4219231459#。”

 银行：“请把下列数字键入你的鉴权单元- 1,2,3,2,8”(查询码)。另一种方法是，如果查询码是被广播的或预先存储在个人机中，则该步骤被跳
10 过。

 “请键入你的个人身份号码。”

 用户：把他的PIN键入个人机。个人机在显示器上显示一个查询响应如19283746。用户在电话机键盘上键入“19283746”。

 银行：“键入款项的帐号以接收付款”

15 用户：“4313950678#。”

 银行：“美国Anytown的Jane Doe先生的帐户。键入数量”

 用户：“\$500.00。”

 银行：“\$500.00已转帐到Jane Doe先生的帐户。交易参考号码123456。”

20 用户：挂机。

 当发生错误时该过程可能会因为要执行中断操作而复杂，在一次呼叫中处理多于一种业务处理，使用家中另一部电话机等等而复杂化。

 第二个示范的过程涉及使用一个特种业务节点(SSN)对长途呼叫收费。在该例中，当通过一家长途电话公司对长途电话收费时提供鉴权。

25 用户：特种业务节点电话是，如前缀900后面跟着要呼叫的长途电话号码如900 555-1212。

 SSN：“给出ID和查询响应。”

 用户：把PIN键入个人机(它已经接收到一个通过无线发送的查询码)，个人机在显示器上显示一个查询响应，例如“19283746。”然后按下一个
30 按钮，把个人机的扬声器靠近电话机的麦克风，发出音频DTMF输出发送到SSN如“#0859032843#19283746#”它包括个人身份号码以及跟随的对查询码的响应。

SSN: 检查响应码的真实性, 如果可接受, 提供连接。

相同的个人机可以用于以上两种业务处理。可以实现一种更自动化的业务处理。例如, 个人机可能包括有一个接收机和一个 DTMF 发射机, 在这种情况下, 用户仅仅发起对某项业务的访问, 收到提示语后键入用户输入如 PIN。

为避免寻呼系统在大范围的寻呼网络中发射查询码的等待时间, 例如有可能发射几个(如 3 个)查询码, 它可以存储在个人机 20 直到键入 PIN 产生一个响应码才使用。如果由于错误重复键入, 随后产生的查询码不使用多于一次。

鉴权中心 30 可以决定何时用无线信号给便携机提供额外的查询码, 因为它为了执行鉴权要接收该响应。另一种方法是, 如果业务节点 26 收到响应, 业务节点 26 请求鉴权中心 30 发送下一个期望的响应到业务节点 26, 这样鉴权中心可以对产生的或使用的响应码计数。如前所述, 鉴权中心 30 可以与业务节点 26 相结合或单独设立并让几个业务节点共同使用它。

使用现存的网络, 不用耗资大量的成本在现存的网络和业务节点间建立适当的数据交换, 对任何适合的业务节点 26 都可以实现本发明。如果终端能发送数据, 使用任何网络中的任何终端, 响应码可以用于鉴权。该响应码可以通过鉴权网络 28(如通过无线信号)发送。

根据本发明的实施方案, 提供一种鉴权的方法, 它可以用于用户所申请的所有的电子业务, 而不需要记住众多的口令。为达到这些, 鉴权网络 30 可以连接到所有的电子网络或业务节点 26。当某用户通过一个具体的业务节点 26, 请求一项业务, 业务节点 26 向鉴权中心发送一个请求要求鉴权。接收到对用户鉴权的请求, 鉴权中心 30 产生一个查询码, 通过业务节点 26, 它被发送到该用户。该用户可能把查询码和一个用户输入如 PIN 手动键入他的个人机, 以得到一个响应码, 响应码显示在个人机 20 的显示器上。该响应可以被手动键入到终端 22, 用作访问该项业务。然后可以通过鉴权中心或业务节点 26 执行鉴权检查。

查询码也可以通过无线从鉴权中心 30 发送到个人机, 或例如通过一部 PSTN 电话机作为 DTMF 信号被发出。

这种鉴权方法不要求对现存的终端作任何改变。该方法容许响应码被发送到以适合这种业务应用的方式执行鉴权检查的节点。用作激活个人机中响应码的计算的 PIN 码是唯一的“口令”或用户必须记住的 PIN。

在不离开本发明的精神和主要特征的情况下，本发明当然可以以其它具体的方式而不用那些这儿所提出的方式完成。因此，从所有的方面考虑本发明都是说明性的而不是限制性的，并且将包括所有的在附加的权利要求的精神和等价范围内的变化。

说明书附图

图 1

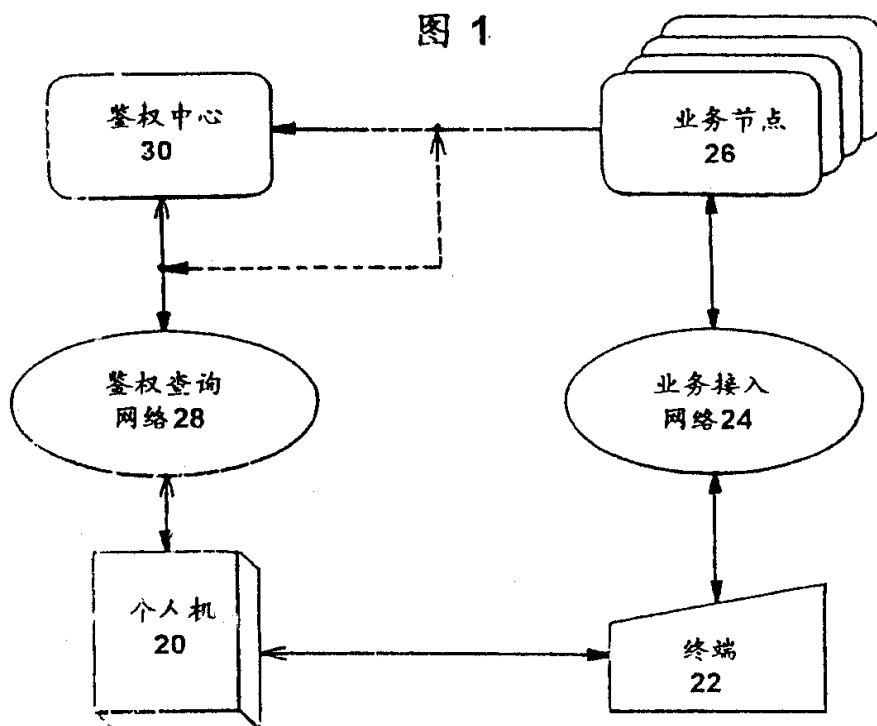
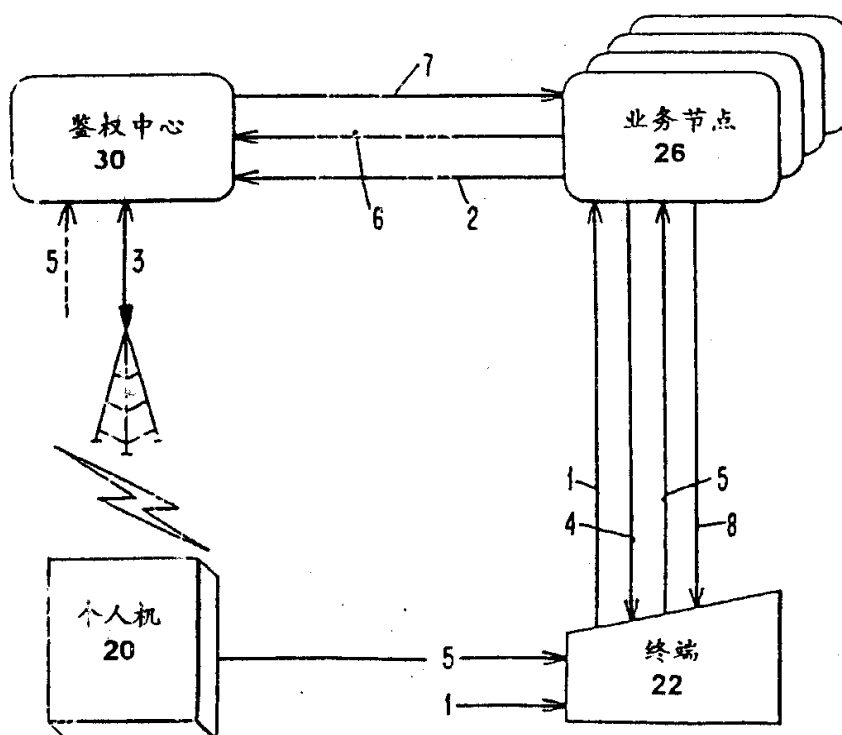


图 1A



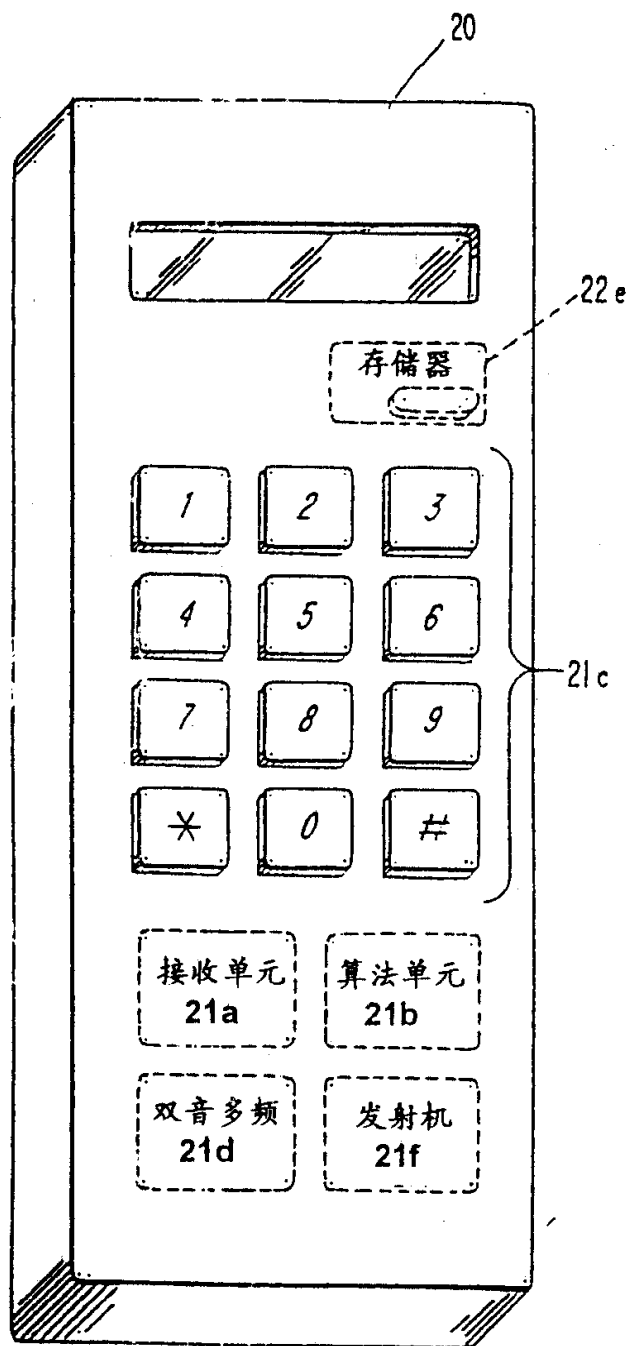


图 2

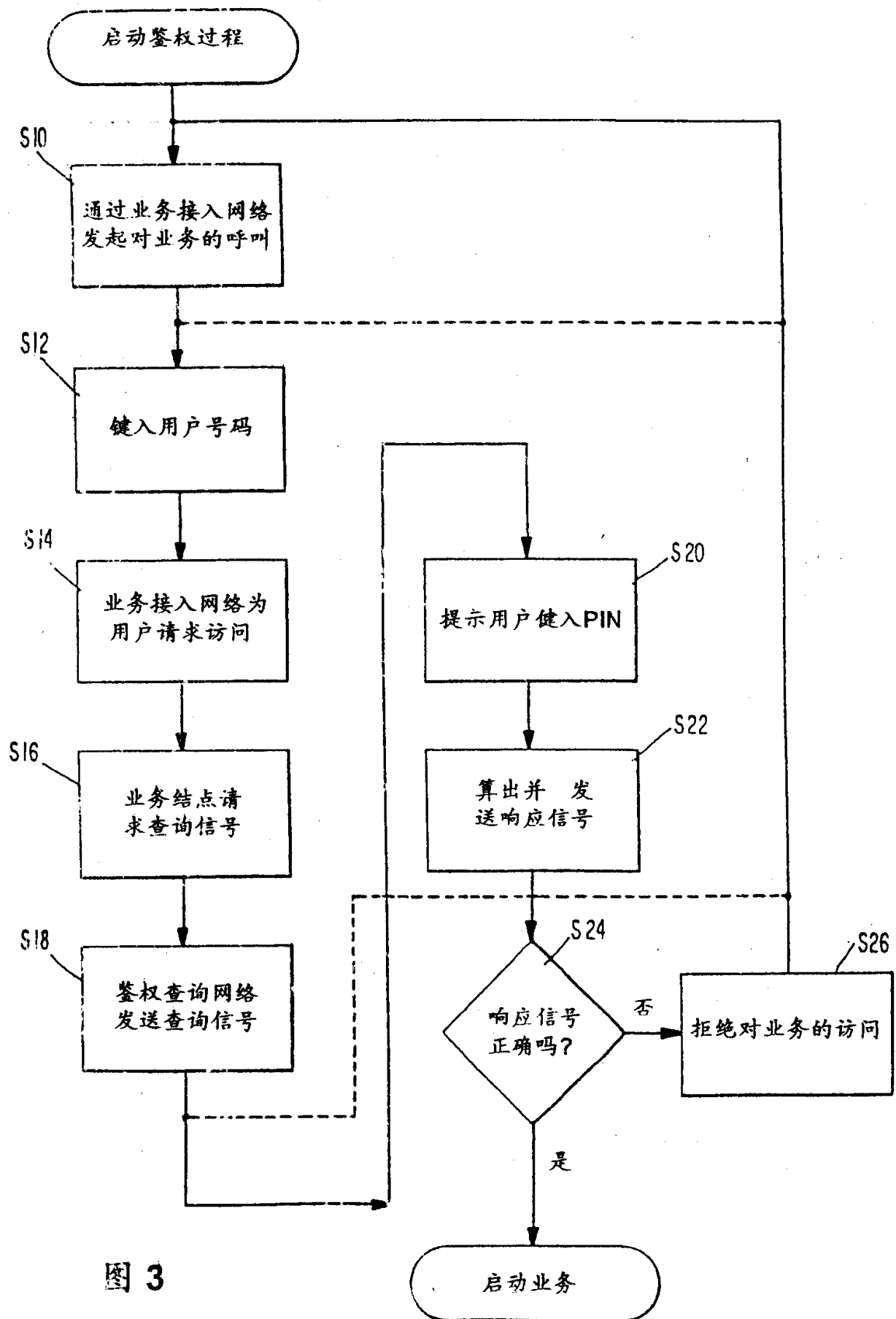


图 3