(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 103891196 B
(45)授权公告日 2018.10.09

(21)申请号 201280050254.3

(22)申请日 2012.09.12

(65)同一申请的已公布的文献号
申请公布号 CN 103891196 A

(43)申请公布日 2014.06.25

(30)优先权数据
1158132 2011.09.13 FR

(85)PCT国际申请进入国家阶段日
2014.04.11

(86)PCT国际申请的申请数据
PCT/EP2012/067847 2012.09.12

(87)PCT国际申请的公布数据
WO2013/037828 FR 2013.03.21

(73)专利权人 萨热姆通信宽带简易股份有限公司
地址 法国吕埃尔-马尔迈松

(72)发明人 托马斯·兰戴斯

(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 余朦 王艳春

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
US 2003185399 A1,2003.10.02,
CN 1294457 A,2001.05.09,

审查员 夏晓蕾

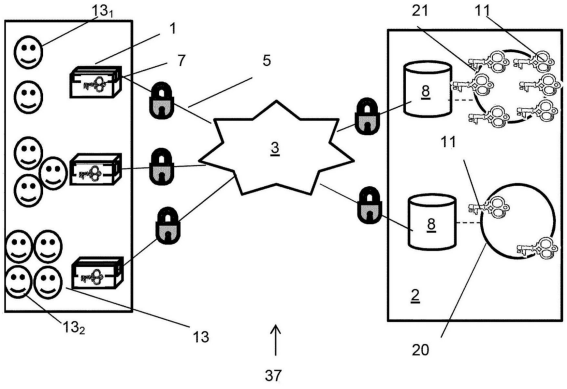
权利要求书3页 说明书11页 附图4页

(54)发明名称

安全数据交换方法及实施该方法的通信设备和系统

(57)摘要

本发明涉及用于通过通信网络(3)在服务提供者(2)的服务器(8)与通信设备(1)之间安全地交换数据(5)的一种方法,通信设备(1)使得通信设备(1)的至少一个用户(13)能够使用由该服务提供者(2)提供的服务(4),该方法的特征在于,该方法包括用于在服务提供者(2)的至少一个服务器(8)与通信设备(1)之间交换数据(5)的以下步骤:为了发送数据(5),使用物理密钥(7)加密所发送数据(5)的至少一部分,其中,物理密钥(7)对服务提供者(2)来说是已知的,并被物理地写入通信设备(1)的电子芯片(6)的只读存储器中;以及,在接收数据(5)时,使用所述物理密钥(7)将接收的数据解密。



CN 103891196 B

1.用于通过通信网络(3)在服务提供者(2)的服务器(8)与通信设备(1)之间安全地交换数据(5)的方法,所述方法的特征在于,在至少一个所述服务器(8)与所述通信设备(1)之间交换的所述数据(5)允许创建和访问社区(20、21、23),所述社区(20、21、23)将多个用户和特定服务分组,

其中,所述数据(5)的交换步骤包括:

-关联一个或多个用户的非对称公开密钥(11)与由所述一个或多个用户请求的至少一个所述社区,所述通信设备的多个用户中每个都具有对其特定的所述非对称公开密钥(11),

-通过识别每个用户的所述非对称公开密钥,允许所述用户访问所述社区的所述服务和/或与所述社区的其他用户进行交换,以及

-通过硬件密钥(7)加密被发送的所述数据(5)的至少一部分,并在接收所述数据(5)时通过所述硬件密钥(7)将接收的所述数据(5)解密,保护所述用户与所述社区之间和/或同一所述社区的用户之间的数据交换,其中,所述硬件密钥(7)对所述服务提供者(2)是已知的,并且在物理上写入每个用户的所述通信设备(1)的电子芯片(6)的只读存储器(9)中。

2.根据权利要求1所述的方法,其中:

用户(13)在所述通信设备(1)处注册(101),其中所述通信设备(1)生成:

○至少一个所述非对称公开密钥,所述非对称公开密钥对所述用户(13)是特定的并被传输至所述服务提供者(2)(104、105),

○至少一个非对称私人密钥,所述非对称私人密钥对所述用户(13)是特定的并存储在所述通信设备(1)中(102,103),以及

在所述通信设备(1)与所述服务提供者(2)之间交换的所述数据(5)包括对于所述用户(13)而言是特定的所述非对称公开密钥,所述非对称公开密钥由所述硬件密钥(7)加密或不加密,所述非对称公开密钥允许识别所述用户(13)和/或识别与所述用户(13)相关联的所述服务提供者(2)的所述服务。

3.根据权利要求1所述的方法,其中,在所述服务提供者(2)的所述服务器(8)与所述通信设备(1)之间交换的所述数据(5)包括至少一个第一级密钥(K_1),所述第一级密钥(K_1)自身允许利用至少一个第二级密钥(K_2)进行解密,连续加密实现至一个或多个第n级密钥(K_n),其中,n是大于等于2的整数,所述第一级密钥(K_1)利用所述硬件密钥(7)进行加密。

4.根据权利要求1所述的方法,其中,在所述服务提供者(2)的所述服务器(8)与所述通信设备(1)之间交换的所述数据(5)包括以下信息中至少之一:

-独特识别符(15),所述独特识别符(15)对于所述通信设备(1)是特定的,并允许所述服务提供者(2)识别所述通信设备(1),所述服务提供者(2)的所述服务器(8)利用所述独特识别符(15)寻找与所述通信设备(1)相关联的所述硬件密钥(7),

-服务识别符(16),所述服务识别符(16)对于由所述用户通过所述通信设备(1)请求的每个服务是特定的,并允许所述服务提供者(2)的所述服务器(8)识别由所述用户通过所述通信设备(1)请求的所述服务,

-与索引(17)相关的信息,所述索引(17)用于选择在所述通信网络(3)上传输的密钥,

-所述服务提供者(2)的所述服务器(8)与所述通信设备(1)之间的安全通信协议(18)。

5.根据权利要求1所述的方法,包括以下相继步骤:

-用户(13)通过所述通信设备(1)请求(201)访问公共社区(21)和/或所述公共社区(21)的用户之间的数据交换,其中所述公共社区(21)提供至少一个服务并由所述服务提供者(2)管理,

-所述通信设备(1)将对所述用户(13)而言是特定的所述非对称公开密钥(11)发送(202)至所述服务提供者(2)的所述服务器(8),

-所述服务提供者(2)的所述服务器(8)将由所述用户请求的所述公共社区(21)与所述用户的所述非对称公开密钥(11)关联(203),从而允许所述用户(13)访问所述公共社区(21)。

6.根据权利要求1所述的方法,包括以下步骤:

-第一用户(13_1)通过所述通信设备(1)请求(301)访问私人社区(20)和/或所述私人社区的用户之间的数据交换,其中所述私人社区(20)提供至少一个服务并由第二用户(13_2)管理,

-所述第一用户(13_1)的请求通过所述服务提供者(2)的所述服务器(8)发送(302)至所述第二用户(13_2)的所述通信设备(1),

-所述第二用户(13_2)通过其通信设备(1)发出(303)接受决定或拒绝决定,所述接受决定或所述拒绝决定被发送至所述服务提供者(2)的所述服务器(8),

-根据所述第二用户(13_2)的决定,所述第一用户(13_1)被授权(304)访问所述私人社区(20),接受决定导致所述第一用户(13_1)的所述非对称公开密钥(11)与所述私人社区(20)之间的关联。

7.根据权利要求1所述的方法,包括用于在第一用户(13_1)与第二用户(13_2)之间交换数据的相继步骤,其中

-所述第一用户(13_1)配有包括第一硬件密钥(7_1)的第一通信设备(1_1),以及

-所述第二用户(13_2)配有包括第二硬件密钥(7_2)的第二通信设备(1_2),

所述第一用户和所述第二用户(13_1、13_2)都是同一社区(23)的成员,所述方法包括以下步骤:

-所述第一用户(13_1)通过所述第一通信设备(1_1)请求(401)访问所述第二用户(13_2)的数据,

-访问提供者(2)的所述服务器(8)向所述第二通信设备(1_2)请求访问所述第二用户(13_2)的所述数据,

-所述第二通信设备(1_2)将所述数据传输(403)至所述访问提供者(2)的所述服务器(8),其中所述数据至少部分利用所述第二硬件密钥(7_2)进行加密,

-所述访问提供者(2)的所述服务器(8)利用所述第二硬件密钥(7_2)将所述数据解密,利用所述第一硬件密钥(7_1)将所述数据重加密并将所述数据传输至所述第一通信设备(1_1),以及

-所述第一通信设备(1_1)利用所述第一硬件密钥(7_1)将所述数据解密,从而允许所述第一用户(13_1)访问所述数据。

8.根据权利要求1所述的方法,其中,所述服务提供者(2)的所述服务器(8)与所述用户-同一社区的成员之间的数据交换包括这样的步骤,根据该步骤,为所述社区的所述用户的至少一部分所共用的多用户密钥(32)用于加密被交换的所述数据。

9.根据权利要求8所述的方法，其中，从所述服务提供者(2)的所述服务器(8)向所述用户-同一社区的成员发送对所述用户相同的数据包括这样的步骤，根据该步骤：

所述服务提供者(2)的所述服务器(8)仅向所述通信网络发送一次利用所述多用户密钥(32)加密的所述数据，其中所述通信网络将所述数据发回至所述用户的所述通信设备。

10.根据权利要求1所述的方法，其中，

所述服务提供者(2)的所述服务器(8)向希望在彼此之间交换数据的用户的至少两个所述通信设备发送加密密钥(31)，以及

所述通信设备通过所述通信网络(3)在彼此之间直接交换数据，并且所述数据不通过所述服务提供者的所述服务器(8)，其中所述数据利用所述加密密钥(31)进行加密。

11.通信设备(1)，其特征在于，包括：

-用于访问通信网络(3)并通过所述通信网络(3)与服务提供者(2)的服务器(8)交换数据的装置(29)，

-用于与用户(13)进行交互的界面(30)，以及

-硬件密钥(7)，对所述服务提供者(2)已知并实际地存储在所述通信设备(1)的电子芯片(6)的只读存储器中，

所述通信设备配置成用于在与所述服务提供者(2)相连接的情况下执行根据权利要求1至10中任一项所述的方法的步骤。

12.通信系统(37)，配置成用于通过通信网络(3)在服务提供者(2)的服务器(8)与通信设备(1)之间安全地交换数据(5)，其特征在于，包括：

-所述服务提供者(2)的至少一个所述服务器(8)，

-至少一个所述通信设备(1)，其包括：

○用于访问通信网络(3)并通过所述通信网络(3)与所述服务提供者(2)的所述服务器(8)交换数据的装置(29)，

○界面(30)，用于与至少一个用户(13)进行交互，以及

○硬件密钥(7)，对所述服务提供者(2)已知并实际地存储在所述通信设备(1)的电子芯片(6)的只读存储器(9)中，

所述通信设备配置成用于根据权利要求1至10中任一项所述的方法通过所述通信网络(3)与所述服务提供者(2)的所述服务器(8)交换数据，并允许所述通信设备(1)的所述用户(13)使用由所述服务提供者(2)提供的服务(4)。

安全数据交换方法及实施该方法的通信设备和系统

技术领域

[0001] 本发明涉及用于通过通信网络在服务提供者与通信设备之间安全地交换数据的方法，以及用户社区的创建和管理。

背景技术

[0002] 已知用户访问由服务提供者提供的服务，例如游戏、视频或信息共享。服务提供者通常是向其订购者提供具体内容或服务的提供者或电信运营商。

[0003] 为此，用户具有允许其通过通信网络(尤其是互联网类型的网络)访问由服务提供者提供的服务的通信设备，例如数字解码器。

[0004] 通常，同一通信设备由多个用户使用，例如包括多个人的家庭的情况。

[0005] 通信设备与服务提供者之间的交换应被保护，以避免第三方访问用户的私人信息。为此，存在用于数据安全交换的协议，如SSL(安全套接层)和HTTPS(超文本传输协议安全)证书。

[0006] 然而，现有的安全交换方法可被第三方转移，第三方例如可向用户提供假的SSL证书。

[0007] 具体地，这些交换对来自所谓中间人的攻击敏感，该所谓中间人涉及成功拦截通信设备与服务提供者之间通信的第三方，尤其是通过伪装成中继装置或路由器。

[0008] 而且，如上文所强调，很多时候，同一通信设备由多个用户使用。服务提供者希望能够区分同一通信设备的用户，以提供适合的、定制的服务。

[0009] 另外，每个用户都希望能够在其他用户不能访问他/她的数据的情况下使用诸如社交网络或电子邮件账号的服务。

[0010] 最后，服务提供者希望给予每个用户创建或连接至用户社区的可能性，以促进交换并使提供给用户的服务多样化。

[0011] 然而，至今尚无任何解决方案满足这些需求，尤其是在安全性、易用性和效率方面。

发明内容

[0012] 在实施方式中，提出了用于通过通信网络在服务提供者的服务器与通信设备之间安全地交换数据的方法，该方法的特征在于在服务提供者的至少一个服务器与通信设备之间交换的数据允许创建和访问社区，其中该社区将多个用户和特定服务分组，其特征在于，数据的交换包括以下步骤：

[0013] -关联一个或多个用户的非对称公开密钥与由该一个或多个用户请求的至少一个社区，通信设备的多个用户中每个都具有对其特定的非对称公开密钥，

[0014] -通过识别每个用户的非对称公开密钥，允许用户访问社区的服务和/或与社区的其他用户交换，以及

[0015] -通过硬件密钥加密发送的数据的至少一部分，并在接收数据时通过所述硬件密

钥将接收的数据解密，保护用户与社区之间和/或同一社区的用户之间的数据交换，其中，硬件密钥对服务提供者是已知的，并且实际地写入每个用户的通信设备的电子芯片的只读存储器中。

[0016] 在实施方式中，交换的数据包括以下信息中至少之一：

[0017] -独特识别符，对通信设备是特定的，并允许服务提供者识别通信设备，服务提供者的服务器利用独特识别符寻找与通信设备相关联硬件密钥，

[0018] -服务识别符，对于由用户通过通信设备请求的每个服务是特定的，并允许服务提供者的服务器识别由用户通过通信设备请求的服务，

[0019] -与索引相关的信息，索引用于选择在所述通信网络上传输的密钥，

[0020] -服务提供者的服务器与通信设备之间的安全通信协议。

[0021] 在实施方式中，在服务提供者的服务器与通信设备之间交换的数据包括至少一个第一级密钥，第一级密钥自身利用至少一个第二级密钥加密，该连续加密实现至第n级密钥，其中，n是大于等于2的整数，第一级密钥利用硬件密钥被加密。

[0022] 在实施方式中，每个用户都在通信设备处注册，并且被分配给对其特定的非对称公开密钥以及对其特定的非对称私人密钥。在服务提供者服务器与通信设备之间交换的数据包括对用户特定的非对称公开密钥，该非对称公开密钥利用硬件密钥进行加密或没有利用硬件密钥进行加密，非对称公开密钥允许识别用户，和/或识别与该用户相关联的服务提供者的服务。

[0023] 在实施方式中，用户可请求访问由访问提供者管理的公共社区。该访问通过由用户的非对称公开密钥的服务提供者的服务器与公共社区的关联来实现。另外，用户可请求访问由其他用户管理的私人社区。该访问在其他用户同意后通过用户的非对称公开密钥的服务提供者的服务器与私人社区的关联来实现。

[0024] 在实施方式中，服务提供者的服务器与用户-同一社区的成员之间的数据交换包括这样的步骤，根据该步骤，为社区的用户的至少一部分所共用的多用户密钥用于加密交换的数据。

[0025] 具体地，根据一方面，从服务提供者的服务器向同一社区的用户成员的发送对用户相同的数据包括这样的步骤，根据该步骤，服务提供者的服务器仅向通信网络发送一次利用多用户密钥加密的数据，其中通信网络将这些数据发回至每个用户-同一社区的成员。

[0026] 在实施方式中，服务提供者的服务器向希望在彼此之间交换数据的用户的至少两个通信设备发送加密密钥，并且通信设备通过通信网络在彼此之间直接交换数据，并且数据不通过服务提供者的服务器，其中该数据利用加密密钥被加密。

[0027] 通信设备与服务提供者之间的交换受益于提高的安全性。具体地，来自第三方的、包括将其自身插入通信设备与服务提供者之间的攻击不再可能。

[0028] 该提高的安全性并没有改变用于使用通信设备的界面，其中该界面配置成对用户保持简单直观。

[0029] 此外，使同一通信设备的每个用户的识别和服务定制成为可能。

[0030] 服务提供者可通过具有高附加值的安全服务。因此，能够以高效且安全的方式实现提供一种或几种服务、创建和管理用户的社区。另外，不同通信设备的不同用户之间的通信也具有提高了的安全性和更高的效率。

[0031] 如果有必要，可在不改变服务提供者的带宽的情况下提高服务的质量和保护服务。

附图说明

[0032] 参照附图，通过阅读以下描述，本发明的其他特征和优点将变得显而易见，并且以下描述完全是说明性且非限制性的，在附图中：

[0033] 图1是包括通过通信网络与服务提供者的服务器交换数据的通信设备的通信系统的实施方式的示意图；

[0034] 图2是通信设备的实施方式的示意图；

[0035] 图3是连续密钥加密的示意图；

[0036] 图4是用于用户在通信设备注册的实施方式的示意图；

[0037] 图5是在服务提供者的服务器与通信设备之间交换的数据的格式(帧)的示意图；

[0038] 图6是用户访问公共社区的实施方式的示意图；

[0039] 图7是用户访问私人社区的实施方式的示意图；

[0040] 图8是同一社区的用户之间的交换的实施方式的示意图；

[0041] 图9是用户之间的交换以及服务提供者与用户之间的交换的实施方式的示意图。

具体实施方式

[0042] 通信系统的元件的描述

[0043] 图1示出了通信系统37，其配置成用于通过通信网络3在服务提供者2的至少一个服务器8与通信设备1之间安全地交换数据5。

[0044] 通信网络3例如是(但以非限制性方式)IP(互联网协议)网络类型的Internet网络或3G类型的电话网络或本地网络。

[0045] 服务提供者2是能够向用户提供服务的运营商。服务尤其指服务提供者2可通过用户的通信设备1向用户提供的用于用户之间交换的系统(社交网络、视频交换、电子邮件……)或任何内容(音乐、电影、游戏、Internet访问……)。

[0046] 例如，这是电信运营商，用户向其订购以能够访问通信网络，该运营商还向其订购者提供另外的服务。

[0047] 可替代地，这是专门向用户提供服务的服务运营商。

[0048] 服务提供者2通常包括至少一个服务器8，其能够例如通过物理连接(ADSL或光纤)或天线(例如在移动运营商类型的提供者2的情况下)连接至通信网络3。

[0049] 如果有必要，服务提供者2包括允许与通信网络3连接的一系列天线或多个物理连接(线缆、光纤等)。

[0050] 通常，服务提供者2包括多个服务器。

[0051] 服务器管理8管理通过通信网络3与通信设备1进行的数据交换。服务器8包括多个处理单元或计算机、受控程序、存储器以及用户界面(如果必要)。

[0052] 服务提供者的结构是标准的，并且主要取决于与通信网络的连接类型(例如：ADSL、3G运营商或该类型的其他标准-1G、2G、……4G的运营商、Wi-Fi、光纤、本地网络等)。

[0053] 如图2示意性示出，通信设备1包括用于访问通信网络3以通过该网络3与服务提供

者2的服务器8交换数据的装置29。

[0054] 访问装置29例如是无线电发送与接收装置或Wi-Fi装置，或是天线型装置或有线通信装置或允许与通信网络3连接的任何其他技术装置。

[0055] 通信设备1位于用户侧。例如，通信设备1位于用户的工作场所或家中。可替代地，通信设备1是用户可随身携带的移动设备，例如移动电话设备。

[0056] 设备1还包括界面30，允许其与用户进行交互。界面30通常是软件界面，该软件界面在与设备1连接的屏幕上显示允许用户控制设备1的选择和指示。可替代地，设备1自身包括屏幕，并且界面30包括与屏幕相关联的上述软件界面。

[0057] 以标准的方式，通信设备1包括电力供应装置33(电池、电源插座等)以及管理设备1的不同功能的至少一个处理器34。

[0058] 通常，通信设备1还包括硬盘型或可移动存储器型的存储器35，其允许存储被接收或交换的数据。

[0059] 如图2所示，设备1包括硬件密钥7，其被实际地写入通信设备1的电子芯片6的只读存储器9中。

[0060] 只读存储器9是存储器，其内容在包括该存储器的芯片6的制造过程中实际地永久地写入。因此，其内容在制造过程中被限定，并且无法修改。因此，硬件密钥7在通信设备1的制造过程中生成。

[0061] 电子芯片是指可包括只读存储器的任何电子组件。

[0062] 硬件密钥7是加密密钥，并允许设备1将数据加密或解密。

[0063] 硬件密钥7物理地写入通信设备1的电子芯片6的只读存储器中。硬件密钥7是有点复杂的比特集，该比特集通过只读存储器9的物理部件(晶体管等)产生。

[0064] 密钥7不能由例如软件从外部查看。事实上，只读存储器9嵌入在电子芯片6中，以防止第三方从外部查看其内容。

[0065] 因此，鉴于制造者实际上限定并制造硬件密钥7，只有芯片6的制造者知道该硬件密钥7。

[0066] 在服务提供者2购买通信设备1时，芯片的制造者将该硬件密钥7传给服务提供者2，以使得服务提供者2可如下文描述的那样使用该硬件密钥7。当然，服务提供者2可自己制造电子芯片6。

[0067] 在非限制性的实施方式中，这是128比特或更多(例如192比特、256比特)的AES(高级加密标准，其为对称加密算法)密钥。根据安全需求(56比特的DES密钥(数据加密标准)，三重64比特DES密钥等)，可使用在其他加密算法中使用的其他密钥。这些密钥类型不是限制。

[0068] 在实施方式中，该硬件密钥7对每个设备1都是唯一的。

[0069] 通信系统中的安全交换

[0070] 在实施方式中，提出了用于在通信系统37中通过通信网络3在服务提供者2的服务器8与通信设备1之间安全地交换数据的方法，通信设备1允许通信设备1的至少一个用户13使用由服务提供者2提供的服务。

[0071] 因此，通过通信网络3在服务提供者2的服务器8与通信设备1之间进行的数据5的交换包括用于发送数据的步骤，该步骤包括通过硬件密钥7加密被发送数据5的至少一部

分，其中该硬件密钥7对服务提供者2已知且实际地写入通信设备1的电子芯片6的只读存储器中。

[0072] 因此，在通信设备1侧，通信设备1将待发送的数据发送至包括硬件密钥7的电子芯片6，电子芯片6发回被加密的数据。然后，通信设备1通过其装置29将被加密的数据发送至通信网络3，其中该装置29用于访问通信网络3。

[0073] 对于服务提供者2的服务器8，情况也是如此。服务器8具有硬件密钥7，并因此可例如通过处理器或电子芯片使用该密钥7将数据加密。

[0074] 在实施方式中，服务提供者2具有包括该密钥7的芯片，其中该密钥7存储在该芯片的只读存储器中。

[0075] 另外或可替代地，服务提供者2的服务器8存储包括该密钥的软件数据库，其中在该软件数据库中，该密钥由组成比特表示。

[0076] 鉴于硬件密钥7并不在通信网络3上交换，并且仅对服务提供者2已知，所以数据交换被保护，并且没有由第三方拦截的任何风险。在设备1侧，该密钥7不能从芯片6的只读存储器9提取，并且甚至对实际用户也不是已知的。

[0077] 因此，服务提供者2的服务器8与通信设备1之间的交换受到保护。

[0078] 在接收数据5时，接收的数据通过该硬件密钥7被解密。

[0079] 在通信设备1侧，通信设备1将待解密的数据发送至包括硬件密钥7的电子芯片6，其中电子芯片6将被解密的数据发回至通信设备1。在服务提供者2的服务器8侧，情况同样如此，服务器8使用硬件密钥7和处理器将数据解密。

[0080] 在随后详细描述的示例性实施方式中，在服务提供者2的服务器8与通信设备1之间交换的数据允许创建和访问社区，其中社区将多个用户和特定服务分组，并且对社区的访问允许使用这些服务和/或与社区其他用户的数据交换。

[0081] 因此，这些社区的创建以及对这些社区的访问通过刚描述的安全交换来保护。

[0082] 在通信系统中被交换的数据的示例

[0083] 各种类型的数据可在服务提供者2的服务器8与通信设备1之间进行交换。

[0084] 在这种交换中，例如银行交易，必须通过通信网络3传输加密密钥。

[0085] 在本发明的实施方式中，使用了用于密钥的连续加密的机制。

[0086] 图3中示出了该实施方式。

[0087] 在该实施方式中，在通信设备1与服务提供者2之间交换的数据5包括至少一个第一级密钥K_1，该第一级密钥K_1自身由至少一个第二级密钥K_2加密，该连续加密实现至第n级的一个或多个密钥K_n，其中n是大于等于2的整数，第一级密钥K_1由硬件密钥进行加密。

[0088] 密钥K_1、……、K_n是由专用算法或软件生成的软件密钥，即随机比特序列。

[0089] 第一级密钥K_1允许将整体第2级密钥K_2解密，第2级密钥K_2自身允许将整个第3级密钥K_3解密，依次类推。

[0090] 该连续加密机制加强了安全性。因此，如果服务提供者2的服务器8决定在网络上传输第n级密钥K_n，则第三方将必须找到密钥K_1至K_{n-1}，以能够获得被交换的密钥K_n。

[0091] 现在，为了找到密钥K_1，必须找到允许将密钥K_1解密的硬件密钥7。但是，如上所述，硬件密钥7物理地且永久地放置在设备1的芯片6中，并且任何第三方都不能够访问。

[0092] 因此保证了交换的安全性。

[0093] 服务提供者2可选择与每个级相对应的密钥的数目。

[0094] 在示例性实施方式中，服务提供者2设置了64个第1级密钥，每个第1级密钥允许破译16个第2级密钥，这样给出共1024个第2级密钥(密钥1、第2密钥、……、第1024密钥)。

[0095] 如果由服务提供者2向通信设备1的用户提供的服务是银行应用，则服务提供者2的服务器8例如可控制服务并将服务编程，以使得其从第1009密钥至第1024密钥中随机选择一个密钥。

[0096] 在实施方式中，服务提供者2将服务编程，以使得其随机选择数字，0到15之间的所谓索引。服务提供者2还将服务编程，以使得每个索引都与第1009密钥至第1024密钥中的密钥相关联。因此，通过索引的随机抽取来完成密钥的选择，索引自身与密钥相关联。索引的选择和随机抽取仅对服务提供者2是已知的。

[0097] 用户和通信设备的记录和识别

[0098] 在实施方式中，服务提供者2希望能够知道通信设备1的用户的身份。这具有多个优点，如定制为用户提供的服务、跟踪其配置以及其消费的跟踪、保护其数据以防其他用户等。

[0099] 因此，根据实施方式，执行用户13在通信设备1处的注册，该注册的结果通过通信网络3传至服务提供者2的服务器8。

[0100] 这在图4中示出，其中用户13在通信设备1处注册(步骤101)，通信设备1生成：

[0101] -至少一个非对称公开密钥11，其对用户13是特定的(步骤104)，并被发送至服务提供者2的服务器8(步骤105)；以及

[0102] -非对称私人密钥，其对用户13是特定的(步骤101)，并存储在通信设备1中(步骤103)。

[0103] 在没有来自用户的任何干扰的情况下，通信设备1决定密钥类型、密钥长度、密钥有效性的持续时间。如果必要，设备1限定秘密句子，该秘密句子随机地取自句子词典并与私人密钥存储在通信设备1的安全区中。该秘密句子例如使用在创建非对称密钥的过程中，并用作助记提醒。

[0104] 因此，服务提供者2的服务器8可通过对用户13特定的非对称公开密钥来识别用户13。

[0105] 事实上，在实施方式中，当用户使用通信设备1时，在服务提供者的服务器8与通信设备1之间交换的数据5包括对用户13的特定非对称公开密钥，其中该非对称公开密钥允许识别用户13，和/或与该用户13相关联的服务。

[0106] 在实施方式中，在通信设备1与服务提供者2的交换过程中传输的用户非对称公开密钥由硬件密钥7加密。然而这不是强制性的。

[0107] 用户13在通信设备1处的注册通常通过与通信设备1的界面30的交互来执行。

[0108] 在示例性实施方式中，界面30向用户请求识别符和密码的限定，以注册该用户。如果必要，界面30向用户请求强制性信息(名字、姓、电子邮件)和可选信息(注释、别名等)。

[0109] 一旦这些步骤已执行，就执行用于生成特定于用户的密钥的过程。

[0110] 在实施方式中，为了避免通信设备1的用户试图欺骗性地识别其自己而不是该设备1的另一用户，制定了以下规定：错误输入多个(例如三个)密码导致限制使用通信设备1。该限制使用只可由访问提供者2移除。

[0111] 在实施方式中，在服务提供者2的服务器8与通信设备1之间交换的数据5包括特定于通信设备1的独特识别符15，从而允许服务提供者2的服务器8识别通信设备1。

[0112] 使用这种识别符15的优点为服务提供者2的服务器8可迅速识别向其发送数据的通信设备1，并且因此可更迅速地选择与该通信设备1相对应的硬件密钥7。识别符15例如是数字和/或字母序列。

[0113] 在实施方式中，在服务提供者2的服务器8与通信设备1之间交换的数据5包括服务识别符16，服务识别符16特定于由用户通过通信设备1请求的每个服务，并允许服务提供者2识别由用户通过通信设备1请求的服务。

[0114] 利用识别符16，服务提供者2的服务器8可以更短的响应时间代表用户应答访问服务的请求。

[0115] 另外，在通信设备1侧，该识别符16允许加速数据处理。

[0116] 在实施方式中，在服务提供者2的服务器8与通信设备1之间交换的数据5包括与索引17相关的信息，其中索引17用于选择在通信网络3上传输的密钥。在一个实施方式中，该索引可为密钥的编号。

[0117] 在另一实施方式中，索引给予在预定的表中指示实际用于加密/解密的密钥的可能性。例如，在具有N个输入的表的情况下，对密钥的访问可通过预定的计算给出并仅对运营商已知。计算的示例为：表的密钥索引＝(预定数+索引)，以表的大小N为模

[0118] 此外，该索引给予从服务提供者2侧和通信设备1侧更迅速地处理交换的数据的可能性。

[0119] 在实施方式中，交换的数据包括在通信设备1与服务提供者2之间被保护的通信协议18。例如这是HTTPS(超文本传输协议安全)或VPN(虚拟私人网络)类型的协议。

[0120] 根据服务提供者的选择，这些不同的实施方式可进行组合或不进行组合。

[0121] 数据帧

[0122] 在实施方式中，交换的数据5遵守具体帧格式。

[0123] 在图5中，具体帧类型用于传输数据。

[0124] 帧包括被保护的通信协议18、特定于通信设备1的独特识别符15、服务识别符16、与索引17相关的信息，其中服务识别符16对由用户通过通信设备1请求的每个服务是特定的，索引17用于选择在通信网络3上传输的密钥。帧可包括其他信息或仅包括该信息的一部分。

[0125] 帧还包括对用户特定的一个或多个非对称公开密钥，如上所述，该非对称公开密钥可选地利用硬件密钥7加密。

[0126] 帧还包括在通信设备1与服务提供者2之间交换的内容22。这些内容利用硬件密钥7进行加密。这些内容与和用户使用的服务相关的有用信息(文本、视频等)相对应。

[0127] 可替代地，内容22通过上文所述的连续加密机制加密。然后，如上所述，内容22采用包括最后的硬件密钥的多个加密密钥连续地加密。

[0128] 通过将数据交换并入具体帧，设备1和/或服务提供者2的服务器8可只接受遵守该帧的交换，这样避免了来自第三方的、包括大量发送数据块(名为“arp欺骗”的技术)的攻击，此外，这样便于数据处理以及加速交换。

[0129] 创建和管理用户社区

[0130] 在实施方式中，在服务提供者2的服务器8与通信设备1之间数据5的交换涉及社区的创建、管理以及对这些社区的访问。因此，根据需要，数据交换的不同实施方式在这里作为组合或单独地应用。

[0131] 社区将多个用户和特定服务分组。对社区的访问允许使用特定服务和/或与社区的其他用户的数据交换。

[0132] 用于创建社区的参数(社区类型、成员数量、用户名、访问权限、某些数据等)存储在服务提供者2的服务器8侧。

[0133] 通过上述数据交换的不同实施方式，社区的创建、管理以及对这些社区的访问被保护。

[0134] 例如，可创建钓鱼业余爱好者的社区。因此，该社区的用户、成员可在彼此之间交换与钓鱼相关的内容或照片。用户还可以在例如专用于钓鱼的讨论论坛上彼此交谈。因此，与该社区相关的服务包括讨论论坛、访问钓鱼比赛、在线购买设备、接受促销优惠券等。

[0135] 服务类型以及用户之间的交流的类型可根据需要进行调整。

[0136] 在实施方式中，在公共社区21与私人社区20之间进行区分(参照图1)。

[0137] 公共社区21由服务提供者2管理，而私人社区20由一个或多个用户来管理。具体地，在公共社区的情况下，服务提供者2通过服务器8决定其他用户是否可加入公共社区，而在私人社区的情况下，由私人社区的负责用户来做出该决定。

[0138] 即使社区是公共的，服务提供者也可决定对该社区的访问为付费访问。

[0139] 另外，在公共社区21中提供的服务可以是免费的、不免费的，或可为付费服务和免费服务的混合。

[0140] 还可创建具有中间状态的社区，由用户和服务提供者二者来管理，授权其他用户的访问需要用户和服务提供者的同意。

[0141] 参照图1和图6描述了来自用户13对公共社区21的访问请求的实施方式。

[0142] 用户13通过通信设备1请求访问公共社区21，其中该公共社区21提供至少一个服务和/或社区用户之间数据交换(步骤201)。

[0143] 该请求可通过通信设备1的界面30执行，例如通过在界面30中选择社区21。

[0144] 该公共社区21由服务提供者2管理，服务提供者2决定与该社区相关联的服务以及用户的访问权。

[0145] 如上所述，已在通信设备1处注册的每个用户13都具有对其特定的非对称公开密钥11。

[0146] 因此，通信设备1将特定于用户13的非对称公开密钥11发送至服务提供者2的服务器8(步骤202)。该密钥11可选地利用设备1的硬件密钥7进行加密。

[0147] 然后，服务提供者2的服务器8将用户请求的公共社区21与用户的非对称公开密钥11关联(步骤203)，从而允许用户使用由该社区21提供的一个或多个服务。

[0148] 该关联包括将用户的密钥11的副本存储在服务器8中以及将用户的密钥11的副本并入社区21的参数中，其中该参数存储在服务器8中。

[0149] 访问公共社区21不需要其他用户的批准。

[0150] 随后，当用户希望访问社区的服务时，提供者的服务器8在数据交换过程中识别其非对称密钥，并且确定用户具有与社区相关联的非对称密钥。

[0151] 与社区的不同数据交换根据上述一个或多个不同的实施方式实现(利用硬件密钥加密和/或使用数据帧等)。

[0152] 作为示例,这是与徒步旅行业余爱好者有关的社区21。该社区的服务例如为提供徒步旅行地图、在徒步旅行业余爱好者之间建立关系等。

[0153] 参照图1和图7描述了来自用户13的、用于访问公共社区21的请求的实施方式。

[0154] 第一用户13_1通过通信设备1请求(步骤301)访问私人社区20,该私人社区20提供至少一个服务和/或社区用户之间数据交换,并且该私人社区由第二用户13_2管理。

[0155] 第一用户13_1的请求通过服务提供者2的服务器8发送(步骤302)至第二用户13_2的通信设备。

[0156] 第二用户13_2通过其通信设备1发出接受决定或拒绝决定(步骤303),该接受决定或拒绝决定被发送至服务提供者2的服务器8。

[0157] 根据第二用户13_2的决定,第一用户13_1被授权访问私人社区20,接受决定导致第二用户13_2的非对称公开密钥11与私人社区20之间的关联。

[0158] 该关联包括将用户13_1的密钥11的副本存储在服务器8中以及将用户13_1的密钥11的副本并入社区20的参数中。

[0159] 因此,当第一用户13_1希望使用私人社区20的服务和/或与其他用户的数据交换时,服务提供者2识别其密钥11,并授权其访问这些服务。

[0160] 由第二用户13_2进行的接受机制可采取不同的形式。

[0161] 在实施方式中,第二用户132接收告诉其第一用户13_1希望加入其私人社区20的消息。该消息可以是标准的或定制的信息,并由第一用户13_1自身亲自所写。该信息通过第二用户13_2的通信设备1的界面显示。

[0162] 然后,第二用户13_2可通过其界面30发出接受决定或拒绝决定。

[0163] 参照图8描述了用于在同一公共社区或私人社区的用户之间交换数据的实施方式。

[0164] 该交换基于通信设备与服务提供者之间数据交换的上述不同实施方式。

[0165] 如图8所示,第一用户13_1配有包括第一硬件密钥7_1的第一通信设备1_1。

[0166] 第二用户13_2配有包括第二硬件密钥7_2的第二通信设备1_2。

[0167] 用户13_1和用户13_2都是同一社区23(公共或私有)的成员。因此,如上所述,第一用户13_1的非对称公开密钥11_1和第二用户13_2的非对称公开密钥11_2与社区23相关联。

[0168] 第一用户13_1请求访问第二用户13_2的数据(步骤401)。

[0169] 访问提供者2的服务器8向第二通信设备1_2请求访问第二用户13_2的数据(步骤402)。

[0170] 第二通信设备1_2将至少部分采用第二硬件密钥7_2加密的这些数据发送至访问提供者2的服务器8(步骤403)。用于交换数据的不同的实施方式以及该加密在上文进行了讨论。

[0171] 访问提供者2的服务器8通过第二硬件密钥7_2将这些数据解密,用第一硬件密钥7_1对其重加密并将其传输至第一通信设备1_1(步骤404)。

[0172] 第一通信设备1_1然后利用第一硬件密钥7_1将数据解密。

[0173] 因此,交换被保护。在实施方式中,交换的数据部分或全部遵守图5中所示的帧。

[0174] 在实施方式中,服务提供者2的服务器8与用户即同一社区的成员之间的数据交换

包括这样的步骤，根据该步骤，对社区的至少一部分用户共用的多用户密钥32用于将交换的数据加密。

[0175] 在实施方式中，多用户密钥32是包括一连串比特的软件密钥。

[0176] 根据该实施方式的一方面，将数据从服务提供者2的服务器8发送至用户即同一社区的成员包括这样的步骤，根据该步骤，服务提供者2的服务器8向通信网络仅发送一次这些数据，通信网络将这些数据发送回每个用户即同一社区的成员，其中这些数据对用户相同。

[0177] 图9中示意性地示出了这种实施方式的示例。

[0178] 访问提供者2的服务器8将多用户密钥32发送至同一社区的用户的至少一部分。该密钥是加密密钥，并且通常具有时间上受限的有效性，即，仅是临时密钥。根据需要，访问提供者2的服务器8可定期更新多用户密钥32。

[0179] 为了接收多用户密钥32，用户应在访问提供者2处预先注册。注册例如要求将来自用户的通信设备1_1、通信设备1_2的请求发送至服务器8，服务器8作为回报接收多用户密钥32。

[0180] 这些交换根据上述被保护的数据交换的实施方式产生(用硬件密钥加密，并且如果必要，以如上所述的帧的形式发送数据)。注册可以是自动的。例如，用户一旦访问社区，其通信设备就自动接收代表服务提供者2的服务器8的多用户密钥。

[0181] 向通信设备发送多用户密钥32根据上述安全数据交换的实施方式来实现。具体地，多用户密钥32可由服务器8发送至每个通信设备，并且利用每个通信设备的硬件密钥进行加密。可替代地，多用户密钥32可通过采用上述的连续加密机制发送至每个通信设备。

[0182] 随后，服务器8仅向通信网络3发送一次带有多用户密钥32的加密数据，通信网络3将带有多用户密钥32的加密数据发回至用户的通信设备。

[0183] 根据数据的大小，由服务提供者2的服务器8进行多次连续发送可能是必须的，但是由服务提供者向通信网络进行的每次数据发送仅执行一次，并且不对每个用户进行重复。

[0184] 然后，通信网络3负责将数据发送至社区用户的每个通信设备。

[0185] 相关用户的通信设备(本文中1_1和1_2)通过多用户密钥32将数据解密。

[0186] 因此，在较少带通拥塞的情况下实现了从服务提供者的服务器至社区用户的通信设备的数据流的发送。这种由多个用户共用的密钥加密的信息的单次发送给予节省带宽的可能性。

[0187] 实现了对通信网络的单次发送，而不是由服务提供者将相同数据数次发送至多个用户。因此，这是多路广播类型的发送。服务器8不再必须通过为每个用户不同地加密数据来数次发送数据。

[0188] 在实施方式中，服务提供者2的服务器将加密密钥31发送至希望在彼此之间交换数据的用户的至少两个通信设备(例如1_1和1_2，参照图9)。该发送根据上述安全交换的实施方式(用硬件密钥加密、和/或遵守帧、和/或连续加密等)中的一个来实现。

[0189] 加密密钥通常是临时的。根据需要，加密密钥可被更新。

[0190] 然后，通信设备通过通信网络3直接在彼此之间交换数据，其中该数据利用加密密钥31加密。这些交换不再通过服务提供者2的服务器8，而是通过通信网络3直接在相关通信

设备之间实现。

[0191] 这些交换可在多个通信设备之间实现，如在与几个用户进行视频会议过程中实现。

[0192] 因此，这是不再通过服务提供者2的服务器8的点对点通信。

[0193] 服务提供者2可为该点对点通信服务向用户收费，例如根据持续时间和/或通过一次性付款。

[0194] 在示例性实施方式中，交换的数据涉及在IP上的语音类型的通信。

[0195] 因此，用户之间的这些直接交换得到最大的保护并允许更高效的通信。

[0196] 通常，所提出的解决方案允许提高通信设备与服务提供者之间数据交换的安全性。具体地，来自第三方的、包括将其自身插入在通信设备与服务提供者之间的攻击是不再可能。

[0197] 除了使交换更安全之外，同一通信设备的用户的定制和识别也是可能的，从而允许识别通信设备的每个用户以及识别与该用户相关联的服务。

[0198] 尽管本发明提供了增强的安全性和定制，但是用于使用通信设备的、展示给用户的界面仍然简单且直观。

[0199] 因此，服务提供者找到了用于以高效和安全的方式创建和管理社区、提供一个或几个服务的强大工具。而且，不同通信设备的不同用户之间的通信被保护且更高效。

[0200] 最后，在提供了提高的服务水平的质量同时，服务提供者的带宽没有改变。

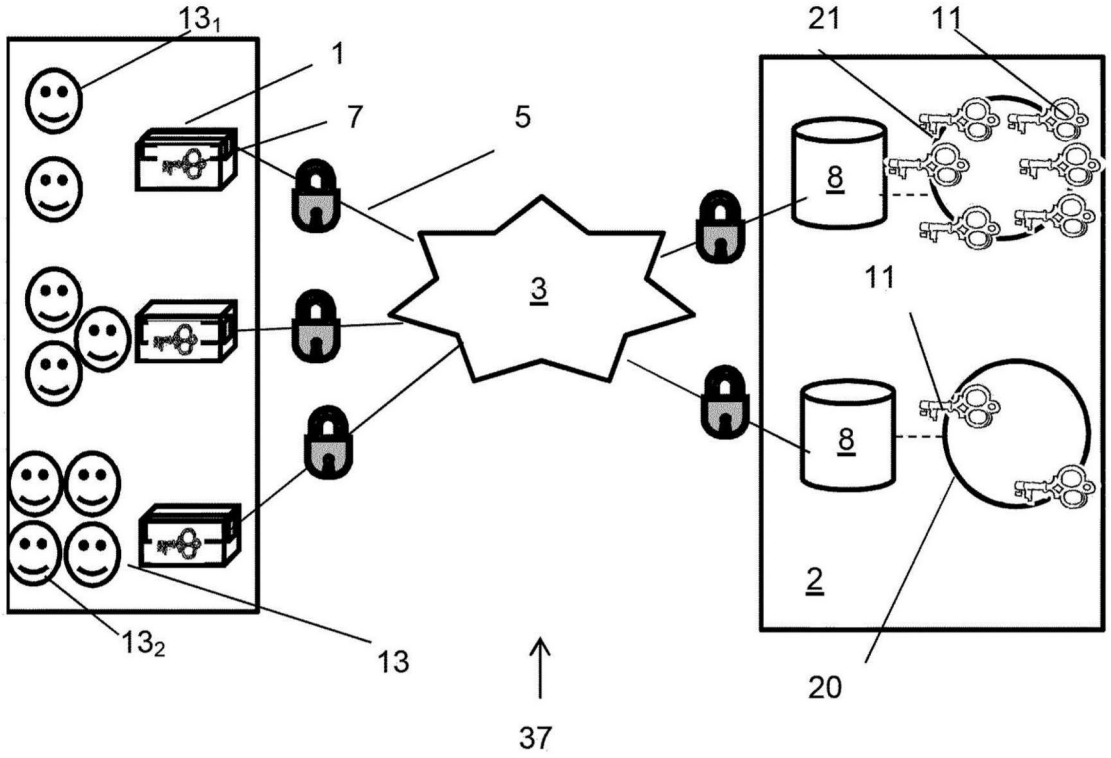


图1

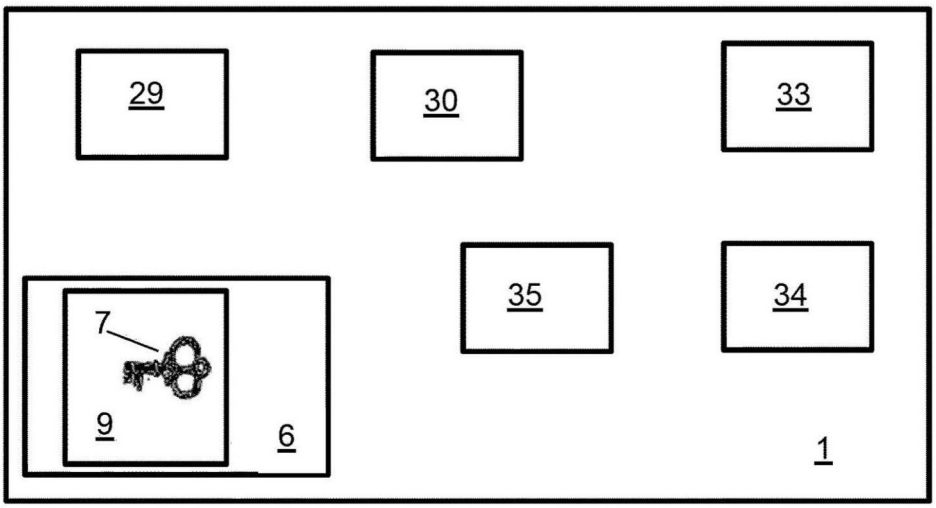


图2

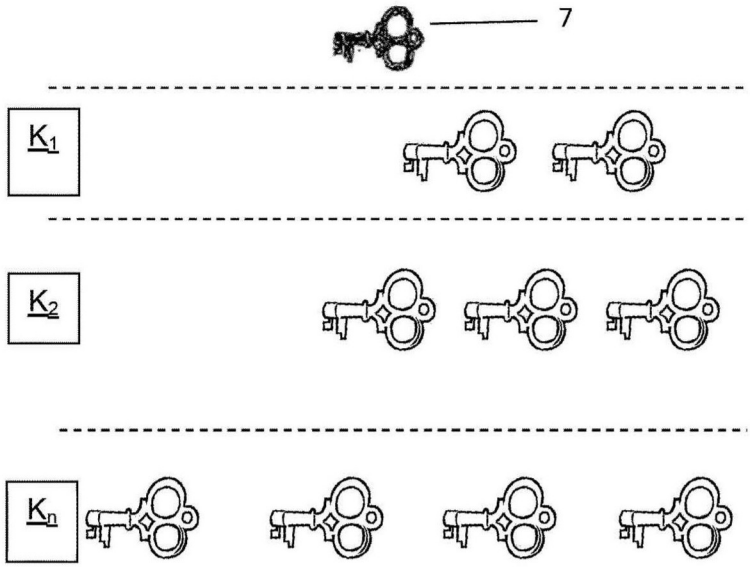

7
K1
K2
Kn

图3

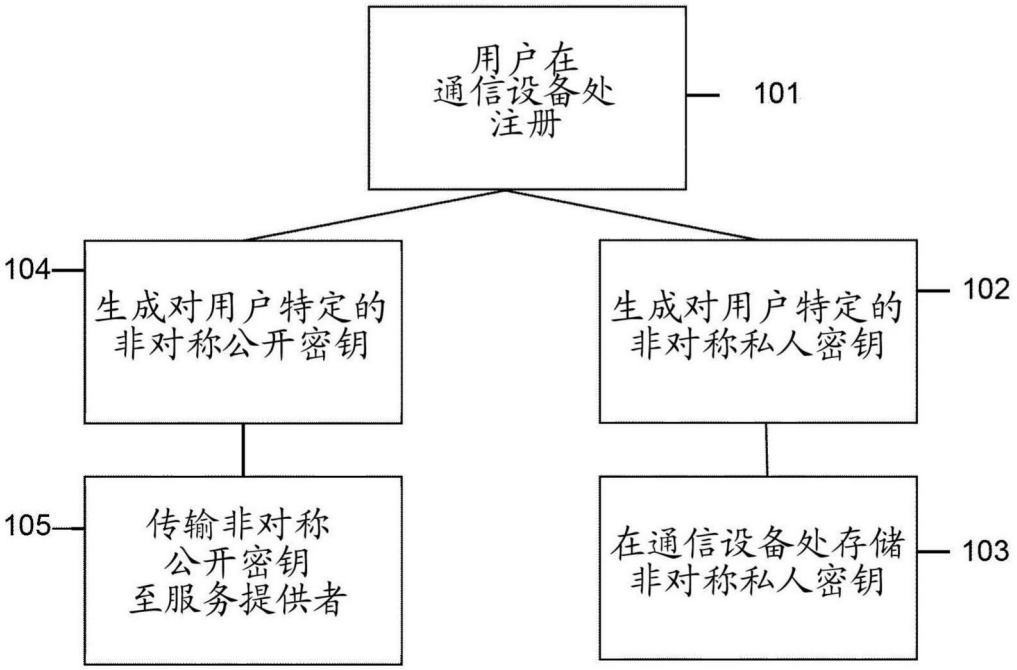

用户在
通信设备处
注册
101
104
生成对用户特定的
非对称公开密钥
生成对用户特定的
非对称私人密钥
102
105
传输非对称
公开密钥
至服务提供者
在通信设备处存储
非对称私人密钥
103

图4

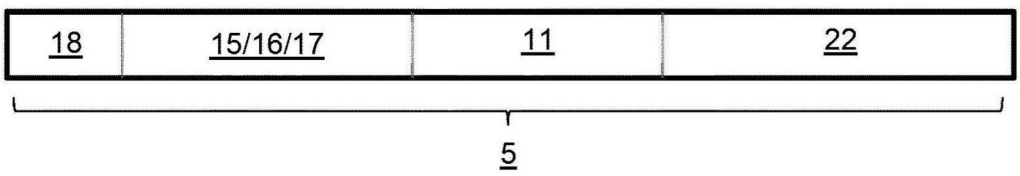

18
15/16/17
11
22
5

图5

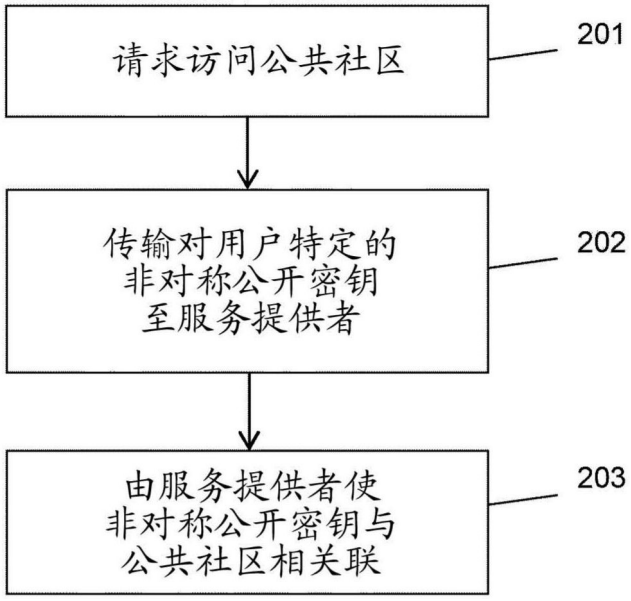

请求访问公共社区
201
传输对用户特定的
非对称公开密钥
至服务提供者
202
由服务提供者使
非对称公开密钥与
公共社区相关联
203

图6

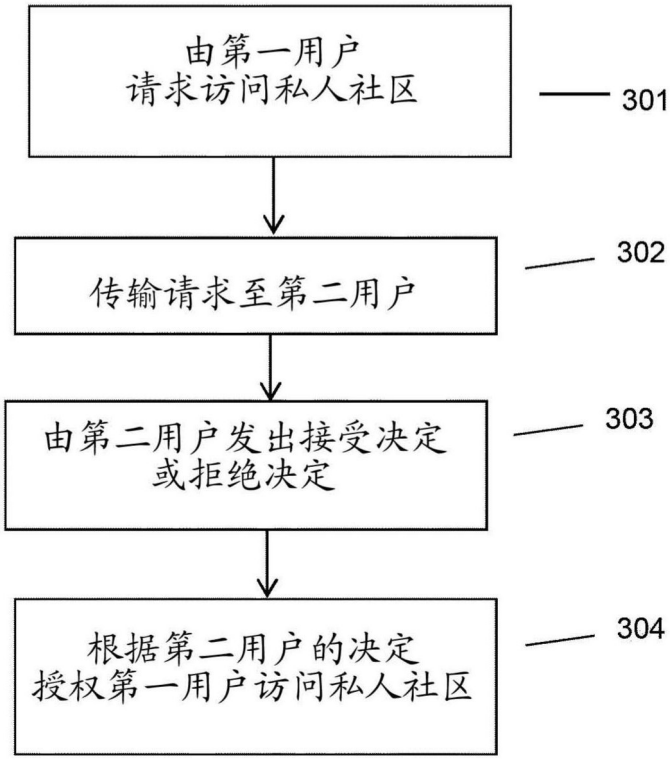

由第一用户
请求访问私人社区
301
传输请求至第二用户
302
由第二用户发出接受决定
或拒绝决定
303
根据第二用户的决定
授权第一用户访问私人社区
304

图7

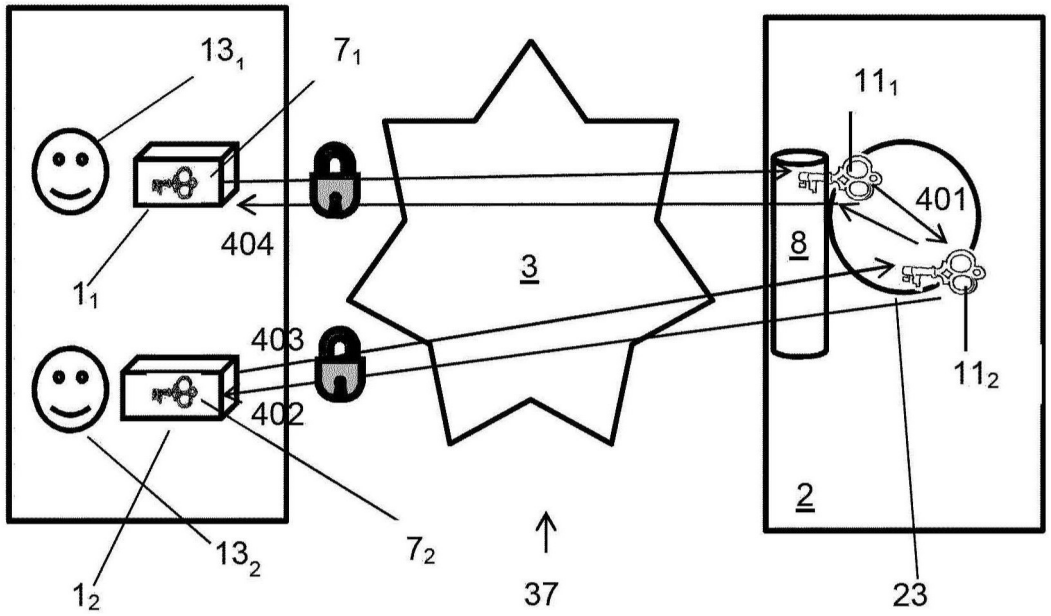

13₁
7₁
11₁
401
404
3
8
1₁
403
11₂
402
2
13₂
7₂
37
1₂
23

图8

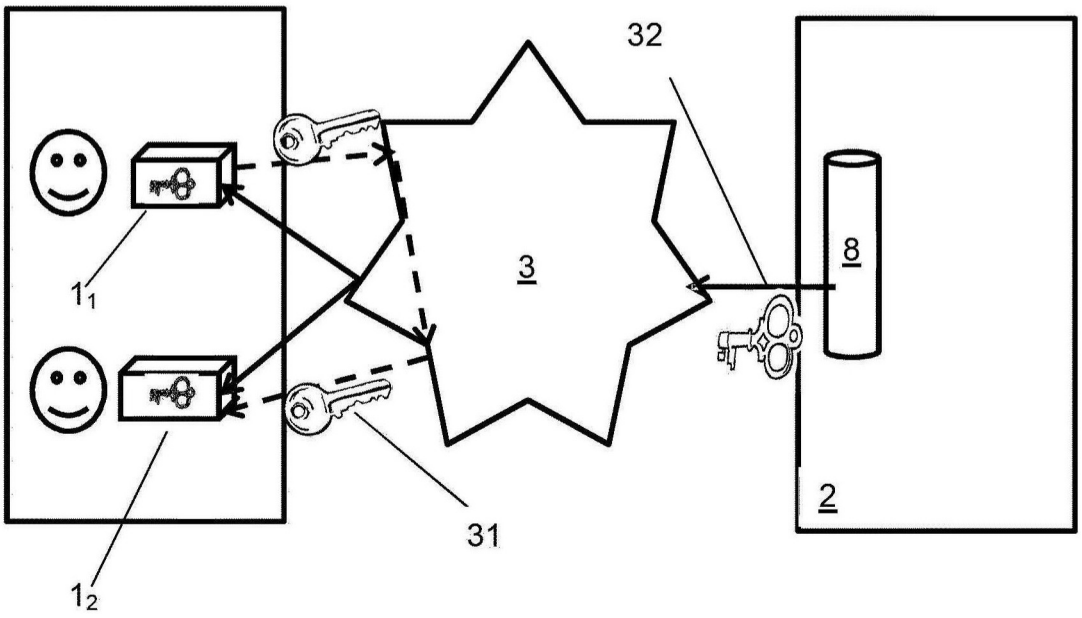

32
8
3
1₁
2
31
1₂

图9