

(12) 发明专利

(10) 授权公告号 CN 101171860 B

(45) 授权公告日 2011. 02. 09

(21) 申请号 200680015595. 1

代理人 杨晓光 李峰

(22) 申请日 2006. 04. 06

(51) Int. Cl.

H04L 29/06 (2006. 01)

(30) 优先权数据

0503469 2005. 04. 07 FR

(56) 对比文件

0510314 2005. 10. 10 FR

US 20010052077 A1, 2001. 12. 13, 全文.

(85) PCT申请进入国家阶段日

CN 1204431 A, 1999. 01. 06, 全文.

2007. 11. 07

US 20040157584 A1, 2004. 08. 12, 说明书第

2, 9-12, 60-62, 78-87, 附图 4.

(86) PCT申请的申请数据

审查员 李刚

PCT/FR2006/050306 2006. 04. 06

(87) PCT申请的公布数据

WO2006/106270 FR 2006. 10. 12

(73) 专利权人 法国电信公司

地址 法国巴黎

(72) 发明人 A · 费拉齐尼 D · 安扎 P · 朔瓦德

(74) 专利代理机构 北京市中咨律师事务所

11247

权利要求书 2 页 说明书 5 页 附图 3 页

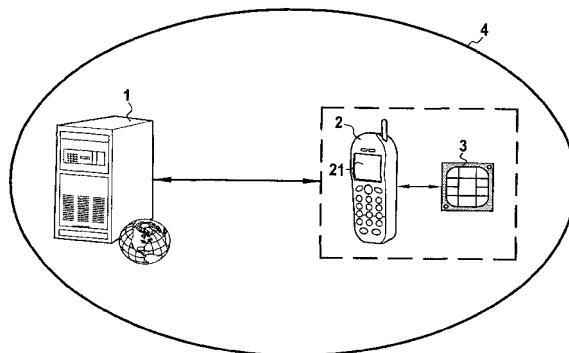
(54) 发明名称

管理接入多媒体内容的安全方法和设备

(57) 摘要

本发明提供了一种管理向配备有安全模块(3)的移动终端(2)发送多媒体内容的方法，所述多媒体内容经由通信网络(4)从广播服务器(1)以加密形式被发送。所述方法包括以下步骤：a) 向移动终端(2)发送多媒体内容的使用权限数据；b) 在移动终端(2)的安全模块(3)中存储使用权限数据；c) 生成加密/解密密钥序列，解密密钥序列是从存储在安全模块(3)中的使用权限数据中生成的；d) 向移动终端(2)发送多媒体内容，所述内容是利用来自自己生成的加密密钥序列中的连续密钥而被加密的；以及e) 移动终端接收多媒体内容并且利用来自在移动终端的安全模块中生成的解密密钥序列中的解密密钥来解密该多媒体内容。

B CN 101171860



CN

1. 一种管理发送多媒体内容到配备有安全模块 (3) 的移动终端 (2) 的方法, 所述多媒体内容经由通信网络 (4) 从广播服务器 (1) 以加密形式被发送, 所述方法包含以下步骤:

- a) 向所述移动终端 (2) 发送所述多媒体内容的使用权限数据;
- b) 将所述使用权限数据存储在所述移动终端 (2) 的安全模块 (3) 中;
- c) 生成加密 / 解密密钥序列, 所述解密密钥序列是从存储在所述安全模块 (3) 中的使用权限数据中生成的;
- d) 发送所述多媒体内容到所述移动终端 (2), 所述内容是利用已生成的加密密钥序列中的连续密钥而被加密的; 以及
- e) 所述移动终端接收所述多媒体内容, 并且利用来自在所述移动终端的安全模块中生成的解密密钥序列中的解密密钥来解密所述多媒体内容,

其特征在于, 所述广播服务器 (1) 利用所述加密密钥序列中一个不同的加密密钥来对多媒体内容中的每个帧加密, 以使得每个帧是以一个不同的加密密钥来标识的, 所述移动终端 (2) 的安全模块 (3) 生成与所述加密密钥序列类似的解密密钥序列,

并且, 在发送所述多媒体内容中断的情况下, 所述方法还包括: 步骤 f), 其中所述移动终端向所述广播服务器发送来自中断发生时所使用的加密密钥的参考数据; 以及步骤 g), 其中根据在步骤 f) 所发送的所述加密密钥来恢复所述多媒体内容的广播。

2. 根据权利要求 1 的方法, 其特征在于, 在步骤 c) 中, 每个加密 / 解密密钥是在与由所述广播服务器 (1) 发送的每个帧所定义的时间间隔相对应的时间内被生成的。

3. 根据权利要求 1 或 2 的方法, 其特征在于, 它还包括步骤 h), 其中在所述移动终端 (2) 中检验所述使用权限的有效性, 所述检验是通过查询存储在所述安全模块中的使用权限数据并且将其与存储在数据库中的使用权限数据相比较来实现的。

4. 根据权利要求 1 到 3 中任一个的方法, 其特征在于, 在步骤 c) 中, 所述解密密钥序列中的密钥是基于基本密钥和密码而被迭代地计算的, 所述密码被预先定义并且在所述移动终端 (2) 和所述广播服务器 (1) 之间被交换。

5. 一种适于包含在移动通信终端 (2) 中的安全模块 (3), 所述终端用于接收以用加密密钥序列被加密的形式而发送的多媒体内容, 所述模块包括用于存储所述多媒体内容的使用权限的装置, 以及用于从所存储的使用权限数据中计算解密密钥序列并且存储它们的装置, 其特征在于, 多媒体内容中的每个帧是利用所述加密密钥序列中一个不同的加密密钥来被加密的, 以使得每个帧是以一个不同的加密密钥来标识的, 并且所述安全模块 (3) 包括用于生成与被用来加密所述多媒体内容的加密密钥序列类似的解密密钥序列的装置和用于发送来自在发送多媒体内容到所述移动终端中断时所使用的加密密钥的参考数据的装置。

6. 一种包括显示装置的移动终端 (2), 其特征在于, 它包括根据权利要求 5 的安全模块。

7. 一种广播服务器, 包括用于经由通信网络 (4) 向配备有安全模块 (3) 的移动终端 (2) 以加密形式发送多媒体内容的装置, 所述服务器包括用于将所发送的多媒体内容的使用权限数据发送给所述移动终端的装置, 其中所述使用权限数据包括用于计算与由所述服务器计算的加密密钥序列相类似的解密密钥序列的数据, 其特征在于, 所述广播服务器包括用于利用所述加密密钥序列中一个不同的加密密钥来对多媒体内容中的每个帧加密以

使得每个帧是以一个不同的加密密钥来标识的装置，并且所述广播服务器适于在广播所述多媒体内容中断的情况下向所述移动终端（2）的安全模块（3）查询中断时所使用的加密密钥。

8. 根据权利要求 7 的服务器，其特征在于，它包括用于存储被发送给所述移动终端的使用权限数据的数据库，以及用于查询存储在所述移动终端的安全模块中的使用权限数据并将其与存储在所述数据库中使用权限数据相比较的装置。

9. 一种多媒体内容传输管理系统，其特征在于，它包括根据权利要求 6 的移动终端（2），所述终端配备有根据权利要求 5 的安全模块（3），以及根据权利要求 7 或 8 的广播服务器。

## 管理接入多媒体内容的安全方法和设备

### 技术领域

[0001] 本发明涉及向移动终端发送数字或多媒體內容，并且特別是视听节目形式的加密內容。

### 背景技术

[0002] 大多数当前用于通过电缆或卫星广播加密视听节目解决方案存在着被众多欺诈者利用的重大安全缺陷。目前，欺诈者甚至组织网络来分发用于生成对于解密广播节目（有些具有高附加值，例如电影或者现场足球比赛）不可或缺的代码的代码和软件。

[0003] 这部分上是由于现有系统缺少永久且独立的与用户的双向连接并且因此无法实时检验用户观看加密节目的权限所造成的。很多用户办理基本订购，却成功获得了与更高级权限对应的代码，并且因而可以从这些权限中获益而无需付费。

[0004] 此外，目前没有方法恢复加密内容在中断处的重放，所述中断是由于用户的有意中断或无意中断。例如，在移动电话中的接收器的情况下，观看可能会由于电话呼叫或者网络覆盖中断而被频繁中断。这个限制对用户来说相当麻烦，尤其是在移动背景下。

### 发明内容

[0005] 本发明的目的是弥补上面提到的缺陷，并且提出一种可以使移动电话用户以更安全的方式观看加密视听节目并且可以从中断发生处恢复接收的解决方案。

[0006] 上述目的通过一种管理向配备有安全模块的移动终端发送多媒體內容的方法而被实现，所述多媒體內容以加密方式从广播服务器、经由通信网络而被发送，其特征在于，所述方法包含以下步骤：

[0007] a) 向移动终端发送多媒體內容的使用权限数据；

[0008] b) 在移动终端的安全模块中存储所述使用权限数据；

[0009] c) 生成加密 / 解密密钥序列，解密密钥序列是从存储在安全模块中的使用权限数据中生成的；

[0010] d) 发送多媒體內容到移动终端，所述内容是用来自己生成的加密密钥序列中的连续密钥来加密的；

[0011] e) 移动终端接收多媒體內容，并且利用解密密钥来解密多媒體內容，所述解密密钥来自移动终端的安全模块中生成的解密密钥序列。

[0012] 因此，例如视听节目多媒體內容可以通过在广播服务器和移动终端中并行地动态改变加密 / 解密密钥、以安全的方式被发送到移动终端。

[0013] 根据本发明的一个方面，能够实现重放以在发送多媒體內容中断的情况下恢复，所述方法还包括：步骤 f)，其中移动终端向广播服务器发送来自最后接收的帧或来自中断时所使用的加密密钥的参考数据；以及步骤 g)，其中根据所述参考数据恢复多媒體內容的广播。在步骤 c) 中，每个加密 / 解密密钥是在与由广播服务器发送的每个帧所定义的时间间隔相对应的时间内生成的。

[0014] 因此,在本发明的方法中,用户可以返回到与不论是由用户还是外部因素引起的节目中断接近的地方。

[0015] 根据本发明的另一方面,所述方法还包括步骤 h),其中,在移动终端中检验使用权限的有效性,所述检验是通过查询存储在安全模块中的使用权限数据并且将其与存储在数据库中的使用权限数据相比较来实现的。

[0016] 根据所述检验的结果,服务提供商可以随时(假设电话在网络覆盖区域内)检验权限的有效性、修改权限并且在必要时中断服务。

[0017] 为了加强经由通信网络发送的多媒体内容的安全性,在步骤 c) 中,解密密钥序列中的密钥是基于基本密钥和密码而被迭代计算的,所述密码被预先定义并且在移动终端和广播服务器之间被交换。

[0018] 例如,对于配备有(U)SIM 卡的移动电话,本发明提出了一种利用密钥来加密程序的方法,所述密钥根据只有(U)SIM 卡和服务提供商知道的序列来随时间动态地变化。这些密钥是基于在程序被发送前用户获得的并被存储在(U)SIM 卡中的权限而被迭代计算的。假设用户在网络覆盖区域内,那些权限的有效性可以随时被检验。服务提供商可以随时否定如此检验的权限(或认可)。

[0019] 通过向服务器传送由(U)SIM 卡提供的参考,可以在与用户有意中断或无意中断接近的时刻重新初始化解密过程。所述方法包括以下步骤:

[0020] (a) 在(U)SIM 卡中存储包含基本加密密钥的用户权限;

[0021] (b) 以服务提供商定义的频率生成用于加密程序的密钥序列,所述生成是基于基本密钥的并且在卡或终端中以及在加密并发送程序的服务提供商的服务器中并行地进行;

[0022] (c) 向服务提供商传送由(U)SIM 卡提供的参考(例如密钥号码或者密钥本身),并且为了重新发送程序而指示解密被中断的位置。

[0023] 本发明还提供一种适于包含在移动通信终端中的安全模块,所述终端用于接收以加密形式发送的多媒体内容,所述模块的特征在于,它包含用于存储多媒体内容的使用权限数据的装置,和用于从所存储的使用权限数据中计算解密密钥序列并存储它们的装置。

[0024] 这个模块还可以包括用于存储来自最后接收的帧或者来自在发送多媒体内容到移动终端中断时所使用的加密密钥的参考数据的装置。

[0025] 本发明还提供了一种配备有如上述的安全模块的移动终端,以及用于在所述移动终端中执行的计算机程序,所述程序包括:用于生成加密/解密密钥序列的指令,其中所述解密密钥序列是从由移动终端接收的使用权限数据中生成的;以及用于利用来自自己生成的解密密钥序列中的解密密钥来解密由移动终端接收的多媒体内容的指令。

[0026] 本发明还提供一种广播服务器,其包含用于经由通信网络向配备有安全模块的移动终端以加密形式发送多媒体内容的装置,其特征在于,它包含用于将所发送的多媒体内容的使用权限数据发送给移动终端的装置,其中所述使用权限数据包括用于计算与由所述服务器计算的加密密钥序列相类似的解密密钥序列的数据。

[0027] 所述服务器还包含用于存储发送给移动终端的使用权限数据的数据库,以及用于查询存储在移动终端的安全模块中的使用权限数据并将其与存储在数据库中的使用权限数据相比较的装置。

[0028] 所述广播服务器可以借助于计算机程序来实现,所述计算机程序包括:用于生成加密 / 解密密钥序列的指令;用于向移动终端发送多媒体内容的使用权限数据的指令,所述使用权限数据包括用于计算与由所述服务器计算的加密密钥序列相类似的解密密钥序列的数据;以及用于发送多媒体内容到移动终端的指令,所述内容是利用来自自己生成的加密密钥序列中的连续密钥来被加密的。

[0029] 最后,本发明还在于一种多媒体内容传输管理系统,其包括配有安全模块的移动终端和如上面定义的广播服务器。

## 附图说明

[0030] 参考附图,本发明的特征和优点通过以下描述而变得更清楚,该描述是作为说明性且非限制性例子而给出的,其中:

[0031] - 图 1 概略地示出了本发明所使用系统;

[0032] - 图 2 说明了根据本发明的 (U)SIM 卡中的数据管理的一个例子;

[0033] - 图 3 说明了传送加密视听节目的一个例子;

[0034] - 图 4 说明了根据本发明的用于重新接收节目的密钥恢复的一个例子;

[0035] - 图 5 说明了使得服务提供商能根据他们的检验来否定用户权限(或认可)的权限检验的一个例子。

## 具体实施方式

[0036] 本发明适用于移动电话,或者配有屏幕和安全模块的、能够通过标准移动电话网络通信并且能够接收例如数字视听流的多媒体内容的任何类型的移动终端。这些设备越来越多地构成袖珍计算机,其如众所周知的那样以较小的规模而包括标准计算机中的基本资源。更确切地说,这些电话特别包括例如用于执行程序的处理器的处理装置,以及用于存储数据的存储装置。众所周知,所述处理器可以是 SIM(用户识别模块)或者 USIM(通用用户识别模块,通常写作 (U)SIM)微芯片卡的一部分,其额外地构成不可侵犯的保险箱从而提供等同于或者超过标准终端的安全级别。如下文详细解释的,这就是根据本发明的解决方案提供这样一种装置的原因:该装置用于使用安全模块及其至运营商网络的永久双向连接来使得终端能够管理人工服务中断并且使得服务提供商(例如 Orange<sup>TM</sup>)能够立即接入用于初始化、修改、检验和撤销权限的安全程序。然而,一些移动终端没有独立的物理介质,例如没有微芯片卡。安全模块因而直接在移动终端的处理和存储装置中被实现,移动终端的一部分存储器被预留给发送到安全模块的数据,详见下文。

[0037] 该详细描述仅限于配备有 (U)SIM 卡的移动电话终端。

[0038] 图 1 简单地说明了用于节目传输系统中的主要单元与根据本发明的方法之间的关系。如图 1 所示,所述系统包括服务器 1 以及含有屏幕 21 和可拆卸 (U)SIM 用户卡 3 的电话 2。所述系统还包括能实现服务器 1、电话 2 和 SIM 卡 3 之间的通信的移动电话网络 4。服务器 1 控制传输及内容安全管理(特别是加密)。

[0039] 电话 2 和 (U)SIM 用户卡 3 通过软件接口以本领域已知的方式进行通信。例如,在移动电话中,该接口由 ETSI(欧洲电信标准协会)标准化。因此,服务器 1 可以通过移动电话网络 4 和其中插入卡的电话 2、以读模式和写模式访问 (U)SIM 用户卡 3 的存储器。

[0040] 图 2 说明了服务器 1、电话 2 和 (U)SIM 卡 3 之间的通信。这个经由移动电话网络 4 的通信能够识别和验证用户的移动终端和 (U)SIM 卡 (步骤 S1 和 S2)，并且使得用户获得的使用权限能够被安全地发送并被存储在 (U)SIM 卡中 (步骤 S3)。这些权限通常包括与权限所涉及的节目的关联、解密密钥、保证权限真实性的元素等等，并且已经被各种组织标准化 (尤其是开放数字权限语言倡议以及开放移动联盟)。例如，SIM 工具应用程序可以将这些权限安全分配到卡存储区中的某个位置。存储权限使得服务提供商能够在此后任何时候进行检验、修改，并且如果必要否定存储在 (U)SIM 卡上的权限，假定电话是在移动网络覆盖范围内使用并且符合标准的 GSM/UMTS 协议。

[0041] 所述场景的一个特定实例是在用户和服务提供商的发起下对这些权限的修改，这可以通过移动网络立即实现。如果服务提供商希望修改权限，则存储新的权限来替换旧权限就足够了。

[0042] 下面参考图 3 和图 4 解释根据本发明的用于重新发送 TV 节目的步骤。

[0043] 如图 3 所示，在 (U)SIM 卡 3 如前所述获得使用权限之后，服务器 1 以加密的形式通过移动通信网络 4 向电话 2 发送视听节目。根据用于通过移动电话网络 (如 UMTS (3G) 网络) 发送数据的传输技术，视听节目以连续的 T1 到 Tn 的帧被广播，每个帧定义一个时间间隔  $\Delta t$ ，在该时间间隔内视听节目的一部分数据被发送给电话 2。因此，根据它在传输系统中的位置以及它所代表的时间间隔，每个帧与被传送的视听节目的特定时刻 (或者时间跨度) 相对应。根据本发明的第一方面，(U)SIM 卡可以存储若干接收到的帧，并且从而可以在中断时指出最后一个接收到的帧号码。根据本发明的另一方面，每个帧可以利用它自己的加密密钥被加密，以便从 T1 到 Tn 的每个帧都可以利用不同的加密密钥而被识别，在图 3 中分别是从 T1 到 Tn。已接收用于对发送到电话的节目解密的权限的 (U)SIM 卡 3，生成与加密密钥序列相类似的解密密钥序列 C1 到 Cn。(U)SIM 卡因而能够在传输过程中随时指出加密 / 解密密钥。

[0044] 因此，如果节目广播中断，则移动电话 2 请求重新发送先前中断的节目 (步骤 S4，图 4)。然后，服务器 1 向 (U)SIM 卡 3 请求节目传输中断的时间 (步骤 S5)。(U)SIM 卡然后通过给服务器关于最后接收的帧或者用于加密最后接收的帧的密钥的参考来响应服务器，以指示中断发生的时间 (步骤 S6)。如果必要，服务器更新存储在 (U)SIM 卡上的权限从而重新发送中断处的节目 (步骤 S7)。

[0045] 下面描述管理用于加密广播内容的密钥的参考的例子。

[0046] 存在生成这些密钥的各种不同的方式。一种特别安全的解决方案是使用服务提供商和用户卡共用的密码 (例如 PIN) (根据所采用的解决方案，所述密码可以可选地利用密码多样化算法而被个性化)。所述密码可以在个性化卡时或者在从服务提供商获得订购时通过安全下载而被加入卡中。

[0047] 然后，这个共用密码用于从包含在与数字内容相关的权限中的第一解密密钥中计算用于加密 / 解密连续内容帧的加密 / 解密密钥序列，在服务器侧用于加密而在卡侧用于解密。

[0048] 为了计算这个序列，可以使用一种密码学函数，例如像 AES (高级加密标准) 算法的另一种加密算法，或者任何适用于这个解密密钥长度的算法 (传统上是 128 比特)。所述算法被迭代地应用于先前使用的密钥以及用于获得下一个要使用的密钥的密码。这个过程

是利用密码学函数的“INPUT”密钥与解密并行进行的。

[0049] 密码可以根据服务提供商的需求、利用 GSM 安全密钥下载工具在服务提供商的发起下自然地被更新。

[0050] 所述算法也可以在其已被科学界超越时被更新，这将在安全体系结构方面给予服务提供商完全的灵活性。此外，必要时，多个算法可以存在于卡中，以在必要时从一种算法改变到另一种算法。

[0051] 因此，在广播服务器和卡二者中迭代相同的算法，并且因此在两个实体中可以具有相同的密钥序列，并且因而生成参考序列，其可以是帧号码或者是用于该帧的密钥值（用另一密钥被加密）。

[0052] 因此，为了中断后恢复观看，所述卡动态地存储这个参考并在服务器请求它时发送给服务器就足够了。用于借助于所述参考恢复观看的方法，按照是点到点传输还是点到多点广播而变化。这些方法在本领域中是已知的，并且为了简明此处不再详细描述。

[0053] 图 5 说明了为检验使用权限而执行的步骤。

[0054] 移动电话 2 在移动电话网络 4 覆盖范围内，并且可能可选地正在读取（即解密）由服务提供商发送的视听内容（步骤 S8 和步骤 S9）。服务器 1 发送用于检验用户所持有的并存储在用户的 (U)SIM 卡 3 中的权限的有效性的命令（步骤 S10）。然后，(U)SIM 卡 3 通过指示用户所持有的权限来响应服务器。从 (U)SIM 卡至服务器的响应形式取决于所使用的协议。例如，(U)SIM 卡可以通过向服务器发送对应于用户权限的加密 SMS 消息来响应它（3GPP 标准 23.048）。授予用户的使用权限可以非常多样化。它们通常与使用多媒体内容的约束或限制相对应。那些约束或限制由 DRM 代理解释（实现指定数字权限管理操作的软件）并且适用于相关的多媒体内容。例如，使用权限可能涉及：

[0055] • 内容的使用限定日期；

[0056] • 内容可以被使用的次数；

[0057] • 内容可以与其关联的身份；

[0058] • 使用的特定条件（例如，用户必须在移动网络覆盖区域内从而能够使用内容）。

[0059] 使用权限可以根据所采用的权限管理技术而以多种语言来表达。例如，当用于 OMA（开放移动联盟）标准中时可将使用权限写为 ODRL（开放数字权限语言），或者当被 Windows Media® DRM 平台使用时可将使用权限写为 XrML（可扩展权限标记语言）。

[0060] 由于移动网络中存在双向通信，关于用户所持有的使用权限的 (U)SIM 卡的响应因而经由移动网络被发送给服务提供商（步骤 S11）。因此，服务器可以通过将它们与用户预先获得并存储在用户数据库中的权限相比较来检验权限的有效性。如果存在差异，则它可以进行搜索来解释该差异（例如在最近的事务之后同步数据库时产生的时延）。当检测到用户试图欺骗时，提供商可以立即采取适当的措施，例如毁掉卡中所包含的任何权限，或者对接入非法添加给该卡的节目计费。用于毁坏权限的方法与前面已经解释的用于在卡中存储或修改权限的方法相似（参考图 1）。

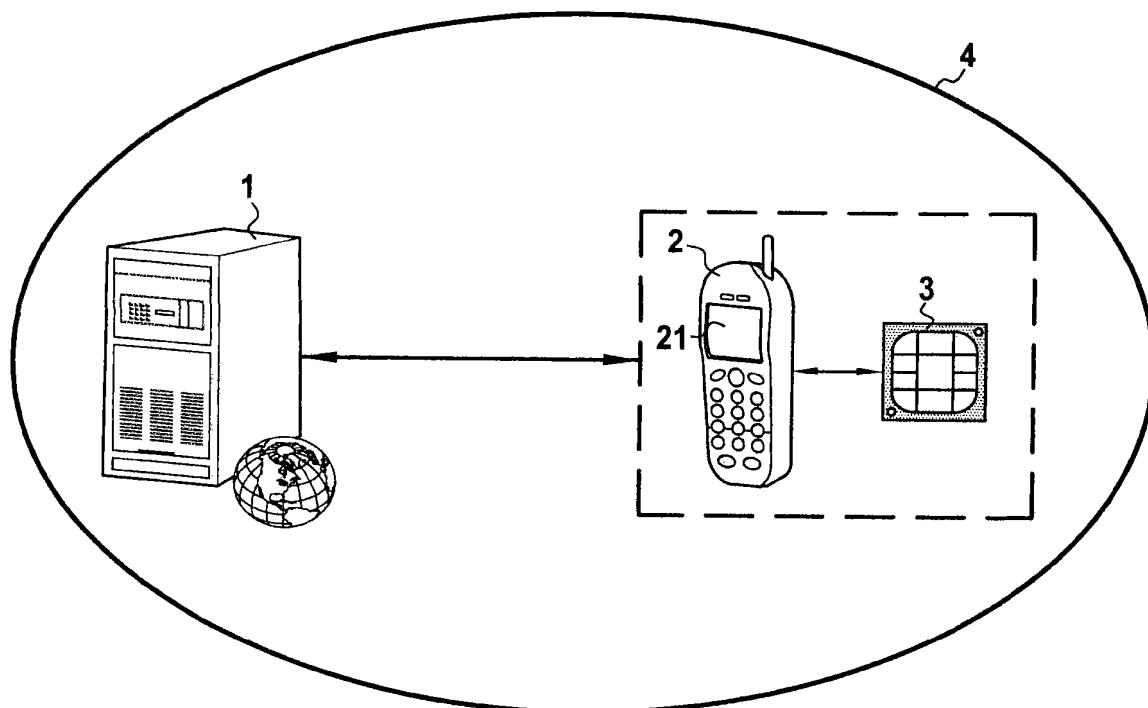


图 1

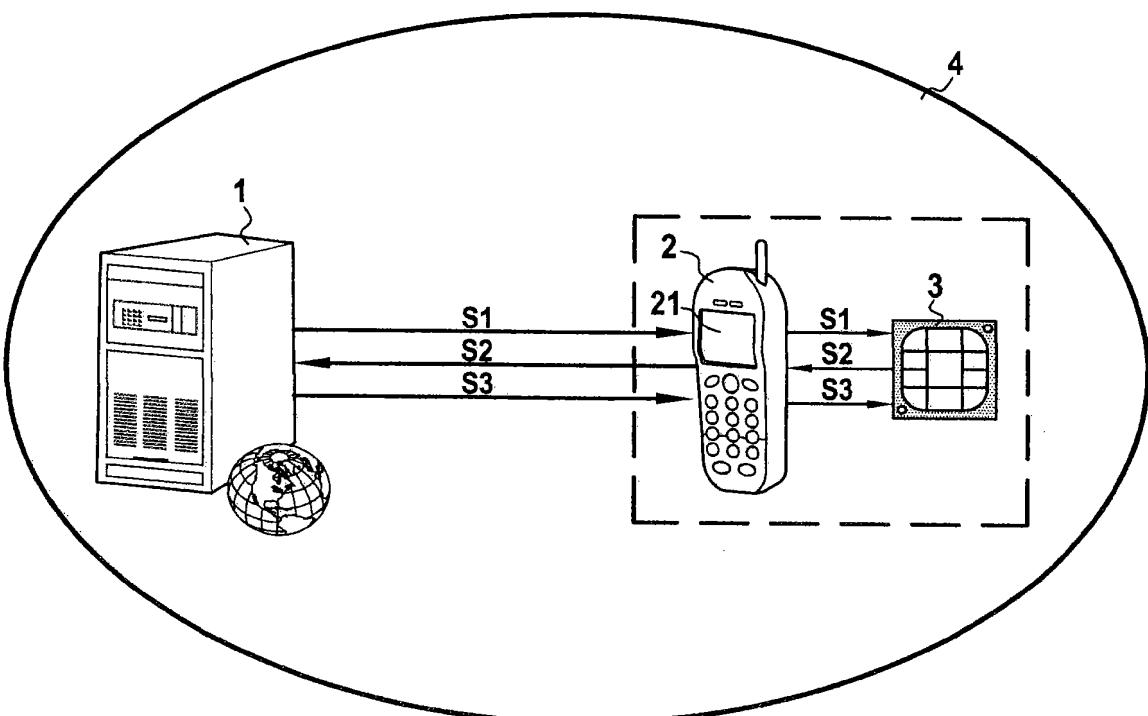


图 2

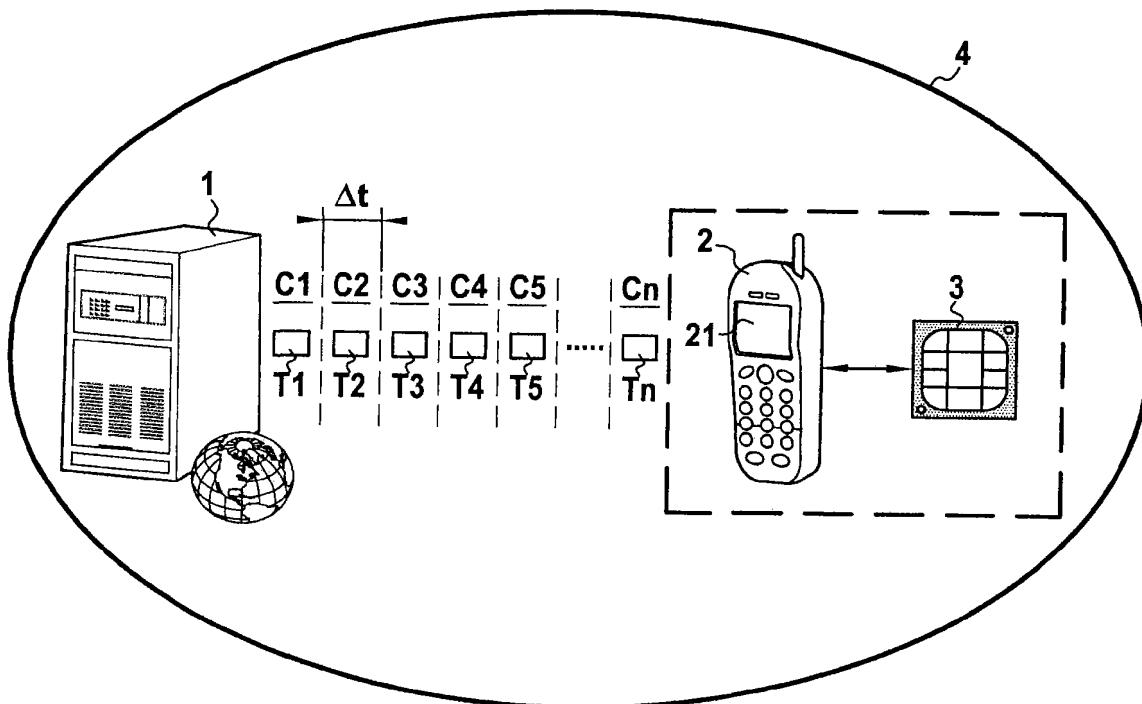


图 3

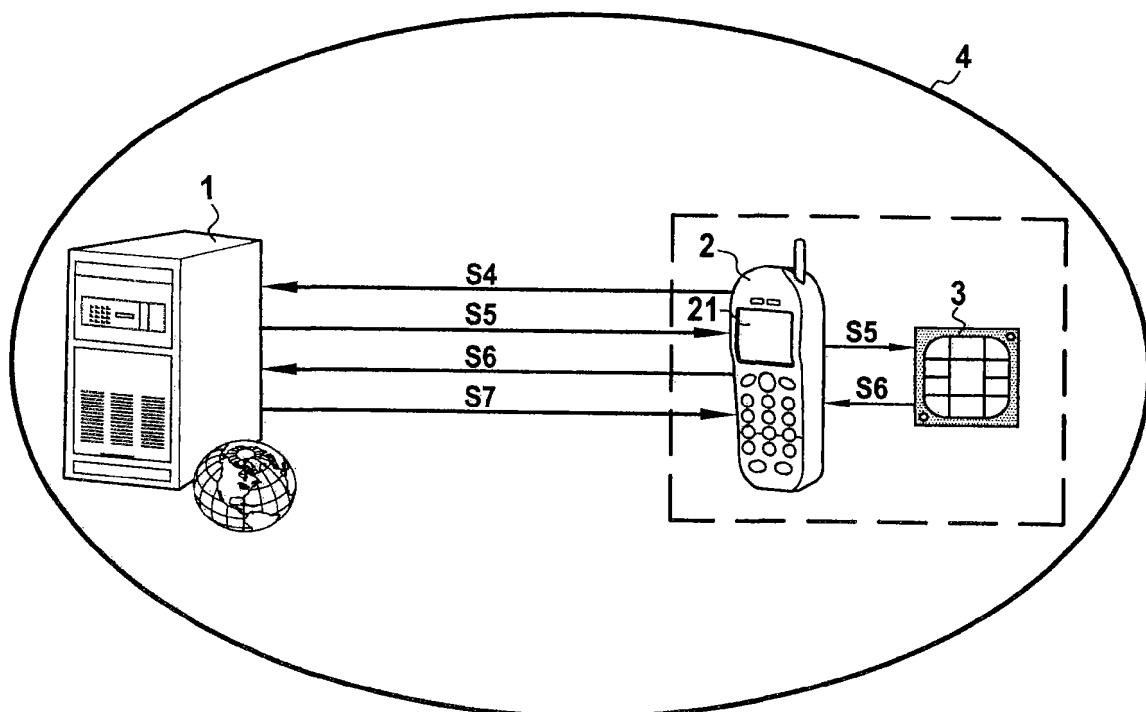


图 4

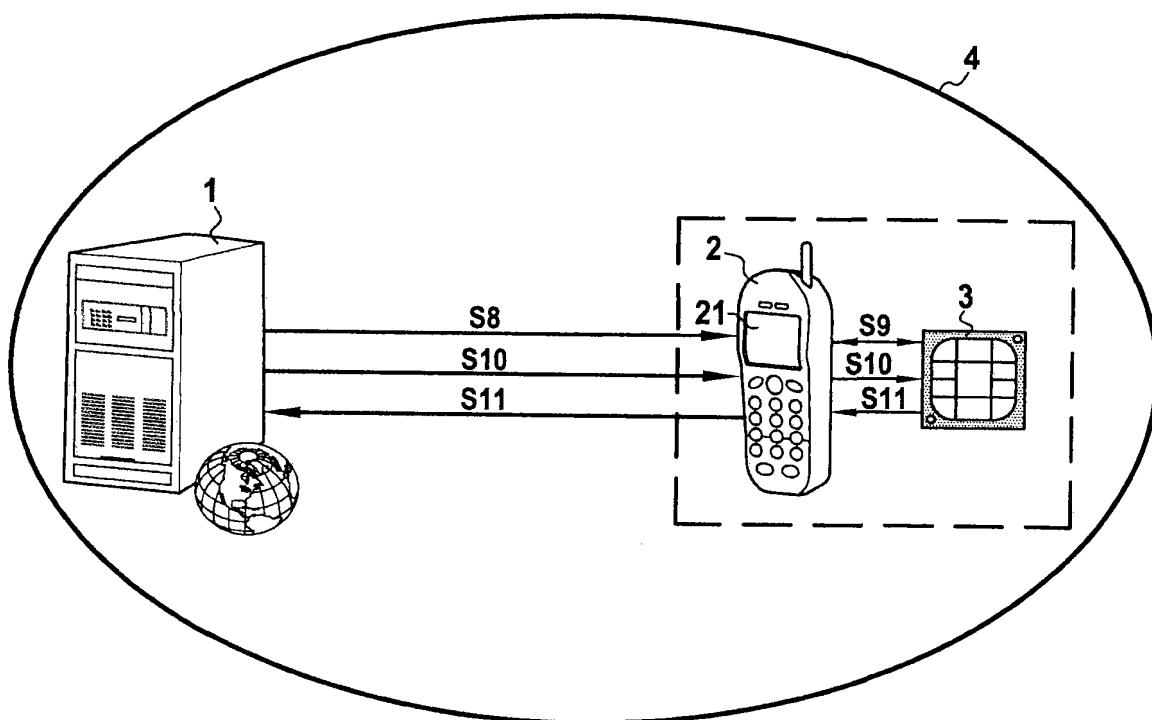


图 5