[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38
H04Q 7/22

[12] 发明专利说明书

[21] ZL 专利号 98802920.0

[43] 授权公告日 2003 年 4 月 16 日

[11] 授权公告号 CN 1106133C

[22] 申请日 1998.2.26 [21] 申请号 98802920.0
[30] 优先权
[32] 1997. 2.28 [33] DE [31] 19708189.4
[86] 国际申请 PCT/DE98/00569 1998.2.26
[87] 国际公布 WO98/38826 德 1998.9.3
[85] 进入国家阶段日期 1999.8.27
[71] 专利权人 德国电信移动网有限公司
地址 联邦德国波恩
[72] 发明人 弗莱德·帕尼斯
帕特里克·朗格斯多姆
沃尔特·摩尔斯
[56] 参考文献
EP0740482 1996.10.30 H04Q7/32
WO9502927 1995.01.26 H04B1/38
审查员 吴东捷

[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 王以平

权利要求书 2 页 说明书 6 页 附图 2 页

[54] 发明名称 与公用移动通信系统兼容的无线通信系统及其运行方法

[57] 摘要

本发明涉及一种无线通信系统，它在无线接口上与至少具有确认功能的公用移动通信系统本质上兼容，其中无线通信系统的基站装配有用于读和写识别模块中(上)的信息的装置并配置有合适的软件，以与从识别模块上获得的数据一起完成归属位置寄存器(HLR)及确认中心(AUC)的功能。 在识别模块上还有无线通信系统基站的全部初始化参数，它们将在网络运营者的控制之下而不被操纵。

ISSN1008-4274

1.一种无线通信系统的运行方法，该系统具有一个公用移动通信系统的移动终端（3），具有一个与公用固定网（2）相连接的基站（1），基站在无线接口上与至少具有确认功能的移动通信系统兼容，其特征在于，

基站（1）借助于读/写设备从至少一个识别模块（7）中/上读/写信息，基站（1）所用识别模块（7）中数据的范围与有权进入的移动终端（3）的芯片卡（SIM）的数据相同，所述数据包括单个用户用于确认的数据并且不能被改动，

借助于一个配置在基站（1）中的软件处理读出的数据，

根据从识别模块（7）读出和处理的数据面向基站（1）进行移动终端（3）的确认，其中基站（1）完成与移动通信系统中归属位置寄存器及确认中心相同的功能和任务，并且

当确认成功时移动终端（3）在公用固定网（2）上运行。

2. 如权利要求 1 所述的方法，其特征在于，移动通信系统的网络运营者可以停止移动终端（3）在无线通信系统的基站（1）进行登录的权利。

3. 如权利要求 1 或 2 所述的方法，其特征在于，在识别模块（7）上还有其它的数据，即可用频率，基站（1）和移动终端（3）允许的最大输出功率，允许的业务和所有其它的初始化参数，对于它们网络运营者将施加影响并且它们是无线通信系统的基站（1）运行的依据，它们不能被改动。

4. 如权利要求 1 所述的方法，其特征在于，无线通信系统的基站（4）的无线接口工作在公用移动通信系统的频谱内。

5. 如权利要求 1 所述的方法，其特征在于，在无线接口上应用了对传输数据的加密。

6. 如权利要求 1 所述的方法，其特征在于，基站（1）含有一个定时器，它由网络运营者编程在一个规定的时间上，它在基站（1）被

用户合法使用时持续自动减少，基站不被使用时，即定时器中编程的时间间隔期满后失去将其发射机置于移动通信系统的频率上运行的权利。

7. 如权利要求6所述的方法，其特征在于，在基站（1）由于定时器期满而自动关闭时可以紧急恢复运行。

8. 如权利要求7所述的方法，其特征在于，基站（1）的紧急恢复运行仅在一个规定的时间段内是可能的。

9. 运行一个公用移动通信系统的移动终端（3）和一个与公用固定网（2）相连接的基站（1）的无线通信系统，基站在无线接口上与至少具有确认功能的移动通信系统兼容，其特征在于，

一个装配在基站(1)的读/写设备用于读/写至少一个识别模块(7)上/中的信息，基站（1）所用识别模块（7）中数据的范围与有权进入移动终端（3）的芯片卡（SIM）的数据相同，所述数据包括单个用户用于确认的数据并且不能被改动，并且

在基站（1）中配置的软件用于处理读出的数据并根据从识别模块（7）读出和处理的数据面向基站（1）进行移动终端（3）的确认，其中基站(1)完成与移动通信系统中归属位置寄存器及确认中心相同的功能和任务。

10. 如权利要求9所述的无线通信系统，其特征在于，识别模块（7）是用于移动通信系统的常规芯片卡（SIM）。

与公用移动通信系统兼容的无线通信系统及其运行方法

技术领域

本发明涉及一种与公用移动通信系统兼容的无线通信系统及其运行方法。

背景技术

如今的移动通信系统在公用移动通信系统，例如全球移动通信（GSM）系统，和例如按照数字 DECT 标准（数字式欧洲无线电信标准）工作的私人无线通信系统之间存在明显的区别。这导致各种不同的设备制式，它们或是适合于移动通信，或是适合于无线运营。

曾经试图设计出适合于两种不同的移动通信系统的终端，特别是移动终端。由于不同标准的不兼容性，使得解决方案相对地不方便于使用者并且造价昂贵。

另一种尝试是如此建立无线通信系统的基站，使得它与公用移动通信系统兼容，即能用公用移动通信系统常规的移动终端通信。然而没有合适的解决方案实现例如所要求的保安功能。问题在于无线通信系统的基站与有线固定网相连接，这样，通过移动通信系统直接作用于基站是不可能的。

WO－A－95/24106 公开的是一种保安个人通信系统，它基于一个连接于公用固定网的基站，它允许移动通信系统终端运行。通信安全性通过使用移动通信网中常规的确认方法来保证，其中基站通过公用固定网与移动通信系统的保安设备连接，而且与其交换保安信息，以实现移动终端在基站的登录。这种方法基于一方面在移动终端和基站间交换信息，另一方面在基站和移动通信网的设备之间交换信息。

WO－A－95/02927 公开了一种控制无线通信系统的发射/接收装置的方法。其中发射/接收装置装配有所谓的智能卡读出设备，智能卡上

存储无线通信系统运营者不用的、发射/接收装置可以使用的频率信息。

发明内容

本发明的目的在于提出一个具有保安功能的无线通信系统及其运行方法，它与公用移动通信系统兼容并且允许使用所属的移动终端。

进一步的目的还在于，无线通信系统除具有私人系统特性外还应具备以下可能性：在移动通信网运营者的控制下被设置和运行。

根据本发明的一个方面，提供了一种无线通信系统的运行方法，该系统具有一个公用移动通信系统的移动终端，具有一个与公用固定网相连接的基站，基站在无线接口上与至少具有确认功能的移动通信系统兼容，其特征在于，基站借助于读/写设备从至少一个识别模块中/上读/写信息，基站所用识别模块中数据的范围与有权进入的移动终端的芯片卡（SIM）的数据相同，所述数据包括单个用户用于确认的数据并且不能被改动，借助于一个配置在基站中的软件处理读出的数据，根据从识别模块读出和处理的数据面向基站进行移动终端的确认，其中基站完成与移动通信系统中归属位置寄存器及确认中心相同的功能和任务，并且当确认成功时移动终端在公用固定网上运行。

根据本发明的另一个方面，提供了运行一个公用移动通信系统的移动终端和一个与公用固定网相连接的基站的无线通信系统，基站在无线接口上与至少具有确认功能的移动通信系统兼容，其特征在于，一个装配在基站的读/写设备用于读/写至少一个识别模块上/中的信息，基站所用识别模块中数据的范围与有权进入移动终端的芯片卡（SIM）的数据相同，所述数据包括单个用户用于确认的数据并且不能被改动并且在基站中配置的软件用于处理读出的数据并根据从识别模块读出和处理的数据面向基站进行移动终端的确认，其中基站完成与移动通信系统中归属位置寄存器及确认中心相同的功能和任务。

本发明的要点在于，无线通信系统的基站装备一个合适的读/写设备，用它可以读和写常规识别模块的信息，它们可以是例如芯片卡，SIM（用户识别模块），以及所有有源的信息存储和信息处理数据载体。与适当的软件和识别模块上的数据一起，无线通信系统的基站现在能真正

完成移动通信网基站的功能，确切地说，完成归属位置寄存器（HLR）及确认中心（AUC）的功能。这样，每个有权在无线通信系统中使用的移动终端均可被登录并且通过固定网通信。

在以下说明中如果不另加说明，“基站”一词是指无线通信系统的基站。

下面以 GSM（全球移动通信）系统为例说明本发明的许多可能方案中的一个。然而本发明不局限于 GSM 移动通信系统。

在无线通信系统的基站中配置一个或多个芯片卡读/写器和一个常规的 SIM 芯片卡可以实现基站在 GSM 网络运营者的控制下工作，并且像在 GSM 移动通信网中运营那样给“GSM－无线运营”中的用户提供保安标记，如确认和语音数据的加密。重要的是如通常在 GSM 移动终端中那样由网络运营者单独发行基站运行所必需的芯片卡。

在基站中使用的芯片卡与一个合适的，配置在基站中的软件一起完成归属位置寄存器（HLR）及确认中心（AUC）的功能，这就是说，移动终端是面向无线系统的基站进行确认，而不是像通常那样面向移动通信网进行确认。为此，借助于基站中配置的软件产生一个随机数，它分别由两个芯片卡（即基站的芯片卡和移动终端的芯片卡）中相同的 k_i 密钥和 GSM 系统所用的 A3 算法变换为各一个 SRES－应答（确认结果）。当两个确认结果（基站的和移动终端的）一致时就完成了确认过程。此确认过程与 GSM 系统所用的方法相同。

由相同的随机数用 k_i 密钥和 A8 算法以熟知的方法产生密钥 K_c，用它来对无线运行中无线接口上的通信进行加密（如 GSM 系统中那样）。

在基站的 SIM 上除了通常的个人专用数据外还可以有其它数据，例如可用频率，基站和移动终端允许的最大输出功率，允许的业务（电话，数据传输，传真等）和所有其它的初始化参数，对于它们网络运营者将施加影响并且基站可以使用这些数据，它们都不能被操纵。至少在业务上这相应于熟知的 GSM 移动通信网的归属位置寄存器（HLR）中的权限管理。

通过合适的密钥管理可以实现诸如家庭成员这样的多个用户通过

一个这样的基站进行通信。为此，第一种方案是每个要使用该基站的用户具有其自己的第二张 SIM 卡，它能被插入基站。这时基站需要多个读卡设备。另一种方案是在基站的 SIM 卡上存储多个用户的数据和密钥。

此外也可以在基站中用一个组密钥，它允许对多个单个用户进行确认。

重要的是基站中使用的芯片卡在核心部分具有与 GSM 移动终端的芯片卡相同的信息，这些信息用于基站运行。仅当两张卡上的个人使用者数据，尤其是保安功能相符合时，移动终端才能在基站上确认和登录。

正式 GSM 用户关系的解约最好通过 GSM 无线接口在移动终端的 SIM 卡中取消与基站通信的权利来实现。这样，基站在此网络运营者所用频率上的继续运行不再可能，因为移动终端不能再被基站确认。

此外存在以下这种可能的实施形式：基站含有一个定时器（Timer），它由网络运营者编程在一个规定的时间上，并且在基站被用户使用时持续自动减少。在不使用基站时，例如用户关系被解约后，基站在编程的时间间隔期满后失去将发射机置于移动通信系统的频率上运行的权利。如果较长时间不使用基站，定时器的功能可通过关闭基站而被冻结。

如果发生诸如在进入长时间假期之前用户忘记关闭基站并且基站自动失效的情况，存在在规定时间段内紧急恢复的可能性。

为了实现与 GSM 兼容的基站，首先它被装配一个用于 GSM－SIM 卡的读卡器。此外基站必须能够以 GSM 标准频率发送和接收。基站功能的控制通过诸如在 GSM 终端中所用的合适的软件实现，并且软件完成和控制 GSM 通常的确认和其它功能。

移动终端本身只需进行较少的软件变动。

附图说明

图 1 简要示出本发明系统一个例子的物理结构。

图 2 简要示出本发明系统一个例子的逻辑结构。

具体实施方式

图 1 简要示出了一个公用移动通信系统的一些装置。其中有一个移动终端 3，它位于移动通信系统的一个基站 4 的服务区内，并且通过无线接口可与基站进行加密通信。移动通信系统的基站 4 与交换机 5 连接，它具有连接公用固定网 9 的通道。此外，交换机 5 与移动通信网的归属位置寄存器（HLR）和确认中心（AUC）相连接。如果移动终端 3 已在移动通信网中登记，则以熟知的方法在归属位置寄存器和确认中心 6 执行对移动终端 3 的确认。

此外，一个同样与公用有线固定网 2（公共交换电话网 PSTN，综合业务数字网 ISDN）连接的无线通信系统的基站 1（HBS）被示出。由于微小的输出功率，该基站的服务区相对较小。基站 1 通常位于公用移动通信网的一个或多个基站 4 的服务区内。

如图 2 所示，移动终端 3 在移动通信运行中通过移动通信网被确认，并且确认过程借助于一个专用的识别密钥（k_i 密钥）完成，它一方面在移动终端 3 的 SIM 卡 8 中获得，另一方面在移动通信系统的归属位置寄存器及确认中心（AUC）6 中获取。

按照本发明，无线通信系统的基站 1 装配着一个识别模块 7（例如同样是一张 SIM 卡）和一个合适的软件，以与从识别模块 7 上获得的数据一起完成上述由归属位置寄存器和确认中心所完成的功能和任务，这样，只要移动终端 3 位于无线通信系统的服务区内并且具有进入的权利，它就被它所从属的无线系统基站 1 确认、登录并能进行加密通信。

仅当在基站 1 所用的识别模块 7 中数据的主要部分与具有进入权利的移动终端 3 的芯片卡（SIM）上获取的数据相符时上述确认等才是可能的。

按照本发明，无线系统的基站 1 与移动通信系统兼容，即在备用模式中无线系统的基站 1 周期性地发送一个专用的识别信号，以显示其的存在和已准备好。移动终端 3 按照基站 1 专用的识别信号使用频带，当移动终端 3 进入基站 1 的服务区并且其识别信号无干扰地被接收时，移动终端 3 以前述方法在基站 1 试图登记。为此如 GSM 系统一样，在基站 1 和移动终端 3 之间交换确认信息和初始化消息。如果确认完成，移动终端 3 能通过固定网 2 通信，而无需经移动通信网迂回。

当然这也是可能的：在没有公用固定网 2，9 或移动通信网参与的条件下多个被确认的移动终端 3 通过无线通信网的基站 1 相互进行加密通信。

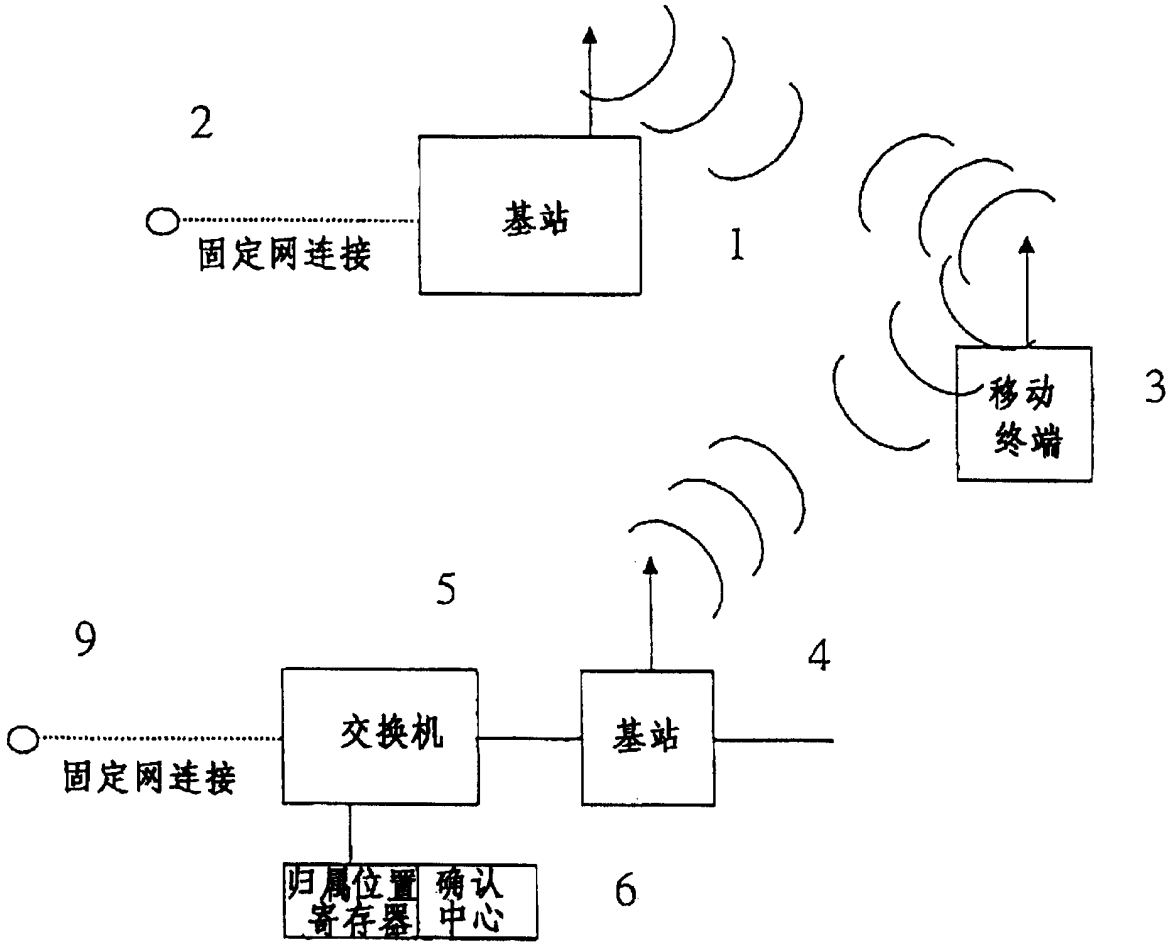

图 1

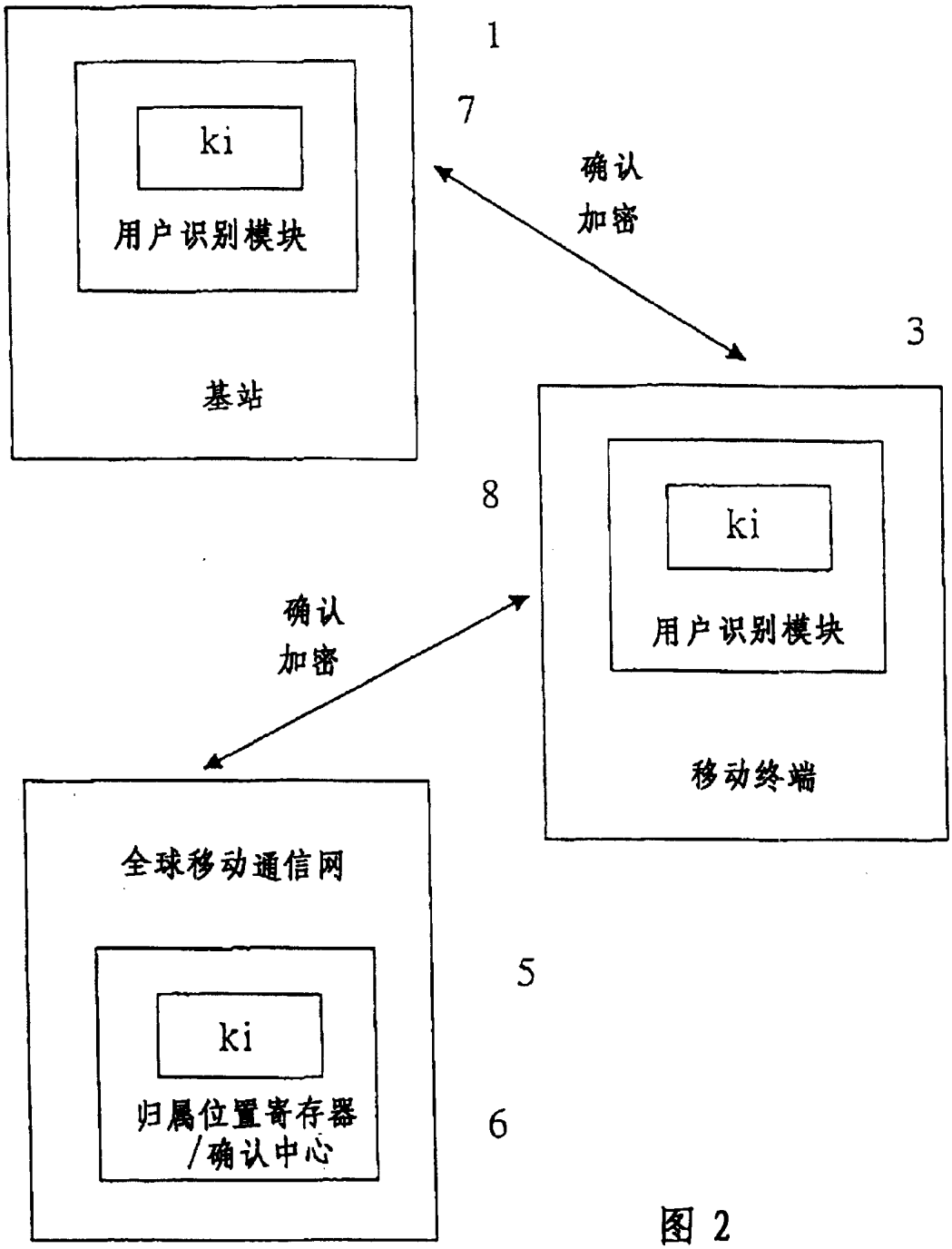
1
ki
用户识别模块
基站
7
确认
加密
3
8
ki
用户识别模块
移动终端
确认
加密
全球移动通信网
5
ki
归属位置寄存器
/确认中心
6

图 2