

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04W 12/06 (2009.01)

H04L 9/32 (2006.01)



[12] 发明专利说明书

专利号 ZL 200310125469.X

[45] 授权公告日 2009 年 7 月 15 日

[11] 授权公告号 CN 100515135C

[22] 申请日 2003.11.21

[21] 申请号 200310125469.X

[30] 优先权

[32] 2002.11.22 [33] FR [31] 02/14669

[73] 专利权人 塞格特尔集团有限公司

地址 法国巴黎

[72] 发明人 迈克尔·邦西蒙 菲利普·卡卢德

塞德里克·波蒂恩

尼古拉斯·普吕内尔

[56] 参考文献

WO9724831A 1997.7.10

WO0002358A 2000.1.13

审查员 傅海望

[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 郭思宇

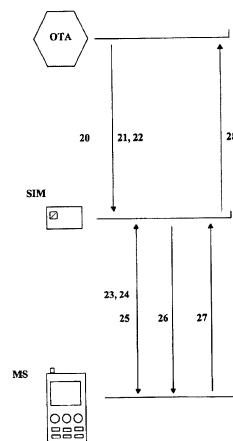
权利要求书 3 页 说明书 14 页 附图 3 页

[54] 发明名称

在芯片卡与无线终端之间建立并管理一种信任模式的方法

[57] 摘要

本发明涉及用于在一个识别模块(SIM)和一个无线终端(MS)之间建立和管理一个信任关系的方法,该方法包括通过所述识别模块(SIM)的一个终端(MS)鉴权步骤,该鉴权步骤通过使用比如一个密钥的鉴权装置来进行,所述鉴权装置或者在一个初始化步骤或类似步骤,或者在一个更新步骤,通过移动无线网络至少被提供给所述识别模块。根据本发明的方法中,一个密钥取消步骤由识别模块(SIM)终端(MS)或无线网络主动进行,该取消步骤包括擦除所述识别模块(SIM)的存储器中与终端(MS)相关的密钥。



1. 一种用于在识别模块和无线终端之间建立和管理信任模式的方法，其特征在于，该方法包括：

- 5 - 提供包括至少一个鉴权密钥的终端鉴权装置；
- 通过所述识别模块的终端鉴权步骤，所述鉴权步骤通过所述鉴权装置执行，在一个初始化步骤或者在一个更新步骤，所述鉴权装置通过移动无线电话网络被提供给所述识别模块，或者通过识别模块被提供给所述终端；
- 10 - 通过所述模块对终端的至少一个特有特性的控制步骤，所述特有特性从所述移动无线电话网络的一个安全服务器通过无线电话预先发送到所述模块。

2. 根据权利要求1的方法，其中识别模块中的所述终端鉴权装置被配置有有效期，该有效期由一个确定的终止时间限制。

- 15 3. 根据权利要求1或2的方法，其中所述识别模块是用于第三代网络的SIM型芯片卡或USIM卡，或者是在存储器中包含代表性预订数据的等效的卡。

4. 根据权利要求1的方法，其中通过产生鉴权装置，以及然后通过基于最初从无线终端可获得的鉴权装置借助于保密交换机制将该鉴权装置

20 提供给无线终端，识别模块保持与无线终端的信任关系。

5. 根据权利要求1的方法，包括在所述初始化步骤或更新步骤期间的产生一个信任密钥的产生步骤，该产生步骤至少通过所述识别模块来执行，所述信任密钥被所述模块用来加密至少在识别模块和终端之间的交换数据。

- 25 6. 根据权利要求2的方法，其中所述鉴权装置的初始化步骤由无线电话网络主动地在由所述模块或者移动无线电话网络或者无线终端启动的密钥被拒绝后、在密钥的有效期终止后或者甚至在识别模块初始化时执行。

7. 根据权利要求1的方法，其中所述鉴权步骤包括下面的步骤：

- 30 - 在终端中由在终端中存储的至少一个第一鉴权算法使用在终端中存

储的至少一个第一鉴权密钥的使用步骤, 所述第一密钥有一个由预定的终止时间限定的有效期;

- 通过识别模块由在识别模块中存储的至少一个第二鉴权算法使用在识别模块中存储的至少一个第二鉴权密钥的使用步骤, 所述第二密钥与第一密钥是相同的或互补的, 而且与终端是相关的, 所述第二密钥有一个由所述预定的终止时间限定的有效期;

- 识别模块中用来比较通过所述第一鉴权算法和第二鉴权算法得到的结果的比较步骤。

8. 根据权利要求 2 的方法, 其中鉴权步骤包括: 在比较过程使用所述预定终止时间。

9. 根据权利要求 7 的方法, 其中所述初始化步骤是通过移动无线网络开始的并还包括:

- 通过识别模块产生至少所述第一和第二密钥中的一个;
- 在识别模块中存储所述第二密钥;
- 通过识别模块传送所述第一密钥到终端, 所述第一密钥通过使用信任密钥被加密。

10. 根据权利要求 7 至 9 之一的方法, 其中所述比较步骤在两个应答结果之间进行, 其中一个应答结果通过所述第一鉴权算法得出, 存储在终端的存储器中并传送到所述识别模块, 另一个应答结果通过所述第二鉴权算法得出并存储在识别模块的存储器中。

11. 根据权利要求 7 的方法, 其中所述第一密钥是不对称的专用密钥 K_s , 所述第二密钥是与第一密钥互补的公共密钥 K_p 。

12. 根据权利要求 7 的方法, 其中所述第一密钥是对称的, 存储在识别模块存储器中的所述第二密钥与第一密钥相同, 这些密钥形成了单对称鉴权密钥。

13. 根据权利要求 7 的方法, 包括所述第一和第二密钥的更新步骤, 该步骤在所述预定终止之前通过识别模块开始, 所述更新步骤包括下面的子步骤:

- 使用所述第一和第二密钥在终端和识别模块之间进行鉴权;
- 通过识别模块的更新算法, 根据用来替换至少所述第一和第二密钥

中的一个信息,产生至少一个更新的密钥;

- 在识别模块中存储用于替换所述第二密钥的更新密钥;
- 通过识别模块传送更新密钥到终端。

14. 根据权利要求 13 的方法,其中所述更新步骤还包括对终端和/或
5 识别模块的至少一个标识符的控制。

15. 根据权利要求 13 的方法,其中对更新密钥到终端的所述传送进行
密钥加密,所述密钥加密通过所述信任密钥来进行。

16. 根据权利要求 13 的方法,其中更新步骤还包括下面的步骤:

- 在终端和模块之间的所述鉴权之后,通过识别模块产生一个新的信
10 任密钥;
- 在识别模块中存储新的信任密钥;
- 通过识别模块传送新产生的信任密钥到终端。

17. 根据权利要求 13 的方法,其中通过检测验证完成所述更新步骤,
所述检测验证包括:在终端部分上返回发送用于表示在更新步骤期间对通
15 过识别模块传送的数据的有效接收的至少一个数据。

18. 根据权利要求 5 的方法,其中所述信任密钥是与所述对称鉴权密
钥相同的对称加密/解密密钥。

19. 根据权利要求 5 的方法,其中所述信任密钥是一个可擦除的会话
密钥。

20. 根据权利要求 7 的方法,其中一个取消步骤由识别模块、终端或
20 相应的无线网络主动执行,所述取消步骤包括擦除所述识别模块的存
储器中与终端相关的至少所述第一密钥。

21. 一种实现根据权利要求 1 的方法的一个终端中的识别模块,其特
征在于,它包括用于存储至少一个鉴权密钥以及至少一个鉴权算法的装
25 置,用于执行将所述鉴权密钥应用到在识别模块中存储的所述鉴权算法中
的至少一个步骤的计算装置,通信装置,用于启动一个取消的装置和用于
取消所述鉴权密钥的取消装置,用于存储终端的特有特性的装置和用于启
动一个更新算法用来更新所述鉴权密钥的装置,通信装置能够提供至少一
个鉴权密钥到终端并能接收来自移动无线网络的安全服务器的数据。

在芯片卡与无线终端之间建立
并管理一种信任模式的方法

5

技术领域

本发明涉及移动无线电话通信领域。本发明尤其涉及一种为了在卡和终端之间进行安全交换而在无线通信终端和 SIM 芯片卡或类似的卡之间建立一种信任关系的方法。

10 为了上述目的，终端可以是能在移动无线电话网络中工作的任何便携、手提式发射接收装置，所述移动无线电话网络比如是 GSM，GPRS，UMTS 以及任何类型的类似网络，例如 WLAN。本发明用于配有芯片下的移动电话，例如 SIM 芯片卡，特别涉及移动电话的安全内容的分配。

背景技术

15 在现有技术中，关于安全交换和数据处理基础结构的问题已进行了长期的研究。对数据来说，已经提出的很多解决办法都是基于已知的加密技术。特别是公共密钥的管理基础结构（“公共密钥基础结构”PKI），是一种基于不对称密钥技术（公共 K_p ，专用 K_p ）的解决办法，该技术得到了最大发展。具有数字序列的公共密钥 K_p 用于加密和解密在发送机和接收机间
20 传送的消息，该公共密钥与一对也称为专用密钥 K_s 的秘密密钥有关。因此，该消息可以通过被一组用户公知的公共密钥加密并使用只被单个接收机所知的密钥解密，或者相反地通过专用密钥 K_s 加密并通过公共密钥解密。通过公共密钥 K_p 加密保证消息的机密性，而通过专用密钥 K_s 加密保证其完整性。

25 该解决办法基于一种思想，即，安全交换或访问安全内容的初始化是基于使用公共密钥 K_p ，保证仅是相关专用密钥 K_s 的持有者能解密该消息，并能验证在安全模式中相关的使用该公共密钥 K_p 的伙伴的标识，因为它是通过认证机构 AUC（“鉴权中心”的缩写）被验证（使用专用密钥 K_s 加密）的。

30 鉴权中心 AUC 保证已知模式中的用户和参与者的数据的机密性的鉴定，

该数据通过在任何给定时间连接的在移动终端和基站之间的无线接口传送。

然而，前面提到的解决办法并不是完全安全的。因为有多个鉴权局，而这些鉴权局验证策略往往不具有相同的安全级，所以鉴权处理的初始化是一薄弱点。一般的用户不知道这一点，也不知道例如接受被某些鉴权局验证过的验证可能是很危险的。

而且，专用密钥 K_s 的存储数据库也是有问题的，特别是在这样的情况下，即可能用户为了接入到保护信息对获知相应的密钥感兴趣。防止内容被复制的保护措施实际必须适应这种情况，即“攻击者”不是来自外界，而典型地是用户本身。现有的解决办法没有考虑到这种可能。

由于安全保护措施失败，现有技术提供一种移动终端的取消策略，但实际上很难实行。

也是作为公知的现有技术，接入到保护信息可以通过例如使用 DRM（“数字权管理”）的接入权。DRM 的基本原理包括提供给用户一个加密内容以及一个用户的许可证。该许可证包括用户权以及使解密该内容成为可能的相关密钥。为了使用户无法得到该通常对称的相关密钥，该许可证可以通过一个使“阻塞”用户读取相关密钥成为可能的信道发送以及传送，或者通过该相关密钥被加密。该当前提出的 DRM 解决办法采用了对称密钥或复对称密钥，这些密钥在终端中需进行复杂的编码。这另外的密钥使加密所述的与许可证相关的密钥或产生一个或几个所述多样化的密钥来加密与许可证相关的密钥成为可能。该过程在终端被执行，来保证与包含在许可证本身内的密钥相同的所述许可证的解密密钥可被终端获知但不被用户获知。

当前有关保护内容的解决办法中，移动终端特定的 IMEI（“国际移动设备标识”）标识码被用于在 SIM 或 USIM（公知的用于第三代网络）卡与移动终端之间建立一个信任模式。理论上，移动终端有一个唯一的 IMEI 码，设计的方法主要是包括通知 SIM 卡一个 IMEI 码，根据该 IMEI 码（U）SIM 卡能有一个信任关系。

这些方法的一个主要的缺点是 IMEI 码不是保密号码。例如，从一个带有芯片卡读取器的 PC 机很容易发送 IMEI 信任码到（U）SIM 卡，这样

在 PC 机和 (U) SIM 卡之间创建一个信任模式。而且, 当前多数移动电话的 IMEI 码很容易改变。因此, 可以修改移动终端的先前不可信赖的 IMEI 码以使用一个信任的 IMEI 代替它。

因此, 安全内容的使用权与移动终端相关而不与用户个体相关。为了
5 能使用户权与用户相关, 在不设置终端保护以防操作的情况下和不能通过 (U) SIM 卡或其他很难破坏的装置被鉴定的情况下, 必须更多地了解 SIM 卡和终端之间的安全手段。

而且, 在 DRM 技术中, 如果一对密钥, 比如所述的一对密钥, 被拒绝或终止, 则终端不能再被使用, 也不会提供重新初始化的方法。另外, 任
10 何成对密钥的拒绝都使对保护内容的假定的检测成为必要, 该保护信息将被提供给终端而在例如因特网上将不再被保护。

发明内容

因此本发明的一个目的是在无线通信终端和 SIM 卡或类似装置之间提供并管理一种信任模式。

15 本发明的另一个目的是通过定义一个使 SIM 卡和终端之间的安全交换成为可能的过程来消除一个或多个现有技术的缺点, 其中移动无线网络的操作者重新设置鉴权, 该过程使得有可能创建一个 SIM 卡或 USIM 卡和可操作的通过网络被鉴定的终端之间的安全的能取消的关系, 该过程也使
20 对于 DRM 技术来说在 SIM 卡或 USIM 卡中安全地保存所述成对密钥成为可能。

为了这个目的, 本发明涉及一种在识别模块和无线终端之间建立和管理一个信任模式的方法, 其特征在于包括:

- 通过所述识别模块的终端鉴权步骤, 所述鉴权步骤通过鉴权装置执行, 在通常所说的初始化步骤或类似步骤时, 或者在通常所说的更新步骤时,
25 所述鉴权装置通过移动无线网络提供给所述识别模块, 或者通过识别模块提供给所述终端;
- 通过所述模块的终端的至少一个特性的控制步骤, 所述的特性指标从所述移动无线网络的安全服务器被预先的通过无线电话发送到所述单元。

30 根据本发明的另一个特征, 当前在识别模块中的所述终端鉴权装置的

持续操作时间由一个确定的终止时间限制，所述鉴权装置包括至少一个鉴权密钥。

根据本发明的另一个特征，所述识别模块是用于第三代网络的 SIM 或 USIM 芯片卡，或者是在存储器中包含代表性的用户数据的等效的卡。

- 5 根据本发明的另一个特征，通过产生鉴权装置，然后通过基于无线终端开始可用鉴权装置由保密交换机制提供该鉴权装置到无线终端，识别模块保持与无线终端的信任关系。

- 因此本发明使得可用保密功能和保密数据在 SIM 或 USIM 卡中的存储以及终端和该卡之间的信任模式的建立成为可能。在电信领域不同的参与者都对促成移动终端和 (U) SIM 卡之间的关系以便所述卡可以提供保密功能有日益增高的要求。这些功能可以是加密功能，电子钱包或者还可以是接入和存储功能。

- 15 根据本发明的另一个特征，按照本发明的方法包括在所述初始化或更新步骤时的产生一个通常所说的信任密钥产生步骤，该步骤至少通过所述识别模块被执行，所述信任密钥被所述模块用来加密至少在识别模块和终端之间的交换数据。

根据本发明的另一个特征，所述鉴权装置的初始化步骤由无线网络主动地在由所述单元或者移动无线网络或者无线终端初始化的密钥被拒绝后、在密钥的有效期终止时或者甚至在识别模块初始化时执行。

- 20 根据另一个特征，所述鉴权步骤特别地包括下面的步骤：
- 在终端中由在终端中存储的至少一个第一鉴权算法中使用在终端存储的至少一个第一鉴权密钥的使用步骤，所述第一密钥有一个由预定的终止时间限定的有效期；
 - 通过识别模块由在识别模块中存储的至少一个第二鉴权算法中使用在识别模块存储的至少一个第二鉴权密钥的使用步骤，所述第二密钥与第一密钥是相同的或互补的，而且与终端是相关的，所述第二密钥有一个由所述预定的终止时间限定的有效期；
 - 识别模块中用来比较通过所述第一和第二算法得到的结果的比较步骤。

根据另一个特征，鉴权步骤包括所述预定终止时间的使用。

- 30 根据另一个特征，所述初始化步骤通过移动无线网络开始并还包

括:

- 通过识别模块产生至少所述第一和第二密钥中的一个;
 - 在识别模块中存储所述第二密钥;
 - 通过识别模块传送所述第一密钥到终端, 所述第一密钥通过使用信任密
- 5 钥来加密。

根据另一个特征, 所述比较步骤在两个应答结果之间进行, 其中一个应答结果通过所述第一算法得出, 存储在终端的存储器中并传送到所述识别模块, 另一个应答结果通过所述第二算法得出并存储在识别模块的存储器中。

- 10 根据另一个特征, 所述第一密钥可以是不对称的专用密钥 K_s ; 所述第二密钥是与第一密钥互补的公共密钥 K_p 。

根据另一个特征, 所述第一密钥可以是对称的, 存储在识别模块的存储器中的所述第二密钥是与第一密钥相同的, 这些密钥组成了一个唯一的对称的鉴权密钥。

- 15 根据另一个特征, 按照本发明的方法包括所述第一和第二密钥的更新步骤, 在所述预定终止之前通过识别模块开始, 所更新步骤包括下面的子步骤:

- 在终端和识别模块之间通过所述第一和第二密钥进行鉴权;
 - 通过识别模块的更新算法, 考虑用来替换至少所述第一和第二密
- 20 中的一个的信息, 产生至少一个被更新的密钥;
- 用于替换所述第二密钥的被更新的密钥被存储在识别模块中;
 - 所述第一密钥的类似的被更新的密钥通过识别模块被传送到终端。

根据另一个特征, 所述更新步骤还包括对终端和/或识别模块的至少一个标识符的控制。

- 25 根据另一个特征, 对第一密钥的类似的被更新的密钥到终端的传送, 执行对密钥的加密, 所述密钥的加密通过所述信任密钥来进行。

根据另一个特征, 更新步骤还包括下面的步骤:

- 在所述终端和单元之间的鉴权之后, 通过识别模块产生新的信任密
- 钥;

- 30 - 在识别模块中存储新的信任密钥;

— 通过识别模块新产生的信任密钥被传送到终端。

根据另一个特征，通过检测验证由终端部分返回的表示在更新步骤期间通过识别模块传送的数据的有效接收的至少一个数据，所述修改步骤被完成。

5 根据另一个特征，所述信任密钥是与所述对称鉴权密钥类似或相同的对称加密/解密密钥。

根据另一个特征，所述信任密钥是可擦除的会话密钥。

根据另一个特征，所述所谓的取消步骤由识别模块、终端、或相应的无线电话网络主动执行，所述取消步骤包括擦除所述识别模块的存储器中
10 与终端相关的至少所述第一密钥。

本发明的另一个目的是通过定义一个实现本发明方法的识别模块，提供对现有技术中遇到的一个或更多问题的解决办法。

该目的通过用于实现本发明方法的终端中的一个识别模块而达到，其特征在于该单元包括用于存储至少一个鉴权密钥以及至少一个鉴权算法的
15 装置，用于执行至少将所述鉴权密钥应用到在识别模块中存储的所述鉴权算法中的步骤的计算装置，通信装置，用于启动一个取消的装置和用于取消所述鉴权密钥的取消装置，用于存储终端的特性指标的装置和用于启动一个更新算法来更新所述鉴权密钥的装置，通信装置能够提供至少一个鉴权密钥到终端，并能够接收通过移动无线电话网络的安全服务器发送的数据。
20 据。

附图的简要说明

本发明的特征和优点在参考附图而理解说明书的基础上将更加明显，而不仅仅局限于实施例，其中：

图 1 表示本发明中实现的初始化过程；

25 图 2 表示按照本发明的方法在识别模块中终端的鉴权；

图 3 表示本发明中实现的用于更新终端和识别模块共用的密钥的方法的一个例子；

图 4 表示现有技术中用于 DRM 技术的操作原理；

图 5 表示现有技术中当在终端和 SIM 卡之间没有建立信任模式时对 DRM
30 来说存在的问题的一个例子。

具体实施方式

特别地，在移动电话领域，主要有三个要素起作用。第一个要素，终端（MS），实现对保密数据的接入、存储和通信功能。第二个要素，识别模块（SIM），使得有可能标识用户和存储保密信息。最后，第三个要素，网络，能通过终端（MS）以安全模式同识别模块通信。在本发明的一个实施例中，识别模块（SIM）是芯片卡，例如是用于第三代网络或类似网络的SIM或USIM卡，在存储器中包括代表用户的数据，还包括微处理器和执行以下特别功能的操作程序。

识别模块（SIM）可以包括这样的通信装置，使识别模块可能同时与终端和网络的安全服务器（SS）通信。可以有一个这样的改变，使用的终端（MS）可以被构造成当终端接收到从安全服务器（SS）发送的将识别模块（SIM）作为目标的专用安全命令分组类型的消息时，能进行相应的工作。例如，安全服务器（SS）可以发送带有通过指示器装置指定的作为目标的模块（SIM）的地址的短消息SMS。可以提供一个目标字段来表明是否该消息应由终端（MS）或模块（SIM）接收。

图4表示当前用于DRM（“数字权管理”）技术的原理的一个例子。对保密内容的存取首先被传送到由授权者定义的用户权的表达式，然后获得该内容的解密密钥。如图4所示，第一步是通过下载操作（E1）装置在内容服务器（S）和移动终端（MS）之间分配加密内容。然后第二步，为了使用该内容的必要的相关许可证通过MMS-C（“多媒体消息服务中心”）被发送（E2）到终端（MS），该许可证带有一个称为“前传锁定”的锁定。该许可证包含用户权和内容的对称解密密钥。依照技术和标准，该许可证可以与内容一起或分别传送到终端。在移动电话领域，终端（MS）鉴权装置一直是薄弱的，不存在用来保护许可证的解决办法。因此，加密密钥不能被保护，对信息的攻击因而是容易的。同样，如图4所示，OMA论坛的一个方案包括在许可证的发送步骤（E2）提供解密码到移动终端（MS）。该方案例如是WAP DOWNLOAD中的内容，其中内容通过第一信道发送而许可证通过另一个信道发送（E2），比如MMS，在理论上防止密钥传送到其他终端。该信道在理论上可能地“阻塞”用户读取密钥以及传送许可证。此类处理过程尤其具有以下缺点：

- 包含在许可证中的密钥被永久保存，并位于终端（MS）的解密码中；
- 许可证仅用于终端（MS），而不用户；
- 保护很容易被破坏，比如使用配备有 GSM/GPRS 调制解调器的 PC 机。

另一个方案包括在移动终端（MS）中通过密钥分类硬编码提供不被用户所知的对称加密密钥。然而，在这第二种方案中，与终端（MS）保持连接的许可证可能被黑客修改。而且，控制密钥的完整性几乎是不可能的，在没有将移动终端（MS）变成不能用的移动终端时使取消不能被执行。

按照本发明的方法使可能识别模块（SIM），比如 SIM 或 USIM 卡，与终端（MS）之间的数据安全交换。为了这个目的，通过所述识别模块（SIM）的终端的一个鉴权步骤以这种方式被执行来验证使用的终端（MS）实质上是信任终端。终端（MS）能通过对称的或不对称的密钥由识别模块（SIM）来标识本身。如果使用对称密钥，该密钥必须被同时保存在终端的存储器和识别模块（SIM）的存储器中。如果使用不对称密钥，也就是至少一个公共密钥 K_p 和至少一个相关的专用密钥 K_s 被使用，仅须专用密钥 K_s 被保存在终端中。公共密钥 K_p 被保存在识别模块（SIM）的存储器中。根据使用不对称密钥的实施例的一个改变，识别模块（SIM）与终端（MS）之间的鉴权过程通过保存在识别模块（SIM）存储器中的一个公共密钥 K_p 和保存在终端（MS）存储器中的相关的一个专用密钥 K_s 来完成。不对称公共密钥 K_p 和不对称专用密钥 K_s 是互补的。该鉴权机构也可以用于初始化期间的整个第一鉴权（23）。可选择地，对第一鉴权过程来说，公共密钥 K_p 和专用密钥 K_s 可以由对称密钥替换。

在本发明的一个实施例中，通过在移动无线网络初始化步骤或更新步骤期间传送的密钥或类似的鉴权装置，至少被提供给识别模块（SIM）。该鉴权装置的传送在安全条件下在网络的初始化阶段被完成，其中通信系统被认为是信任系统，比如，与一个安全 OTA（“在空中接口上”）服务器（SS）保持通信。如图 1 所示，一个或多个鉴权密钥，在安全 OTA 服务器（SS）初始化过程中的密钥初始化请求（20）期间，被最终传送到（21）识别模块（SIM）。至少一个鉴权密钥能够，例如与终端（MS）中存在的密钥相对应。至少一个终端（MS）的特性，例如 IMEI 码或者理论上的终端的最大输出，也通过安全 OTA 服务器（SS）被传送到

(22) 识别模块 (SIM)。所述通过识别模块 (SIM) 的第一终端 (MS) 鉴权步骤, 通过终端 (MS) 的鉴权密钥被完成。该第一鉴权步骤 (23), 伴随着终端 (MS) 的特性, 例如 IMEI 码的控制 (24), 通过识别模块 (SIM) 被完成。这使识别模块 (SIM) 能保证该终端 (MS) 是一个信任终端, 事实上
5 识别模块 (SIM) 应提供解密密钥或类似数据仅仅给它的信任终端 (MS)。在另一个变化的实施例中, 初始化过程可以不使用初始化密钥而实现。

为了使鉴权装置的传送成为可能, 识别模块 (SIM) 必须是“主动的”类型, 换句话说, 必须配备有用来发送命令到终端 (MS) 以便终端执行该命令的装置。而且, “牵引 (pulling)”方式可能被执行, 换句话说, 终端
10 (MS) 将周期性的询问识别模块 (SIM) 来保证识别模块 (SIM) 没有数据发送给终端。

所述信任密钥, 例如可能是清楚和以会话密钥起作用的, 由识别模块 (SIM) 的密钥产生算法产生 (25)。该信任密钥被预定用于终端 (MS) 和识别模块 (SIM), 来加密在识别模块 (SIM) 与终端 (MS) 之间交换的数据。该信任密钥被保存在识别模块 (SIM) 的存储器和终端 (MS) 的存储器
15 中。在密钥更新请求期间, 识别模块 (SIM) 至少产生一个新的鉴权密钥用于下一次在终端 (MS) 和识别模块 (SIM) 之间的鉴权。就不对称密钥来说, 识别模块 (SIM) 在其存储器之一中存储了公共密钥 K_p 后, 发送 (26) 相关的专用密钥 K_s 到终端。该发送 (26) 在新的专用密钥 K_s 使用信任密钥加密的情况下是安全的。在本实施例的一个改变中, 所述信任密
20 钥可以是对称的加密/解密密钥。例如, 其中产生一个对称的鉴权密钥, 信任密钥例如可能是与在鉴权过程中使用的该对称密钥类似的或相同的密钥。在本发明的一个实施例中, 当终端 (MS) 响应于鉴权标准 (23)、控制标准 (24) 或这两个标准 (23, 24), 然后肯定地在存储器中接收到被
25 发送的密钥, 终端可以发送, 例如一个确认消息 (27) 到识别模块 (SIM)。然后, 以类似的方式, 识别模块 (SIM) 发送一个确认消息 (28) 到网络的 OTA 服务器 (SS)。

因此, 如图 1 所示, 网络可以发送一个消息 (20) 到识别模块 (SIM), 通过提供给识别模块一个初始化密钥 (21), 例如是一个对称密
30 钥, 允许识别模块随后鉴权终端 (MS) 和/或加密与终端 (MS) 之间的交

换。然后识别模块 (SIM) 可以通过使用该初始化密钥来初始化一个新的密钥的传送 (23), 以使鉴权终端 (MS) 和/或识别模块 (SIM) 或者加密交换。该初始化也可以由终端 (MS) 的任何特性指标来控制, 比如初始化密钥和终端 (MS) 中的现有初始化证明。而且, 可通过网络被验证的终端 (MS) 的特性, 比如 IMEI 或终端的最大输出, 也可以被传送到模块 (SIM), 以便所述模块可以辅助的控制终端 (MS)。

与初始化步骤相同或类似的重新初始化和再激活的步骤, 显而易见的也可以按照本发明的方法来完成。在本发明的一个实施例中, 所述初始化步骤可以在例如密钥被拒绝之后, 密钥的有效期终止之后或制造中识别模块的初始化期间被执行。

特别地, 鉴权步骤可以包括, 首先, 存储在终端 (MS) 中的一个对称的或不对称的鉴权密钥应用到一个或多个存储在终端 (MS) 中的算法中。以同样的方式, 在识别模块 (SIM) 中, 存储的对称的或不对称的相关密钥, 可以被应用到一个或多个存储在所述识别模块 (SIM) 中的算法中。终端 (MS) 产生的响应, 可以比如被存储在终端中并随后被发送到 (11) 识别模块 (SIM), 如图 2 所示。该响应与识别模块 (SIM) 中同样产生的响应进行比较 (12), 如果响应是对应的, 则终端 (MS) 通过了第一测试, 表明该终端最终可被认为是一个信任终端。如果一个特性指标, 比如 IMEI 的控制 (24), 也确认该终端肯定地是应该“可信的”, 数据的交换 (13) 也可以被实现, 比如仅仅经预定可存取的并通过无线网络发送的内容的交换。在图 2 的示例中, 鉴权步骤可以由识别模块 (SIM) 的一个请求 (10) 开始。在其它实施例中, 鉴权步骤可以由终端 (MS) 开始。

当终端 (MS) 不能用来对付时间上的攻击, 一个密钥的持续工作时间最好应受到限制。如同在终端 (MS) 中, 在识别模块 (SIM) 中一个比较程序被执行, 来比较是否一个密钥的有效期是当前的日期, 以便于如果需要, 可能地进行一个更新。在本发明的一个实施例中, 存储在终端 (MS) 和识别模块 (SIM) 中的密钥的有效期是相对较短的, 通过一个预先确定的终止来限制, 该终止也就是指有效期的终止。这些密钥的一个更新机制, 比如是以规则的间隔, 使得有可能避免与终端 (MS) 在持续时间上的保护有关的问题。

现在本发明将参考图 3 和图 5 进行描述。

更新原理包括利用识别模块 (SIM) 和终端 (MS) 的共同定位。首先, 我们认为识别模块 (SIM) 和终端 (MS) 有一个公共的对称密钥, 使两者的相互鉴权成为可能。在该密钥的有效期终止之前, 终端 (MS) 与识别模块 (SIM) 开始对该密钥的一个更新, 反之亦然。在图 3 的例子中, 由识别模块 (SIM) 发出一个更新请求 (30)。识别模块 (SIM) 然后负责产生一个新的密钥, 即所说的更新密钥, 并存储, 以及传送到终端 (MS)。通过所述模块 (SIM) 的一个更新算法来产生更新密钥, 并考虑比如原来的公共密钥的有效期等信息。在更新期间, 终端 (MS) 和最终所述模块 (SIM) 通过原来的公共密钥鉴权其本身 (31)。在本发明的一个实施例中, 在识别模块 (SIM) 的存储器中更新密钥的存储可以通过简单的仅仅替换原来的密钥而实现。一个终端 (MS) 和/或识别模块 (SIM) 的标识符, 无论是否基于一个验证证明, 都可能被用于该阶段以促进系统的管理以及终端 (MS) 和识别模块 (SIM) 的鉴权。另外, 更新密钥的交换 (33) 通过加密更新密钥来实现。可以通过用于加密的公共密钥的使用, 或通过产生一个会话密钥的方式, 来进行加密, 并在终端 (MS) 和识别模块 (SIM) 之间的所述鉴权之后进行。在这种更新期间, 不进行与网络的交换, 识别模块起到了“证明者”的作用。

在本发明的一个实施例中, 一个所述信任密钥, 比如一个会话密钥或类似密钥, 在识别模块 (SIM) 中产生, 然后该信任密钥被存储在所述模块 (SIM) 的存储器中。所述信任密钥进而被发送到终端 (MS) 并存储在终端 (MS) 中。在另一个改变中, 该密钥同时在终端 (MS) 和识别模块 (SIM) 中产生。当验证检测到终端 (MS) 部分对至少一个通过识别模块 (SIM) 在更新步骤发送的数据的一个发送返回, 或者表示通过识别模块 (SIM) 发送的信息的满意接收的数据, 则更新被完成。比如, 当终端肯定地接收并存储了从识别模块 (SIM) 发送 (33) 来的所述更新密钥时, 它发送给识别模块 (SIM) 一个确认消息 (34)。

根据本发明的方法, 保密使比如 DRM 技术中遇到的问题的解决成为可能。图 4 表示在现有技术的方法中, 比如在移动终端和 SIM 卡之间的内容交换期间, 缺少保密措施。首先, 终端 (MS) 仅控制 (E3) SIM 卡支持的信

息的使用规则。然后 SIM 卡发出一个“使用”信息的许可 (E4) 和一个解密密钥传送许可。接下来 SIM 卡发送解码的解密密钥到终端 (MS)。在这种方法中, 理论上通过用户无法接入的数据, 被公开的提供给终端, 比如配备有芯片卡读取器的 PC 机终端。另外, 如果交换过程没有加密, 利用探测器也可能获得对保密数据的了解。根据本发明的方法, 由通过识别模块 (SIM) 的一个真正的终端 (MS) 鉴权步骤和对交换过程的加密, 可保证交换的可靠的保密性, 避免这样的失败。

在本发明的一个实施例中, 可能取消与终端 (MS) 相关的密钥。该密钥可能在识别模块 (SIM) 初始化或网络初始化时被拒绝, 也可能通过终端 (MS) 被拒绝。原理包括在识别模块 (SIM) 中拒绝密钥, 最后使用存储在所述单元 (SIM) 中的程序来通知网络和终端 (MS) 所述拒绝。取消包括至少清除在所述识别模块 (SIM) 的存储器中与终端 (MS) 相关的要被拒绝的密钥。因此, 如果终端 (MS) 要拒绝密钥, 比如在这样的情况下, 其中终端检测到它的 OVERALL SURVIVAL 已经被修改, 它通知识别模块 (SIM) 该拒绝, 识别模块 (SIM) 可以通过分类安全 OTA 机制通知网络。如果网络要拒绝密钥, 比如在这样的情况下, 其中它检测到终端 (MS) 的特性指标, 比如 IMEI 或终端 (MS) 的最大输出理论值已经改变, 网络使用分类安全 OTA 机制通知识别模块 (SIM) 该拒绝。然后, 识别模块 (SIM) 可以通知终端 (MS)。如果识别模块 (SIM) 要拒绝密钥, 它可以通知终端 (MS) 和可能的网络该拒绝。在终端 (MS) 和/或识别模块 (SIM) 中的鉴权密钥和加密的清除是可选择的。从这一点上说, 识别模块 (SIM) 将不再能够鉴权终端 (MS), 重新初始化将是必要的。

在本发明的一个实施例中, 识别模块包括用于存储至少一个鉴权密钥, 一个加密密钥以及至少两个算法的装置。识别模块 (SIM) 也可以包括用于存储加密密钥以及利用终端 (MS) 的加密算法的装置。这些装置可以是比如 EEPROM 存储器, ROM 存储器或这两种存储器的结合。识别模块 (SIM) 还包括用于执行至少将所述鉴权密钥应用到识别模块中存储的算法中的步骤的计算装置, 以及用于启动所述鉴权密钥的一个更新算法的装置。识别模块 (SIM) 还包括用于开始一个取消的装置和用于取消与终端 (MS) 相关的鉴权密钥的取消装置, 用于在存储器中存储终端 (MS) 的特

性指标的装置，以及用于启动一个更新与终端（MS）相关的鉴权密钥的更新算法的装置。另外，在本发明的一个实施例中，识别模块（SIM）也可以对应一个预先激活（主动的）的芯片卡。

取消装置使得有可能或者用来清除包含鉴权密钥的存储器位置，或者
5 定位与该位置相关的一个比特。对后者来说，该比特将对每一个接入到该位置的请求而被系统地读出，根据它的值，接入将被授权（有效密钥）或拒绝（无效密钥）。

在拒绝之后，或密钥的有效期终止，或在初始化期间，密钥的初始化的启动被发送到网络。当网络确定终端是一个信任终端时，网络决定初始化或重新初始化信任模式。网络通过基于比如 GSM03.48 标准提供的机制的
10 分类安全 OTA 机制发送一个消息到识别模块（SIM），表明所述单元（SIM）可以与终端（MS）交换密钥。该消息也可以通过网络发送到其他两个实体（SIM, MS）。在单元（SIM）与终端（MS）之间没有交换保护时初始化或重新启动也可以实现。但是这可能也基于一个初始化密钥的使用，该
15 密钥是终端（MS）中现有的，并通过安全 OTA 方式被提供到识别模块（SIM）。

在本发明中，可以被使用的密钥的数目是不限的。显而易见地，多个密钥可以被使用和产生。因此可以使用一个密钥来鉴权终端（MS），以及使用一个密钥来加密交换，或者每个交换类型都有一个密钥来加密。同
20 样，由不对称密钥的使用来代替对称密钥的使用也是可能的。

按照本发明的方法的一个优点是以一种通用的节约的模式来考虑终端相对于识别模块（SIM）的鉴权的基本问题：在识别模块（SIM）与终端（MS）开始通话时，识别模块（SIM）必须证明该终端肯定地就是它要求的那个终端，它肯定地执行预期的机制。代替基于验证终端的固定不变的机制，该方法提出利用网络作为动态验证手段动态验证终端，因为功能性：
25 如果终端肯定地是识别模块要求的那个终端，必须能成功地通过多个测试，尤其包括在识别模块（SIM）的控制下与该识别模块（SIM）的交换。而得到可以接入安全环境中的鉴权/保密密钥的终端的模拟设备是很难的，因为这需要该终端正确地执行所有测试操作，在实践中这是很难做到的。

30 本发明相对于现有技术的另一个优点，就是即使出现某些不保密终端

(MS)已破坏了前面提到的机制,为了不许可第三者接入保密信息,很容易无效这些终端(MS),因为识别模块(SIM)一直是装置的主要组成部分,网络可以在任何时间发送给它一个无效命令。

5 本发明的另一个优点在于识别模块(SIM)与终端(MS)之间的连接可以用于保护公知的和可修改的用户数据,比如接入用户数据库的“注册”和密码,还可用于存储用户不能修改的数据,比如软件或音乐的用户权。该连接还可以用于存储用户不应该了解的数据,比如存储在执行之前音乐的解密密钥。通过识别模块(SIM)发送到终端(MS)的功能可以是密码功能,电子钱包功能,或者是数据存储和存取功能。

10 本发明有多种应用。因此,在DRM应用中,SIM卡可用于存储用户权和任何信息解密密钥。当终端(MS)请求需要其密钥之一时,可以查询终端(MS)来识别该请求并由SIM卡予以鉴权。从这一点上来说,SIM卡为了授予该终端(MS)可信,可以对每个请求控制密钥的用户权,然后发送需要的密钥到该请求。密钥的传送可以通过使用会话密钥,或使用专为此目的提供的密钥,或使用加密密钥来进行加密。

15 显而易见的对本领域技术人员来说,本发明允许实施例在本发明权利要求所请求的保护范围内有其他多种特定形式。因此,现有的实施例作为示例而可以在权利要求的范围所确定的领域内进行修改,本发明不局限于上述细节描述。

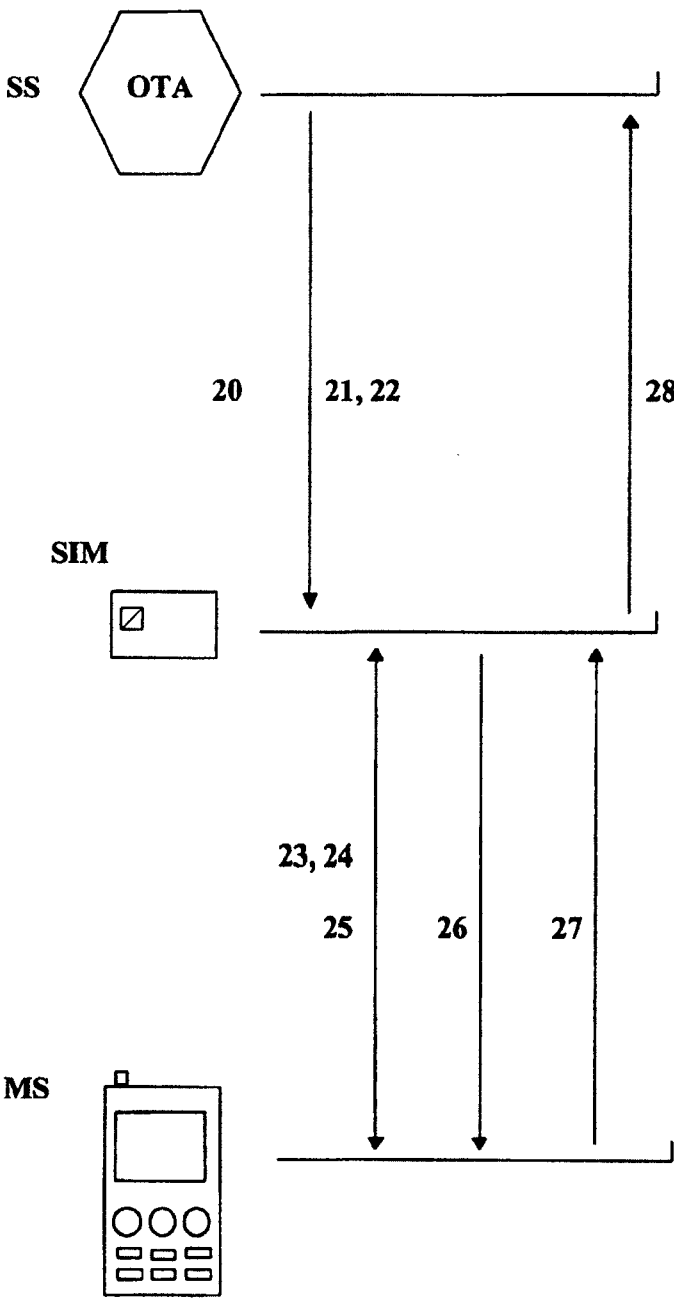


图1

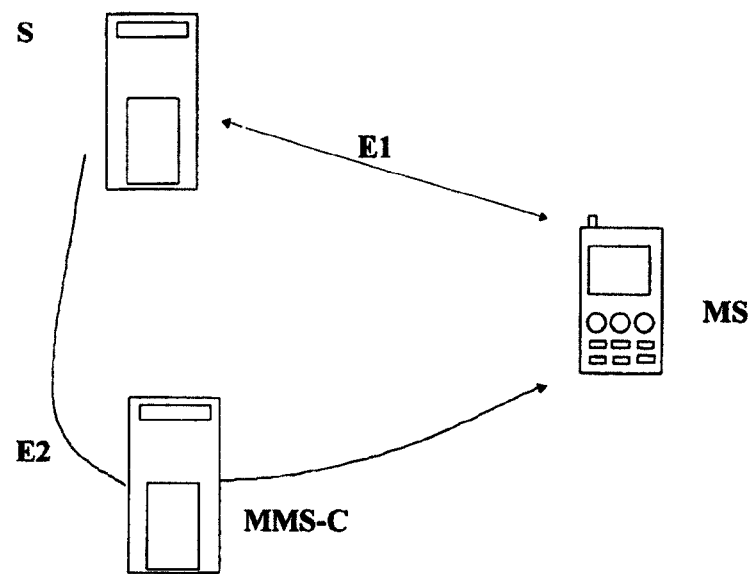


图 4

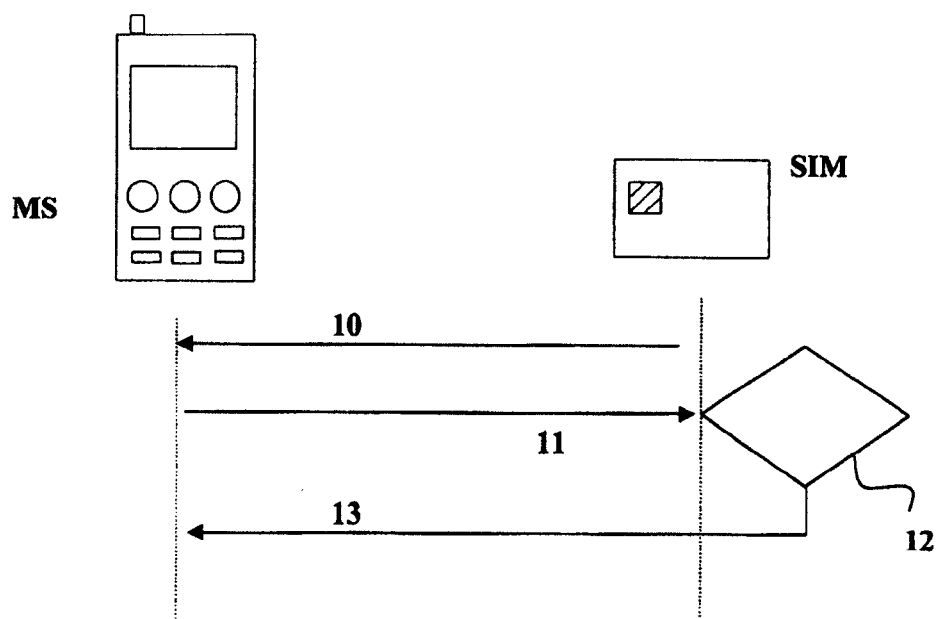


图 2

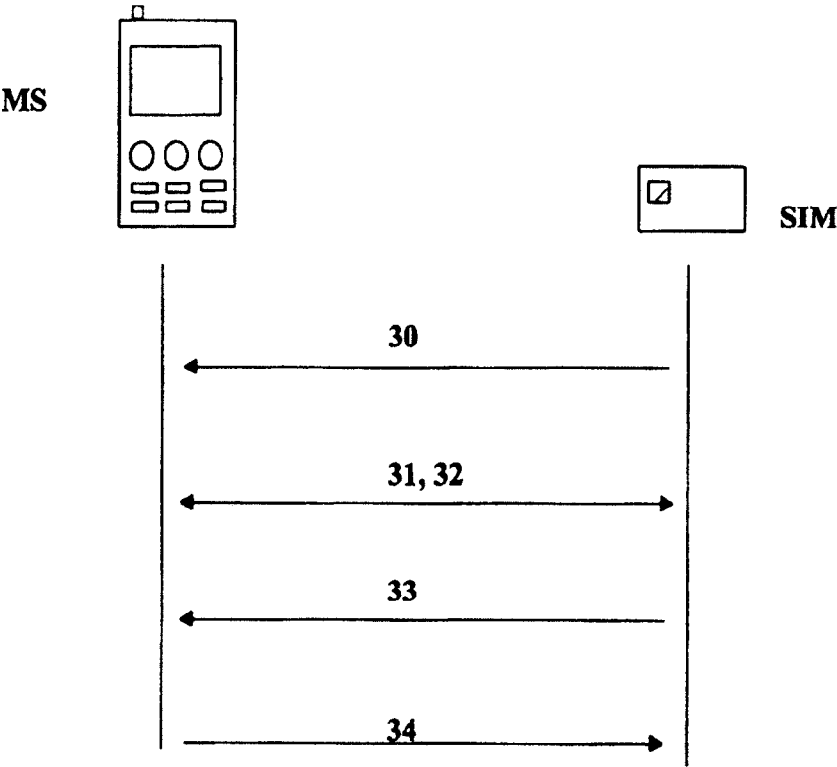


图 3

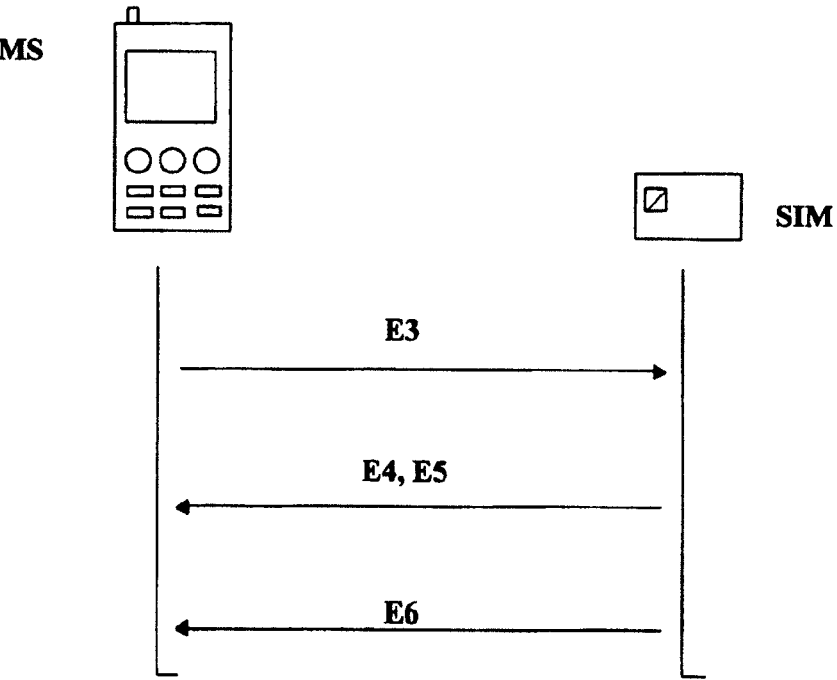


图 5