[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G07F 19/00 (2006.01)
G07F 7/08 (2006.01)
H04Q 7/38 (2006.01)

[12] 发明专利说明书

专利号 ZL 02805204.8

[45] 授权公告日 2008 年 10 月 1 日

[11] 授权公告号 CN 100423030C

[22] 申请日 2002.5.28 [21] 申请号 02805204.8

[30] 优先权

[32] 2001. 6. 1 [33] FR [31] 01/07286

[86] 国际申请 PCT/FR2002/001799 2002.5.28

[87] 国际公布 WO2002/097751 法 2002.12.5

[85] 进入国家阶段日期 2003.8.20

[73] 专利权人 法国无线电话公司

地址 法国巴黎

[72] 发明人 吉恩·菲利普·万瑞

丹尼尔·阿尼森德

[56] 参考文献

EP1014317A 2000.6.28

CN1248367A 2000.3.22

WO9901848A1 1999.1.14

WO9852151A1 1998.11.19

审查员 王屹东

[74] 专利代理机构 北京集佳知识产权代理有限公司

代理人 王学强

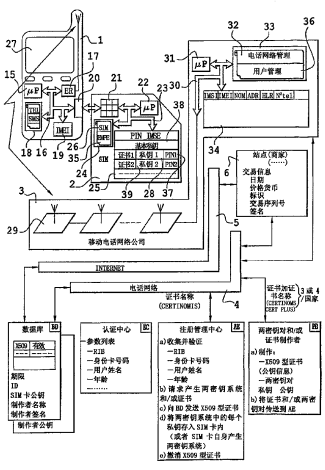
权利要求书 3 页 说明书 12 页 附图 2 页

[54] 发明名称

交易认证的方法和装置

[57] 摘要

采用在移动电话(1)中直接无效用于签署和/或发送关于待被证实的交易的证书的子程序(26)，而解决延时得到对公共数据库(BD)中一个 X509 型证书进行实时撤消和无效的问题。 已经表明这种操作可以在信号通知或者撤消请求发出十分钟之内实现无效，而采用通常管理信道(AE，PB)需要 24 到 48 个小时。



1.一种移动电话内移动电话用户和交易伙伴之间的认证方法,其中,制订该用户和该交易伙伴之间的交易消息,通过签署和认证算法签署该消息,其特征在于,为授权对实时交易的撤消,通过在移动电话内使要被验证的交易证书的签署和/或发送的方法无效,而使得该交易消息不能被正确签署和/或正确发送。

2.如权利要求1的方法,其中:

所述制订(7)用户(1)和交易伙伴(6)之间的交易消息的步骤进一步包括,

利用用户的私钥(28)签署(8)该交易消息,该私钥存储(2)在用户的移动电话内,

将所签署的交易消息发送(9)到交易伙伴,

该交易伙伴必须获得(10)与用户相对应的公钥,且

该交易伙伴必须验证(12)采用对应公钥所签署的交易消息,

其中,所述使要被验证的交易证书的签署和/或发送的方法无效包括无效对保存在移动电话中的私钥的使用。

3.如权利要求2所述的方法,其特征在于,为无效对所述私钥的使用,

对移动电话SIM卡内的私钥的地址进行修改。

4.如权利要求2或3所述的方法,其特征在于,为无效对所述私钥的使用,

改变移动电话SIM卡内的私钥。

5.如权利要求4所述的方法,其特征在于,为无效对所述私钥的使用,

对移动电话SIM卡内的或者移动电话程序存储器内的签署算

法进行修改。

6. 如权利要求5所述的方法,其特征在于,为无效对所述私钥的使用,

对移动电话SIM卡或者移动电话程序存储器内签署算法的至少一条指令的地址进行修改。

7. 如权利要求6所述的方法,其特征在于,为无效对所述私钥的使用,

使该私钥与有效性标记相匹配,且对该标记的值进行修改。

8. 如权利要求7所述的方法,其特征在于,

在移动电话中,数据库一接收到撤销命令后(36),就使该交易消息不能被正确签署和/或者正确发送。

9. 如权利要求8所述的方法,其特征在于,

在移动电话中,通过在其中提示对该移动电话首次联接网络的修改或在重新定位期间修改,使该交易消息不能被正确签署和/或正确发送。

10. 如权利要求9所述的方法,其特征在于,

所述使要被验证的交易证书的签署和/或发送的方法无效的步骤包括:

操作者向移动电话发送预防消息,

在移动电话内验证有关该操作者发送预防消息的权利(37),并且

如果该权利许可,则执行相应预防消息的预防算法。

11. 如权利要求10所述的方法,其特征在于

所述操作者为移动电话的操作者。

12. 如权利要求10所述的方法,其特征在于,

通过发送由SMS传送的预防消息实现移动电话内的预防操作。

13．如权利要求12所述的方法，其特征在于，

使移动电话发送消息，根据该消息该交易不可能进行。

14．如权利要求13所述的方法，其特征在于，

通过网络的远程传输，在移动电话内形成证书、相应此证书的私钥、以及管理认证密钥的记录。

15．一种认证交易信息的装置，包括：

移动电话（1），配有秘存（25），

处理用微处理器（22），以及

程序存储器（24），包含算法（26），该算法利用存储在秘存中的私钥（28）对该交易消息进行签署，以及用于发送所签署交易消息的子程序（26），

其中，该认证装置包括：

用于使所述签署和/或发送错误的装置（35）。

16．一种如权利要求15所述的装置，其特征在于，所述装置（35）包括用于执行无效子程序的无效装置。

17．一种如权利要求16所述的装置，其特征在于，该无效子程序包括由存储在秘存中的管理密钥（37）制约的验证操作。

交易认证的方法和装置

技术领域

本发明旨在提供一种交易认证的方法和装置。设计本发明主要用于各种移动电话（GSM，GPRS，UMTS 等），以实现对移动电话用户和交易伙伴之间交易的管理。

背景技术

公知的交易是那些涉及购买和出售的交易。然而，也可以将对交易伙伴的信息传输以及委托交易伙伴确定传输给他的信息真假的任务视为一个交易。也可以考虑在访问控制的框架下应用本发明；此时，交易是由一个访问许可请求而产生的。为简单起见，本发明将以销售操作为背景而给予说明，这是因为销售操作真实代表在这种交易过程中可能出现的各种问题。然而，本发明涉及各种交易。

进行购买交易，特别是进行互连网购买时，诸如一个移动电话用户的购买者，连接到一个互连网址，特别地在无线应用协议（WAP）会话中。在此会话过程，他准备同交易伙伴，即商品或者服务的供应商，进行一个交易，该供应商提供商品或者服务在因特网网站上出售。一个交易不可避免地包括交易信息的制定。此信息可由交易中的任一个执行者，移动电话的用户或者他正在通话的交易伙伴，制作并发布。无论何种情况，此交易伙伴，当然，不仅指自然人或者法人，而且也指计算机类型的装置，以连接到用户移动电话并且对于交易信息的本质达成共同协议。在进行销售时，交易信息必须包括某种必要信息项。通常这些信息项为日期、交易价格、货币、物品标识、交易序列号以及购入方名称。最后交易包括得到购买的货物或者服务，并因此而支付运送费用。

就其机密性而言，必须确保交易信息的安全。一种可能的保证交易安全的方式是采用对称加密算法。另外一种可能保证交易安全的方式是

采用非对称密钥加密算法或者两密钥加密算法，即采用一个私钥用于签署信息和一个公钥用于验证所签署交易信息的可靠性。由于采用签署交易信息的数字签名技术，两个表示有效确保交易安全的基本参数首先涉及交易的不可否认性，其次，涉及通过对信息内容进行加密从而许可的保密性。图 1 所示为对应于签署这种交易所采用的方法步骤，而图 2 所示为实现如图 1 所示方法所需的装置。

用于制作并输出交易信息的装置（图 2）包括一个移动电话 1，优选地对移动电话安装一个智能卡 2（优选为 SIM（用户身份识别模块）卡或者用于第三代移动网络的USIM卡)并且使其能够链接到移动电话网络3。SIM 卡是一种智能卡，其芯片包括移动电话用户的签名以及签别信息。移动电话网络 3 可以通过一种传统交换电话网络 4，或者通过因特网 5 而与商家站点 6 连接，通常附加由移动电话 1 用户正在通话的交易伙伴的地址。站点 6 优选地是一个因特网网址，但是并不是强制的。可以设想一种小型终端型站点。移动电话 1 和/或站点 6 包括在第一步骤 7（图 1）中制作和输出交易信息的装置。然后在步骤 8 中，移动电话 1 确保交易信息的安全。特别地通过采用存储在移动电话 1 秘存中的一个密钥，特别地该秘存包含在 SIM2 中，发布方签署该交易信息。

然后，在步骤 9 中移动电话 1 将所签署的信息传送到站点 6。该站点然后对所收到的交易信息执行验证其一致性和可靠性的操作。该验证步骤必须采用发布方的公钥。该密钥通常采用数字证书的形式（例如 X509 型）。在步骤 10 中参考密钥数据库执行了对此证书的提供或者恢复。

实际交易中，设置一个非对称型的认证系统需要几个组织或者机构对公钥和密钥管理行为的一致性。

首先，一个标准设定或者规范组织类型的认证中心(EC)，定义认证的条件。特别地，对于支付信息，认证中心 EC 确定交易信息必须包括的参数表，例如，银行帐户细节(RIB)，身份卡号码，不同用户的姓氏和名字，他们的年龄和其他特点。该标准设定认证中心 EC 规定了注册管理中

心(AE)的工作条件。这些注册管理中心负责以下各种操作。

首先，a)，他们负责根据认证中心所产生的参量列表，收集并验证必须在证书中出现的信息。

其次，b)，这些注册管理中心 AE 负责请求产生一个电子证书（优选地一个 X509.V3 或者 V4 型证书）。可能存在两种情况：

一种情况是：在 SIM 卡中已存在一个两密钥对，可通过对此卡进行读取而提取公钥，

另外一种情况是：需要产生此两密钥对，此时，可以由 SIM 卡自身产生此两密钥对（优选地，采用这种方法可以使用户私钥得到限制），然后此私钥使所产生公钥有效（可在外部总线读取）。另外，注册管理中心 AE 可以产生一个两密钥算法并将其安装在 SIM 卡中。然而，这种方案对于确保安全问题是较不充分的。

第三，c)，注册管理中心 AE 负责向一个数据库 BD 管理组织发送已请求并得到的证书。然后，机构 AE 能够将该已收集的识别数据与证书之内的用户的公钥联系起来。

第四，d)，注册管理中心 AE 将两密钥系统中的每个私钥存入在一个 SIM 卡内的某一个位置，在该位置不能对此私钥进行读取也不能将其显示在移动电话 1 的外部总线。作为本发明的另一种变换，SIM 卡自身可以产生两密钥系统并将私钥记录在 SIM 卡中，前提是其程序存储器中存储实现这种功能的程序。用户可通过从 SIM 卡或者移动电话的安全区对此证书下载而直接获得其证书，或者通过采用一个逻辑方法而间接获得，该方法是通过在 SIM 卡中设置一个因特网网址（URL），而不是证书的值而实现。该 URL 直接指向数据库(BD)字段。选择此方法的优势在于对于证书管理提供了更大灵活性。

第五，e)，注册管理中心 AE 负责撤消用户已请求不能被采用的 X509 证书。这种撤消可以因交易原因，或者因 SIM 卡和/或移动电话 1 被偷等简单原因而请求执行。

通常任何使用者均可通过因特网对数据库 BD 进行读取，但是只有注册管理中心 AE 可通过采用电话网络 4 的专用链接对其进行读/写操作。将证书记录在数据库 BD 中。每个证书的记录包括一个与有效性标记相匹配的证书，例如一个 X509 型的证书。此证书只要没有经注册管理中心 AE 撤消即是有效的。为产生该证书，注册管理中心 AE 与证书和/或两密钥对的制作者(CE/PB)通信。a) 此类证书的制作者 PB 制作一个 X509 证书以及，可能地，包括一个私钥和一个公钥的两密钥对。b) 此外这种制作者(PB)负责将该证书和/或者两密钥对传送到注册管理中心 AE。所有这些制作和传送过程都是高度安全的。

在实际操作中，一个完全未加密的证书包括一个时间期限形式的证书有效性标识以及一段鉴别用户身份的信息，该信息通常为用户的姓名，可能还包括其地址。该证书也包括 SIM 卡的公钥（当两密钥对的私钥，就其自身来说，已经被安装到 SIM 卡 2 的保密区）。该 X509 证书还包括证书制作者 PB 的名称以及此制作者对证书的签名。此签名是一个数字序列，实际上是一串由认证者的私钥所加密的二进制码序列。为验证证书的一致性，数据库 BD 或者另一数据库在处理认证者过程中设置一公钥，以实现该验证。

因此，验证所签署的交易信息的步骤 10 可以不经历过多的困难而完成。为实现此目标，该签署的交易信息包括证书制作者 PB 的

参考资料以及移动电话 1 的用户身份。因此，站点 6 可以访问数据库 BD，或者至少可以访问相关两密钥制作者 PB 的数据库的子段。在此过程中，站点 6 可能根据所知晓的用户名在此数据库中检索 X509 证书。在接收此请求时，在步骤 11 中，数据库 BD 将所请求的证书发送到站点 6。站点 6 可以进一步验证该证书的一致性。

此外，特别地由于站点 6 参与交易信息 7 的制作，所以首先知晓交易。其次，由于移动电话 1 将所签署的交易信息传输到站点 6，而使站点 6 获知此信息。因此，站点 6 在步骤 12 中，对此交易制作了一个数字签

章。通过单向散列函数可得到例如 MD5 或者 SHA.1 型的签章。在步骤 13 中，站点 6 验证按上述方法而计算出的签章是否对应所接收到的已签名的交易信息。通过利用用户公钥解密签名可实现此验证过程。如果此解密的结果与步骤 12 中所计算出的数字签章一致，站点 6 将随之验证该签名是否真正与交易信息相关以及用户是否是其真实的信源。如果此验证是决定性的，站点 6 将提示交易确认 14。此交易确认信息，在访问受控的情况，可使移动电话的用户能够对一个被保护的地点进行访问。此确认也可以在传送信息时不被干扰地采用所传送的信息。当进行销售时，此确认引起一个计数器的物理开始（在约定地点），该计数器用于使移动电话 1 用户在此交易中所得到的货物或者服务有效，并且更普遍地将这些货物或者服务传递给他。

因此设计此安全程序用以防止虚假交易，特别地可防止利用失窃移动电话而进行欺诈交易。在实际上，当用户的移动电话被偷盗或者当他希望不再使用一个证书时(例如由于注册管理中心 AE 与他刚刚终止关系的一个银行关系密切)，他要求注册管理中心 AE 撤消数据库 BD 中的相关 X509 证书。这样，所有对应此撤消证书而起动所有交易都将在步骤 13 中失败，并且最终中止交易。然而，这种撤消要承受实时过程中的低效率的缺点。实际上，不论所涉及的机构是位于相同的国家还是不同的国家，或者甚至在不同于站点 6 管理者服务器所处的国家，证书的撤消都需要 24 到 28 个小时。

此外，网络 4 特别是网络 5 的拥挤会引起通信困难和其他的问题。例如，在步骤 10 中，由于网络的临时拥挤而不能访问数据库 BD。由于同样的原因，也可能发生无法传送包括有撤消公钥的证书（或者尽管在数据库 BD 没有更新前已撤消此证书，但是仍以一个有效状态而传送此证书)。这样随之发生交易伙伴的安全被暂时剥夺，暂时无法获得，并且接受所提出的交易。然后该交易者完全由其自身而招致被欺骗的风险。因此，实时撤消问题成为必须解决的一个严重问题。

发明内容

本发明通过实时或者近乎实时地使移动电话不能正确签署交易信息或者发送任何所签署的交易信息，而解决目前不能够解决的实时撤消问题。此方法极大地增加了交易认证操作的保密性。为达到此目标，通过使网络 3 的移动电话操作者进行向移动电话 1，特别是向 SIM 卡 2 发送一条信息的服务而实现实时预防性操作。此信息的目的在于使定义在用户 SIM 卡中的私钥的正确使用无效。此信息可以使 SIM 卡 2 失去正确使用私钥进行解码的方法。这些正确使用的方法将在不同的阶段发挥作用，即限制一个正确签署信息的产生或者限制正确签署信息的传送。通过采用这种方式，在本发明中，从第 8 步开始或者第 9 步开始以下的交易过程将停止。或者通过移动电话的用户 1 通知移动电话网络 3 的操作者，或者通过数据库 BD 通知上述操作者都可以激活这种实时干预。无论在何种情况，不访问数据库 BD 都不会导致确认一不希望的交易并由此导致取消或者撤消该交易的情况。

本发明所提供方法的另外一个优点在于交易的电子签名和认证有效性的参考系统之间的完全异步性。

本发明的一个目标在于提供移动电话用户和交易伙伴之间的移动电话内的一种认证方法，其中制订该用户和交易伙伴之间的交易信息，此信息由签名方法和鉴别算法签署，其中，为授权该实时交易的撤消，在移动电话内通过使即将验证的交易证书的签署和传送方法无效，而使该交易信息不能被正确签署或者正确传送。

另外，本发明的方法不依赖于用于制作数字签名的加密技术，因此可以被应用于保密密钥技术（对称加密算法）或者两密钥（非对称密钥和非对称加密算法）技术。

因此，本发明的一个目标是提供移动电话和交易伙伴之间的移动电话内的一种交易认证方法，包括如下步骤：

制订用户和交易伙伴之间的交易信息，

采用用户的私钥签署该交易信息，此私钥存储在用户的移动电话之中，

将签署的交易信息传送到交易伙伴，

交易伙伴必须取得对应于该用户的公钥，

交易伙伴必须验证由相应的公钥而签署的交易信息，

其中，为实时授权一个交易的撤消，包括如下步骤：

通过无效存储在移动电话中私钥的使用，使得在移动电话中该交易信息不能被正确地签署和/或者正确地发送。

本发明的另外一个目标也提供一个交易信息认证的装置，包括：

配置一密存的一个移动电话，

一个微处理器，以及

一个程序存储器，包含用于签署存储在密存中的私钥的算法，以及用于传送所签署信息的子程序，

其中，该装置包括：

用于制作签名和/或者交易错误的装置。

附图说明

结合以下说明和附图可以更加清晰地理解本发明。提供这些附图完全是用以说明，无论从哪个角度都不应理解为对本发明的限制。

图 1，在以上内容中已提及，所示为相应于现有技术的认证过程的步骤；

图 2 所示为用于实现相应于现有技术的认证并且执行本发明的认证撤消过程的装置。

具体实施方式

图 2 所示的移动电话 1 能够用于实现本发明的方法。该移动电话 1 传统上包括一个微处理器(μP)15，通过数据、地址以及控制总线 16 而与

传送/接收线路(ER)17、程序存储器 18、以及一个数据存储器 19 链接。总线 16 也与接口 20（实际上是一个连接装置）相连，该接口 20 通过连接装置 21 建立与智能卡 2，特别是 SIM 型卡的连接。采用相同的方式，智能卡 2 的芯片包括一个微处理器(μP)22，微处理器 22 通过与总线 16 相同类型的总线 23 而与程序存储器 24 以及数据存储器 25 连接。微处理器 22 能够执行存储在程序存储器 24 中的一个子程序 26，在此称为 SIM。SIM 子程序是一个典型程序，特别地在移动电话 1 与移动电话网络 3 的首次连接过程中，用于请求键入使用移动电话的个人身份号码(PIN)，并且将国际移动用户身份号码 (IMSI)传送到操作者业务。将该 PIN 和 IMSI 信息保存在存储器 25 的秘区。特别地为了使用户不能够在移动电话 1 的屏幕 27 上察看这些信息，用户不能对这些秘区进行访问。

在签署交易的情况下，子程序 26 还包括一个加密算法。该加密算法采用一个存储在存储器 25 中的私钥 28 签署一个数字签章或者一条交易信息。交易信息根据屏幕 27 所显示的项目制订，并且该项目特别地是通过网络 3 和因特网 5 而与站点 6 交换信息过程中进行协商的目标。此外，该交易信息本身可由站点 6 通过采用如上述的地址的私钥而签署。实际上，交易信息也可来自因特网 5。然而，优选地由网络 3 和网络 4 将所签署的交易信息送达到站点 6。

在用户的首次连接过程中，特别地，当此用户重新连接其移动电话 1 的电池时，网络 3 接收到由移动电话 1 发送并由基站 29 之一接收的信令消息。在经过对移动网络的访问控制阶段之后(通过特别采用 SIM 卡中的一条秘密数据，而执行对网络固有用户进行鉴别的方法)，认为用户已被定位。从此刻开始，用户可以通过他的移动电话与外部(通过电话呼叫方式)或者与网络本身(例如通过 SMS(短信息业务)流方式)通信。

只要定位了用户(在激活移动电话或者退出一个信道等之后)，电话网络能够与移动电话和 SIM 卡以及用户通信，并且可独立于用户的操作而实现。特别地，当设置了一个语音或者“数据”(数据传输)呼叫之后，移

动电话能够接收到 SMS。

实际上，该基站 29 通过总线 30 的方式向处理器(μP)31 传送这些信令信号，该处理器 31 执行存储在程序存储器 33 中的电话网络管理程序 32。在操作器业务的数据存储器 34 中，程序 32 产生各种记录，这些记录在用户的 IMSI 号码，以及可能其移动电话号码(IMEI)，该用户的姓名(NOM)，其地址(ADR)(以便根据他所使用的连接时间向他发送发票)，其移动电话的位置(HLR)，及其移动电话号码(N^0tel)之间建立通信。其他信息可被引入存储器 34 的一条记录中的通信。地址 HLR 可用于识别基站 29，该基站将移动电话 1 和网络 3 链接起来。电话号码用于，特别地通过网络 4，发送从外部对该号码进行的移动电话呼叫。

相应于本发明，移动电话 1，更严格地说为 SIM 卡 2，具有使交易信息不能被正确地签署和/或者传送的装置。例如，这些预防装置包括一个子程序 35(EMPE)，以使签名或者传送不能正确进行。子程序 35 优选地存储在程序存储器 24 中。可以用各种方式使用该子程序 35。

优选地，在 GSM 型移动电话或者其他类型的电话系统中通过 SMS 消息使 SMS 子程序 35 付诸使用。使用 SMS 型的传送模式构成三类消息：可由 SIM 卡 2 的处理器 22 执行的消息，可由移动电话 1 的处理器 15 执行的消息，可不经过处理而直接存储在数据存储器 19 中的消息。优选地，预防消息(由此也为无效)将为第一类型的消息(当然也可以通过第二类型的消息而启动无效处理)。

该无效处理包括，例如，或者改变私钥 28 或者改变子程序 26 中对应该加密的部分(特别地使有关此私钥的签名失效)，或者另一方面改变子程序 26 中对应发送所签署的交易信息的部分。例如，可以在存储器 25 中改变私钥 28 的值。实际上，通过改变一位二进制编码的值就足以使采用这种私钥的签名与利用被认为与其相对应的公钥而制作的签章校验不再一致，该公钥本应该是站点 6 在数据库 BD(在其被正确更新之前)中提取的。

另外，也可以在子程序 26 中在有关签名算法指令的位置，改变指定提取加密密钥的地址。通过这种方式，可以不需接触该密钥，进而可以完全不受侵犯地保护该密钥。否则，也可以通过改变签名操作中的一个参量，特别地改变一个位移算符或者此算法的一个算术运算而实现。

作为本发明的一个变形，也可以用标记有效性标记标记配合密钥 28，对密钥 28 来说，其这一部分不再需要将其放置在一个不可侵犯区，并且有利地，密钥 28 可以拥有一个特性，即只能将其从第一有效状态不可逆地转换到第二无效状态。因此，子程序 26 的加密算法包括一个基本步骤：通过访问该有效性标记验证即将采用的私有签字密钥是否有效。

可以对算法的指令本身进行所有对私钥 28 而进行的所有修改。特别地，可以采用将会被无效的有效性标记来匹配子程序 26 自身中对应此签名的部分。

以下是本发明所提供方法的实施过程。移动电话 1 的用户与移动电话网络 3 的操作者的通用业务链接。为实现对上述证书的撤消，移动电话 1 的用户也可以直接呼叫向其发放证书的认证实体或者中心 EC。然后认证中心 CE 链接该移动网络的操作者以完成该撤消。如果移动网络的操作者提前已提供必要的技术装置，则认证中心 EC 自身可以在网络自动执行该链接。因此，有可能特别是通过该操作者的代理，来执行一个用户管理程序 36。根据本发明，程序 36 包括一个向移动电话 1 和/或者 SIM 卡 2 发送无效消息的子程序。程序 36 因此包括通过 HLR 信息定位该移动电话连接的基站 29，该移动电话的 IMSI 号码对应于刚刚呼叫的用户的姓名和电话号码。因而特别地通过一个信令信道(特别是采用 SMS 型消息)，子程序 36 将无效方法发送到移动电话 1。由于消息是通过信令信道发送的，因此不对移动电话用户进行专门提醒。然后，将此消息发送到移动电话 1，即使此时该电话处于备用模式。随之将移动电话 1 所接收的无效消息发送到 SIM 卡 2，SIM 卡 2 执行引起希望的无效的子程序 35。

当程序 36 制作并发布信令消息时，如果切断移动电话 1 的连接，特

别地，如果移动电话 1 断电，则 HLR 信息标记移动电话 1 的连接错误。这样网络 3 不能呼叫移动电话 1。这种切断也可能是由于恶劣的接收条件(例如在一个隧道中的一个通路)而引起的临时切断所导致。在重新连接的过程中，移动电话的重新定位提示对存储器 34 中的 HLR 信息进行更新。然后根据适用于本发明的子程序 36 的改变，对 HLR 信息进行更新，以便传送一条已经制定的无效消息。换言之，如果 HLR 信息有效，则发送此无效信息，否则在重新连接或者重新定位过程中，保持无效消，并当 HLR 型信息转变成有效时立即将其发送出去。

为确保移动电话 1 和/或 SIM 卡 2 可以正确地接收该无效信息，此无效消息包括一个接收证实消息。优选地，必须通知内存 34 对该无效消息的有效接收和执行。为达到此目标，优选地采用 SMS 型协议，这是因为这种协议固有地包括一个类似的接收证实消息。

为采取措施以避免不适时的撤消，子程序 35 包括一个对发送无效消息的操作者身份的验证过程。然而此操作者并不一定就是移动电话网络 3 的操作者，而可能是其他类型网络的操作者。例如，可能是用户所通话的银行。因此该无效消息包括必须可由子程序 35 识别的身份密钥。或者同样，该无效消息是由自身加密并且/或者签署，而且一定可由程序 35 而解密并且/或者验证。为实现上述过程，使该私钥的记录 28 与管理密钥 37 的记录，即用于私钥 28 的 PIN1 匹配。此时，子程序 35 读取密钥 37，并且利用密钥 37，解密或者授权执行无效程序，并且无效对应的密钥 28。如果需要的话，可将密钥 37 存储在存储器 19 中，由微处理器 15 执行子程序 35 并且将其存储在程序存储器 18 中。换言之，如果密钥 37 所代表的权利许可则执行对应该预防消息的预防算法。

作为本发明的另外一种变形，不是采用私钥 28 改变签名模式的方法，该无效处理可以有效防止发送移动电话 1 所签署的消息（相应于步骤 9）。在这种情况下，将存储在存储器中 18 的操作移动电话 1 的 TEL 程序的相应部分进行改变(或者等效地使其无效)。作为本发明的一种变形，不是禁

止传送一条正确签署的交易信息，本发明优选地采用发送，当然是错误的消息，但是重要的是该消息，优选以未加密方式表示不能包含交易签名，或者加密密钥已被无效。否则本发明非加密或者编码形式引起发送任何其他消息，该消息能够以未加密或编码方式阻止执行有关正确交易实验的步骤 10 到步骤 13 中的一个步骤，并且如果没有启动步骤 10 到步骤 13 的操作，则至少阻止交易的验证 14。

正是因为对于高度敏感的操作(特别地如购买)，有必要具有一个请求注册管理中心 AE 和两密钥对和证书的制作者 PB 干预的过程，所以在某种情况下，例如对于成本和重要性都较低的交易，这个过程可能显得较麻烦。例如有可能一个私有机构，一个石油公司希望自己对指令和所签署的私钥以及所产生的证书的无效进行管理。在这种情况下，在使用存储在存储器 25 中的基本私钥 38 时，该中心可以提示在存储器 5 中对证书，补充私钥以及无效解密码的记录 39。通常，密钥 39 是由以 JAVA 语言编程的称为 APPLETS 的程序单元而产生的，其能够由存储在 SIM 卡 2 的程序 26 中的虚拟机进行解释，并且使这些更新可以从网络 3 下载。可将这些程序单元自身下载在存储器 24 中。.

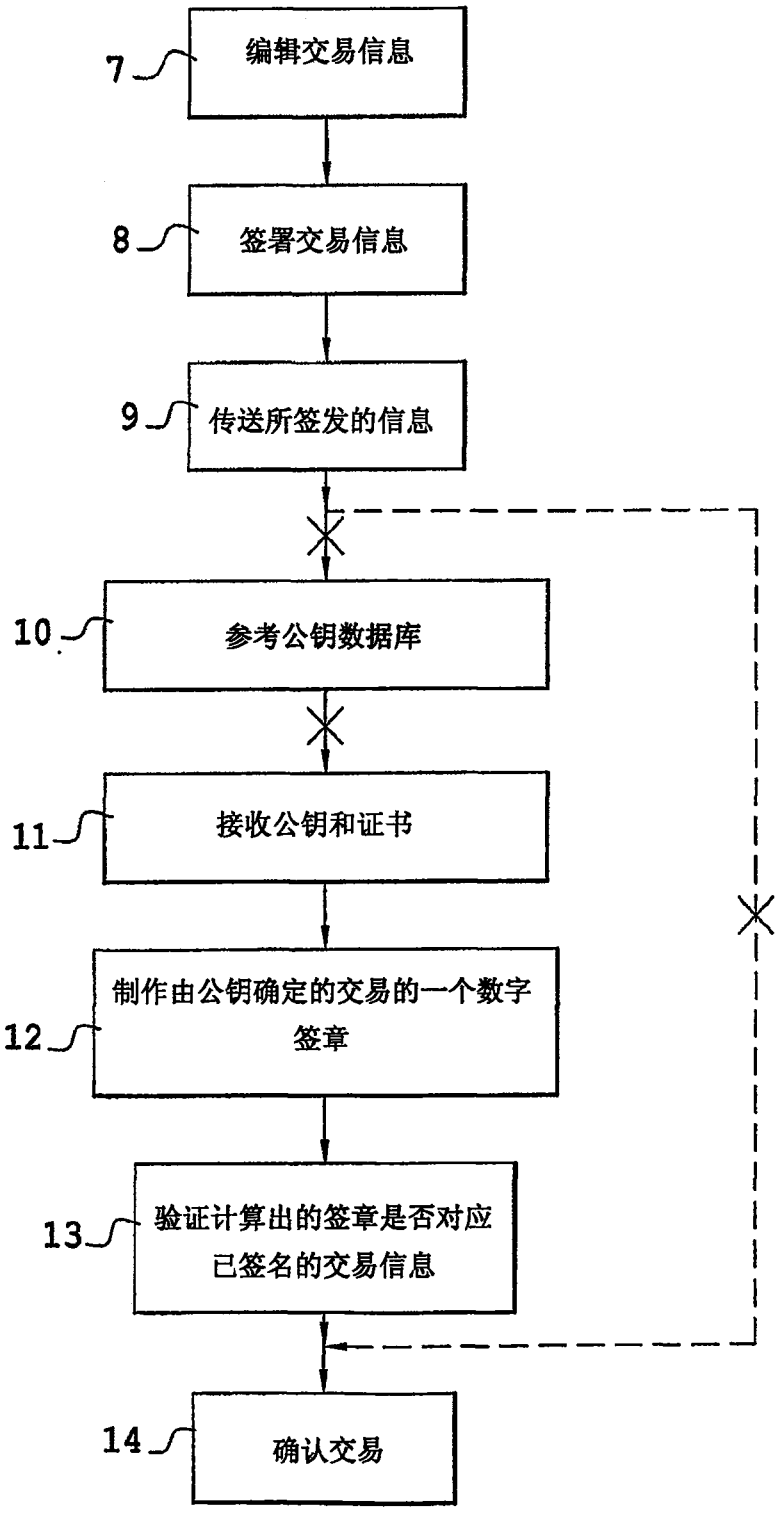

7
编辑交易信息
8
签署交易信息
9
传送所签发的信息
10
参考公钥数据库
11
接收公钥和证书
12
制作由公钥确定的交易的一个数字签章
13
验证计算出的签章是否对应已签名的交易信息
14
确认交易

图 1

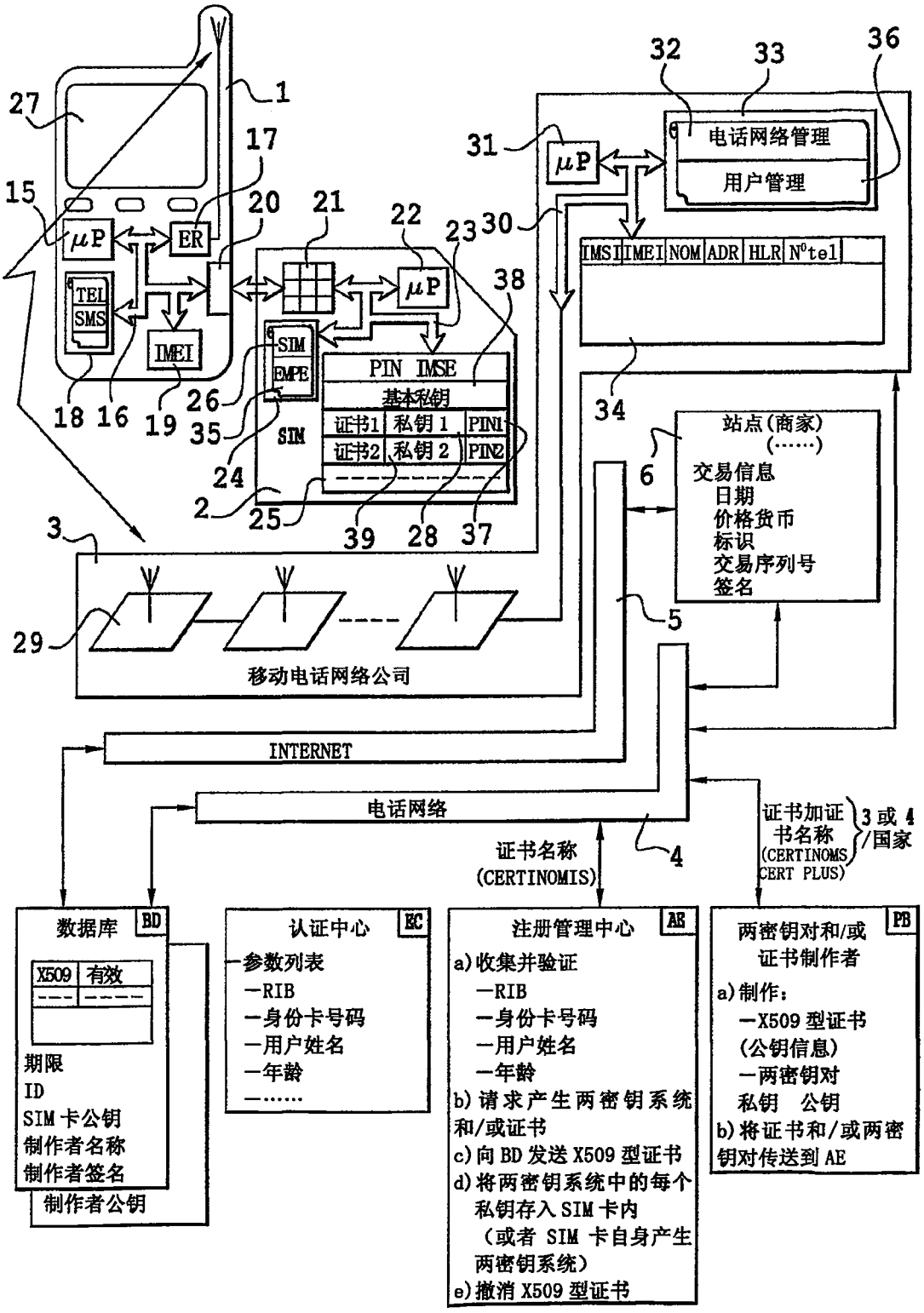

27
1
17
15
20
21
22
23
30
31
32
33
36
38
μP
ER
TEL
SMS
IMEI
SIM
EMPE
PIN IMSE
基本私钥
证书1 私钥1 PIN1
证书2 私钥2 PIN2
SIM
电话网络管理
用户管理
IMSI IMEI NOM ADR HLR N°tel
18 16 19 26 35 24 2 25 39 28 37
34
站点(商家)
(……)
交易信息
日期
价格货币
标识
交易序列号
签名
6
3
29
5
移动电话网络公司
INTERNET
电话网络
证书加证书名称(CERTINOMS CERT PLUS) 3或4/国家
证书名称(CERTINOMIS)
4
数据库 BD
X509 有效
期限
ID
SIM卡公钥
制作者名称
制作者签名
制作者公钥
认证中心 EC
参数列表
—RIB
—身份卡号码
—用户姓名
—年龄
—……
注册管理中心 AE
a)收集并验证
—RIB
—身份卡号码
—用户姓名
—年龄
b)请求产生两密钥系统和/或证书
c)向BD发送X509型证书
d)将两密钥系统中的每个私钥存入SIM卡内
(或者SIM卡自身产生两密钥系统)
e)撤消X509型证书
两密钥对和/或证书制作者 PB
a)制作:
—X509型证书
(公钥信息)
—两密钥对
私钥 公钥
b)将证书和/或两密钥对传送到AE

图 2