[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G07F 7/10

[12] 发明专利说明书

专利号 ZL 01821075.9

[45] 授权公告日 2005 年 12 月 21 日

[11] 授权公告号 CN 1232935C

[22] 申请日 2001.12.19 [21] 申请号 01821075.9
[30] 优先权
[32] 2000.12.22 [33] CH [31] 20002519/00
[86] 国际申请 PCT/IB2001/002603 2001.12.19
[87] 国际公布 WO2002/052515 法 2002.7.4
[85] 进入国家阶段日期 2003.6.20
[71] 专利权人 纳格拉影像股份有限公司
地址 瑞士洛桑
[72] 发明人 让－鲁克·杰奎尔 马克·萨塞尔利
审查员 陈 立

[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 李 强

权利要求书 2 页 说明书 4 页

[54] 发明名称 匹配控制方法

[57] 摘要

本发明的目的在于提供一种方法，该方法通过专用于该对用户单元/安全组件的匹配密钥，来确保安全组件和用户单元之间交换数据的加密，且同时允许该安全组件与其他用户单元配对。依照本发明，此目的通过包含下述步骤的方法来实现：由用户单元检测所连接的安全组件与其是否配对，如果匹配，则使用专用于该对用户单元/安全组件的唯一配对密钥来加密交换数据，如果不匹配，则请求操作中心授权与该安全组件配对，请求附有该用户单元以及该安全组件的标识符，由操作中心来验证该匹配请求的符合度，并且将结果传送到用户单元，如果给予授权，则建立属于该对用户单元/安全组件的配对密钥，以用来加密交换数据。

ISSN1008-4274

1、一种安全组件和用户单元之间的配对管理方法，所述用户单元具有与操作中心进行通信的双向通讯装置，其特征在于：该方法包括：

－由用户单元检测所连接的安全组件与其是否配对，

－如果匹配，则使用专用于该对用户单元/安全组件的唯一配对密钥来加密用户单元与安全组件之间交换的数据，

－如果不匹配，则请求该操作中心授权所述用户单元与该安全组件配对，该请求附有该用户单元以及该安全组件的标识符，

－由操作中心来验证所述配对请求的符合度，并且将结果传送到用户单元，

－如果给予授权，则建立属于该对用户单元/安全组件的配对密钥，以用来加密用户单元与安全组件之间交换的数据。

2、根据权利要求 1 所述的方法，其特征在于：该配对密钥可以是对称密钥，也可以是非对称密钥，或者是一对非对称密钥。

3、根据权利要求 1 或 2 所述的方法，其特征在于：该方法包括：将具有用户单元标识符的配对密钥存储在该安全组件中。

4、根据权利要求 1 所述的方法，其特征在于：该方法包括：将包括所有先前在用户单元与安全组件之间执行的配对数据传送到操作中心，后者通过已授权的用户单元并根据请求次序验证所述安全组件是否已配对。

5、根据权利要求 1 或 2 所述的方法，其特征在于：该配对密钥在该操作中心中产生，且以加密形式被传送到用户单元和该安全组件。

6、根据权利要求 1 或 2 所述的方法，其特征在于：该配对密钥由该用户单元或该安全组件产生，或者由所述用户单元和所述安全组件中的每个部分地产生，由此所述组合形成所述密钥。

7、根据权利要求 1 所述的方法，其特征在于：该用户单元是移动电话，而该安全组件是 SIM 卡。

匹配控制方法

技术领域

本发明涉及一种用户单元和安全组件之间安全信息传送的管理方法，特别是在该安全组件与多个用户单元相互作用期间。

背景技术

这些用户单元与一个或多个提供产品或服务的网络相连。

这些产品或服务需进行有条件的访问，使用这些产品须以任何形式进行支付，例如通过定购或特殊购买。

这些用户单元能以多种形式出现，例如，收费电视解码器、计算机，甚至是移动电话、掌上型电脑、PDA、收音机、电视机、多媒体工作站、自动柜员机。

对于产品或服务，我们理解不仅包括电影、体育消息广播、音乐、计算机程序、游戏、股票市场或新闻信息，而且包括诸如访问及使用网络，识别或电子支付的服务。该产品或服务可以在用户能够连接到其上，并且为安全起见而使用了加密装置的网络上获得。

为了管理使用这些产品或服务的授权，用户单元还包括有设置在安全组件中的安全装置。

该安全组件一般以智能卡、信用卡或微处理器，甚至是包括加密处理器（USIM,WIM）的 SIM 卡的形式出现。通过使用存储在加密处理器的存储器中的密钥的解密操作，该卡允许提供必要的信息，以便授权使用该产品，而这被认为是不可违反的。

该安全组件负责与用户单元交换机密消息，例如，当在收费电视领域中传送产品的解密密钥时，该密钥在安全组件中被解密，并传送到用户单元以处理数据。

这就是为了防止与这些数据干扰，对安全组件和用户单元之间

的通讯装置，由被称为配对密钥的专用于这两个元件的密钥进行解密的原因。这种结构在 PCT/IB99/00821 的申请中描述过，其中专用密钥最初在解码器中，而后在初始化阶段的期间被装入该安全组件。一旦安全组件与解码器相匹配，则此组件就不能在其他任何单元中运行。

此解决方案显现出的第一个不便之处，是其阻止了该安全组件在另外的解码器中任意使用，即使该解码器属于同一用户。此方法的另一个不便之处，是其不能防止使用克隆卡（cloned card），该克隆卡在任一解码器中首次使用后，其就能与此解码器配对。

发明内容

本发明的目的在于提供一种方法，该方法用于确保在安全组件和用户单元之间交换的数据的解密，同时消除了上述的不便之处。

此目的通过安全组件和用户单元之间的配对管理方法来实现，所述用户单元具有与操作中心进行通信的双向通讯装置，其特征在于：该方法包括：

－由用户单元检测所连接的安全组件与其是否配对，

－如果匹配，则使用专用于该对用户单元/安全组件的唯一配对密钥来加密用户单元与安全组件之间交换的数据，

－如果不匹配，则请求该操作中心授权所述用户单元与该安全组件配对，该请求附有该用户单元以及该安全组件的标识符，

－由操作中心来验证所述配对请求的符合度，并且将结果传送到用户单元，

－如果给予授权，则建立属于该对用户单元/安全组件的配对密钥，以用来加密用户单元与安全组件之间交换的数据。

由此，该匹配管理以一种动态的方式来执行，并且不再是用户单元中安全组件连接的结果。其通过操作中心来管理，该操作中心确定是接受还是拒绝此配对。这就是为什么要将该请求，附加上这两个元件的标识符、诸如它们的序列号的数据的原因。该请求能够附加关

于该单元位置、由其他装置所获得的数据，例如其网络上该单元的呼叫号码或者地址。

具体实施方式

对匹配密钥，我们理解为对称或非对称密钥，例如，公共或私有密钥。在后面的情况下，将提出下列三种情况:

－每个部件都包括两个公共和私有密钥。向其他部件的通讯，由公共密钥进行加密，然后由私有密钥进行解密。

－每个部件都包含公共或私有密钥中的一个。在一种倾向中，数据将由公共密钥进行加密，然后由私有密钥进行解密，而在另一种倾向中，数据由私有密钥进行加密，然后由公共密钥进行解密。

－每个部件都包含其他部件的公共密钥以及其自身的私有密钥。数据由其他部件的公共密钥进行加密，而由其自身拥有的私有密钥进行解密。

应该注意到，安全组件能够与多个用户单元进行配对。其存储器具有用于存储一组匹配密钥的分区，每个密钥都与用户单元的识别号相关联。

由此，在用户单元中的这种组件的每个连接过程中，初始协议包括相互识别以及使用专用于该对用户单元/安全组件的密钥（或多个密钥）。

依照一个实施例，用户单元同样能够具有匹配密钥的分区，且由此使得该用户单元能够与多个安全组件配对。

该单一的密钥能够通过多种方法来产生。其能够由该操作中心产生，并以加密的形式，通过匹配授权的情况下传送，以加密的形式被获知。根据公知的程序，使用根据对话密钥而建立的加密，将该密钥传送到安全组件。

获得此专用密钥的另一种方法是在用户单元，或安全组件，或者部分在这些元件中的每一个产生它，且合并后由此形成该密钥。

在本发明方法的一个实施例中，对操作中心的请求不仅附加了

该对用户单元/安全组件的识别数据，而且附加了包含在配对存储器分区中的数据，该存储器分区包括所有先前的配对。

操作中心于是核对该安全组件已经与它已经授权用户的用户单元，并按照请求的顺序配对。

由此，如果安全组件已经被克隆，当此克隆组件需要与用户单元配对时，传送到操作中心、涉及先前匹配的数据，将不同于那些原始组件。为此，该操作中心具有用于识别克隆组件的装置。

首次操作时，操作中心部将接受此克隆卡与新用户单元 B 的配对。如果已经大规模地使用真实卡的克隆，那么下一张克隆卡，该卡具有相同的用户标识符，请求与新的用户单元 C 进行配对，则操作中心部将无法找出先前与用户单元 B 进行匹配的任何痕迹。这种指示将能够检测到欺诈的企图，并且由此而发挥作用。此外，如果该真实卡的用户想在新的单元 D 上使用该卡，那么由此组件传送的配对数据，将不包含单元 C 的任何痕迹，且操作中心将拒绝此次配对，并甚至引起完全阻塞该安全组件。