[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)

[12] 发明专利说明书

专利号 ZL 02827644.2

[45] 授权公告日 2009 年 4 月 8 日

[11] 授权公告号 CN 100477579C

[22] 申请日 2002.11.26 [21] 申请号 02827644.2

[30] 优先权

[32] 2001.11.28 [33] NO [31] 20015812

[86] 国际申请 PCT/NO2002/000446 2002.11.26

[87] 国际公布 WO2003/047161 英 2003.6.5

[85] 进入国家阶段日期 2004.7.28

[73] 专利权人 特伦诺有限公司

地址 挪威福内布

[72] 发明人 L·桑贝里

[56] 参考文献

US6061791A 2000.5.9

CN1319966A 2001.10.31

审查员 庄 湧

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 程天正 陈景峻

权利要求书 3 页 说明书 5 页

[54] 发明名称

用于注册和启用 PKI 功能性的方法

[57] 摘要

本发明公开了一种通过预先打印多个密封的信封来注册和激活 SIM(用户识别模块)卡中的 PKI 功能性的方法，每一个信封包含在未开启时隐藏的激活码和在信封上可见地打印的参考号码或代码。 每个信封的参考号码或代码以及相关的激活码被存储在集成于 PKI 中或连接到 PKI 的安全服务器的表中。 将密封的信封之一和申请表格一起提供给用户。 用户被要求在申请表格上填写参考代码或号码以及个人数据，且这被传送到 PKI 和安全服务器。当注册被 PKI 批准时，批准信息传送到用户，要求他在他的终端中输入激活码。 同时，表中与参考代码或号码相关的激活码以及与用户智能卡相对应的智能卡身份被提供给 PKI 的激活模块。 刚一在终端中输入激活码，激活码就与智能卡身份一起从终端传送至激活模块。 激活模块刚一接收到激活码和智能卡身份，就判定接收的激活码和智能卡身份是否与先前由安全服务器提供的那些匹配，如果匹配，激活模块就执行必要的程序以启用智能卡的 PKI 部分。

1．一种用于可靠并安全地启用移动终端的智能卡的公共密钥基础设施部分的方法，所述移动终端连接到提供对公共密钥基础设施服务器的接入的移动通信网络，其中所述移动终端的用户被提供一个参考号和一个相关的激活码，所述参考号和相关的激活码被存储在由所述公共密钥基础设施服务器访问的表中，该方法的特征在于下述步骤：

a）在公共密钥基础设施服务器以电子的形式接收用于智能卡公共密钥基础设施部分的一个请求，所述请求包括一个参考号；

b）在所述公共密钥基础设施服务器处理所述请求，

c）在所述公共密钥基础设施服务器生成文本消息，该文本消息的文本内容是对处理所述请求的响应，该文本消息被传送到所述移动终端，

d）从所述移动终端接收对发送的文本消息的响应，所述响应包括提供给所述移动终端的所述用户的激活码和与所述移动终端关联的 SIM 卡身份，作为文本消息到公共密钥基础设施服务器；

e）将所述激活码与所述表中的带有在所述请求中接收的参考号的一个关联的激活码相比较，如果两个激活码匹配，就从所述公共密钥基础设施服务器发送消息到所述移动终端，指示匹配，其中所述消息是公共密钥基础设施密钥启用命令。

2．根据权利要求 1 的方法，其特征在于，进一步包括步骤：

f）向所述公共密钥基础设施服务器传送验证公共密钥，

g)所述移动终端的用户被要求在所述移动终端上输入一个自选的 PIN 码，

h）所述公共密钥基础设施服务器连接到颁证机构，颁证机构通过发布具有与所述移动终端用户相关的公共密钥的有效证书来响应，

i）在所述移动终端接收成功认证的确认，其中与所述终端相关的 SIM 卡中的公共密钥基础设施功能被启用。

3．根据权利要求 1 或 2 的方法，其特征在于还进一步包括安全服务器与一个激活模块通信，其中所述安全服务器是以下之一：

所述公共密钥基础设施服务器的完整部分；或

直接与所述公共密钥基础设施服务器相连。

4．根据权利要求 3 的方法，其特征在于还进一步包括所述安全服务器更新带有状态数据的表，所述状态数据根据接收的所述请求，与所述

请求关联。

5. 根据权利要求 4 的方法，其特征在于以电子的形式接收一个请求和处理所述请求还包括:

-在公共密钥基础设施服务器处理的结果被传送到所述安全服务器，所述安全服务器用当前的请求状态更新所述带有状态数据表，

-所述公共密钥基础设施服务器生成文本消息，其中文本消息的文本内容是对处理所述请求的响应，其中当该文本消息被传送到所述移动终端时，所述安全服务器同时传送所述相关的激活码到所述激活模块，所述相关的激活码与智能卡的被请求部分相关。

6. 根据权利要求 5 的方法，其特征在于响应所述文本消息还包括:

-在所述移动终端启用与公共密钥基础设施操纵相关的菜单，

-用户输入一个激活码，所述移动终端将所述输入的激活码和与所述移动终端相关的 SIM 卡身份作为文本消息发送到所述公共密钥基础设施服务器。

7. 根据权利要求 6 的方法，其特征在于比较所述激活码还包括:

-向所述公共密钥基础设施服务器的激活模块部分发送所述输入的激活码和相关的 SIM 卡身份，所述激活模块将所述输入的激活码与所述相关的激活码进行比较，如果两个激活码匹配，激活模块就发送消息到所述移动终端，指示匹配，其中所述消息是公共密钥基础设施密钥启用命令。

8. 根据权利要求 6 的方法，其特征在于发送验证公共密钥还包括:

-向所述公共密钥基础设施服务器的激活模块部分发送验证公共密钥。

9. 根据权利要求 1 的方法，其特征在于，所述通信网络是 GSM 或 3G 网络，所述终端是 GSM 或 3G 移动电话，并且所述智能卡是 SIM 卡。

10. 根据权利要求 9 的方法，其特征在于，所述智能卡身份是 MSISDN 和 ICCID。

11. 根据权利要求 1 的方法，其特征在于，公共密钥基础设施功能存储在所述智能卡中，但是对用户隐藏，直到启用。

12. 根据权利要求 1 的方法，其特征在于，所述文本消息通过 SMS、电子邮件或邮寄来传送。

13. 根据权利要求 2 的方法，其特征在于，所述验证公共密钥作为加

密的文本消息来发送。

用于注册和启用 PKI 功能性的方法

技术领域

本发明涉及 PKI（公共密钥基础设施），尤其涉及在 SIM（用户识别模块）卡中注册和激活 PKI（公共密钥基础设施）功能性。

背景技术

为了充分发挥通信网络的潜在性能，必须存在一种标准化的网络以使用户能够以具有与基于纸件的事务处理相关联的可信度来从事电子事务处理。

由于这个原因，PKI 已经作为全球商业和通信的主要平台而被发展起来。PKI 确保：敏感的电子通信是秘密的并且被保护不被篡改。PKI 用于数字签名、鉴权和加密。

PKI 基于密码学的使用，其意味着通过数学公式和虚拟密钥对信息进行加扰，以使只有使用相关密钥的被授权方才能对其进行解码。PKI 使用由被称作颁证机构（CA）的可信任第三方提供的密码密钥对。PKI 工作的中心是，由 CA 发布用于识别持有者身份的数字证书。CA 保持有效证书的可访问目录，和它已经撤消的证书的列表。

传统地，PKI 功能性由数据终端使用，该数据终端使证书和密钥存储在智能卡中。然而，由于蜂窝电话和数据终端的整合，在电话中也将同样需要 PKI 功能。正常地是将证书和密钥存储在用户卡中，例如，存储在例如用于 GSM 电话的 SIM（用户识别模块）卡中。

对于可信的 PKI 系统，当通过发布数字证书来登记新的用户时，必须存在一个安全的例程。某人必须 100%地确信正请求数字证书的人是他或她所声称的人。这正常地是通过用户本人到办公场所（例如到邮局）现场填写表格，并用如护照等的可信的身份证明标识他自己，而完成的。当邮局柜台的职员已核实该身份证明信息时，数据表格以电子的形式传送到 CA。CA 控制且刷白（whitewash）数据并以 SIM 卡或智能卡的形式连同一个激活码一起发布一个 PKI 卡。现在，将 PKI 卡和激活码以挂号邮件的形式发送给用户。再次地，用户必须本人到邮

局且通过例如他的护照来标识自己，以被允许收取该邮件。

在办公场所的这一两次出现已经成为普及 PKI 的一个问题，这只是因为人们看来对利用有高门槛（意味着必须做出很大的初始努力）的新技术有抵抗性。而且，这个过程自然也是耗费时间的，从用户定下证书到用户得到对 PKI 功能的访问权将至少过去一个星期的时间。

从数字证书发布者的观点来看，发布程序的成本相对较高，尤其是因为挂号邮件的执行和发送。

因此，有必要简化发布过程，以便让发布者和用户都受益。

发明内容

本发明的一个目的在于提供一种消除上述缺点的方法。在所附的权利要求中定义的特征表征了该方法。

更具体地，本发明提供了一种公共密钥基础设施（PKI）的方法，用于注册 PKI 的用户并通过预先打印多个密封的信封来启用用户智能卡的 PKI 部分，每个密封的信封都包含一个在未开启时隐藏的激活码，以及在该信封上可见地打印的参考号码或代码。每个信封的该参考号码或代码和相关激活码存储在集成于 PKI 中或连接到 PKI 的安全服务器的表中。将其中一个密封的信封和申请表格一起提供给用户。要求用户在申请表格上与个人数据一起，填写参考代码或号码，且这被传送到 PKI 和安全服务器。

当注册被 PKI 批准时，发送批准信息到用户，要求他在他的终端中输入激活码。同时，与表中的参考代码或号码相关的激活码和与用户的智能卡相对应的智能卡身份被提供给位于 PKI 中的激活模块。刚一在终端中输入激活码，激活码就和智能卡身份一起从终端传送到激活模块。激活模块刚一接收到激活码和智能卡身份，就判断接收的激活码和智能卡身份是否和先前由安全服务器提供的那些匹配，如果匹配，激活模块就执行必要的过程来启用该智能卡的 PKI 部分。

更确切地，本发明提供了一种用于可靠并安全地启用第一移动终端的智能卡的公共密钥基础设施-PKI-部分的方法，所述移动终端连接到提供对 PKI 服务器访问的移动通信网络，连接到同样网络的是控制机构-CA。本方法进一步由下述步骤定义：在 PKI 服务器处以电子的形式接收对于用户智能卡 PKI 部分的第一请求。所述 PKI 服务器处理所述

请求。PKI 服务器生成一个文本消息，其中该文本消息的文本内容是对处理该第一请求的响应，该文本消息被传送到第一移动终端。第一移动终端通过发送与第一移动终端相关的第二激活码和 SIM 卡身份作为文本消息到 PKI 服务器，来响应接收到的文本消息。PKI 服务器将所述第二激活码与先前接收的第一参考激活码相比较，如果两个激活码匹配，PKI 服务器就发送消息到第一移动终端，指示该口令的匹配，所述消息是 PKI 密钥启用命令。

具体实施方式

现在将通过用户打算为他的 GSM 电话订购具有 PKI 功能性的 SIM 卡的示例实施方案来详细描述本发明。

如前所述，用户必须本人到该用户正预订的被授权的办公场所现

场，例如与邮局、银行，或者是电话运营者。

在被授权的办公场所，用户将收到一个预先打印的密封的信封和一个要求用户填写的申请表格。打印在信封的显著区域上的参考号码标识该信封。用户在办公场所收到的表格和密封的信封彼此唯一地相关联：所提到的参考号码也同样打印在该表格上，或作为要求用户填写的数据之一。

填写完表格之后，办公人员将检查给出的个人信息是否与用户必须产生的身份卡上的那些一致，以及参考号码是否与打印在信封上的号码相对应。如果个人信息和号码没问题，就转发表格到另外的执行过程，同时，将要求用户保存该打开的信封，一直到他收到他新的 SIM 卡为止。

密封的信封包含一个激活码，当信封未开启时该激活码是不可见的。关于所有预先打印的信封的数据存储在例如连接到 PKI 或集成在 PKI 中的安全服务器内的表中。对于每一个信封，至少存储相应的参考号码、激活码和状态，以便一旦安全服务器知道了申请表格的参考号码或代码，它也就知道与申请表格一起给用户的、信封中的激活码，以及该申请当前处于执行的哪个阶段。该状态可以是下述中的一个：未使用、考虑中、已批准、但未激活、已激活、未被批准。初始地，该状态被设定为“未使用”。

转到用户例子中，表格数据优选地以电子的形式被读取，并传送到安全服务器。同时，在表中存储的信封状态从“未使用”变成“考虑中”。表格信息，在该例子中应该被认为是对 PKI SIM 卡的申请，在 CA 的控制下被 PKI 服务器以一种被普通技术人员熟知的、按照现有技术水平的方式执行。此外，信封的状态将会根据执行的结果而在安全服务器中改变。如果申请被拒绝，则相应的状态改为“未被批准”。相反，如果申请被批准，则相应的状态自然地改为“已批准”。

申请执行的结果然后将通过通信网络以消息发送到用户，优选地是通过 SMS 等载送，以及可替代地是电子邮件或邮寄来载送。新的 SIM 卡可以发送给用户，但不必使用挂号邮件，因为用户将能够通过使用隐藏在信封中的激活码来证明他的身份。可选择地，如果用户已经具有安装了 PKI 功能性的 SIM 卡，但迄今为止还不可访问，则将不必发布新的 SIM 卡。同时，安全服务器将向激活模块提供与参考号码或代

码相关的激活码和有关该相应的SIM卡的必要身份信息。

代表肯定结果的消息将例如读为，“您的申请已被批准，请打开密封的信封并将里面的激活码使用在你的SIM卡上”。

然而，在用户可输入激活码之前，必须启用一个“SIM PKI菜单”。当启用了“SIM PKI菜单”时，用户在他的手持装置中输入激活码来登记到该服务。激活码与SIM卡身份一起通过SMS发送到PKI。用户可以有3次尝试以正确地输入这个代码。

激活模块取回激活码和SIM卡身份，并验证它是否和已经由安全服务器提供的激活码和SIM卡身份相匹配。激活模块然后传送一个“生成PKI密钥启用命令”返回给SIM，而在SIM卡中的密钥生成应用生成包含一个私有密钥和一个验证公共密钥的密钥对。

该验证公共密钥（VPuK）通过SMS发送到激活模块，SMS优选地根据用于敏感信息保护的GSM03.48加密。

然后用户被要求选择一个PIN_SIGNKEY，它是一个个人自选择的用于例如事务签名和鉴权的签名PIN。

在成功验证的情况中，激活模块连接到CA以发布一个具有与用户相关联的公共密钥的有效证书。这个证书同时被发送给认证目录。

成功认证的确认发送回用户，而PKI菜单接着将在SIM中被禁用。因而，SIM卡中的PKI功能被启用。

本发明提供了一种用于注册和激活PKI（公共密钥基础设施）功能性的方法，使用户不必本人超过一次地到被授权办公场所现场。由于在用户的身份被分配给激活码，特别是在RA中被分配给激活码之前，他将拥有激活码，因此在第一身份确认之后发送与PKI功能性相关的项目和数据将不是必须的。这保证了在第一次个人出现的时候正确的人就已经拥有了正确的激活码。

从用户的观点来看，本发明考虑了在提供PKI功能性时的较少的努力。从发布者的观点来看，本发明将很可能增长PKI用户的数量。此外，由于执行时间将缩短，且将消除挂号邮件的必要，所以每个注册的花费将降低。