[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32

[12] 发明专利申请公开说明书

[21] 申请号 03822034.2

[43] 公开日 2005 年 10 月 12 日

[11] 公开号 CN 1682489A

[22] 申请日 2003.9.17 [21] 申请号 03822034.2

[30] 优先权

[32] 2002. 9.17 [33] EP [31] 02020818.7

[86] 国际申请 PCT/EP2003/010327 2003.9.17

[87] 国际公布 WO2004/028076 德 2004.4.1

[85] 进入国家阶段日期 2005.3.17

[71] 申请人 西门子公司

地址 德国慕尼黑

[72] 发明人 M·海恩特尔 A·福尔希

M·弗兰克 O·普法夫

[74] 专利代理机构 中国专利代理(香港)有限公司

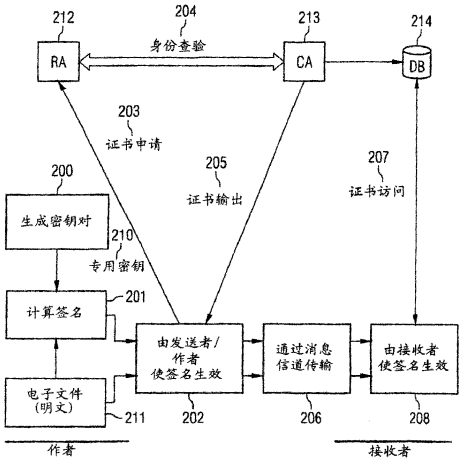
代理人 吴立明 张志醒

权利要求书 1 页 说明书 5 页 附图 2 页

[54] 发明名称 产生和/或确认电子签名的方法

[57] 摘要

本发明涉及一种产生和/或确认电子签名的方法。通过这种方法产生一个不对称的密钥对，此密钥对包含一个专用签名密钥和一个公开的确认密钥。此外，借助专用签名密钥和通过使用为至少一个电子文件的一个预先可确定的签名函数计算至少一个电子签名。在至少一个电子签名计算之后颁发一个公开确认证书。



ISSN1008-4274

1、产生和/或确认电子签名的方法，其中，

- 产生一个不对称的密钥对，它包含了一个专用签名密钥和一个公开确认密钥。

- 借助于专用签名密钥和运用为至少一个电子文件可预先给定的签名函数，计算至少一个电子签名，

- 在计算至少一个电子签名之后，公开确认密钥被颁发证书。

2、根据权利要求 1 的方法，其中，

- 在确认时仅有以下签名被确认为有效，即在公开确认密钥被颁发证书之前的时刻产生和/或者已经产生的签名。

3、根据权利要求 1 或者 2 的方法，其中，

- 在公开确认密钥被颁发证书时，除用户标识和公开确认密钥之外还至少包括一个对至少一个电子文件的参考。

4、根据权利要求 3 的方法，其中，

- 通过对该至少一个电子文件的一个散列值的计算，实现该至少一个参考的实施。

5、根据权利要求 1-4 中之一的方法，其中，

- 在计算签名之后和向收件人传送该签名之前由该至少一个电子文件的作者进行确认，以检验通过该至少一个电子文件表达的意愿行为。

产生和/或确认电子签名的方法

使用电子签名为保证实现真实性、约束性、完整性。假如作为意愿表述的电子数据能被解释，那么一个电子签名检验的肯定结果可以被作为其权利生效的证据应用。电子签名过程靠两个密钥进行，这两个密钥一起建立并在数学上具有相互依赖性。其中之一在下面称为专用密钥，它被保密，可以用来产生电子签名。另外一个密钥（下面称公开密钥）是公开的，它可以用来检验被提供的签名。为了把电子电子签名分配到人，需要将个人名字连接到相应的公开密钥。这种连接通过一个特别的电子文件的形式来实现。这个特别电子文件是由可靠的第三方机构来签发并作为证书表示。

从技术性上看，证书是一种含有信息的数据结构，通过它保证了一个密钥拥有者与公开密钥的连接。一个公开密钥与一个确定的密钥拥有者的具体的连接是通过可信赖的中立的认证授权单位（CA—certification authority）进行。这个认证授权单位验证带有它的电子签名的所属完整的证书。这个证书只有有限的有效期，这个有效期同样作为证书的组成部分由认证授权单位同时签署。

认证授权单位执行姓名审核，然后通过电子签名(用专用密钥)把这个人的名字与公开密钥连接。一个公开密钥的验证结果是一个证书。使用 X.509 标准作为证书结构。这样一个证书除了公开密钥外，还包括进行签署的认证授权单位的名字，一个有效时间段、所有者名字和进行签署的认证授权单位的一个唯一号码。在此的先决条件是，所有参与人员充分信赖这个认证授权单位的该公开密钥。认证授权单位拥有用于证书签名的分离的密钥对、以及为与其他通信伙伴进行通信的禁用清单(Speerlisten)和时间印记(Zeitstempeln)。

已知的签名方法由一个用于产生电子签名的算法和一个用于验证电子签名的配合的算法组成。电子签名为之建立的电子数据通常作为附件附在该电子签名数据上。每一个用于产生电子签名的算法，作为入口参数含有至少一个要签名的数据以及签字人的专用密钥并作为电子签名的结果提供。用于验证电子签名的配合的算法，作为入口参数含有至少一个电子签名数据以及签字人的公开密钥，并按照验证成功与否提供相应的肯定或否定的验证结果。

到目前为止，电子签名的产生按照下面的顺序进行：

- 产生一个带有专用和公开密钥的不对称密钥对，
- 为公开密钥颁发一个证书，
- 为要签名的数据确定一个散列值，
- 通过使用一个预先给定的签名函数计算电子签名，
- 输出该电子签名。

到目前为止，电子签名的验证按照下面的顺序进行：

- 从电子签名附件确定电子数据的一个散列值，
- 对电子签名和散列值使用一个预先给定的验证函数，
- 输出验证结果。

签名方法通过被使用的签名和验证函数(例如 RSA、DSA 或者 ECDSA)、确定散列值使用的散列算法(例如 SHA-1 或者 RIPEMD-160)以及可能使用的微调方法(在 RSA 中)相互区别。如果散列值的长度需要匹配，则使用微调方法通过一个可预先给定的字符串补足散列值。

目前所知道的签名方法在对被分配有个人密钥的人一侧来说，持久安全防止不合法访问个人密钥总体上是一个较高开销。

此发明的任务是提供一种用于产生电子签名的方法，这个方法不需要对被分配有个人密钥的人一侧来说持久地安全防止不合法访问个人密钥。

根据本发明该任务通过具有权利要求 1 给定的特征的方法解决。本发明方法的其它有利的改进在从属权利要求中给出。

此发明的一个主要方面在于，仅在计算电子签名后，执行公开确认密钥的证书颁发。因此仅在证书申请过程范围内产生签名后才执行通过签名的文件表示的来自电子文件的作者的意愿的处理。因为不是计算电子签名的发起、而是证书申请表示这一意愿处理，因此不需要在计算电子签名后保存与公开确认密钥相应的专用签名密钥。因此可以把专用签名密钥在电子签名计算后毁掉，并因而不必再为防止不合法访问保存。

下面根据附图详细说明本发明的一个实施例。

图 1 描述了一个常规签名方法的流程，

图 2 描述了本发明的签名方法的流程。

在图 1 中描述了一个常规签名方法的流程，在这个流程中首先产生一个密

钥对，它包括专用签名密钥 110 和公开确认密钥（步骤 100）。接着在注册权威机构 112（RA）提交证书申请(步骤 101)。在注册权威机构 112 和认证授权单位 113（CA—certification authority）共同作用下，进行涉及到每个申请人的身份检验(步骤 102)。

在检验结果是肯定的时，认证授权单位 113 为每一个申请者分配一个公开确认密钥证书(步骤 103)并在一个属于认证授权单位 113 的数据库 114 中保存所颁发的证书的相应记录，这个数据库为证书查询可公开进行访问。此外，在数据库 114 中存储证书禁用清单，它通报有关禁用证书。在公开确认密钥颁发后，对一个将要签署的电子文件 111，应用专用签名密钥 110 和一个预先给定的签名函数计算电子签名(步骤 104)。接着把计算出的签名和电子文件 111 作为消息通过一个消息信道从电子文件 111 作者传输到电子文件 111 的收件人(步骤 105)。

为确认电子签名，在收件人一侧还进行证书询问(步骤 106)。在此或者从数据库 114 中询问分配给作者的公开确认密钥，或者询问数据库 114 中分配有在所传输的消息中包含的公开确认密钥的记录，这一记录证明所分配的证书的有效性。最后收件人确认传送来的消息中包含的签名(步骤 107)。通过收件人进行电子签名确认时，一方面借助公开确认密钥解码签名，另一方面为电子文件 111 计算一个散列值。最后比较解码的签名和计算的散列值的一致性。在解码的签名和计算的散列值一致时在接收侧被承认有效。

图 2 描述了该发明的签名方法的流程，其中首先产生一个不对称的密钥对(步骤 200)。借助于一个由所生成的密钥对包含的专用签名密钥 210 和一个预先给定的签名函数，在作者侧从电子文件 211 计算一个电子签名(步骤 201)。在计算电子签名后，由作者确认该电子签名以便保证计算的电子签名对应通过电子文件 111 说明的意愿行为(步骤 202)。

对肯定的确认结果，在注册权威机构 212 申请一个为一个相应于专用签名密钥 210 的公开验证密钥的证书 (步骤 203)。接着审查证书申请中所含的数据，特别是作者或者申请者的身份(步骤 204)。

对於肯定的检验结果，从认证授权单位 213 对申请者，或者电子文件 211 的作者，输出一个公开确认密钥证书(步骤 205)。此外，在属于认证授权单位 213 的一个数据库中为所输出的证书执行相应的登记。

在电子文件 211 的作者确认计算出的签名和颁发公开确认密钥证书后，电子文件 211 和计算出的电子签名作为消息通过一个消息信道向电子文件 211 的收件人发送(步骤 206)。在收件人一侧以公知的方式施行证书询问(步骤 207)和执行在接收的消息中包含的签名的确认(步骤208)。

在确认电子签名时，仅仅承认那些在颁发公开确认密钥证书之前产生的签名为有效。由此消除了到目前为止的签名方法中公知的有关公开确认密钥的废除问题。此外，用这种方法在颁发公开确认密钥证书后，专用签名密钥不再被滥用。因而不再需要任何机构来长期避免对专用签名密钥210 的不合法访问。

在相应于步骤203 至205 颁发公开确认密钥证书时，除用户标识和该公开确认密钥外还可以包含对每次签名电子文件 211 的一个参考。在根据步骤 208 由收件人一侧确认该签名时另外分析对电子文件 211 的该参考。此外还可能：在颁发公开确认密钥证书中不仅包括对一个唯一的电子文件的参考，而且还包括对在一定时间段内所签署的电子文件的多个参考。对一个电子文件的参考例如通过对该电子文件计算一个散列值实施。然后相应于步骤 208 由收件人一侧对签名的验证与相应散列值相互比较。

本发明的签名方法例如可用于中心硬件安全模块中。在这种情况下，一个封闭的用户群的所有的成员可以共同使用在中心硬件安全模块中的一个专用签名密钥。在用户侧产生要签署的电子文件的散列值并通过一个被保护的传输信道向硬件安全模块传输。这个硬件安全模块不需另外检验直接计算电子签名并将签名发回给每位用户。每个用户在由各用户成功验证该签名后保存这个签署过的电子文件，连同所属的散列值和电子签名。所属散列值在晚些时刻被附加在对公开验证密钥的证书申请上，并由认证授权单位作为附加的属性包含在为公开验证密钥的证书中。这样该证书以唯一的方式与被签署的电子文件相连接。

代替使用中心硬件安全模块也可以为产生签名使用个人安全模块。在此，用于要签署的电子文件的散列值例如在个人电脑上或其他类似设备上产生，并且通过红外接口或者蓝牙接口向个人安全模块传输。

本发明的签名方法进一步应用於一个被修改的和已经备有验证逻辑的打印机。作为入口参数，这样的验证打印机含有一个要签署的电子文件和一个为该电子文件计算的电子签名。在成功检验该电子签名时，这个附属的电子文件向验证打印机发送。接着根据打印件可以让电子文件的作者决定，他将是否允许颁发先前已经使用过的专用签名密钥。

此发明的使用不仅仅局限于这里说明的实施例。

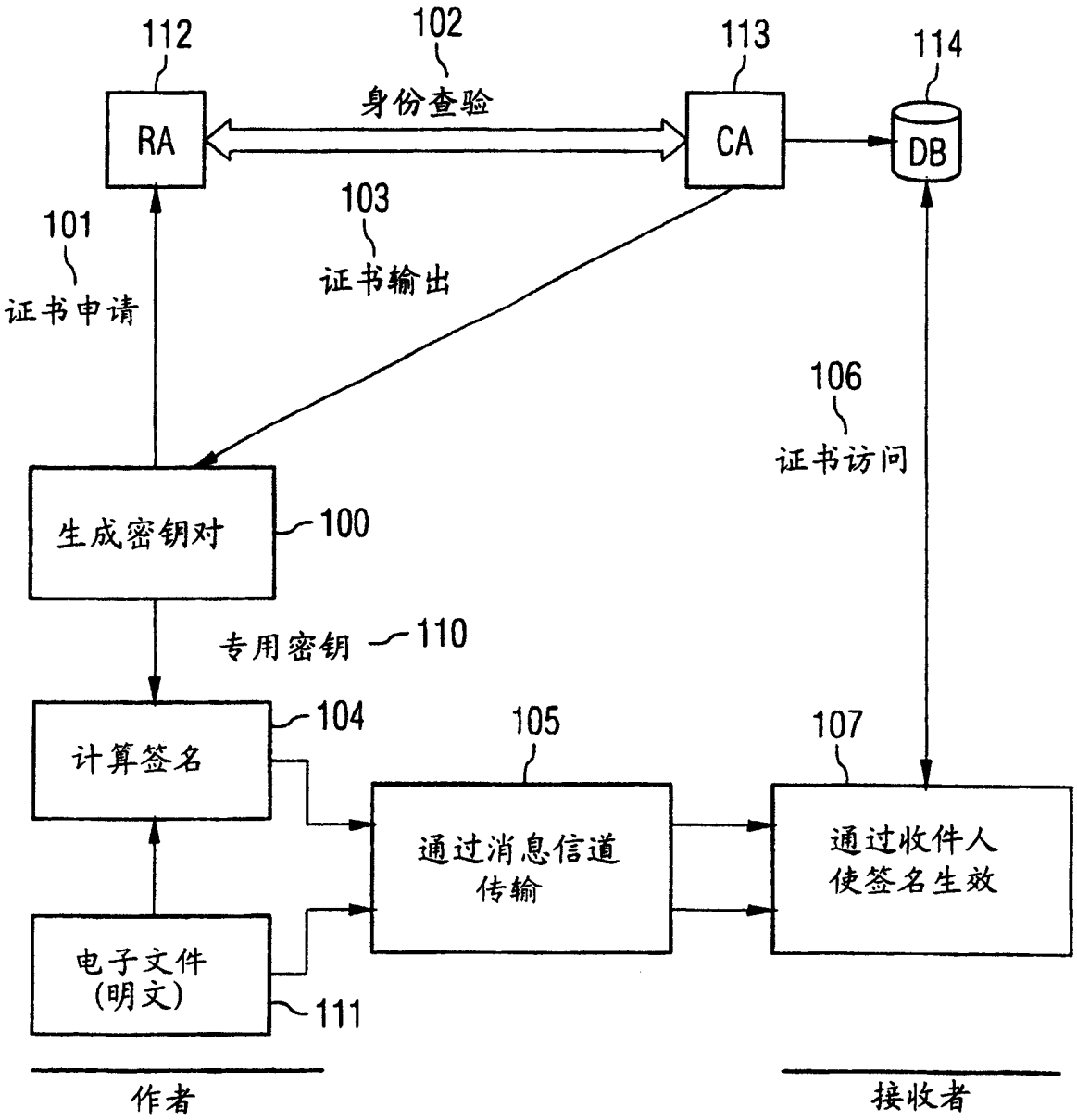

112
102
113
114
RA
身份查验
CA
DB
101
证书申请
103
证书输出
106
证书访问
生成密钥对
100
专用密钥
110
计算签名
104
105
107
通过消息信道传输
通过收件人使签名生效
电子文件(明文)
111
作者
接收者

图 1
现有技术

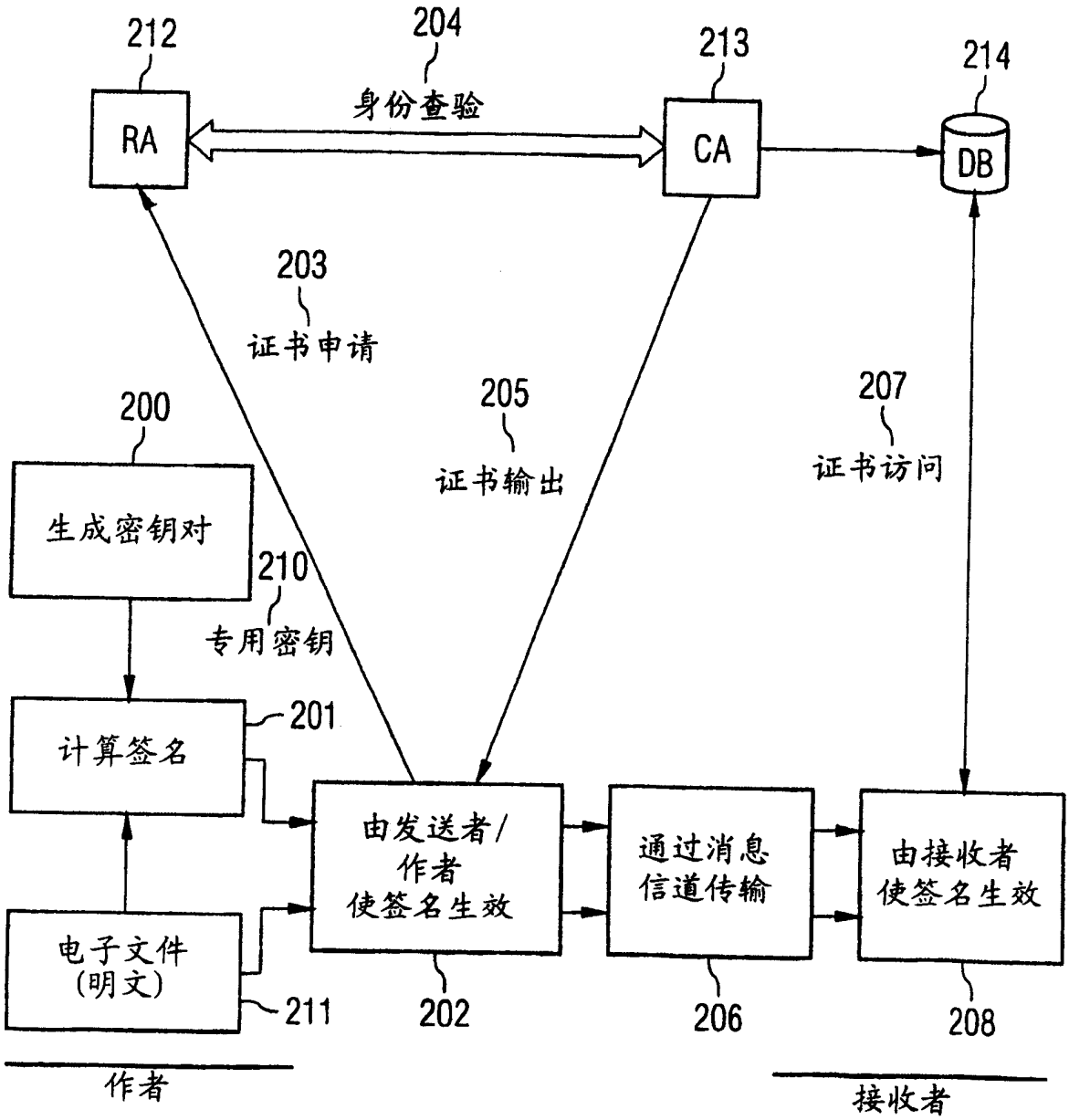

212
RA
204
身份查验
213
CA
214
DB
203
证书申请
205
证书输出
207
证书访问
200
生成密钥对
210
专用密钥
201
计算签名
由发送者/
作者
使签名生效
通过消息
信道传输
由接收者
使签名生效
电子文件
(明文)
211
202
206
208
作者
接收者

图 2