[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 200410007295.1

[45] 授权公告日 2008 年 11 月 19 日

[11] 授权公告号 CN 100435510C

[22] 申请日 2004.2.27
[21] 申请号 200410007295.1
[30] 优先权
[32] 2003.10.10 [33] JP [31] 351509/2003
[73] 专利权人 株式会社日立制作所
地址 日本东京
[72] 发明人 熊谷洋子 藤城孝宏 锻忠司 羽根慎吾 下之薗仁
[56] 参考文献
US6397329B1 2002.5.28
US2002/0046340A1 2002.4.18
US6134550A 2000.10.17
审查员 庄 湧

[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 李德山

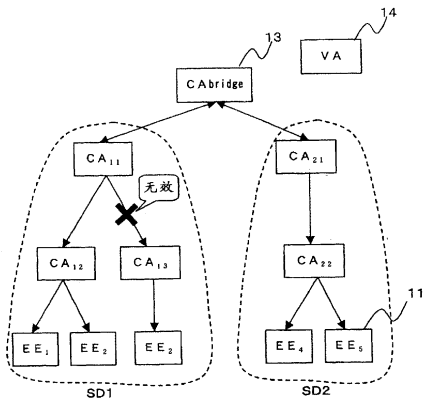
权利要求书 2 页 说明书 19 页 附图 12 页

[54] 发明名称

高速化验证公开密钥证件的方法和装置

[57] 摘要

本发明提供一种高速化验证公开密钥证件的方法和装置。即使是在进行路径检索以后存在新路径的场合，也能应答适当的结果，而且，也能缩短终端实体从委托公开密钥证件的有效性确认到知道其结果所花费的时间。证件的有效性确认局预先定期地检索、验证路径和失效证件表，按照该验证结果，分成有效路径和无效路径，并向数据库登录。另外，在存在来自终端实体的证件有效性确认委托的场合，调查与该委托对应的路径被登录在有效路径数据库还是无效路径数据库中，并判断该公开密钥证件的有效性。另一方面，在与该有效性确认委托对应的路径没有被登录在数据库中的场合，通过重新进行路径检索、验证，进行该公开密钥证件的有效性确认。



1. 一种在证件有效性确认局装置中按照委托进行的公开密钥证件的有效性确认方法，包括:

预先进行路径检索和对检索出的路径进行验证的步骤;

根据所述验证结果，作为有效路径或无效路径登录在数据库中的路径登录步骤; 以及

从终端装置接收公开密钥证件的有效性确认委托，并使用预先登录的路径进行验证的有效性确认步骤。

2. 如权利要求 1 记载的公开密钥证件的有效性确认方法，其中，在该有效性确认步骤中，当与该有效性确认委托相对应的有效路径没有被登录时，通过重新进行路径检索和验证，进行该公开密钥证件的有效性确认。

3. 如权利要求 1 记载的公开密钥证件的有效性确认方法，其中:

在该有效性确认步骤中，当与该有效性确认委托对应的路径作为有效路径或者无效路径登录到该数据库中时，根据该登录结果，进行所委托的公开密钥证件的有效性确认。

4. 如权利要求3记载的公开密钥证件的有效性确认方法，其中还包括:

在该有效性确认步骤中，即便与该有效性确认委托对应的路径作为有效路径被登录，当该公开密钥证件中或该路径所包含的公开密钥证件中记述有限制事项时，也要按照该有效性确认委托进行路径验证，并调查该公开密钥证件以及该路径是否满足该限制事项的步骤; 以及

若满足限制事项，就判断为有效路径的步骤。

5. 如权利要求3记载的公开密钥证件的有效性确认方法，其中还包括:

在该有效性确认步骤中，即使与该有效性确认委托对应的路径作为有效路径被登录，当该有效性确认委托或该公开密钥证件或该路径中所

包含的公开密钥证件中记载有政策时，也要按照该有效性确认委托进行路径验证，并调查该公开密钥证件和该路径是否满足电子手续的政策的步骤；以及

在满足该政策的场合，判断为有效路径的步骤。

6. 如权利要求 3 记载的公开密钥证件的有效性确认方法，其中：

该路径登录步骤包括：

检索从委托机构认证局到用于发行终端实体证件的认证局的路径的步骤；

取得、验证与用于发行该终端实体证件的认证局所发行的终端实体证件相关的失效表的步骤；以及

与该失效表的验证结果一起登录失效表的步骤。

7. 如权利要求 6 记载的公开密钥证件的有效性确认方法，其中，在该有效性确认步骤中，在与该有效性确认委托对应的路径作为有效路径登录在该数据库中时，不进行该失效表验证地确认该公开密钥证件没有失效的事实。

高速化验证公开密钥证件的方法和装置

技术领域

本发明涉及用于在公开密钥基础设施（Public Key Infrastructrure: 以下叫做“PKI”）中验证对于某终端接受的电子手续的署名的公开密钥证件，并涉及适用于确认其有效性的技术。

背景技术

在民用系统、公共系统的各种组织、团体中，为了将以前在书面上进行的各种手续电子化，而正在进行 PKI 的引入、配备。

图 12 表示在 PKI 中有多个认证局（Certificate Authority:以下，叫做“CA”）时的各 CA 之间的关系的例子。

如图示那样，进行公开密钥证件的发行及其管理的各 CA 形成具有以路由 CA1 为顶点的树形构造的组。该组叫做保密区域，是在 1 个政策管理机关的基础上被运用的 PKI 的单位。路由 CA1 向位于从其自身位置起下游一层的各个 $CA2_1$～$CA2_n$ 发行公开密钥证件。另外，各个 $CA2_1$～$CA2_n$ 向位于从其自身位置起下一层的各个 $CA3_1$～$CA3_{n1}$ 发行公开密钥证件。这样，在树（形结构）上，位置上一层的 CA 向位于其自身的下一层的 CA 发行公开密钥证件。然后，位置在最下层的 CAs_1～CAs_{nm}（以下，叫做“末端实体证件发行 CA”）向办理电子手续的用户（末端实体：以下叫做“EE”）EE_1～EE_x 发行公开密钥证件。

在 EE_1～EE_x 各自的装置生成电子文档时使用的保密密钥（署名密钥）的正当性通过由容纳自身的终端收容认证局 CAs_1～CAs_{nm} 发行的公开密钥证件被证明，在生成由终端收容认证局 CAs_1～CAs_{nm} 各自的装置发行的公开密钥证件的署名时使用的保密密钥的正当性通过由容纳自身的认证局 CA（s-1）～$CA(s-1)_{n(m-1)}$ 发行的公开密钥证件被证明。因此，在 EE_1～EE_x 各个装置生成署名时使用的保密密钥最终通过由路由认证局 CA 发行的公开密钥证件被证明。将最终证明该 EE_1～EE_x 的装

置在生成署名时所使用的密钥的正当性的认证局，换言之，EE_1～EE_x所信赖的、树形结构最上层的 CA 叫做委托机构(trust anchor)CA。

那么，在图 12 中，EE_1装置用 EE_1保持的自身的保密密钥对于应发送到 EE_x装置的电子文档进行署名。然后在已署名的电子文档中，附加与 CA_1发行的该保密密钥对等的 EE_1的公开密钥证件，并发送到 EE_x装置。

EE_x 装置可使用被附加在该电子文档中的 EE_1的公开密钥证件来验证从 EE_1接收的电子文档的署名。但是，由于 EE_1的公开密钥证件不是 EE_x 的证件发行 CAs_{nm}发行的，如果 EE_x 没有确认该公开密钥证件的有效性是通过作为其自身的委托机构 CA 的路由 CA1 而被证明的，那么就不能信赖该公开密钥证件。该公开密钥证件的有效性确认处理通过以下次序进行。（1）从委托机构 CA 到公开密钥证件发行源的路径检索：以委托机构 CA（此处是路由 CA1）作为起点 CA，调查起点 CA 发行的公开密钥证件的发行目的地，当在该发行目的地中包含 CA 时，反复进行调查该 CA 发行的公开密钥证件的发行目的地的处理，直到在该公开密钥证件的发行目的地中包含 EE 证件发行 CA（此处是发行 EE_1的公开密钥证件的 CAs_1）为止，并检索从委托机构 CA 到 EE 证件发行 CA 的路径。（2）检索的路径的验证：根据通过该（1）检索的路径上的各 CA，得到对路径上位于该 CA 的下一层侧的 CA 发行的公开密钥证件。然后用比发行了该公开密钥证件的 CA（此处是 EE 证件发行 CAs_1）上一层的 CA 所发行的公开密钥证件，验证有效性确认对象的公开密钥证件（此处为 EE 证件发行 CAs_1对 EE_1发行的公开密钥证件）的署名，在可验证的场合，连续进行用再上一层的 CA 所发行的公开密钥证件验证该上一层的 CA 所发行的公开密钥证件的署名的处理，直到该上一层的 CA 变成委托机构 CA 为止。然后，在这样的公开密钥证件的署名验证可进行到委托机构时，确认有效性确认对象的公开密钥证件的有效性被确认。

在 EE_x装置使用被添加到电子文档中的 EE_1的公开密钥证件验证从 EE_1 装置接收的该电子文档的署名的同时，通过按照该（1）、（2）所示的次序确认在该电子文档的署名验证中所使用的 EE_1的公开密钥证件的

有效性，能够确认该电子文档的正当性。

此外，以上将用 EE 装置进行公开密钥证件的有效性确认处理作为前提。但是，公开密钥证件的有效性确认处理的负载大，为了用 EE 进行该处理，对该 EE 装置要求高的处理能力。因此，设置经由网络与 EE 装置连接的证件有效性确认局（以下，叫做"Validation Authority:VA"），在该 VA 装置中代替该 EE 进行公开密钥证件的有效性确认的技术由作为确定与英特网有关的各种技术的标准化的组织的 IETF（Internet Research Task Force）建议。在 VA 装置中，在进行公开密钥证件的有效性确认的场合，首先，EE 装置将公开密钥证件的有效性确认委托送交 VA 装置。接着，在 VA 装置中，进行该（1）、（2）的处理，最后，将该结果送交 EE 装置。

这时，作为用于缩短从 EE 装置委托公开密钥证件的有效性确认到知道该结果所花费的时间的方法，包括如下方法。

在 VA 装置中，预先定期地检索路径，并登录到路径数据库中。然后，在存在来自某个 EE 装置的公开密钥证件的有效性确认委托的场合，通过在 VA 装置的路径数据库中检索相对应的路径，并进行检索出的路径的验证，来确认该公开密钥证件的有效性（例如，参照专利文献 1）。

另外，还有一种方法，在 VA 装置中，预先定期地检索全部路径，进行检索出的路径的验证。只将验证成功的路径（有效路径）预先登录到路径数据库中。然后，在存在来自某个 EE 装置的公开密钥证件的有效性确认委托的场合，通过调查相对应的路径是否被登录在 VA 装置的路径数据库中，来确认该公开密钥证件的有效性（例如，参照专利文献 2）。

【专利文献 1】

美国专利第 6134550 号说明书

【专利文献 2】

美国专利申请公开第 2002/046340 号说明书

发明内容

使用在该专利文献 2 中所记载的方法，在与从 EE 装置接收的公开密钥证件的有效性确认委托对应的路径没有被登录到路径数据库中的场

合，判定有效性确认对象证件无效。但是，若遵照该方法，那么在接收来自 EE 装置的公开密钥证件的有效性确认委托时，新存在在路径检索时不存在的路径的场合，会将有效的公开密钥证件判断为无效。在该专利文献 2 中，关于这样场合的处理没有被记述。

另外，在该专利文献 1 中，也没有记述对应于从 EE 装置接收的公开密钥证件的有效性确认委托的路径没有被登录在路径数据库中时的处理。

这样，在对应于 VA 接收的有效性确认委托的路径没有被登录在路径数据库中的场合，通过重新进行路径检索、验证，能够应答适当的结果。但是，存在该场合的有效性确认处理时间变长的问题。

目前，在民用系统、公共系统的各种组织、团体中，进行 PKI 的引入、配备，其结果，可以预想到多个保密区域并列在一起，变成复杂的 PKI 构成。而且，若利用 PKI 的应用被普及，那么可以预想将形成大量的有效性确认委托。在这样的场合，从 EE 委托公开密钥证件的有效性确认到知道其结果所花费的时间将变长，并招致服务质量的下降。

本发明提供在路径检索时不存在的路径在路径检索之后被形成的场合下，也能应答适当的结果的技术，和/或进一步缩短从 EE 委托公开密钥证件的有效性确认到知道其结果所花费的时间的技术。

具体地说，在本发明中，经由网络，与多个终端装置（EE 装置）和 CA 装置连接的 VA 装置按照某个 EE 装置的委托，为确认公开密钥证件的有效性而进行以下的处理。

针对通过发行公开密钥证件而被涉及的全部 CA，检索存在的全部路径，并对通过该路径检索而检测出的路径进行验证。另外，取得与位于检测出的路径端点的 EE 证件发行 CA 所发行的 EE 证件相关的失效表（Certificate Revocation List,以下，叫做“CRL”）。对于已取得的 CRL，确认该 CRL 是在有效期间内，同时，利用该 CRL 的发行 CA 的公开密钥证件进行该 CRL 的署名验证。然后，将可验证的路径和不可验证的路径进行分类，并登录在路径数据库中。该路径数据库生成处理独立于来自 EE 的公开密钥证件的有效性确认委托，按照规定的规则重复，例如

定期地进行。

然后，当存在来自某个 EE 的公开密钥证件的有效性确认委托时，调查与它对应的路径是否被登录在路径数据库中，在作为可验证路径被登录在数据库中时，通过使用登录在数据库中的 CRL 来确认该公开密钥证件是否失效，可确认该公开密钥证件的有效性。

另一方面，在与该公开密钥证件对应的路径作为不可验证的路径被登录到数据库中时，除被登录的该无效路径外，调查有效路径是否存在，在不存在的场合，认为该公开密钥证件为不能验证的证件。当检测出新的路径和 CRL 的场合，使用该路径和该 CRL 确认该公开密钥证件的有效性，以该验证结果为基础，在路径数据库中进行追加登录。

另外，在对应于已存在有效性确认委托的公开密钥证件的路径和 CRL 没有被登录在路径数据库中时，通过重新进行路径和 CRL 的检索、验证处理，来确认该公开密钥证件的有效性。这时，在检测出新的路径和 CRL 的场合，以该路径和该 CRL 的验证结果为基础在路径数据库中进行追加登录。

依据本发明，当从某个 EE 接收了公开密钥证件的有效性确认委托时，即使在路径检索之后形成新的路径的场合，也能够应答适当的结果。而且，与有效性确认委托对应的路径在作为可验证的路径登录时，没有必要进行如上述（1）、（2）所示的、从该 EE 的委托机构 CA 到该公开密钥证件的 EE 证件发行 CA 的路径检索、检测出的路径验证、以及与该公开密钥证件对应的 CRL 的署名验证。另外，当与有效性确认委托对应的路径作为不能验证的路径登录时，能够用少量的处理进行路径检索、验证。因此，能缩短从某个 EE 委托公开密钥证件的有效性确认到该有效性被确认所花费的时间。

依据本发明，即使在路径检索之后形成新的路径的场合下，也能够应答适当的结果，和/或能够缩短从 EE 委托公开密钥证件的有效性确认到知道其结果所花费的时间。

附图说明

图 1 是表示本发明的一个实施形态所适用的 PKI 系统的概略构成的

图。

图 2 是表示在图 1 所示的 PKI 系统中的各 CA 的关系的一例的图。

图 3 是表示图 1 所示的 EE 的概略构成的图。

图 4 是表示图 1 所示的 VA 的概略构成的图。

图 5 是表示图 1 所示的 VA 的概略构成的图。

图 6 是表示图 3～图 5 所示的 EE、CA 以及 VA 的各自硬件构成例子的图。

图 7 是用于说明用图 5 所示的 VA 进行的路径检索、验证以及管理动作的流程图。

图 8 是用于说明用图 5 所示的 VA 进行的路径检索、验证以及管理动作的流程图。

图 9 是表示在各 CA 具有图 2 所示的关系时，由 VA 的路径检索部分 51 检测出的全部路径的图。

图 10 是用于说明用图 5 所示的 VA 进行的公开密钥证件的有效性确认动作的流程图。

图 11 是用于说明用图 5 所示的 VA 进行的公开密钥证件的有效性确认动作的流程图。

图 12 是表示在现有的 PKI 中，存在多个认证局时的 CA 关系的一例的图。

具体实施方式

图 1 是表示本发明的一个实施形态所适用的 PKI 系统的概略构成的图。

本实施例的 PKI 系统由办理电子手续的多个 EE_1 装置（11）～EE_N 装置（11）（总称为“EE 装置”），进行公开密钥证件发行业务的 CA_1 装置（13）～CA_M 装置（13），公开密钥证件的有效性确认局 VA（14），以及分别与各部件连接的英特网等网络（以下，叫做“NET”）16 组成。

图 2 是表示在图 1 所示的系统中的各 CA 的关系的一例的图。

如图所示那样，在本实施形态的 PKI 系统中，以所谓的民用系统、政府系统等多个保密区域 SD（SD1～SD2）并存为前提。另外，各保

密区域 S D的路由 CA（在图 2 中为 CA_{11}、CA_{21}），例如，通过在向桥式认证局 CAbridge 发行公开密钥证件的同时，接受从 CAbridge 发行公开密钥证件，进行与 CAbridge 之间的相互认证。通过这么做，在属于某个保密区域 SD 的 CA 和属于其它保密区域 SD 的 CA 之间，形成用于在一方的 CA 中能确认另一方的 CA 所发行的公开密钥证件的有效性的路径。

接着，说明关于构成图 1 的 PKI 系统的各装置。

首先，使用图 3 说明 EE 装置（11）。

EE 装置（11）具有处理部分 30a 和存储部分 30b，经由 NET16 用于与其它装置通信的通信部分 30c，以及进行用户（EE）生成的电子文档和从其它的 EE 接收的电子文档的输入输出以及接收来自用户的指示的输入输出部分 30d。

处理部分 30a 具有生成对电子文档的署名的署名生成部分 31，进行署名验证的署名验证部分 32，以及总控制 EE 装置的各部分的控制部分 33。

存储部分 30b 具有用于保持用户生成的电子文档的电子文档保持部分 34，用于保持保密密钥（署名密钥）、与之相对的公开密钥的公开密钥证件、运用该 EE 装置的 EE 所信赖的 CA 的自己署名证件的密钥保持部分 35，以及用于保持附有从其它 EE 接收的署名的电子文档和公开密钥证件的验证对象保持部分 36。

在这样的构成中，控制部分 33 经由输入输出部分 30d 从用户接收到表示应将保持在电子文档保持部分 34 中的电子文档发送到其它 EE 的的指示时，从电子文档保持部分 34 中读出该电子文档，并将它传送到署名生成部分 31。署名生成部分 31 使用保持在密钥保持部分 35 中的保密密钥生成对所传送的该电子文档的署名。

控制部分 33 将在署名生成部分 31 中所生成的署名附加到从电子文档保持部分 34 读出的电子文档中，生成附有署名的电子文档，并经由通信部分 30c 向用户所指示的发送目的地的 EE 装置发送所生成的附有署名的电子文档和保持在密钥保持部分 35 中的公开密钥证件。若控制部分 33 经由通信部分 30c 从其它 EE 装置接收到附有署名的电子文档和公开

密钥证件，那么使它们相关联，并保持在验证对象保持部分36中，同时，将这些验证请求通知给署名验证部分32。

署名验证部分32接收该请求后，使用对应的公开密钥证件验证保持在验证对象保持部分36中的附有署名的电子文档的署名。署名验证部分32将该署名验证中所使用的公开密钥证件的有效性确认委托发送给VA装置（14）。这时，按照要求，将想要用该附有署名的电子文档进行的与电子手续有关的政策（例如，交易额等的可靠性）的验证委托包含在该确认委托中。然后，在VA装置（14）中，只在也包含该政策验证的该公开密钥证件的有效性被确认时，才将附有署名的电子文档作为正当的文档处理，并根据需要从输入输出部分30d输出。

接着，使用图4说明CA装置（13）。

CA装置（13）具有处理部分40a，存储部分40b，用于经由NET16进行与其它装置通信的通信部分40c，进行公开密钥证件等的输入输出、来自该装置的操作者的指示的接收以及处理结果的输出的输入输出部分40d。

处理部分40a具有发行公开密钥证件的发行部分41，进行由发行部分41发行的公开密钥证件的管理的管理部分42，以及总体控制CA装置的各部分的控制部分43。

存储部分40b具有用于保持发行部分41发行的公开密钥证件的公开密钥证件数据库44，用于保持记述了保持在公开密钥证件数据库44中的各公开密钥证件的发行目的地的发行目的地管理表的发行目的地管理表保持部分45，以及失效证件表保持部分46。

在这样的构成中，控制部分43若经由输入输出部分40d接收公开密钥证件的发行委托，就将该内容传给发行部分41。发行部分41在接收它之后，生成与之相对应的公开密钥证件。这时，用CA的保密密钥在公开密钥证件中进行署名。另外，根据需要，在公开密钥证件中，记述该公开密钥证件的有效期限、没有委托的其它认证局的名称(Name Constrains)用于该公开密钥证件的有效性确认的所容许的最大路径长度（路径上容许的最大认证局个数）以及表示电子手续的交易额等政策。

然后，经由输入输出部分 40d 或通信部分 40c，通过邮送或通信将已生成的公开密钥证件发送给发行委托源。在将该公开密钥证件登录在公开密钥证件数据库 44 中的同时，将它的发行目的地（即发行委托源）的信息记述在发行目的地管理表保持部分 45 中所保持的发行目的地管理表中。

控制部分 43 若经由输入输出部分 40d 或通信部分 40c 接收公开密钥证件的失效委托，那么就将该委托传送到管理部分 42。管理部分 42 接受它之后，从公开密钥证件数据库 43 中删除失效对象的公开密钥证件，同时，从发行目的地管理表保持部分 44 所保持的发行目的地管理表中删除该公开密钥证件的发行目的地的信息。然后，管理部分 42 定期地生成记述关于因失效委托而从公开密钥证件数据库 43 中删除的公开密钥证件信息的失效证件表，并将它保持在失效证件表保持部分 45 中。此外，管理部分 42 使下次预定生成失效证件表的时日记述在所生成的失效证件表中。

另外，控制部分 43 若经由通信部分 40c 从其它装置接收关于公开密钥证件的失效信息的询问，就检索失效证件表保持部分 45 中所保持的失效证件表，并调查所询问的公开密钥证件是否失效。然后，也能够经由通信部分 40c 在进行询问的其它装置中应答该结果。（作为在这样的询问应答中使用的通信协议，包括 OSCP(Online Certification status protocol)。

管理部分 42 调查在公开密钥证件数据库 44 中所存储的各公开密钥证件的有效期限，也进行从发行管理表保持部分 45 中所保持的发行管理表中删除超过有效期限的公开密钥证件的发行目的地信息。

接着，使用图 5 说明 VA 装置（14）。

如图 5 所示那样，VA 装置（14）具有处理部分 50a，存储部分 50b，用于经由英特网 NET16 与其它装置进行通信的通信部分 50c，以及进行公开密钥证件等的输入输出和来自用户指示的接收的输入输出部分 50d。

处理部分 50a 具有路径检索部分 51，路径验证部分 52，有效期限/失效状态调查部分 53，有效性确认部分 54，以及总体控制 VA 装置的各部分的控制部分 55。另外，存储部分 50b 具有路径数据库 56，以及失效

证件表生成预定时日数据库57。其中，路径数据库56具有有效路径数据库56A，以及无效路径数据库56B。

路径检索部分51，例如定期地将任意CA作为委托机构CA，检索从该委托机构CA到发行EE证件的全部EE证件发行CA的路径。另外，取得检测出的路径的EE证件发行CA所发行的、关于EE证件的失效证件表（CRL）。委托机构CA能够通过设置全部的CA或设定作为一部分的CA来进行检索。

路径验证部分52每当在路径检索部分51中进行路径检索，进行对该路径检索部分51中检测出的路径的验证。在路径检索部分51中能取得与该路径对应的CRL的场合，进行该CRL的验证。然后，与变成位于该路径两端的委托机构CA的名称和EE证件发行CA的名称对相对应地，根据该验证结果将构成该路径的各CA名、各证件、以及有关EE证件的CRL登录在有效路径数据库56A或无效的数据库56B中。

有效期限/失效状态调查部分53对于登录在有效路径数据库56A中的各个路径调查构成该路径的各公开密钥证件的有效期限和有无失效。然后，根据该结果，更新路径数据库56。另外，有效期限/失效状态调查部分53将从各CA的失效证件表保持部分46得到的失效证件表中所记述的下次失效证件表生成预定时日与该CA相对应地登录在失效证件表生成预定时日数据库57中。

有效性确认部分54按照来自EE装置的委托，将委托机构CA作为委托起点，进行公开密钥证件的有效性确认。

此外，图3～图5所示的各EE装置（11），CA装置（13）和VA装置（14），例如能建立在一般的电子计算机上，该计算机具备象图6所示那样的CPU61，存储器62，硬盘等外部存储装置63，从具有CD-ROM等移动性存储媒体69中读取信息的读取装置64，用于经由NET16与其它装置通信的通信装置65，键盘和鼠标等输入装置66，监视器和打印机等输出装置67，以及在这些装置之间进行数据发送接收的接口68。

然后，CPU61通过执行从外部存储装置63装入到存储器62上的规定程序，能实现该各处理部分。即，通信部分30c、40c、50c通过CPU61

利用通信装置 66 而实现，输入输出部分 30d、40d、50d 通过 CPU61 利用输入装置 66、输出装置 67 和读取装置 64 而实现，以及存储部分 30b、40b、50b 通过 CPU61 利用存储器 62 和外部存储装置 63 而实现。另外，处理部分 30a、40a、50a 作为 CPU61 的处理而实现。

该规定程序可以预先存储在外部存储装置 63 中，也可以存储在该电子计算机可利用的存储媒体 69 中，经由读取装置 64，根据需要被读出，或者，从与利用在作为该电子计算机可利用的通信媒体的网络或英特网上传输的载波的通信装置相连接的其它装置，根据需要被下载，并被引入到外部存储装置 63。

接着，说明该构成的 VA 装置（14）的动作。

本实施形态的 VA 装置（14）的动作被分成路径检索、验证和管理动作，以及公开密钥证件的有效性确认动作。

使用图 7～图 8 的流程图说明在 VA 装置（14）中所进行的路径检索、验证和管理动作。

控制部分 55 若经过由 VA 的经营者决定的规定时间（例如 1 日）（步骤 S1001），那么将一次清除路径数据库 56 的登录内容（S1002），并在路径检索部分 51 中委托路径检索。路径检索部分 51 接收该委托后，检索到以任意 CA 为委托机构 CA 时的 EE 证件发行 CA 的路径（步骤 S1003）。

具体地说，路径检索部分 51 访问委托机构 CA，得到委托机构 CA 发行的并被保持在发行目的地管理表保持部分 45 中的公开密钥证件的发行目的地信息。然后，在得到的各发行目的地是 CA 的场合下，访问各发行目的地，再调查保持在发行目的地管理表保持部分 45 中的、各 CA 所发行的公开密钥证件的发行目的地。通过将该处理持续到公开密钥证件的发行目的地变为 EE，检索从委托机构 CA 到 EE 证件发行 CA 的路径。此处，为了防止通过路径环路使该处理无限地反复，当在从某个 CA 得到的发行目的地中包含在之前形成的部分路径中存在的 CA 时，不进行将该 CA 设定为发行目的地的该处理。另外，取得向位于路径端点的 EE 发行证件的 CA 所发行的 CRL。

以各 CA 具有图 2 所示的关系的情况为例，更具体地说明在步骤 S1003 中的路径检索处理。

首先，路径检索部分 51 将委托机构 CA 作为 CAbridge 进行路径检索。路径检索部分 51 访问 CA bridge，得到 CA_{11}、CA_{21} 的信息，作为保持在发行目的地管理表保持部分 45 中的、CA bridge 发行的公开密钥证件的发行目的地信息。

接着，路径检索部分 51 对从 CAbridge 得到的发行目的地（CA_{11}、CA_{21}）中的任何一个，实行以下的处理。即，若所关注的发行目的地是 CA（以下，假定叫做“关注 CA”），就设定所谓 CAbridge-关注 CA 的部分路径。然后，访问关注 CA 的发行目的地管理表保持部分 45，得到该关注 CA 所发行的公开密钥证件的发行目的地信息。此处，假定关注的发行目的地是 CA_{11}，设定所谓的 CAbridge-CA_{11} 部分路径，从 CA_{11} 得到 CAbridge 、CA_{12}、CA_{13} 的信息，作为发行目的地的信息。

接着，路径检索部分 51 调查在从认证局 CA_{11} 得到的发行目的地（CAbridge 、CA_{12}、CA_{13}）中是否包含部分路径上的 CA（以下，假定叫做“环路 CA”）。若包含，则将该发行目的地从关注对象中排除。因此，此处，将 CAbridge 从关注对象中排除。接着，路径检索部分 51 调查在从 CA_{11} 得到的发行目的地中是否包含 EE。在某个 CA 发行的证件的发行目的地中包含 EE 的场合，使该 CA 成为 EE 证件发行 CA。但是，由于从 CA_{11} 得到的发行目的地中没有包含 EE，因此 CA_{11} 不是 EE 证件发行 CA。因此，应将 CAbridge- CA_{11} 的部分路径延长到 EE 证件发行 CA，并关注除从 CA_{11} 得到的环路 CA 以外的发行目的地（CA_{12}、CA_{13}）中的任何 1 个。

若所关注的发行目的地是 CA，那么在以前设定的部分路径中设定连接该关注 CA 的部分路径。然后，访问该关注 CA 的发行目的地管理表保持部分 45，得到该关注 CA 发行的公开密钥证件的发行目的地的信息。此处，假定所关注的发行目的地是 CA_{12}，设定所谓的 CAbridge - CA_{11}-CA_{12} 路径，从 CA_{12} 得到 EE_1、EE_2，作为发行目的地的信息。

接着，路径检索部分 51 调查在从 CA_{12} 得到的发行目的地（EE_1、EE_2）

中是否包含环路 CA。若包含，则将该发行目的地从关注对象中排除。此处，因为没有包含环路 CA，所以路径检索部分 51 移向下一个处理，调查从 CA_{12} 得到的发行目的地中是否包含 EE。此处，因为得到的发行目的地全部是 EE，所以 CA_{12} 是 EE 证件发行 CA。因此，检测出以该 CA_{12} 为端点的路径作为从委托机构 CAbridge 到 EE 证件发行 CA_{12} 的路径（CAbridge - CA_{11}- CA_{12}）。

此外，路径检索部分 51 在检测出到 EE 证件发行 CA 的路径时，访问失效证件表保持部分 46，并取得该 EE 证件发行 CA_{12} 所发行的 CRL。

接着，路径检索部分 51 调查在从位于检测出的路径端点上的 CA_{12} 得到的发行目的地的信息中是否有还未被关注的发行目的地（环路 CA 以外的 CA），若有那样的发行目的地，则将它作为关注 CA 继续该处理。另一方面，若没有那样的发行目的地，就调查在从位于前 1 个的 CA_{11} 得到的发行目的地的信息中是否有还未被关注的发行目的地（环路 CA 以外的 CA）。然后，若有那样的发行目的地，就将它作为关注 CA，继续该处理。此处，由于在从 CA_{11} 得到的发行目的地信息中，还未对 CA_{13} 关注，因此通过将它作为关注 CA 进行该处理，检测出从 CAbridge 到 EE 证件发行 CA_{13} 的路径（CAbridge - CA_{11}- CA_{13}）和 CA_{13} 所发行的 CRL。

这样，路径检索部分 51 对于位于检测出的路径上的每个 CA，通过继续该处理直到在从该 CA 得到的发行目的地的信息中没有还未被关注的发行目的地为止，检测出从 CAbridge 到各 EE 证件发行 CA 的路径。

以上是以任意 CA 为委托机构时的步骤 S1003 的处理。

象后述的那样，即使将 CA_{11}、CA_{21} 各自的 CA 作为委托机构 CA，也同样地进行路径检索。

控制部分 55 若通过路径检索部分 51 检测出路径（在步骤 S1004 中为 YES），那么在路径验证部分 52 委托路径验证，路径验证部分 52 接收之后，进行对路径检索部分 51 检测出的路径的验证（步骤 S1005）。

具体地说，对于由路径检索部分 51 检测出的各个路径进行以下的处理。

即，首先，路径验证部分52访问路径上各CA的公开密钥证件数据库44，并得到各CA对位于该路径上的下1个CA（在访问目的地CA为EE证件发行CA时是EE）发行的公开密钥证件。

接着，路径验证部分52利用EE证件发行CA的公开密钥证件来验证位于路径最后的EE证件发行CA所发行的公开密钥证件的署名，在能验证的场合，利用位于再前一个的CA的公开密钥证件来验证该EE证件发行CA的公开密钥证件的署名。通过将该处理持续到位于该前一个的认证局CA变成委托机构CA为止，来验证该路径。此外，利用该EE证件发行CA的公开密钥证件来对该EE证件发行CA所发行的CRL进行验证。

例如，在验证图2中从CAbridge到EE证件发行CA_{12}的路径（CAbridge - CA_{11}- CA_{12}）和CRL时，首先，使用路径中位于CA_{12}的前1个的CA_{11}的公开密钥证件来验证EE证件发行CA_{12}的公开密钥证件的署名。然后，在能验证的场合，使用路径中位于比CA_{11}更前1个的CAbridge的公开密钥证件来验证CA_{11}的公开密钥证件的署名。然后，在能进行该验证的场合，使用该EE证件发行CA_{12}的公开密钥证件对该EE证件发行CA_{12}所发行的CRL进行验证。在能验证该路径和CRL的场合，假定能验证从CAbridge到EE证件发行CA_{12}的路径。

接着，若路径验证部分52假定不能验证路径，就调查在从该路径上各认证局CA得到的公开密钥证件中是否有关于未委托的其它认证局名称（Name Constrains）和用于该公开密钥证件的有效性确认所容许的最大路径长度（路径上容许的最大认证局个数）等限制的记述。在有那样的记述的场合，调查该路径是否满足该限制，只有在满足的场合，才能验证该路径。

那么，如上述那样做之后，若验证部分52完成了对路径检索部分51检测出的各个路径的验证，控制部分55就进行登录处理。控制部分55在路径验证部分52能验证路径的场合（在步骤S1006中为Yes），使该路径与委托机构CA、EE证件发行CA、EE证件发行CA所发行的CRL相对应地登录在有效路径数据库56A中（步骤S1007），并向步骤S1003

转移。另外，控制部分 55 在路径验证部分 52 不能验证路径的场合（在步骤 S1006 中为 No），使该路径与委托机构 CA、EE 证件发行 CA、EE 证件发行 CA 所发行的 CRL 相对应地登录在无效路径数据库 56B 中（步骤 S1008），并向步骤 S1003 转移。

控制部分 55 反复执行步骤 S1003～步骤 S1008，直到没有路径被检测出为止（在步骤 S1004 中为 No），并生成路径数据库 56。这时，将全部 CA 作为委托机构，检索对应的全部路径。在 CA 构成如图 2 所示的场合，将 CA_{11}、CA_{21}、CAbridge 这 3 个 CA 作为委托机构，检索分别与各 CA 对应的全部路径。

进行步骤 S1003～步骤 S1008 中处理的结果是，在各 CA 具有图 2 所示的关系时，由路径检索部分 51 检测出的全部路径变成图 9 所示那样。

另一方面，有效期限/失效状态调查部分 53 调查在登录在有效路径数据库 56A 中的公开密钥证件中是否有限定有效期限的公开密钥证件（步骤 S1009）。在有限定有效期限的公开密钥证件时，访问该公开密钥证件的发行源 CA 的公开密钥证件数据库 44，并检索对该公开密钥证件的发行目的地重新发行的公开密钥证件（步骤 S1010）。

然后，若在该发行源 CA 的公开密钥证件数据库 44 中没有那样的公开密钥证件，就将有关与该限定有效期限的公开密钥证件对应登录的路径的信息从有效路径数据库 56A 中删除，并登录到无效路径数据库 56B 中（步骤 S1011）。另一方面，若在该发行源 CA 的公开密钥证件数据库 44 中有那样的公开密钥证件，那么就得到该证件。然后，使用代替该限定有效期限的公开密钥证件的、重新得到的公开密钥证件，与该步骤 S1005 相同地进行对与该限定有效期限的公开密钥证件相对应地登录在有效路径数据库 56A 中的路径的验证（步骤 S1012）。

那么，在能验证路径的场合（在步骤 S1013 中为 Yes），将与该路径对应地登录在有效路径数据库 56A 中的该限定有效期限的公开密钥证件置换为重新得到的公开密钥证件（步骤 S1014）。另一方面，在路径不能验证的场合（在步骤 S1013 中为 No），将与该限定有效期限的公开密钥证件对应登录的路径从有效路径数据库 31 中删除，并将置换为重新得到

的公开密钥证件的路径置换到无效路径数据库中（步骤 S1015）。

接着，有效期限/失效状态调查部分 53 调查失效证件表生成预定时日数据库 57，并检索与已经过期的失效证件表生成预定时日对应的 CA（步骤 S1016）。在存在那样的认证局 CA 的场合（在步骤 S1017 中为 Yes），访问该 CA 的失效证件表保持部分 46，并得到该 CA 发行的最新的失效证件表（步骤 S1018）。然后，将与该认证局 CA 对应登录到失效证件表生成预定时日数据库 57 中的失效证件表生成预定时日变更为记述在所得到的最新失效证件表中的失效证件表生成预定时日（步骤 S1019）。

然后，有效期限/失效状态调查部分 53 调查记述在所得到的最新失效证件表中的公开密钥证件是否登录在有效路径数据库 56A 中（步骤 S1020），在登录于其中的场合，从有效的路径数据库 56A 中删除有关与该公开密钥证件对应的路径的信息，并登录到无效路径数据库 56B 中（步骤 S1021）。

下面，说明关于公开密钥证件的有效性确认动作。

图 10～图 11 是用于说明在本实施形态的 VA 装置（14）中进行的公开密钥证件的有效性确认动作的流程图。

若控制部分 55 经由通信部分 50c，从 EE 接收到至少包含了该 EE 委托的委托机构 CA 的名称的、其它 EE 的公开密钥证件的有效性确认委托（步骤 S2001），就将其通知给有效确认部分 54。

有效确认部分 54 接收之后，调查与根据证件有效性确认委托的记述而指定的委托机构 CA 和发行了该证件的 EE 证件发行 CA 相对应的路径是否被登录在有效路径数据库 56A 中（步骤 S2002）。

如果其结果能确认与在证件有效性确认委托中记述的委托机构 CA 和发行了该证件的 EE 证件发行 CA 相对应的路径被登录在有效路径数据库 56A 中（在步骤 S2002 中为 Yes），那么有效性确认部分 54 使用作为该路径端点的 EE 证件发行 CA 的公开密钥证件进行 EE 证件的署名验证。有效性确认部分 54 还使用与该路径对应登录的 CRL 来确认 EE 证件是否没有失效（步骤 S2003）。

在 EE 证件的署名验证失败的场合（在步骤 S2003 中为 No），或 EE

证件被记述在 CRL 中并被失效的场合，有效性确认部分 54 判断为 EE 证件无效，并将该旨意经由通信部分 50c 通知给委托源的 EE（步骤 S2009）。

另一方面，在各证件中具有能够记述对未委托的认证局名称的限制和用于该公开密钥证件的有效性确认所容许的最大路径长度（路径上容许的最大认证局个数）的扩展项。在步骤 S2003 中，EE 证件的署名验证和是否没有失效的确认成功的场合（Yes 的场合），调查包含在 EE 证件和该路径中的各 CA 的证件中是否记述了该限制（步骤 S2004）。

在没有那样的限制记述时，转移到步骤 S2006。

在有那样的限制的记述的场合，转移到步骤 S2005，并调查 EE 证件是否满足该限制。在 EE 证件违反限制事项的场合，有效性确认部分 54 经由通信部分 50c 将公开密钥证件无效通知给委托源的 EE 装置(11)(步骤 S2009)。在 EE 证件没有违反限制事项的场合，转移到步骤 S2006。

在步骤 S2006 中，有效性确认部分 54 调查在从 EE 装置（11）接收的确认委托中是否包含表示该 EE 要进行的电子手续的交易额等政策。

在包含政策的场合，再调查在 EE 证件和构成该路径的各个公开密钥证件中是否有满足该政策的政策记述（步骤 S2007）。

当在 EE 证件和该路径中没有满足该政策的政策记述的场合，判断为在用于委托源的 EE 要进行的电子手续的公开密钥证件的有效性确认中不能利用 EE 证件，并经由通信部分 50c 将公开密钥证件无效的旨意通知给委托源的 EE 装置（11）（步骤 S2009）。

另一方面，在从 EE 接收的确认委托中不包含表示该 EE 想要进行的电子手续的政策时（在步骤 S2006 中为 No），或者，在即便包含、在该路径和 EE 证件中所记述的政策也满足该政策时（在步骤 S2007 中为 Yes），判断为公开密钥证件为有效，并经由通信部分 50c 将公开密钥证件有效的旨意通知给委托源的 EE（步骤 S2008）。

另外，在步骤 S2002 中，当与在证件的有效性确认中所记述的委托源 CA 和发行了该证件的 EE 证件发行 CA 相对应的路径没有被登录在有效路径数据库 56A 中时（在 S2002 中为 No），确认该路径是否登录在无

效路径数据库 56B 中（步骤 S2010）。当该路径没有被登录在无效数据库 56B 中时（在步骤 S2010 中为 No），转移到图 11 的步骤 S2012。

在步骤 S2012 中，路径检索部分 51 检索从确认委托记述的委托机构 CA 到确认对象的 EE 证件的路径。该检索与路径检索部分 51 按照预定的规定规则进行的检索不同，是临时进行的。

在路径检索部分 51 没有检测出从委托机构 CA 到 EE 证件的路径的场合（在步骤 S2013 中为 No），有效性确认部分 54 经由通信部分 50c 将 EE 证件无效的旨意通知给委托源的 EE（步骤 S2019）。另一方面，在检索部分 51 检测出从委托源 CA 到 EE 证件的路径的场合（在步骤 S2013 中为 Yes），在路径验证部分 52 中验证检测出的路径（步骤 S2014）。

在能验证检测出的路径时（在步骤 S2015 中为 Yes），向有效路径数据库登录从该路径的委托机构 CA 到 EE 证件发行 CA 的路径以及 EE 证件发行 CA 所发行的 CRL（步骤 S2016）。然后，有效性确认部分 54 经由通信部分 50c 将 EE 证件有效的旨意通知给委托源的 EE（步骤 S2017）。

另一方面，在不能验证检测出的路径的场合（在步骤 S2015 中为 No），向无效路径数据登录从该路径的委托机构 CA 到 EE 证件发行 CA 的路径和 EE 证件发行 CA 所发行的 CRL（步骤 S2018）。然后，向步骤 S2011 转移，除此前检测出的路径以外，进行路径是否存在的检索，并同样地实行其后的步骤。

另外，在图 10 的步骤 2010 中，当该路径被登录在无效路径数据库 56B 中时（在步骤 S2010 中为 Yes），以及除该登录路径外，还检测出与有效性确认委托对应的路径时（在步骤 S2011 中为 Yes），向步骤 S2014 转移，并进行对该检测出的路径的验证、登录处理（步骤 S2014～步骤 S2019）。

另一方面，在除该登录路径外，没有检测出与有效性确认对应的路径时（在步骤 S2011 中为 No），有效性确认部分 54 经由通信部分 50c 将公开密钥证件无效的旨意通知给委托源的 EE（步骤 S2009）。

在以上的实施形态中，按照与来自 EE 的公开密钥证件的有效性确认委托无关的规定规则，例如定期地进行时从委托机构 CA 到各 EE 证

件发行CA的路径的检索和验证。

经检索、验证的路径被分成有效路径和无效路径，并登录在路径数据库中。然后，通过调查与有效性确认委托相对应的路径是作为有效路径被登录，还是作为无效路径被登录，来判断该EE证件是否有效。

这时，在与该有效性确认委托对应的路径被登录在无效路径数据库中时，检索、验证是否存在除该无效路径以外的对应路径，并进行确认。在对应于该有效性确认委托的路径没有被登录在路径数据库时，临时进行路径检索、验证。因此，在认证局的构成发生变化的场合，由于利用最新的路径信息进行验证，因此也能够应答适当的有效性确认结果。另外，通过缓存(cache)无效路径，能够缩短从接收公开密钥证件到确认该有效性所花费的时间。

另外，在本实施形态中，在登录路径时，与该CRL的验证结果一起登录由作为路径端点的EE证件发行CA所发行的CRL。然后，在从某个EE接收了公开密钥证件的有效性确认委托的场合，使用该CRL确认该EE证件是否失效。因此，能够进一步缩短在公开密钥证件的有效性确认中所花费的时间。

此外，本发明不应受该实施形态的限制，在其发明构思的范围内可以有各种变形。

例如，在该实施形态中，在VA将路径登录在数据库中时，分成有效路径数据库56A和无效路径数据库56B这2个数据库进行登录。但是，也可以在1个数据库中，附加表示该路径状态的标志，从而对有效路径和无效路径进行分类。

另外，在该实施形态中，为了便于说明，如图2所示，假定EE证件发行CA只对EE发行公开密钥证件，其它CA只对CA发行公开密钥证件，本发行也适用于包含向EE和CA双方发行公开密钥证件的CA的情况。

另外，在该实施形态中，为了便于说明，如图2所示，将CA的构成假定为分层结构，但本发时也适用于CA片构成为更复杂的网状结构的场合。

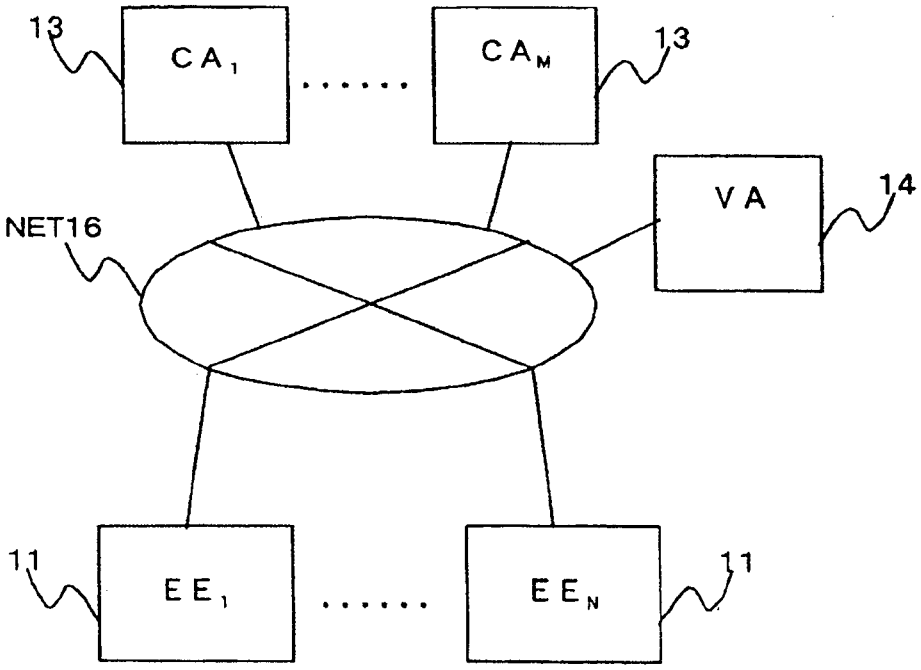


图1

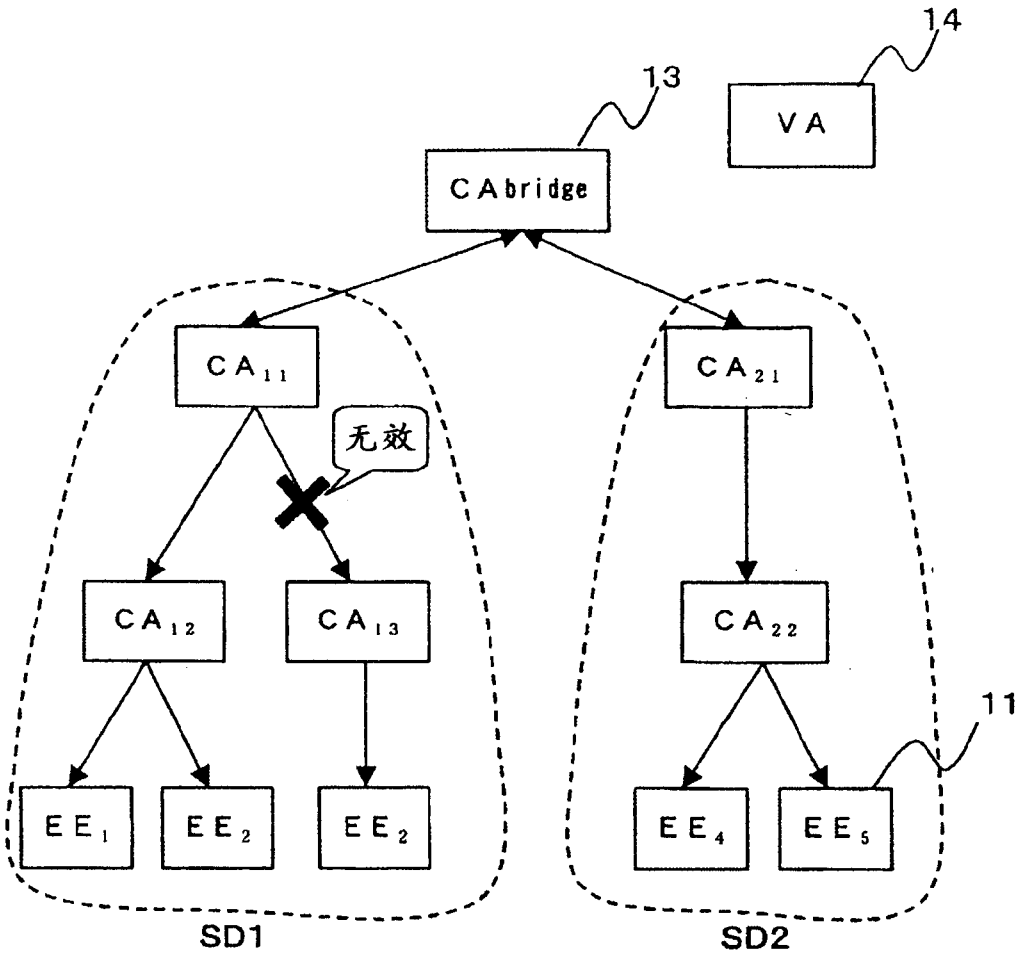

14
13
VA
CAbridge
CA11
无效
CA21
CA12
CA13
CA22
11
EE1
EE2
EE2
EE4
EE5
SD1
SD2

图2

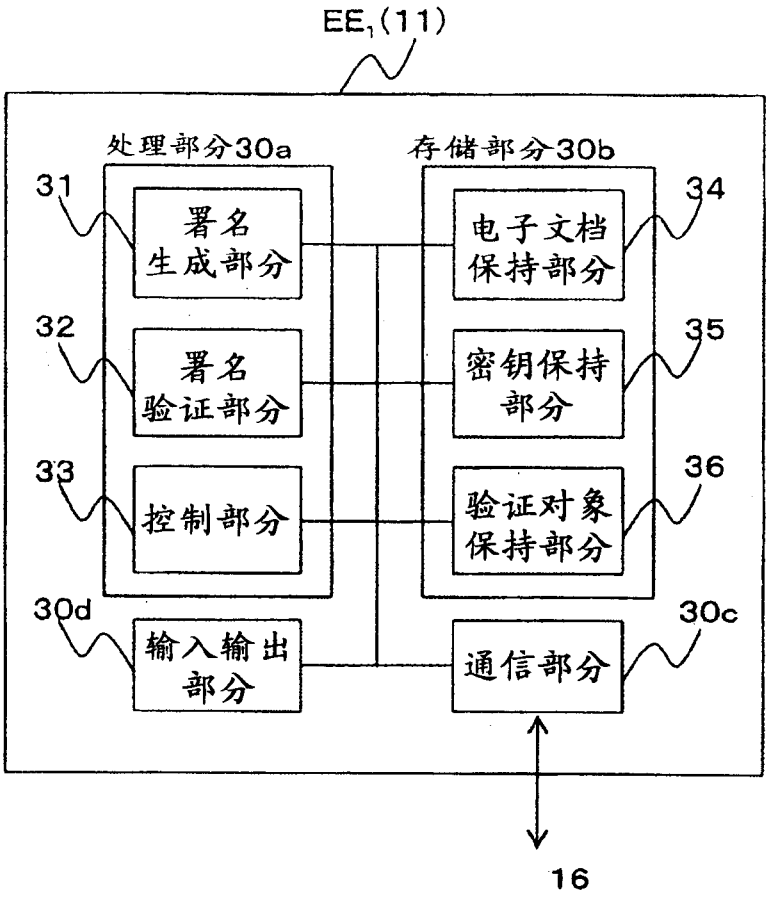

EE1(11)
处理部分30a
存储部分30b
31
署名
生成部分
32
署名
验证部分
33
控制部分
30d
输入输出
部分
34
电子文档
保持部分
35
密钥保持
部分
36
验证对象
保持部分
30c
通信部分
16

图3

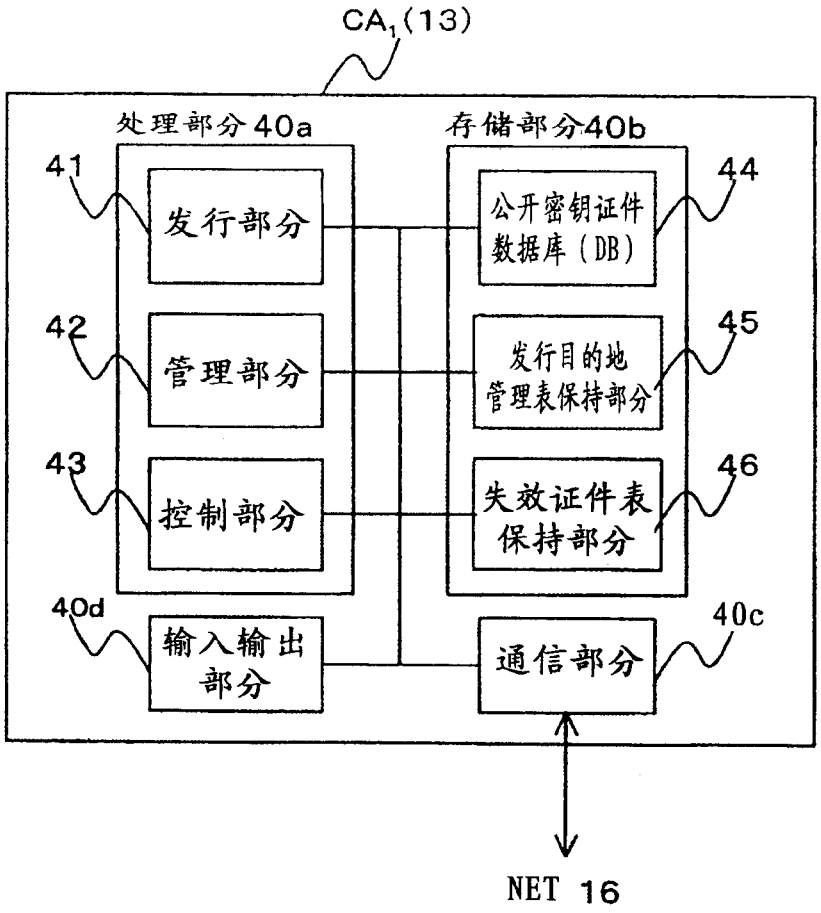

CA1(13)
处理部分40a
存储部分40b
41
发行部分
42
管理部分
43
控制部分
40d
输入输出部分
公开密钥证件数据库(DB)
44
发行目的地管理表保持部分
45
失效证件表保持部分
46
通信部分
40c
NET 16

图4

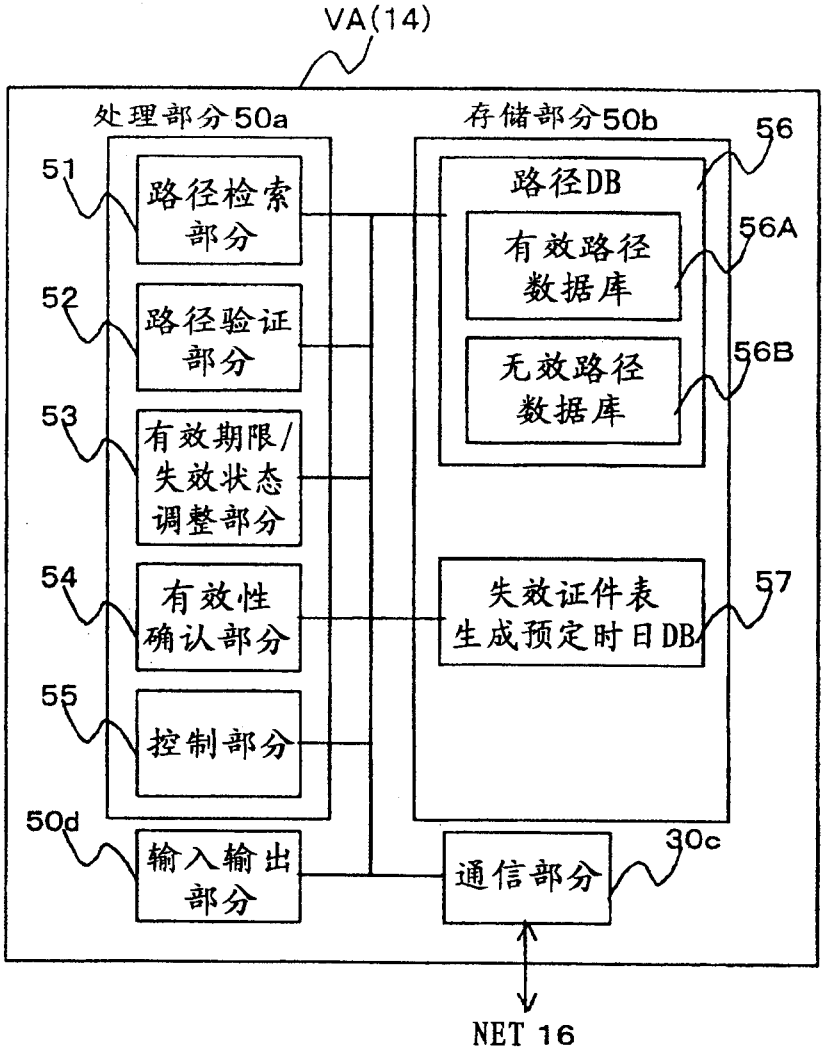

VA(14)
处理部分50a
存储部分50b
56
51
路径检索部分
路径DB
56A
有效路径数据库
52
路径验证部分
56B
无效路径数据库
53
有效期限/失效状态调整部分
54
有效性确认部分
失效证件表生成预定时日DB
57
55
控制部分
50d
输入输出部分
30c
通信部分
NET 16

图5

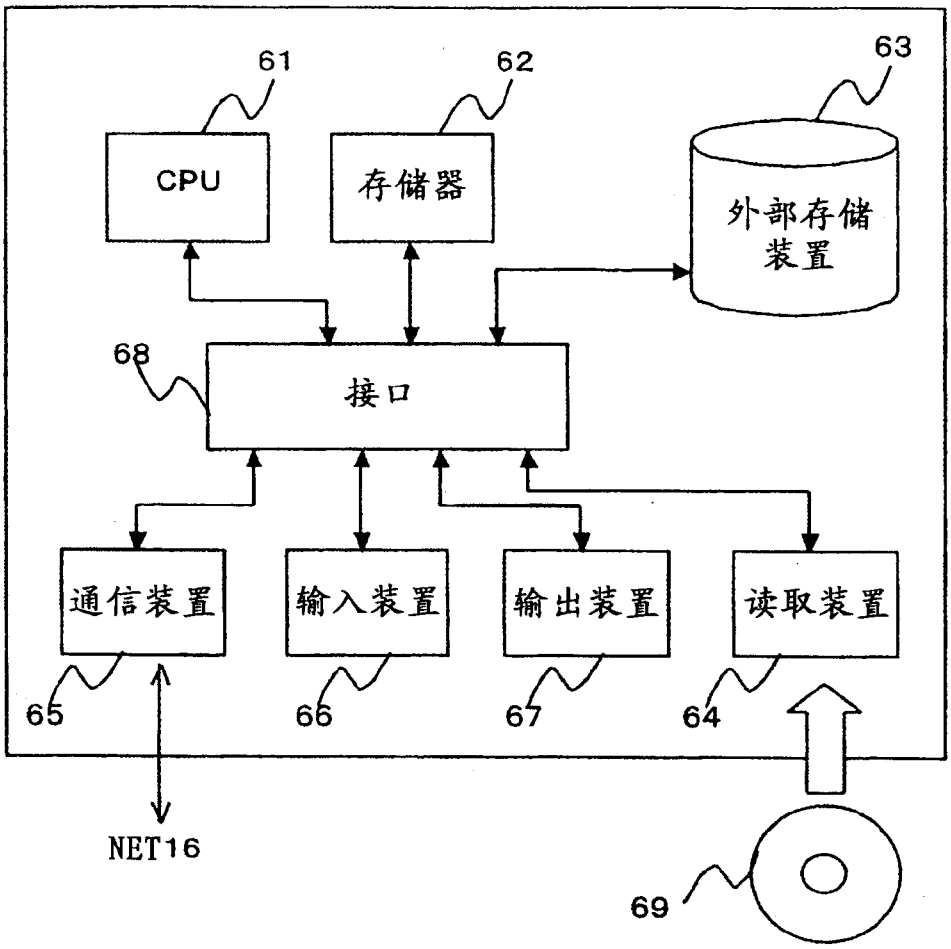

61
62
63
CPU
存储器
外部存储装置
68
接口
通信装置
输入装置
输出装置
读取装置
65
66
67
64
NET16
69

图6

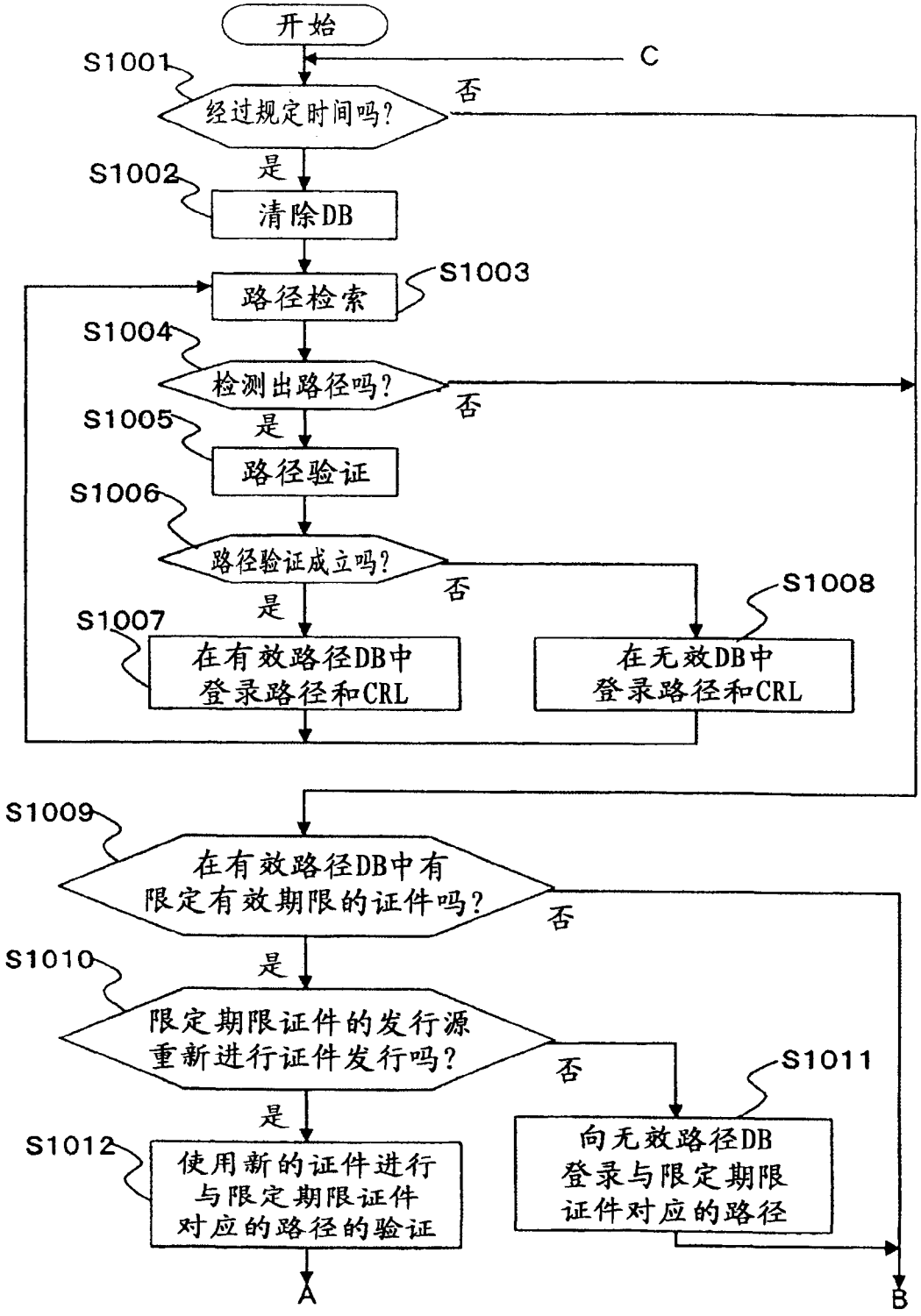

开始
C
S1001
经过规定时间吗?
否
是
S1002
清除DB
S1003
路径检索
S1004
检测出路径吗?
否
是
S1005
路径验证
S1006
路径验证成立吗?
否
是
S1007
在有效路径DB中
登录路径和CRL
S1008
在无效DB中
登录路径和CRL
S1009
在有效路径DB中有
限定有效期限的证件吗?
否
是
S1010
限定期限证件的发行源
重新进行证件发行吗?
否
是
S1011
向无效路径DB
登录与限定期限
证件对应的路径
S1012
使用新的证件进行
与限定期限证件
对应的路径的验证
A
B

图7

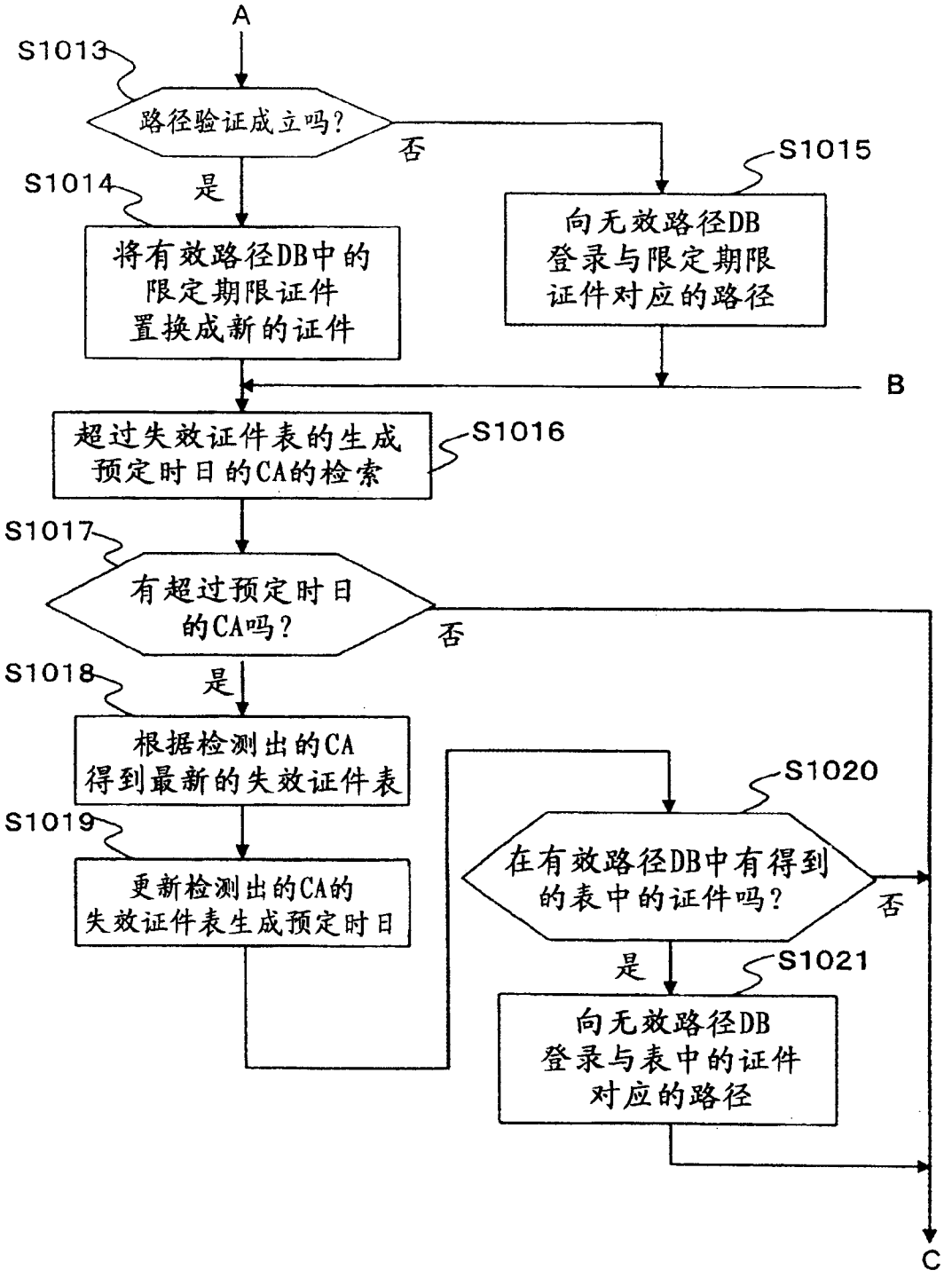

A
S1013
路径验证成立吗?
否
是
S1014
将有效路径DB中的
限定期限证件
置换成新的证件
S1015
向无效路径DB
登录与限定期限
证件对应的路径
B
超过失效证件表的生成
预定时日的CA的检索
S1016
S1017
有超过预定时日
的CA吗?
否
是
S1018
根据检测出的CA
得到最新的失效证件表
S1019
更新检测出的CA的
失效证件表生成预定时日
S1020
在有效路径DB中有得到
的表中的证件吗?
否
是
S1021
向无效路径DB
登录与表中的证件
对应的路径
C

图8

有效路径			
委托机构CA	EE证件发行CA	路径	CRL
CA_{11}	CA_{12}	$CA_{11}-CA_{12}$	有效
	CA_{22}	$CA_{11}-CAbridge-CA_{21}-CA_{22}$	有效
CA_{21}	CA_{12}	$CA_{21}-CAbridge-CA_{11}-CA_{12}$	有效
	CA_{22}	$CA_{21}-CA_{22}$	有效
CAbridge	CA_{12}	$CAbridge-CA_{11}-CA_{12}$	有效
	CA_{22}	$CAbridge-CA_{21}-CA_{22}$	有效

无效路径			
委托机构CA	EE证件发行CA	路径	CRL
CA_{11}	CA_{13}	$CA_{11}-CA_{12}$	无效
CA_{21}	CA_{12}	$CA_{21}-CAbridge-CA_{11}-CA_{12}$	无效
CAbridge	CA_{12}	$CAbridge-CA_{11}-CA_{12}$	无效

图9

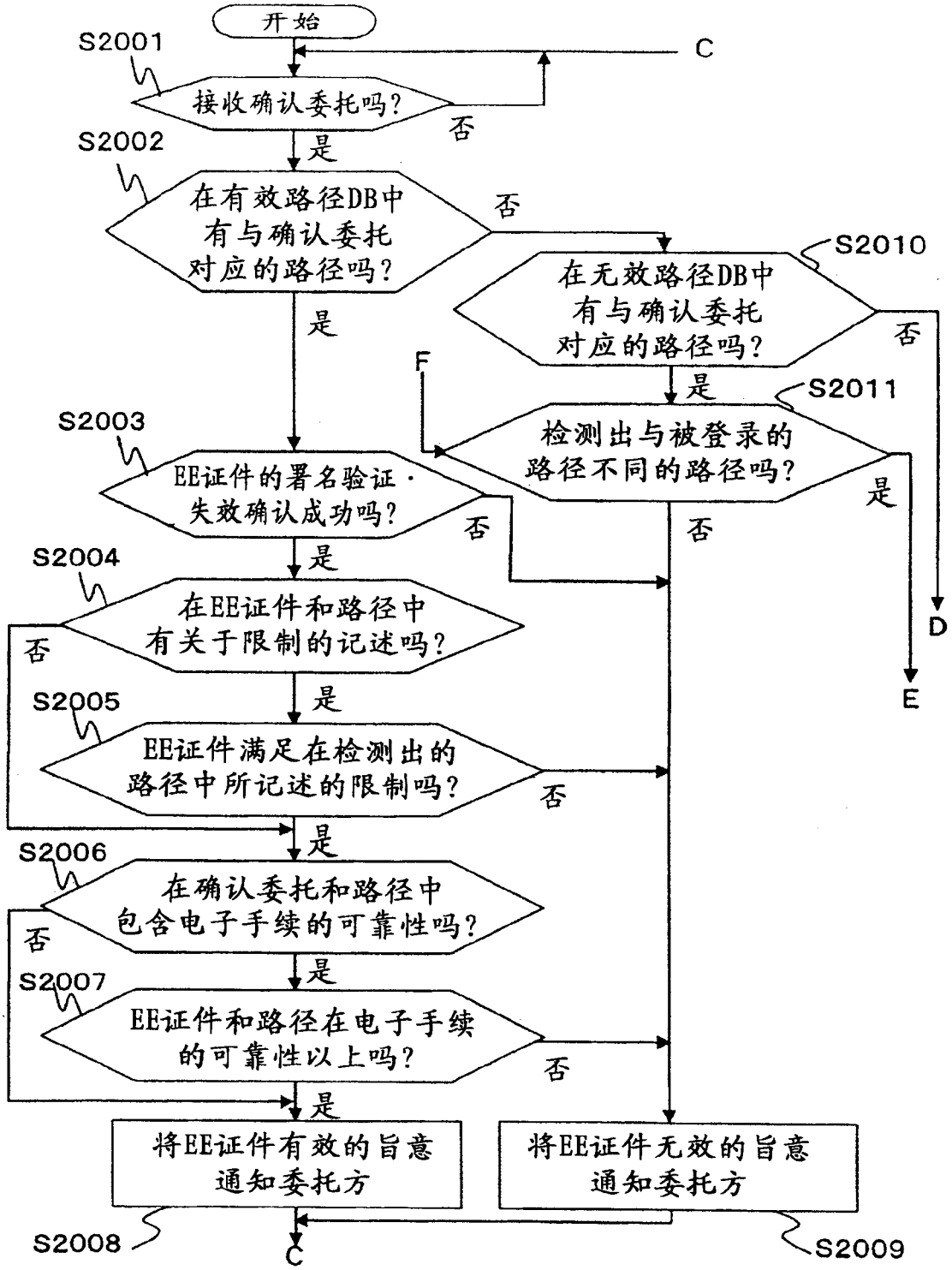

开始
S2001
接收确认委托吗?
否
是
C
S2002
在有效路径DB中有与确认委托对应的路径吗?
否
是
S2010
在无效路径DB中有与确认委托对应的路径吗?
否
是
F
S2011
检测出与被登录的路径不同的路径吗?
是
否
D
E
S2003
EE证件的署名验证·失效确认成功吗?
否
是
S2004
在EE证件和路径中有关于限制的记述吗?
否
是
S2005
EE证件满足在检测出的路径中所记述的限制吗?
否
是
S2006
在确认委托和路径中包含电子手续的可靠性吗?
否
是
S2007
EE证件和路径在电子手续的可靠性以上吗?
否
是
将EE证件有效的旨意通知委托方
将EE证件无效的旨意通知委托方
S2008
S2009
C

图10

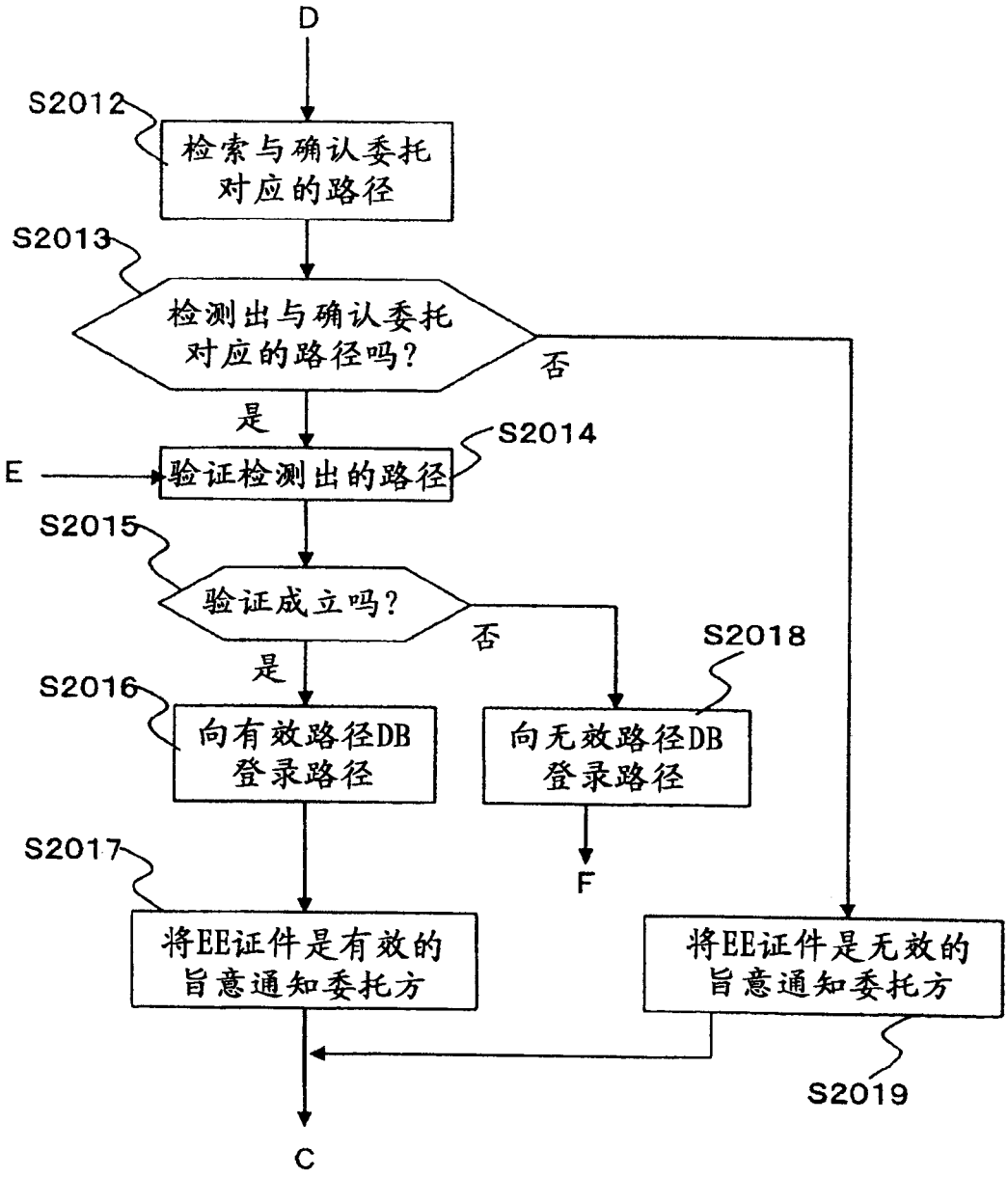

D
S2012
检索与确认委托对应的路径
S2013
检测出与确认委托对应的路径吗?
否
是
S2014
E
验证检测出的路径
S2015
验证成立吗?
否
是
S2018
S2016
向有效路径DB登录路径
向无效路径DB登录路径
F
S2017
将EE证件是有效的旨意通知委托方
将EE证件是无效的旨意通知委托方
S2019
C

图11

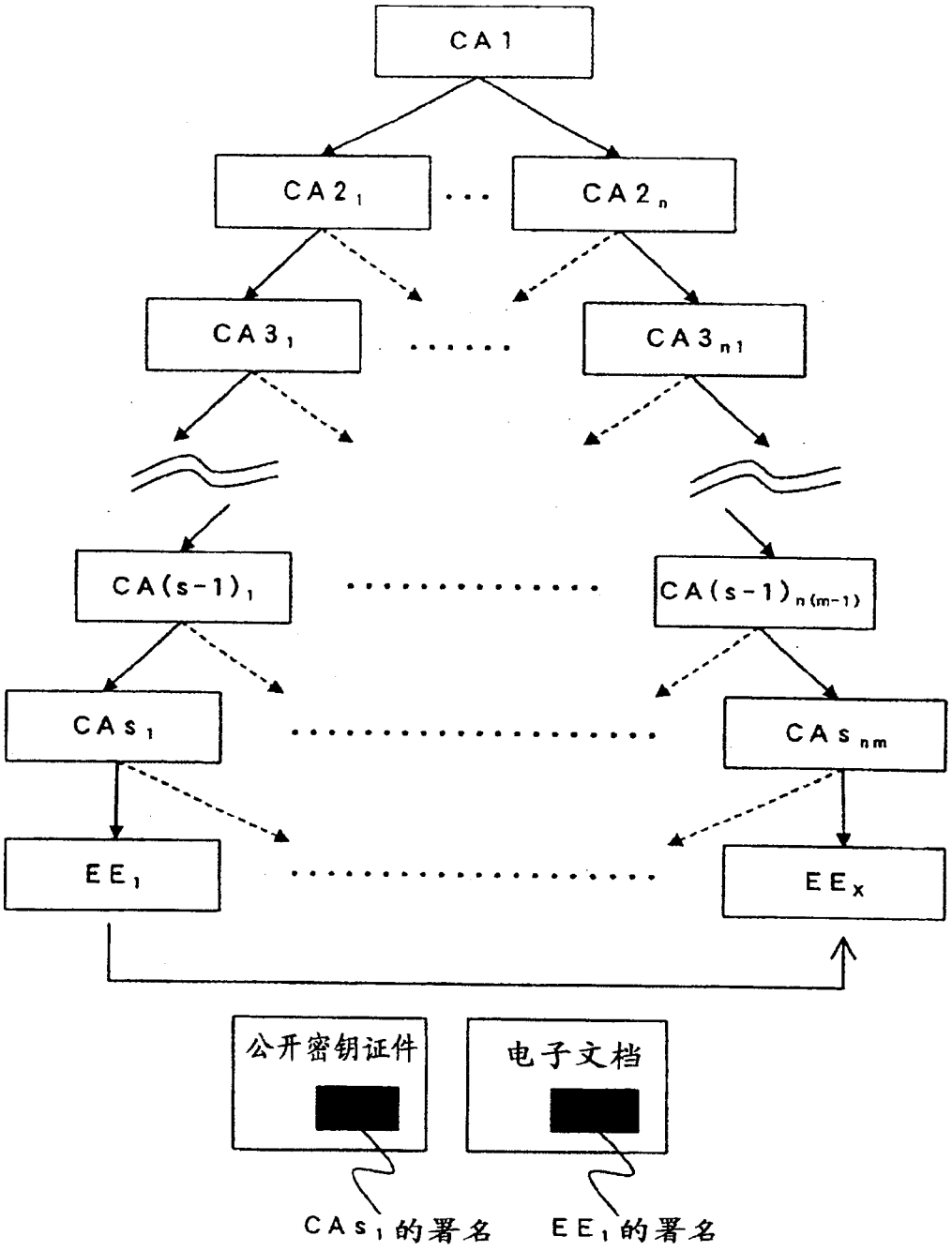

CA1
CA2₁
CA2ₙ
CA3₁
CA3ₙ₁
CA(s-1)₁
CA(s-1)ₙ₍ₘ₋₁₎
CAs₁
CAsₙₘ
EE₁
EEx
公开密钥证件
电子文档
CAs₁的署名
EE₁的署名

图12